ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Διαδίκτυο των Πραγμάτων: Ευφυή Περιβάλλοντα σε Δίκτυα Νέας Γενιάς

Επισκόπηση ασφάλειας στον ομιχλώδη προγραμματισμό

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Γιασιμώ Χριστινίδη

Επιβλέπων: Κυριάκος Κρητικός Αναπληρωτής Καθηγητής

Μέλη εξεταστικής επιτροπής: Μαρία Καρύδα, Καθηγήτρια & Σπυρίδων Κοκολάκης, Καθηγητής

Σάμος, Φεβρουάριος 2025

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του μεταπτυχιακού προγράμματος σπουδών «Διαδίκτυο των Πραγμάτων: Ευφυή Περιβάλλοντα σε Νέας Δίκτυα Γενιάς» του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Πρώτα απ' όλα, θα ήθελα να ευχαριστήσω θερμά τον κύριο Κυριάκο Κρητικό, τον επιβλέποντα καθηγητή της διπλωματικής εργασίας, για την αμέριστη βοήθεια του και την συνεχή καθοδήγηση του με σκοπό την περάτωση της διπλωματικής μου εργασίας. Ακόμα, οφείλω ένα τεράστιο ευχαριστώ στην οικογένεια και τους φίλους μου για την υποστήριξη τους και αστείρευτη αγάπη τους καθ' όλη την διάρκεια των σπουδών μου. Τέλος, θα ήθελα να αφιερώσω αυτή την διπλωματική εργασία στον αείμνηστο πατέρα μου, του οποίου η μνήμη αποτελεί για μένα πηγή έμπνευσης και δύναμης.

Γιασιμώ Χριστινίδη
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

Name	Acronym
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
ACLs	Access Control Lists
AES	Advanced Encryption Standard
ANN	Artificial Neural Network
API	Application Programming Interface
BEC	Business email compromise
BGP	Border Gateway Protocol
BPaaS	Business Process as a Service
CA	Certification Authority
CAA	Certification Authority Authorization
CLI	Command-line Interface
CNN	Convolution Neural Networking
CRM	Customer Relationship Management
CSP	Cloud Service Provider
CSRF	Cross-site request forgery
DDoS	Distributed Denial-of-Service
DMS	Distribution Management System
DoS	Denial-of-service
DRAM	Dynamic Random Access Memory
EID	Endpoint Identifier
EPCNN	Elastic Pooling Convolution Neural Networking
FTP	File Transfer Protocol
HRM	Human Resource Management
HS-DRT	High Security Distribution and Rake Technology
IaaS	Infrastructure as a Service
IBM	International Business Machines
ICN	Information Centric Networking
IDC	International Data Corporation
IoE	Internet of Everything
IoMT	Internet of Medical Things
IoT	Internet of Things
ISP	Internet Service Provider
LAN	Local Area Network

LISP	Locator ID Separation Protocol
MBB	Mobile Broadband
MDC	Micro Data Center
MEC	Mobile Edge Computing
MITM	Man-in-the-Middle
MLE	Message-Locked Encryption
ML-KNN	Machine Learning K-Nearest Neighbors
MONROE	Measuring Mobile Broadband Networks in Europe
MPTCP	Multi-Path Transmission Control Protocol
MTD	Moving Target Defense
MWSN	Mobile Wireless Sensor Network
NFC	Near Field Communication
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PoW	Proof-of-Work
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low-Power and Lossy Networks
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined Protocol
SQL	Structured Query Language
SSD	Solid-state drive
SSL	Secure Sockets Layer
STLs	Smart Traffic Lights
SVMs	Support Vectors Machines
TCP	Transmission Control Protocol
TEE	Trust Execution Environment
TLS	Transport Layer Security
UPS	Uninterruptable Power Supplies
VMM	Virtual Machine Monitor
VPNs	Virtual Private Networks
WSN	Wireless Sensor Network

XACML	Extensible Access Control Markup Language

Περίληψη

Ο ομιχλώδης προγραμματισμός (fog computing) αποτελεί μια υπολογιστική πλατφόρμα που διευρύνει το υπολογιστικό νέφος (cloud computing) στην άκρη του δικτύου (Khan, Parkinson and Qin, 2017). Αυτό το νέο είδος προγραμματισμού αντιμετωπίζει νέα θέματα και προκλήσεις ασφάλειας, εκτός από εκείνα που κληρονόμησε από το υπολογιστικό νέφος. Ως εκ τούτου, η παρούσα διπλωματική εργασία επιδιώκει την επισκόπηση της ασφάλειας σε περιβάλλοντα ομίχλης (fog environments). Ειδικότερα, αναλύονται ποικίλες τρωτότητες και απειλές που επηρεάζουν την ασφάλεια σε ομιχλώδη περιβάλλοντα, καθώς και ορισμένες περιπτώσεις πραγματικών επιθέσεων σε περιβάλλοντα ομίχλης. Επιπλέον, παρουσιάζονται αντίμετρα που μπορούν να ληφθούν για την αντιμετώπιση των επιθέσεων σε περιβάλλοντα ομίχλης, τα οποία συγκρίνονται με βάση συγκεκριμένα κριτήρια που στηρίζονται στην υπάρχουσα βιβλιογραφία. Τέλος, αναδεικνύονται τα υπάρχοντα ερευνητικά κενά στην επίτευξη και διατήρηση της ασφάλειας σε περιβάλλοντα ομίχλης και προτείνονται ερευνητικές κατευθύνσεις για την αντιμετώπισή τους.

Λέξεις Κλειδιά: Ομιχλώδης προγραμματισμός, υπολογιστικό νέφος, ασφάλεια, επιθέσεις, αντίμετρα, τρωτότητες, απειλές, επισκόπηση, κενά , προκλήσεις, ερευνητικές κατευθύνσεις

Abstract

Fog computing is a computing platform that extends cloud computing to the edge of the network (Khan, Parkinson and Qin, 2017). Similar to cloud computing but with distinct characteristics, fog computing faces new security issues and challenges in addition to those inherited from cloud computing. This thesis seeks to review security in fog environments. In particular, various vulnerabilities and threats affecting security in foggy environments are analyzed, as well as some cases of real attacks in fog environments are supplied. Furthermore, countermeasures are presented, which can be taken to counter security attacks in fog environments, while these countermeasures are also compared against specific criteria drawn from the existing literature. Finally, existing research gaps in achieving and maintaining security in fog environments are highlighted and research directions to address them are proposed.

Keywords: fog computing, cloud computing, security, attacks, countermeasures, vulnerabilities, threats, review, gaps, challenges, research directions

1 *Εισαγωγή*

1.1 Ο ομιχλώδης προγραμματισμός

Στις μέρες μας παρατηρείται το φαινόμενο ολοένα και περισσότερες φυσικές συσκευές να συνδέονται με το *Διαδίκτυο των Πραγμάτων* (Internet of Things - IoT). Το IoT αποτελείται από διάφορα «αντικείμενα», όπως αισθητήρες, έξυπνους μετρητές, PDAs, αυτόνομα αυτοκίνητα, έξυπνές φορητές συσκευές, έξυπνα κινητά τηλέφωνα, RFID ετικέτες και ενεργοποιητές. Τα «αντικείμενα» του IoT που παρουσιάζουν ενσωματωμένη ευφυία στο λογιστικό τους και το υλικό τους συνδέονται μεταξύ τους ώστε να επικοινωνήσουν και να ανταλλάξουν δεδομένα (Al-Fuqaha *et al.*, 2015), (Khan, Parkinson and Qin, 2017). Η ανάπτυξη του IoT οδηγεί στη δημιουργία μεγάλων δεδομένων, τα οποία χρειάζονται τεράστιους υπολογιστικούς πόρους, αποθηκευτικό χώρο καθώς και εύρος ζώνης για την μεταφορά των δεδομένων. Η Cisco προβλέπει ότι μέχρι το 2025 θα έχουν συνδεθεί 75.44 δισεκατομμύρια συσκευές (Alam, 2018).

Το *υπολογιστικό νέφος* (cloud computing) είναι ένα υπολογιστικό μοντέλο που επιτρέπει την πανταχού παρούσα και την κατ' απαίτηση πρόσβαση δικτύου σε κοινόχρηστους υπολογιστικούς πόρους, όπως δίκτυα, διακομιστές, αποθηκευτικούς χώρους, εφαρμογές και υπηρεσίες, που απαιτούν ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον πάροχο υπηρεσιών (Mell and Grance, 2011b). Συμφωνά με την έκθεση του IDC, οι επενδύσεις των εταιριών σχετικά με το δημόσιο υπολογιστικό νέφος έχουν αυξηθεί 4.5 περισσότερο σε σχέση με τα παραδοσιακά πληροφοριακά συστήματα (Guan *et al.*, 2018). Αυτό υποδεικνύει την σημασία και το βαθμό υιοθέτησης του υπολογιστικού νέφους.

Αν και το υπολογιστικό νέφος χρησιμοποιείται συχνά για την επεξεργασία μεγάλων δεδομένων, περιορίζεται ως προς το εύρος ζώνης που υποστηρίζει, οδηγώντας σε υψηλή καθυστέρηση και χαμηλή απόδοση υπηρεσιών. Επομένως, το υπολογιστικό νέφος δεν μπορεί να καλύψει όλα τα είδη εφαρμογών IoT, ειδικά εφαρμογών με τις απαιτήσεις χαμηλής καθυστέρησης και μεγάλου εύρους ζώνης. Ευτυχώς, ο ομιχλώδης προγραμματισμός (fog computing) που προτάθηκε από τη Cisco το 2012, αντιμετωπίζει αυτά τα ζητήματα επιτρέποντας την επεξεργασία δεδομένων στην άκρη του

δικτύου, παρέχοντας υπηρεσίες μεταξύ τελικών χρηστών και χρηστών του υπολογιστικού νέφους (Guan *et al.*, 2018).

Ο ομιχλώδης προγραμματισμός είναι μια αρχιτεκτονική δικτύου με αποκεντρωμένους κόμβους ομίχλης που επικοινωνούν με το νέφος, εκτελούν εργασίες σχετικά με τα δεδομένα στα άκρα του δικτύου και χρησιμοποιούν τους διαθέσιμους πόρους του δικτύου (Naha *et al.*, 2018). Αυτό το μοντέλο προγραμματισμού αποτελεί μια υπολογιστική πλατφόρμα που διευρύνει το υπολογιστικό νέφος στην άκρη του δικτύου (Khan, Parkinson and Qin, 2017). Ο ομιχλώδης προγραμματισμός στοχεύει στη μείωση του φόρτου του δικτύου, στην αύξηση της ταχύτητας επεξεργασίας και στην επέκταση των δυνατοτήτων του υπολογιστικού νέφους με τη χρήση αχρησιμοποίητων πόρων καθώς και έξυπνων αντικειμένων από διάφορους κλάδους της καθημερινής μας ζωής (Yousefpour, Ishigaki and Jue, 2017). Τα βασικά πλεονεκτήματα του ομιχλώδους προγραμματισμού σε σύγκριση με το υπολογιστικό νέφος είναι η μειωμένη καθυστέρηση της μετάδοσης των δεδομένων, η βελτίωση της απόκρισης των εφαρμογών καθώς και η εξοικονόμηση του εύρους ζώνης του δικτύου.

1.2 Αντικείμενο διπλωματικής

Αν και ο ομιχλώδης προγραμματισμός έχει κοινά χαρακτηριστικά με το υπολογιστικό νέφος, περιλαμβάνει και ορισμένα ξεχωριστά χαρακτηριστικά (π.χ. ετερογένεια, υποστήριξη κινητικότητας κ.α.), ενώ αντιμετωπίζει νέα ζητήματα και προκλήσεις ασφάλειας, εκτός από εκείνα που κληρονόμησε από το υπολογιστικό νέφος (όντας μια επέκταση του). Τα ζητήματα αυτά σχετίζονται με τα ειδικά χαρακτηριστικά του ομιχλώδους προγραμματισμού, όπως είναι η ετερογένεια και την κατανεμημένη αρχιτεκτονική του, η οποία αυξάνει την επιφάνεια επιθέσεων.

Ως εκ τούτου, η παρούσα διπλωματική εργασία επιδιώκει να πραγματοποιήσει μια πλήρη επισκόπηση της ασφάλειας σε περιβάλλοντα ομίχλης. Με βάση αυτή την ανασκόπηση, προσπαθεί να παρέχει μια βαθιά κατανόηση των βασικών ζητημάτων ασφάλειας αλλά και των τροπών επίλυσης τους, παρέχοντας σημαντική γνώση στον αναγνώστη. Ειδικότερα, η διπλωματική εργασία συνεισφέρει στην κατανόηση και ανάδειξη των τρωτοτήτων, απειλών και επιθέσεων σε περιβάλλοντα ομίχλης. Επίσης, η διπλωματική εργασία αναδεικνύει τη σημασία της μελέτης πραγματικών επιθέσεων που έχουν συμβεί σε περιβάλλοντα IoT / ομιχλώδη προγραμματισμού, αποκτώντας με αυτό τον τρόπο πρακτική εμπειρία και γνώση για τις απειλές που υπάρχουν στα συγκεκριμένα περιβάλλοντα. Επιπλέον, η διπλωματική εργασία αναλύει ενδελεχώς αντίμετρα κατά των επιθέσεων σε ομιχλώδη περιβάλλοντα, τα κατηγοριοποιεί καθώς και τα συγκρίνει με βάση συγκεκριμένα κριτήρια που αντλούνται από την υπάρχουσα βιβλιογραφία. Σκοπός σε αυτό το σημείο είναι να αναδειχθούν εκείνα τα μέτρα που πράγματι μπορούν να ενισχύσουν το επίπεδο ασφάλειας στα ομιχλώδη περιβάλλοντα καθώς και να βοηθηθεί ο αναγνώστης στην επιλογή των καταλλήλων μέτρων με βάση τις ανάγκες και προτιμήσεις του, εφόσον αυτές σχετίζονται με τα επιλεγμένα κριτήρια σύγκρισης. Τέλος, με βάση την συγκριτική ανάλυση των αντιμέτρων και την τρέχουσα βιβλιογραφία, αναδεικνύονται τα υπάρχοντα ερευνητικά κενά στην επίτευξη και διατήρηση της ασφάλειας των ομιχλωδών περιβαλλόντων και προτείνονται ερευνητικές κατευθύνσεις για την αντιμετώπισή τους.

1.3 Δομή της διπλωματικής

Η παρούσα διπλωματική εργασία αποτελείται από επτά κεφάλαια, συμπεριλαμβανομένου του τρέχοντος. Το δεύτερο κεφάλαιο προσφέρει ένα θεωρητικό υπόβαθρο, κατάλληλο για την κατανόηση του υπόλοιπου μέρους της αναφοράς και των σχετικών συνεισφορών της διπλωματικής. Το τρίτο κεφάλαιο περιλαμβάνει την μεθοδολογία που ακολουθήθηκε για την βιβλιογραφική ανασκόπηση ως προς την ασφάλεια του ομιχλώδους προγραμματισμού. Στο τέταρτο κεφάλαιο αναλύονται οι τρωτότητες, οι απειλές και οι επιθέσεις σχετικά με τον ομιχλώδη προγραμματισμό. Ακολουθεί το πέμπτο κεφάλαιο, το οποίο παρέχει μια κατηγοριοποίηση, ανάλυση και σύγκριση των αντίμετρων που πρέπει να ληφθούν για την αντιμετώπιση των επιθέσεων στα ομιχλώδη περιβάλλοντα. Στο έκτο κεφάλαιο επισημαίνονται τα υπάρχοντα κενά στην έρευνα σχετικά με τη ενίσχυση της ασφάλειας στον ομιχλώδη προγραμματισμό καθώς και προτείνονται κάποιες ερευνητικές κατευθύνσεις για την αντιμετώπισή τους**.** Στο τελευταίο κεφάλαιο περιλαμβάνονται τα συμπεράσματα της παρούσας διπλωματικής εργασίας και η σχετική εμπειρία που αποκομίσθηκε από την εκπόνηση της.

2 Υπόβαθρο

Στο κεφάλαιο αυτό αρχικά εστιάζει στην ανάλυση των βασικών εννοιών ασφάλειας για μια κατάλληλη κατανόηση τους ακόμη και από έναν μη ειδικευμένο αναγνώστη. Έπειτα, εξηγεί τι είναι το υπολογιστικό νέφος, ποια είναι τα βασικά χαρακτηριστικά του και ποια είδη υπηρεσιών και μοντέλων ανάπτυξης προσφέρει. Τέλος, προχωρά στο βασικό αντικείμενο της μελέτης ασφάλειας που είναι ο ομιχλώδης προγραμματισμός. Σε αυτή την περίπτωση, παρέχει έναν πλήρη ορισμό του τι είναι ο ομιχλώδης προγραμματισμός, αναφέρει ποια χαρακτηριστικά αυτός παρουσιάζει, εξηγεί πως αυτός διαφέρει από το υπολογιστικό νέφος, προσδιορίζει τις διαφορές μεταξύ αυτών των δύο προγραμματιστικών μοντέλων και τέλος παραθέτει της απαιτήσεις ασφάλειας που πρέπει να ικανοποιούνται σε περιβάλλοντα, εφαρμογές και συστήματα ομίχλης.

2.1 Βασικές έννοιες στην ασφάλεια

2.1.1 Τρωτότητα

Τρωτότητα ή ευπάθεια (vulnerability) ορίζεται ως μια αδυναμία που μπορεί να έχει ένα αγαθό, μια ομάδα αγαθών ή ένα μέτρο ασφάλειας σε ένα σύστημα που μπορεί να γίνει εκμεταλλεύσιμη από μια ή περισσότερες απειλές (Κρητικός, 2023). Οι ευπάθειες μπορεί να διακριθούν με βάση τις διαστάσεις της σκοπιμότητας σε σκόπιμες ή τυχαίες και την διάσταση της υπαιτιότητας, ως ανθρώπινες ή τεχνικές. Ανθρώπινη ευπάθεια ορίζεται η αδυναμία που οφείλεται σε σφάλματα ή αδυναμίες χρηστών του υπολογιστικού συστήματος. Τεχνική ευπάθεια είναι η αδυναμία που οφείλεται σε δυσλειτουργία ή σφάλματα ενός τεχνικού συστατικού ενός υπολογιστικού συστήματος. Σκόπιμη ευπάθεια είναι μια αδυναμία που προκύπτει σκόπιμα από ανθρώπινη ενέργεια ή παράλειψη. Τυχαία ευπάθεια είναι μια αδυναμία που προκύπτει από ενέργειες ή καταστάσεις που δεν προϋποθέτουν κακή πρόθεση και δεν είναι σκόπιμες (Γκρίτζαλης, 2013).

Συμφωνά με τον Κάτσικα υπάρχουν επτά κατηγορίες ευπαθειών (Κάτσικας, 2014):

1. *Προσωπικό*: Αδυναμίες που σχετίζονται με την εκπαίδευση, την ευαισθητοποίηση ή τις ενέργειες του προσωπικού.
2. *Διοίκηση*: Αδυναμίες που σχετίζονται με τις πολιτικές, τις διαδικασίες ή την ηγεσία της διοίκησης.
3. *Μέτρα ασφάλειας*: Αδυναμίες στα υφιστάμενα τεχνικά ή διοικητικά μέτρα ασφάλειας.

4. *Επιχειρησιακές λειτουργίες*: Αδυναμίες που σχετίζονται με τις διαδικασίες και τις λειτουργίες της επιχείρησης.
5. *Παροχή υπηρεσιών*: Αδυναμίες που σχετίζονται με τις υπηρεσίες που προσφέρονται από τον οργανισμό.
6. *Λογισμικό*: Αδυναμίες που σχετίζονται με το λογισμικό που χρησιμοποιείται από τον οργανισμό.
7. *Φυσικό περιβάλλον*: Αδυναμίες που σχετίζονται με τις εγκαταστάσεις, τον υλικό εξοπλισμό (π.χ. τηλεπικοινωνιακό, υπολογιστικό, αποθηκευτικό) ή την υποδομή του συστήματος.

Οι τρεις πρώτες κατηγορίες ευπαθειών μπορεί να εκτιμηθούν χρησιμοποιώντας πληροφορίες για περιστατικά που συνέβησαν στο παρελθόν, αλλά και νέες τάσεις για την εκτίμηση του κινδύνου. Οι υπόλοιπες κατηγορίες ευπαθειών, που εντάσσονται στην γενική κατηγορία, δηλαδή τις τεχνικές ευπάθειες, μπορεί να εκτιμηθούν χρησιμοποιώντας αυτοματοποιημένα εργαλεία εντοπισμού ευπαθειών, τεχνικών δοκιμών και αξιολόγησης της ασφάλειας, δοκιμές διείσδυσης (penetration testing) ή επιθεώρηση κώδικα (Κάτσικας, 2014).

Ο ανθρώπινος παράγοντας καθορίζει την κατάλληλη κλίμακα μέτρησης των ευπαθειών είτε με τρεις ή πέντε βαθμούς κλίμακας. Για παράδειγμα, η τρίβαθμη κλίμακα μπορεί να πάρει τρεις τιμές: χαμηλή, μέτρια και υψηλή. Η τιμή "χαμηλή" εννοεί ότι η πιθανότητα εκμετάλλευσης της ευπάθειας από μια απειλή είναι μικρή και η υφισταμένη προστασία είναι επαρκής για την αντιμετώπιση πιθανών απειλών. Η τιμή "μέτρια" υποδηλώνει ότι υπάρχει αυξημένη πιθανότητα οι απειλές να εκμεταλλευτούν τις ευπάθειες του συστήματος με επιτυχία και η υφιστάμενη προστασία ίσως χρειάζεται ενίσχυση για την αποτελεσματική αντιμετώπιση των πιθανών απειλών. Η τιμή "υψηλή" υποδηλώνει ότι είναι σίγουρο ότι οι απειλές θα εκμεταλλευτούν τις ευπάθειες προκαλώντας σοβαρές ζημίες στο σύστημα και η υφιστάμενη προστασία αδυνατεί να προστατεύσει το σύστημα (Κάτσικας, 2014). Η κατανόηση των διαφορετικών κατηγοριών ευπαθειών, καθώς και των μεθόδων εκτίμησης του κινδύνου, είναι απαραίτητη για την υλοποίηση αποτελεσματικών μέτρων πρόληψης και αντιμετώπισης.

2.1.2 Απειλή

Απειλή ορίζεται ως η πιθανή αιτία ενός συμβάντος που μπορεί να οδηγήσει σε βλάβη σε ένα σύστημα ή έναν οργανισμό. Μια απειλή μπορεί να εκμεταλλευτεί μια ευπάθεια του συστήματος των περιουσιακών στοιχείων που εντάσσονται σε αυτό. Ένας πράκτορας απειλών υλοποιεί απειλές εκμεταλλευόμενος ένα ή περισσότερα τρωτά σημεία (Suryateja, 2018).

Συμφώνα με τον Κάτσικα, οι απειλές διακρίνονται σε σκόπιμες ή τυχαίες (Κάτσικας, 2014). Σκόπιμη απειλή είναι η απειλή που πραγματοποιείται με σκοπό να προκαλέσει σκόπιμα βλάβη. Οι πόροι, η γνώση, η ικανότητα και τα κίνητρα αποτελούν παράγοντες για τους επίδοξους επιτιθέμενους που έχουν ως στόχο να πραγματοποιήσουν απειλές. Από την άλλη πλευρά, τυχαία απειλή είναι η απειλή που προέρχεται από αμέλεια και όχι από κακόβουλη πρόθεση (Γκρίτζαλης, 2013). Η πρόβλεψη των τυχαίων επιθέσεων μπορεί να βασιστεί στα στατιστικά δεδομένα, την

εμπειρία, την τοποθεσία των εγκαταστάσεων του οργανισμού, τα καιρικά φαινόμενα και τον ανθρώπινο παράγοντα.

Οι υπεύθυνοι για την ασφάλεια του πληροφοριακού συστήματος εφαρμόζουν την κατάλληλη κλίμακα (τρίβαθμη ή πεντάβαθμη) μέτρησης της πιθανότητας εμφάνισης απειλών. Για παράδειγμα, η τρίβαθμη κλίμακα μέτρησης προσφέρει μια απλή μέθοδο για την εκτίμηση της πιθανότητας εμφάνισης μιας απειλής. Περιλαμβάνει τρεις δυνατές βαθμολογίες: χαμηλή, μέτρια και υψηλή. Η χαμηλή βαθμολογία σημαίνει ότι η πιθανότητα εμφάνισης είναι μηδαμινή, αλλά δεν είναι αδύνατη η υλοποίηση της απειλής. Η μέτρια βαθμολογία σημαίνει ότι η απειλή είναι πιθανό να εμφανιστεί και υπάρχουν πολλές ενδείξεις ότι είναι πιθανό να πραγματοποιηθεί. Η υψηλή βαθμολογία σημαίνει ότι η απειλή είναι πολύ πιθανό να εμφανιστεί και υπάρχουν πολλά στοιχεία, τα οποία δείχνουν ότι μπορεί να οδηγήσουν με απολυτή βεβαιότητα στην επιτυχημένη πραγματοποίηση της απειλής (Κάτσικας, 2014).

2.1.3 Κίνδυνος

Οι πληροφορίες, δεδομένα και οι υπολογιστικοί πόροι είναι παραδείγματα περιουσιακών στοιχείων ή αγαθών για ένα πληροφοριακό σύστημα. Τα παραπάνω αγαθά έχουν κάποια αξία, κι επομένως, πρέπει να προστατευτούν. Αν δεν προστατευτούν τα αγαθά, υπάρχει κίνδυνος να καταστραφούν, δηλαδή να μειωθεί η αξία τους (Κάτσικας, 2014).

Ο κίνδυνος (risk) είναι το ενδεχόμενο εμφάνισης δυσμενών επιπτώσεων που προκαλούνται όταν συμβεί μια απειλή ή εκμετάλλευση μίας αδυναμίας ενός πληροφοριακού συστήματος. Οι δυσμενείς επιπτώσεις μπορεί να είναι η διακοπή λειτουργίας του συστήματος, η απώλεια δεδομένων, η χρήση ανεπιθύμητων εξουσιοδοτήσεων ή ακόμη και η παραβίαση της ασφάλειας πληροφοριών. Συνεπώς, ο κίνδυνος δεν είναι μόνο να συμβούν οι απειλές αλλά και να πραγματοποιηθούν οι επακόλουθες επιπτώσεις τους. Όταν υπάρχει υψηλός κίνδυνος, δηλαδή υπάρχει μεγάλη πιθανότητα εμφάνισης κινδύνων, είναι πολύ πιθανό να συμβεί ένα ατύχημα ή επιβλαβές γεγονός. Αντιθέτως, όταν το επίπεδο κινδύνου είναι χαμηλό, αυτό σημαίνει ότι υπάρχει χαμηλότερη πιθανότητα εμφάνισης κίνδυνου, επομένως η πιθανότητα ατυχήματος ή επιβλαβούς γεγονότος είναι χαμηλότερη. Πρέπει να σημειώσουμε ότι η αξιολόγηση του κινδύνου είναι μια πολύπλοκη διαδικασία, στην οποία παίζουν ρόλο πολλοί παράγοντες (Κάτσικας, 2014).

2.1.4 Επιφάνεια επίθεσης

Η επιφάνεια επίθεσης (attack surface) είναι ο αριθμός όλων των πιθανών σημείων ή διανυσμάτων επίθεσης (attack vectors) με βάση τα οποία ένας μη εξουσιοδοτημένος χρήστης μπορεί να έχει πρόσβαση σε ένα πληροφοριακό σύστημα για να πετύχει τους κακόβουλους σκοπούς του. Η μείωση της επιφάνειας επίθεσης θεωρείται στρατηγική για την ενίσχυση της άμυνας και την πρόληψη περιστατικών ασφάλειας. (Fortinet, 2024)

Η επιφάνεια επίθεσης και το διάνυσμα επίθεσης είναι διαφορετικές αλλά σχετιζόμενες έννοιες. Ένα διάνυσμα επίθεσης είναι η μέθοδος που χρησιμοποιεί ένας εγκληματίας του κυβερνοχώρου για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση ή να παραβιάσει τους λογαριασμούς ενός χρήστη ή τα συστήματα ενός οργανισμού. Η επιφάνεια επίθεσης είναι ο χώρος τον οποίο μπορεί να εκμεταλλευτεί ένας εγκληματίας του κυβερνοχώρου, για να πραγματοποιήσει επίθεση ή παραβίαση. Όποτε, επειδή σε κάθε "ευπαθές" σημείο του χώρου, μπορεί να υπάρχει μία ή παραπάνω επιθέσεις που μπορεί να πραγματοποιηθούν, θεωρούμε πως η επιφάνεια επίθεσης σχετίζεται με πολλά διανύσματα επίθεσης. (Fortinet, 2024)

Υπάρχουν δύο είδη επιφάνειας επίθεσης: η ψηφιακή και η φυσική. Η ψηφιακή επιφάνεια επίθεσης αντιστοιχεί στο σύνολο όλων των ψηφιακών αγαθών (digital assets), τα οποία συνδέονται με το δίκτυο ενός οργανισμού ή εντοπίζονται στο δικτυωμένο σύστημα του οργανισμού αυτού, και περιλαμβάνει οποιαδήποτε ευπάθεια υπάρχει σε αυτά, η οποία μπορεί να χρησιμοποιηθεί από κυβερνο-εγκληματίες με σκοπό να διεισδύσουν στο σύστημα ώστε να κλέψουν δεδομένα ή να προκαλέσουν ζημία. Τα ψηφιακά αγαθά μπορεί να πάρουν τη μορφή λογισμικού, όπως εφαρμογές, υπηρεσίες, επιχειρησιακές διαδικασίες, διακομιστές ιστού (web servers), μεσισμικό (middleware), εικονικές μηχανές (virtual machines), δοχεία (containers) κ.α., καθώς και δεδομένων χρηστών, όπως τα διαπιστευτήρια σύνδεσης. Από την άλλη μεριά, η φυσική επιφάνειας επίθεσης αντιστοιχεί σε όλες τις συσκευές, που βρίσκονται στην άκρη του δικτύου, όπως υπολογιστές, έξυπνες κινητές συσκευές, σκληροί δίσκοι, φορητοί υπολογιστές, USB μονάδες, τηλεπικοινωνιακός εξοπλισμός (π.χ. μεταγωγείς, δρομολογητές), καθώς επίσης και απορριφθέν υλικό (discared hardware). Επομένως, η φυσική επιφάνεια περιλαμβάνει όλες τις τρωτότητες που μπορεί να έχουν αυτές οι συσκευές και το απορριφθέν υλικό. (Fortinet, 2024)

Κατά τη γνώμη μας, οι ανθρώπινες τρωτότητες μπορούν να αφορούν και τα δύο είδη επιφάνειας επίθεσης. Διότι μπορεί να οδηγήσουν στην υλοποίηση τόσο φυσικών όσο και ψηφιακών απειλών. Για παράδειγμα, ένα άτομο μπορεί άθελά του να πέσει θύμα επίθεσης tailgating, διότι δεν έλεγξε αν υπάρχει κάποιος από πίσω του, έτσι ώστε ένας επιτιθέμενος να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε μια φυσική τοποθεσία. Ως ένα άλλο παράδειγμα, ένα άτομο μπορεί να χρησιμοποιεί ασθενείς κωδικούς, επιτρέποντας έναν επιτιθέμενο, π.χ. με μια επίθεση τύπου brute-force, να διεισδύσει στον λογαριασμό του σε κάποια υπηρεσία ή σύστημα.

Στις κοινές τεχνικές διανυσμάτων επιθέσεων συμπεριλαμβάνονται το ηλεκτρονικό ψάρεμα (phishing), η χρήση κακόβουλου λογισμικού (malware), εκμεταλλεύσεις τρωτοτήτων λογισμικού όπως μη επικύρωση δεδομένων, εκχύσεις (π.χ. έκχυση SQL), brute-force επιθέσεις, επιθέσεις ενδιάμεσου (man-in-the-middle - MiTM), άρνησης υπηρεσίας (denial of service), μη ενημερωμένο λογισμικό (unpatched software), εκμεταλλεύσεις τρωτοτήτων κρυπτογράφησης (encryption issues) και φυσικές επιθέσεις (π.χ. φυσική πρόκληση ζημίας ή πυρκαγιάς σε έναν υπολογιστή ή κέντρο δεδομένων). (Fortinet, 2024).

2.1.5 Υπηρεσία, αντίμετρα & μηχανισμοί ασφάλειας

Η *υπηρεσία ασφάλειας* είναι μια δυνατότητα ή λειτουργία που παρέχεται από έναν φορέα και υποστηρίζει έναν ή περισσότερους στόχους ασφάλειας, όπως η διαχείριση κλειδιών, ο έλεγχος πρόσβασης, η αυθεντικοποίηση, η εμπιστευτικότητα, η ακεραιότητα και η μη άρνηση πληροφοριών, συχνά υλοποιώντας πολιτικές ασφάλειας μέσω μηχανισμών προστασίας (CSRC NIST, 2024).

Αντίμετρο ασφάλειας είναι ένα αμυντικό μέτρο ή μέθοδος που χρησιμοποιείται για να μειώσει ή να εξαλείψει τους κινδύνους και τις ευπάθειες. Τα αντίμετρα μπορεί να είναι διοικητικά, τεχνικά ή νομικά. Συνηθισμένα παραδείγματα αντίμετρων είναι οι έλεγχοι ασφάλειας (security controls), οι διαδικασίες, οι πολιτικές ή οι τεχνολογίες που δημιουργούνται για να αποτρέψουν, ανιχνεύσουν ή να μετριάσουν τις επιπτώσεις των περιστατικών ασφάλειας. (Securiti, 2024)

Ο *έλεγχος ασφάλειας (security controls)* είναι προστατευτικά μέτρα η αντίμετρα που ορίζονται για ένα πληροφοριακό σύστημα ή έναν οργανισμό σχεδιασμένα να προστατεύουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πληροφοριών του και να πληρούν συγκεκριμένες απαιτήσεις ασφάλειας (CSRC NIST, 2024).

Ο μηχανισμός ασφάλειας είναι ένα αμυντικό πλαίσιο που έχει σχεδιαστεί τους υπολογιστικούς πόρους ΤΠΕ (Τεχνολογίες Πληροφορικής και Επικοινωνιών), τα ευαίσθητα δεδομένα, τις υπηρεσίες και τις πληροφορίες μέσω της εφαρμογής αντιμέτρων και των διασφαλίσεων για την ενίσχυση της ασφάλειας του συστήματος. (ScienceDirect, 2024)

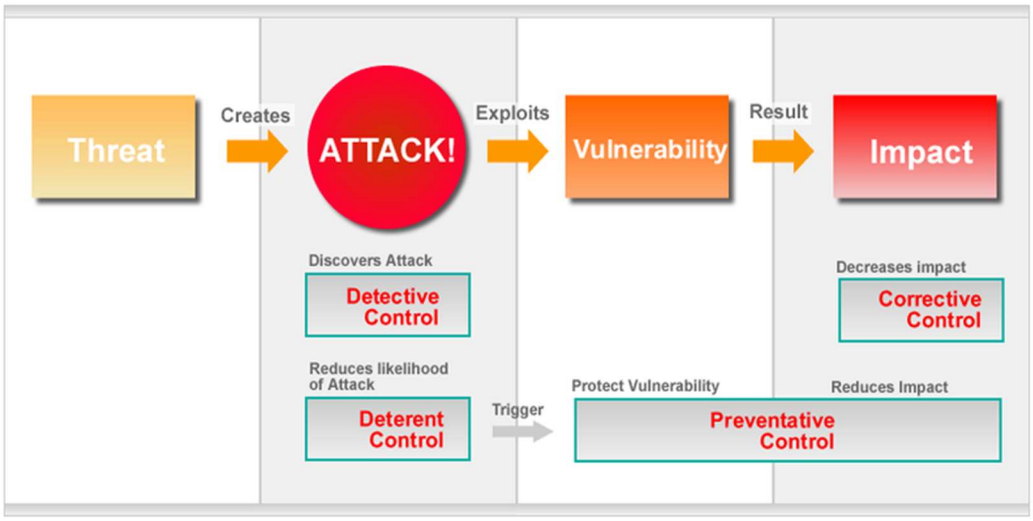
2.1.6 Επίθεση

Με βάση το RFC 2828, η επίθεση μπορεί να οριστεί ως μια έξυπνη πράξη που αποτελεί μια σκόπιμη απόπειρα για να παρακαμφθούν οι υπηρεσίες ασφάλειας και να παραβιαστεί η πολιτική ασφάλειας ενός συστήματος (Shirey, 2000). Επίσης, η επίθεση ορίζεται ως η εκμετάλλευση μιας ευπάθειας από έναν εισβολέα για να πραγματοποιήσει μια απειλή και να προκαλέσει ζημία σε ένα αγαθό (Κρητικός, 2023).

Μπορούμε να διακρίνουμε δύο τύπους επιθέσεων (Stallings and Brown, 2014):

- *Ενεργή επίθεση*: Προσπάθεια αλλαγής πόρων συστήματος ή επηρεασμού της λειτουργίας τους.
- *Παθητική επίθεση*: Μια προσπάθεια εκμάθησης ή χρήσης πληροφοριών από το σύστημα που δεν επηρεάζει τους πόρους του συστήματος ή την λειτουργία του.

Η παρακάτω εικόνα επιδεικνύει και συσχετίζει τις έννοιες ασφάλειας που αναλύθηκαν προηγουμένως.



Εικόνα 1 - Κατανόηση βασικών εννοιών της ασφάλειας πληροφοριακών συστημάτων, όπως η τρωτότητα, η επίθεση, και ο κίνδυνος. Πηγή: (Infocean, 2024)

Με βάση την Εικόνα 1 έχουμε τέσσερις κατηγορίες ελέγχων ασφάλειας (security controls), οι οποίες αναλύονται παρακάτω:

1. *Ανιχνευτικοί έλεγχοι (Detective Controls):* Αυτοί οι έλεγχοι αποσκοπούν στον εντοπισμό παραβιάσεων ή επιθέσεων αφού έχουν πραγματοποιούνται ή έχουν πραγματοποιηθεί. Στην Εικόνα 1 οι ανιχνευτικοί έλεγχοι εντοπίζουν μια επίθεση, αφού αυτή έχει συμβεί. (Open University, 2024)
2. *Αποτρεπτικοί έλεγχοι (Deterrent Controls):* Αυτοί οι έλεγχοι έχουν σχεδιαστεί για να αποθαρρύνουν ή εμποδίσουν πιθανούς εισβολείς. Μπορεί να τους θεωρήσουμε ως την πρώτη γραμμή άμυνας, η οποία στοχεύει στο να κάνει την προσπάθεια των επιτιθέμενων να μοιάζει επικίνδυνη, δύσκολη ή μη ελκυστική. Παρόλο που δεν αποτρέπουν πραγματικά μια επίθεση, μειώνουν την πιθανότητα να πραγματοποιηθεί. Στην Εικόνα 1 οι αποτρεπτικοί έλεγχοι ελαχιστοποιούν την πιθανότητα να συμβεί κάποια επίθεση. (Point Monitor Corporation, 2024)
3. *Προληπτικοί έλεγχοι (Preventative Controls):* Αυτοί οι έλεγχοι δρουν πάνω στην ριζική αιτία μιας δυνητικής επίθεσης ώστε να αποτρέψουν την εκδήλωση της. Θεωρούνται οι ισχυρότεροι έλεγχοι, καθώς εξαλείφουν την δυνατότητα εκμετάλλευσης μιας ευπάθειας. Στην Εικόνα 1 οι προληπτικοί έλεγχοι προστατεύουν τις ευπάθειες. (Open University, 2024)
4. *Διορθωτικοί έλεγχοι (Corrective Controls):* Αυτοί οι έλεγχοι στοχεύουν στην μείωση μιας ζημίας ή το περιορισμό της παραβίασης που προκάλεσε μια επίθεση. Έχουν σχεδιαστεί για να λαμβάνουν μέτρα μετά την παραβίαση και να αποκαθιστούν το σύστημα ή τα δεδομένα σε μια κανονική κατάσταση. Στην Εικόνα 1 οι διορθωτικοί έλεγχοι μειώνουν το αντίκτυπο μιας επίθεσης. (Open University, 2024)

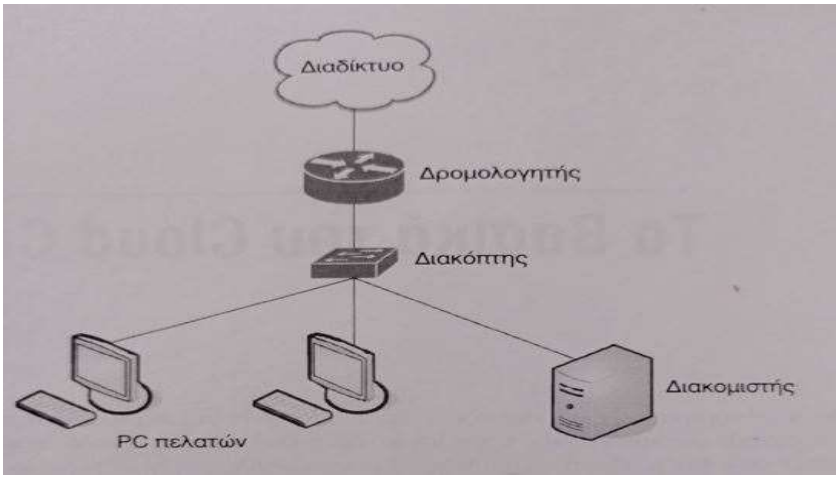
2.2 Υπολογιστικό Νέφος

2.2.1 Ορισμός

Το υπολογιστικό νέφος είναι ένα σχετικά νέο επιχειρηματικό και υπολογιστικό μοντέλο στον κόσμο της πληροφορικής. Με βάση τον ορισμό που δίνεται από τον οργανισμό NIST, το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την πανταχού παρούσα, ανεμπόδιστη και κατ' απαίτηση δικτυακή πρόσβαση σε μια κοινόχρηστη πλατφόρμα υπολογιστικών πόρων (δίκτια, διακομιστές, εφαρμογές και υπηρεσίες), οι οποίοι μπορούν να παρέχονται και να απελευθερώνονται γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης με τον πάροχο υπηρεσιών. (Mell and Grance, 2011a)

Οι Elsenpeter, Velte και Velte (2010) αναφέρουν ότι το υπολογιστικό νέφος ονομάστηκε έτσι από την ομοιότητα με το πώς απεικονίζεται το Διαδίκτυο σε διαγράμματα δικτύων (δείτε Εικόνα 2). Ειδικότερα, το εικονίδιο του σύννεφου χρησιμεύει ως μια οπτική αναπαράσταση για όλα τα "αόρατα" στοιχεία που συνθέτουν το Διαδίκτυο. Με τον ίδιο τρόπο, το υπολογιστικό νέφος λειτουργεί σαν ένα "σύννεφο" υπηρεσιών.

Οι επιχειρήσεις και οι οργανισμοί εξοικονομούν χρήματα και πόρους με την μετάβαση τους στο υπολογιστικό νέφος. Από οικονομικής άποψης, το υπολογιστικό νέφος εξαλείφει τις δαπανηρές επενδύσεις σε υλικό εξοπλισμό (διακομιστές, αποθηκευτικούς χώρους κ.α.), το οποίο παραδοσιακά χρειαζόταν μια επιχείρηση να αγοράσει, να εγκαταστήσει και να συντηρήσει, διότι η κάθε επιχείρηση πληρώνει μόνο τους πόρους του υπολογιστικού νέφους που χρησιμοποιεί και τους προσαρμόζει ανάλογα με τις μεταβαλλόμενες ανάγκες της. Επιπλέον, μειώνονται τα λειτουργικά έξοδα της επιχείρησης, καθώς ο πάροχος υπηρεσιών του υπολογιστικού νέφους αναλαμβάνει την ευθύνη για την συντήρηση και την ενημέρωση του υλικού και του λογισμικού του νέφους με νεότερες εκδόσεις και επιδιορθώσεις (patches) ασφάλειας. (Velte, Velte and Elsenpeter, 2010).



Εικόνα 2 - Απεικόνιση του Διαδικτύου ως σύννεφο σε διαγράμματα δικτύων. Πηγή: (Velte, Velte and Elsenpeter, 2010).

2.2.2 Τα βασικά χαρακτηριστικά του υπολογιστικού νέφους

Υπάρχουν πέντε βασικά χαρακτηριστικά του υπολογιστικού νέφους, όπως ορίζονται από το NIST (Mell and Grance, 2011a):

1. *Αυτό-εξυπηρέτηση κατ' απαίτηση (On-demand self-service):* ο καταναλωτής μπορεί να ανακτά υπολογιστικούς πόρους ή υπηρεσίες και να αποθηκεύει δεδομένα στο νέφος όποτε και όπου χρειαστεί , χωρίς να είναι η αναγκαία η επικοινωνία με τον πάροχο υπηρεσιών.
2. *Πανταχού παρούσα πρόσβαση στο δίκτυο (Ubiquitous access):* Οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε λειτουργίες ή δεδομένα από οποιαδήποτε συσκευή με σύνδεση στο διαδίκτυο, χρησιμοποιώντας διάφορους μηχανισμούς που εξαλείφουν την ετερογένεια, είτε πρόκειται για thin client πλατφόρμες (π.χ. έξυπνα κινητά τηλέφωνα, PDAs, tablet) είτε για thick client πλατφόρμες (π.χ. φορητοί υπολογιστές (laptops), σταθμοί εργασίας (workstations)).
3. *Πολλαπλή μίσθωση (Multi - tenancy):* Ο πάροχος υπηρεσιών του υπολογιστικού νέφους υιοθετεί ένα μοντέλο πολλαπλής μίσθωσης (multi-tenant model) ώστε να συγκεντρώνει και παρέχει υπολογιστικούς πόρους σε πολλούς καταναλωτές, εκχωρώντας δυναμικά φυσικούς και εικονικούς πόρους με βάση τη ζήτηση. Η υλοποίηση της πολλαπλής μίσθωσης στο υπολογιστικό νέφος βασίζεται στην τεχνολογία εικονικοποίησης, η οποία επιτρέπει την απομόνωση και την δυναμική εκχώρηση πόρων σε εικονικές μηχανές, εξυπηρετώντας ταυτόχρονα πολλούς χρήστες με ένα μόνο φυσικό μηχάνημα (Κρητικός, 2023). Η ανεξαρτησία τοποθεσίας διατηρείται, με τους πελάτες να έχουν πρόσβαση στα δεδομένα τους με την προϋπόθεση να υπάρχει σύνδεση στο διαδίκτυο. Οι πάροχοι του υπολογιστικού νέφους προσφέρουν στους χρήστες τη δυνατότητα να καθορίζουν την γενική περιοχή φιλοξενίας των πόρων τους, όπως μια χώρα, μια πολιτεία ή μια συγκεκριμένη γεωγραφική περιοχή. Η επιλογή αυτή μπορεί να αποδειχθεί χρήσιμη για την τήρηση κανονισμών σχετικά με την επεξεργασία δεδομένων ή για την ελαχιστοποίηση της καθυστέρησης (Mell and Grance, 2011a).
4. *Ταχεία ελαστικότητα (Rapid elasticity):* Οι πόροι του υπολογιστικού νέφους, όπως ο χώρος αποθήκευσης και η ισχύς επεξεργασίας, μπορούν να διατεθούν και να απελευθερωθούν με γρήγορο και ευέλικτο τρόπο. Από την οπτική γωνιά του καταναλωτή, οι διαθέσιμοι πόροι του υπολογιστικού νέφους παρουσιάζονται απεριόριστοι, προσφέροντας ευελιξία στην πρόσβαση και χρήση τους σε οποιαδήποτε χρονική στιγμή για οποιοδήποτε μέγεθος.
5. *Μετρούμενη υπηρεσία (measured service):* Οι δυνατότητες μέτρησης χρησιμοποιούνται σε συστήματα υπολογιστικού νέφους για αυτόματη ρύθμιση και βελτιστοποίηση της χρήσης πόρων, διασφαλίζοντας τη διαφάνεια τόσο για τους παρόχους όσο και για τους χρήστες μέσω της παρακολούθησης, διαχείρισης και αναφοράς χρήσης. Αυτή η δυνατότητα μέτρησης υποστηρίζει το μοντέλο πληρωμής "pay-as-you-go" όπου ο χρήστης πληρώνει με βάση τη χρήση των πόρων που δανείζεται από το υπολογιστικό νέφος. Η χρέωση στο μοντέλο πληρωμής "pay-as-you-go" γίνεται με βάση την ποσότητα των υπολογιστικών πόρων που χρησιμοποιεί ένας καταναλωτής (ανά μονάδα χρόνου). Μέσω αυτής της συμφωνίας, οι καταναλωτές μπορούν να έχουν πρόσβαση σε συγκεντρωμένους πόρους με σημαντικά χαμηλότερο κόστος από αυτό που θα πλήρωναν για ένα ιδιωτικό υπολογιστικό

νέφος, ενώ οι πάροχοι επωφελούνται οικονομικά από την εξυπηρέτηση ενός τεράστιου αριθμού πελατών (Νταρζάνος, 2016).

2.2.3 Είδη υπηρεσιών στο υπολογιστικό νέφος

Η βιβλιογραφία χαρακτηρίζει τα μοντέλα υπηρεσιών του υπολογιστικού νέφους ως ιεραρχικές υπηρεσίες ή υπηρεσίες πολλαπλών επιπέδων αρχιτεκτονικής ή ως μοντέλα παροχής υπηρεσιών υπολογιστικού νέφους. Τα μοντέλα υπηρεσιών συχνά αναφέρεται στην βιβλιογραφία ως XaaS, τα οποία προσπαθούν να κατηγοριοποιήσουν όλες τις υπηρεσίες που προσφέρονται από τους παρόχους. Το X μπορεί να αντιπροσωπεύει οποιοδήποτε είδος υπηρεσίας, όπως υποδομή, λογισμικό ή αποθήκευση, ακόμη και αυθαίρετο. Τα υπόλοιπα γράμματα του συμβολισμού (XaaS) προέρχονται από την αγγλική φράση "as a Service - aaS" (μεταφράζεται ως υπηρεσία, οπότε συνολικά έχουμε οτιδήποτε ως υπηρεσία). Το μοντέλο NIST SPI και το μοντέλο υπηρεσίας IBM είναι δύο κύρια μοντέλα υπηρεσιών υπολογιστικού νέφους, που έχουν προταθεί, με το πρώτο να είναι μοντέλο τριών επιπέδων και το δεύτερο τεσσάρων επίπεδων. Τα δυο αυτά μοντέλα διαφέρουν επίσης ως προς τον χρόνο της πρότασης τους. (Κοντόπουλος and Ματσαρίδης, 2013).

2.2.3.1 Το μοντέλο SPI

Παρακάτω αναλύονται τα τρία βασικά είδη υπηρεσιών (SaaS,PaaS και IaaS) του υπολογιστικού νέφους:

1. **Λογισμικό ως Υπηρεσία (Software as a Service - SaaS):** Ο πάροχος (της υπηρεσίας λογισμικού) δίνει την δυνατότητα στους καταναλωτές του να χρησιμοποιούν εξ' αποστάσεως λογισμικό εφαρμογών που τρέχει στην υποδομή του παροχού υπηρεσίας ή ενός παρόχου νέφους, με τον οποίο συνεργάζεται ο πάροχος της υπηρεσίας. Το προσφερόμενο λογισμικό μπορεί να πάρει τη μορφή μιας εφαρμογής ιστού ή μιας υπηρεσία ιστού (SOAP ή RESTful), η οποία καταναλώνεται απομακρυσμένα μέσω του Διαδικτύου (Velte, Velte and Elsenpeter, 2010). Το λογισμικό αυτό είναι προσβάσιμο από διάφορες συσκευές μέσω μιας διεπαφής λεπτού πελάτη (thin client) (για παράδειγμα e-mail και web browser) ή προγραμματιστικής διεπαφής (application programming interface - API). Ο καταναλωτής απλώς χρησιμοποιεί τις εφαρμογές (ιστού) που παρέχονται από τον πάροχο, χωρίς να χρειάζεται να ανησυχεί για τη διαχείριση ή τη συντήρηση τόσο της εφαρμογής όσο και της υποδομής πάνω στην οποία εκτελείται η εφαρμογή (Mell and Grance, 2011a). Βασικό πλεονέκτημα της υπηρεσίας SaaS, είναι η άμεση χρήση της από τους εγγεγραμμένους πελάτες της, αφού δεν απαιτείται εγκατάστασή της από μέρος τους. Αντίθετα, ο πάροχος αναλαμβάνει τη διαχείριση των επίπεδων υποδομής και πλατφόρμας, επιτρέποντας στους πελάτες να επωφεληθούν από την εύκολη πρόσβαση και τον απλό χειρισμό της υπηρεσίας SaaS, σε σύγκριση με άλλες υπηρεσίες υπολογιστικού νέφους. Σε περίπτωση αύξησης του αριθμού των χρηστών τους σε μια υπηρεσία SaaS, οι οργανισμοί-καταναλωτές οφείλουν να αναβαθμίσουν τα υφιστάμενα πρόγραμμα τους ή τις συνδρομές τους, αποφεύγοντας την ανάγκη για αγορά επιπλέον αποθηκευτικού χώρου διακομιστών ή αδειών λογισμικού. Ένα από τα μειονεκτήματα της υπηρεσίας SaaS είναι η έλλειψη ελέγχου, δηλαδή οι καταναλωτές

δεν έχουν τον πλήρη έλεγχο στις υποκειμενικές υποδομές του υπολογιστικού νέφους της υπηρεσίας SaaS. Για παράδειγμα, όταν ο παρόχος της υπηρεσίας SaaS αντιμετωπίζει προβλήματα, όπως είναι η διακοπή της υπηρεσίας ή μια ανεπάρκεια στη λειτουργεία του συστήματος. Επίσης, θα επηρεαστούν και οι χρήστες της υπηρεσίας SaaS, οι οποίοι εκτίθενται σε άμεσες δυσμενείς επιπτώσεις. Οι προσφορές υπηρεσιών SaaS περιλαμβάνουν συνήθως επιχειρησιακές εφαρμογές, όπως το email, η διαχείριση πωλήσεων, η διαχείριση πελατειακών σχέσεων (Customer Relationship Management - CRM), η οικονομική διαχείριση, η διαχείριση ανθρώπινου δυναμικού (Human Resource Management - HRM) και η τιμολόγηση (Rosencrance, 2021).

2. **Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS):** Η υπηρεσία PaaS επιτρέπει στους καταναλωτές να αναπτύσσουν εφαρμογές σε μια πλατφόρμα πάνω από μια υποδομή νέφους χρησιμοποιώντας γλώσσες προγραμματισμού, περιβάλλοντα εκτέλεσης, βιβλιοθήκες, υπηρεσίες και εργαλεία που παρέχονται από τον πάροχο της πλατφόρμας, χωρίς να διαχειρίζονται την υποκείμενη υποδομή. Ο έλεγχος των εφαρμογών, σε αντίθεση με τις υπηρεσίες SaaS περνά στον χρήστη / καταναλωτή, ο οποίος αναπτύσσει και εκτελεί τις εφαρμογές πάνω από την πλατφόρμα (Mell and Grance, 2011a). Η υπηρεσία PaaS προσφέρει μια σειρά πλεονεκτημάτων για τις επιχειρήσεις, τους οργανισμούς και τους προγραμματιστές. Ένα από τα βασικότερα πλεονεκτήματα της πλατφόρμας PaaS είναι η εξάλειψη της ανάγκης για εγκατάσταση περίπλοκου λογισμικού στους υπολογιστές των καταναλωτών της υπηρεσίας PaaS. Ο πάροχος της υπηρεσία PaaS αναλαμβάνει εξ' ολόκληρού την ευθύνη και το κόστος για την τεχνική υποστήριξη της πλατφόρμας PaaS σχετικά με θέματα που αφορούν την συντήρηση της υποδομής (λογικά σε συνεργασία με έναν πάροχο νέφους), του υποστηρικτικού λογισμικού που διατίθεται στην πλατφόρμα και την ασφάλεια (Badger *et al.*, 2012). Επιπλέον, πολλοί πάροχοι υπηρεσιών νέφους (CSP's), οι οποίοι προσφέρουν υπηρεσίες PaaS, διαθέτουν μια ποικιλία διαδικτυακών εργαλείων ειδικά σχεδιασμένων για τους προγραμματιστές, έτσι ώστε να μειώσουν τον χρόνο ανάπτυξης μιας εφαρμογής λογισμικού αλλά και το κόστος της ενώ παρέχουν δυνατότητες συνεργατικής ανάπτυξης εφαρμογής. Τέτοια διαδικτυακά εργαλεία μπορεί να είναι συστήματα ελέγχου εκδόσεων (version control), καθώς και εργαλεία διαχείρισης του κύκλου ζωής των εφαρμογών που ενσωματώνουν ευέλικτες μεθοδολογίες ανάπτυξης λογισμικού. Υπάρχουν πολλά παραδείγματα υπηρεσιών PaaS, όπως το App Engine της Google, το AWS Elastic Beanstalk της Amazon και το Azure App Service της Microsoft (Carlin and Curran, 2012).
3. **Υποδομή ως Υπηρεσία (Infrastructure as a Service - IaaS):** Η υπηρεσία IaaS επιτρέπει στους καταναλωτές να έχουν πρόσβαση σε βασικούς υπολογιστικούς πόρους, δίνοντάς τους έτσι τη δυνατότητα να αναπτύξουν και να εκτελούν αυθαίρετο λογισμικό, συμπεριλαμβανομένων λειτουργικών συστημάτων και εφαρμογών**.** Οι καταναλωτές δεν διαχειρίζονται και ούτε ελέγχουν την υποκείμενη υποδομή νέφους, αλλά μπορούν να ελέγχουν και να διαχειρίζονται εικονικές μηχανές και τις εικόνες τους, λειτουργικά συστήματα, την αποθήκευση και το λογισμικό που αναπτύσσουν, ενώ έχουν περιορισμένο έλεγχο σε μεμονωμένα στοιχεία δικτύου (π.χ. τείχη προστασίας του κεντρικού υπολογιστή), (Mell and Grance, 2011a). Ο πάροχος νέφους της υπηρεσίας IaaS επιλέγει την τοποθεσία για την υποδομή (δηλαδή το κέντρο δεδομένων) της υπηρεσίας IaaS σε περιοχές που

επικρατούν χαμηλά κόστη (φθηνά εργατικά χέρια, μικρό κόστος αγοράς και χαμηλή ενεργειακή χρέωση), μειώνοντας με αυτόν τον τρόπο τα λειτουργικά έξοδα του, έχοντας με αυτό τον τρόπο την ευχέρεια να προσφέρει χαμηλότερες τιμές στην κοστολόγηση των πόρων της υπηρεσίας IaaS αλλά και να αυξήσει το καθαρό κέρδος του. Μια υπηρεσία IaaS επιτρέπει στους καταναλωτές να έχουν μεγαλύτερο έλεγχο άλλα και συνάμα και ευθύνη σχετικά με την διαχείριση της πλατφόρμας IaaS σε σύγκριση με τις πλατφόρμες PaaS και SaaS, οπότε οι καταναλωτές πρέπει να διαθέτουν τις απαραίτητες τεχνικές γνώσεις και δεξιότητες ώστε να μπορούν να εκμεταλλευτούν και διαχειριστούν την πλατφόρμα αυτή. Τέλος, η προσφορά εικονικών μηχανών με προσποιημένη διαμόρφωση (customized configuration) αποτελεί ένα από τα βασικά πλεονεκτήματα της πλατφόρμας IaaS καθώς προσφέρει ευελιξία (π.χ. το περιβάλλον ανάπτυξής είναι περισσότερο προσωποιημένο σε σχέση με μια πλατφόρμα PaaS), ενώ το μοντέλο χρέωσης είναι αρκετά ευνοϊκό και προσαρμόσιμο ανάλογα τις ανάγκες του πελάτη. (Badger *et al.*, 2012) (Pervez, Alandjani, and Babar, 2015)

2.2.3.2 Μοντέλο IBM

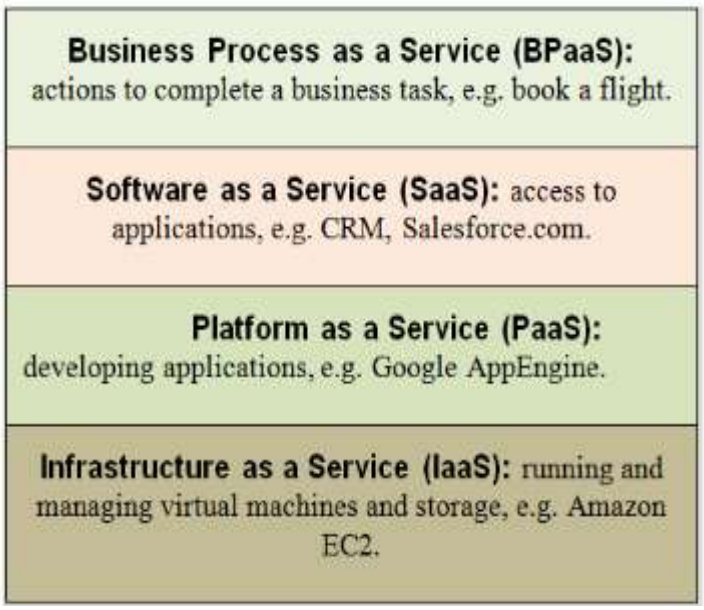
Τέσσερα επίπεδα υπηρεσιών συνθέτουν ένα μοντέλο IBM, σύμφωνα με την αρχιτεκτονική υπολογιστικού νέφους που προτάθηκε από την IBM. Τα επίπεδα αυτά (Εικόνα 3) είναι από πάνω προς τα κάτω τα εξής (Κοντόπουλος and Ματσαρίδης, 2013):

- Business Process as a Service
- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Τα επίπεδα Software as a Service, Platform as a Service και το Infrastructure as a Service του IBM παρέχουν την ίδια λειτουργικότητα με, αυτή που προδιαγράφεται από το μοντέλο SPI, όπως αναλύθηκε προηγουμένως. Το μοντέλο της IBM και το μοντέλο SPI διαφέρουν μόνο ως προς τον αριθμό των επιπέδων, δηλαδή το μοντέλο IBM διαθέτει ένα επιπλέον επίπεδο, το Business Process as a Service (BPaaS) (Επιχειρησιακή Διαδικασία ως Υπηρεσία), (Κοντόπουλος and Ματσαρίδης, 2013).

Σκοπός του BPaaS είναι η επίτευξη επιχειρηματικών στόχων με την οργάνωση, την αυτοματοποίηση και την βελτιστοποίηση των επιχειρησιακών διαδικασιών (business process), οι οποίες περιλαμβάνουν δραστηριότητες που μπορεί να βασίζονται σε υπηρεσίες SaaS, σε υπηρεσίες ιστού ή να αποτελούν χειρωνακτικά βήματα. Μια επιχειρησιακή διαδικασία κατατάσσεται ως μια BPaaS υπηρεσία, εφόσον αυτή εκτελείται εντός του υπολογιστικού νέφους και διαθέτει τα κυριότερα χαρακτηριστικά του, με βάση αυτά που έχουν οριστεί από τον οργανισμό NIST. Ο πάροχος BPaaS παρέχει πόρους στο επίπεδο BPaaS των επιχειρησιακών διαδικασιών, επιτρέποντας στους χρήστες να έχουν πρόσβαση και να τους αξιοποιούν χωρίς να χρειάζεται να προσπελάζουν στα υποκείμενα επίπεδα. (Κοντόπουλος and Ματσαρίδης, 2013)

Το BPaaS είναι κάτι περισσότερο από μια απλή αυτοματοποίηση διαδικασιών βασισμένη στο υπολογιστικό νέφος. Οι προγραμματιστές θα πρέπει να μπορούν να σχεδιάζουν και να υλοποιούν προσαρμοσμένες επιχειρηματικές διαδικασίες για την υπηρεσία BPaaS, οι οποίες θα έχουν την ικανότητα να αλληλοεπιδρούν και με άλλες υπηρεσίες του υπολογιστικού νέφους, όπως τις PaaS, SaaS και IaaS υπηρεσίες. Η υπηρεσία BPaaS αποτελεί ένα ισχυρό εργαλείο για την ενίσχυση της ευελιξίας των οργανισμών, επιτρέποντας την εύκολη και γρήγορη προσαρμογή των επιχειρηματικών διαδικασιών στις εκάστοτε πολιτικές τους (Lynn *et al.*, 2014). Μερικά παραδείγματα υπηρεσιών BPaaS περιλαμβάνουν τις διαδικασίες διαχείρισης των επιδομάτων των εργαζομένων, καθώς και τις διαδικασίες δοκιμών λογισμικού, συμπεριλαμβανομένων των ελέγχων του προσωπικού (Δασυγένης, 2013).



Εικόνα 3 - Η στοίβα των υπηρεσιών του υπολογιστικού νέφος. Πηγή: (Lynn et al., 2014)

2.2.3.3 Αλλά Είδη Υπηρεσιών Νέφους

Στην αγορά υπάρχει μια πληθώρα ειδών υπηρεσιών νέφους, λόγω των στρατηγικών του κάθε παρόχου υπηρεσιών υπολογιστικού νέφους. Δύο έξτρα είδη υπηρεσιών σε σχέση με αυτά που αναφέρθηκαν πριν είναι το Database as a Service (DaaS) και το Hardware as a Service (HaaS) (Κοντόπουλος and Ματσαρίδης, 2013).

Database as a Service (DaaS) Μοντέλο

Το μοντέλο DaaS αφορά μία υπηρεσία λογισμικού βασισμένη στο υπολογιστικό νέφος, η οποία χρησιμοποιείται για την διαχείριση δεδομένων σε αποθήκες ή βάσεις δεδομένων (data warehouses / databases) και την εξαγωγή αναλύσεων των δεδομένων που ενισχύουν την επιχειρηματική ευφυΐα (business intelligence). Με άλλα λόγια, μια υπηρεσία DaaS προσφέρεται ως μια εξειδικευμένη υπηρεσία SaaS, η οποία παρέχει εξειδικευμένες δυνατότητες για την διαχείριση και ανάλυση των

δεδομένων. Το μοντέλο DaaS προσφέρει υπηρεσίες κατ' απαίτηση, ανεξάρτητα από τον γεωγραφικό ή οργανωτικό διαχωρισμό μεταξύ του παρόχου και του καταναλωτή (Wikipedia, 2024). Η υπηρεσία DaaS υποστηρίζει την κάθετη ή οριζόντια κλιμακωσιμότητα των πόρων, προσφέροντάς ένα ευέλικτο μοντέλο για την διαχείριση των πόρων ενός ολοκληρωμένου συστήματος βάσεων δεδομένων ενός οργανισμού (Posey, 2022).

Το μοντέλο DaaS στοχεύει στη μείωση του υψηλού κόστους διατήρησης μιας ιδιωτικής ολοκληρωμένης υπηρεσίας διαχείρισης βάσης δεδομένων εξαλείφοντας την ανάγκη της ύπαρξης πλεονασματικών συστημάτων διαχείρισης βάσεων δεδομένων για την επίτευξη υψηλής διαθεσιμότητας. Έτσι, οι χρήστες της υπηρεσίας DaaS μπορούν να επικεντρωθούν στην χρήση των δεδομένων και στην ανάλυση τους, αντί να χρειάζεται να ανησυχούν για την ανάληψη ευθυνών σχετικά με την συντήρηση της υποδομής και των υπηρεσιών του μοντέλου DaaS, αφού την ευθηνή την αναλαμβάνει όλη ο πάροχος της υπηρεσίας DaaS.

Αυτή η ολοκληρωμένη υπηρεσία διαχείρισης βάσεων δεδομένων, η οποία παρέχεται ως ένα είδος απομακρυσμένης διαχειριζόμενης υπηρεσίας, παραμένει λειτουργική και αποτελεσματική, καθώς και μπορεί να συνεργαστεί με άλλες υπηρεσίες (π.χ. SaaS) για να παρέχει προστιθέμενη (επιχειρηματική) αξία (Κοντόπουλος and Ματσαρίδης, 2013). Ο πάροχος υπηρεσιών DaaS προσφέρει μια ποικιλία διασαφών σχετικών με την διαχείριση του συστήματος των βάσεων δεδομένων, όπως API, CLI και ειδικών σχεδιασμένων εφαρμογών για την απλοποιημένη διαχείριση των συστημάτων βάσεων δεδομένων (Chen, 2023).

Οι εταιρίες, όπως η Mulesoft, η Oracle Cloud και η Microsoft Azure, σχεδιάζουν λύσεις για υπηρεσίες DaaS, οι οποίες μπορεί να επεξεργαστούν μεγάλους όγκους δεδομένων, τα οποία αναλύονται γρήγορα και στέλνονται προς δημοσίευση μέσω RESTful APIs (*Data as a service - Wikipedia*, 2024).

Hardware as a Service (HaaS) Μοντέλο

Στο πλαίσια του μοντέλου HaaS, οι πελάτες της παρούσας πλατφόρμας μπορούν να μισθώσουν μια σειρά πόρων υλικού εξοπλισμού. Με αλλά λόγια οι καταναλωτές της πλατφόρμας HaaS έχουν την δυνατότητα τους να στήσουν το δικό τους κέντρο δεδομένων (data center), αποφεύγοντας με αυτό τον τρόπο να δαπανήσουν χρήματα για τον απαιτούμενο εξοπλισμό. Σε γενικές γραμμές, το HaaS επιτρέπει στους χρήστες να ενοικιάσουν φυσικούς πόρους, όπως εξυπηρετητές, εξοπλισμό για δίκτυα, αποθηκευτικούς χώρους και κύριες μνήμες, σε αντίθεση με τις υπηρεσίες IaaS όπου συνήθως ενοικιάζονται εικονικοί πόροι, όπως οι εικονικές μηχανές. Η υποδομή του HaaS μοντέλου είναι ευέλικτη και υποστηρίζει την οριζόντια κλιμάκωση των πόρων κατ' απαίτηση, δηλαδή ένας χρήστης μπορεί να αποκτήσει απομακρυσμένη πρόσβαση σε φυσικούς πόρους όποτε το θελήσει (Stanik, Hovestadt and Kao, 2012). Επιπλέον, στα πλαίσια του ίδιου φυσικού πόρου (π.χ. ένα μηχάνημα) είναι δυνατή η κάθετη κλιμάκωση μιας εφαρμογής εφόσον δεν ξεπερνούν οι απαιτήσεις τα όρια δυναμικότητας του πόρου. Οι παραπάνω πόροι μπορούν να χρησιμοποιηθούν από πολλούς

χρήστες του οργανισμού που τους δανείζεται ενώ ανάλογα με την χρήση τους υπάρχει και το αντίστοιχο αντίτιμο για τον οργανισμό (Velte, Velte and Elsenpeter, 2010).

2.2.4 Είδη μοντέλων ανάπτυξης υπολογιστικού νέφους

Υπάρχουν τέσσερα διαφορετικά μοντέλα ανάπτυξης υπολογιστικού νέφους με βάση τον οργανισμό NIST (Mell and Grance, 2011a):

1. **Ιδιωτικό νέφος (Private cloud):** Η ιδιωτική υποδομή νέφους παρέχεται αποκλειστικά σε μια εταιρεία με πολλούς χρήστες. Η εταιρεία ουσιαστικά παίζει τόσο το ρόλο του παρόχου όσο και του πελάτη του νέφους αυτού. Η διαχείριση και η λειτουργία της παραπάνω υποδομής γίνεται από την ίδια την εταιρεία ή από τρίτους φορείς και μπορεί να λαμβάνει χώρα εντός ή εκτός των εγκαταστάσεων της εταιρείας (Mell and Grance, 2011a). Το μεγαλύτερο πλεονέκτημα του ιδιωτικού νέφους είναι ότι εξασφαλίζει μεγαλύτερη ασφάλεια και ιδιωτικότητα σε σύγκριση με το δημόσιο νέφος, αφού ο καταναλωτής μπορεί να έχει τον πλήρη έλεγχο της υποδομής του νέφους, ακολουθώντας κατάλληλα πρότυπα και μια ενιαία αρχιτεκτονική ασφάλειας, ενώ δικαίωμα πρόσβασης στο νέφος αποκτούν μόνο εξουσιοδοτημένα άτομα, ουσιαστικά εσωτερικοί χρήστες του παρόχου / καταναλωτή του νέφους. Το κύριο μειονέκτημα του ιδιωτικού νέφους αφορά το κόστος αγοράς του απαραίτητου εξοπλισμού και λογισμικού καθώς και το κόστος στελέχωσης, λειτουργίας και συντήρησης του ιδιωτικού νέφους που συχνά είναι υψηλότερο σχέση με το δημόσιο νέφος (υπό την προϋπόθεση πως μιλάμε για χρήση του δημόσιου νέφους έναντι πλήρους διαχείρισης και λειτουργίας του ιδιωτικού νέφους) (Goyal, 2014).
2. **Κοινοτικό νέφος (Community cloud):** Η κοινοτική υποδομή νέφους παρέχεται αποκλειστικά σε μια συγκεκριμένη κοινότητα οργανισμών με κοινές ανησυχίες (για παράδειγμα στόχους, απαιτήσεις ασφάλειας, πολιτικές και ζητήματα συμμόρφωσης). Η προαναφερθείσα υποδομή νέφους μπορεί να τελεί υπό ιδιοκτησία, να διαχειρίζεται και να λειτουργεί από έναν είτε περισσότερους οργανισμούς της κοινότητας, είτε από τρίτους φορείς, είτε ένα συνδυασμό των δύο προηγούμενων εναλλακτικών, ενώ μπορεί να λαμβάνει χώρα εντός ή εκτός των εγκαταστάσεων των οργανισμών της κοινότητας (Mell and Grance, 2011a). Η δημιουργία ενός κοινοτικού νέφους είναι φθηνότερη από την εγκατάσταση ενός ιδιωτικού νέφους, καθώς το κόστος μοιράζεται μεταξύ όλων των συμμετεχόντων της κοινότητας του κοινοτικού νέφους. Η διαχείριση του κοινοτικού νέφους μπορεί να ανατεθεί σε έναν αμερόληπτο τρίτο μέρος ή να πραγματοποιείται από κοινού μεταξύ των μελών της κοινότητας. Τα εργαλεία που βρίσκονται στο υπολογιστικό νέφος μπορούν να αξιοποιηθούν για πληροφορίες καταναλωτών και της αλυσίδας εφοδιασμού, βελτιώνοντας την αποτελεσματικότητα και την εξυπηρέτηση πελατών από την κοινότητα. Η ασφάλεια του κοινοτικού νέφους είναι μεγαλύτερη από αυτήν του δημοσίου νέφους, ειδικότερα εφόσον το κοινοτικό νέφος διοικείται από τα μέλη του και δεν επιτρέπεται (συνήθως) η εξωτερική πρόσβαση σε αυτό. Ωστόσο, είναι σημαντικό να ληφθούν υπόψη τα μειονεκτήματα που υπάρχουν στο κοινοτικό νέφος (Goyal, 2014). Ένα μειονέκτημα είναι ότι το κοινοτικό νέφος έχει υψηλότερο κόστος από ένα δημόσιο νέφος (όσον αφορά τη χρήση του δημόσιου νέφους). Παρόλου που το κόστος μοιράζεται μεταξύ των μελών της κοινότητας, το συνολικό

κόστος του κοινοτικού νέφους παραμένει υψηλό. Το παραπάνω ισχύει ιδιαίτερα όταν ένας οργανισμός έχει τις δικές του απαιτήσεις, οι οποίες αθροιστικά μοιάζουν σαν να έχει εκμισθωθεί ένα ιδιωτικό νέφος για κάθε κοινοτικό μέλος (Koshkin, 2024). Ακόμα, ένα μειονέκτημα είναι ο πιθανός περιορισμός της διαθεσιμότητας των πόρων μεταξύ όλων των μελών του κοινοτικού νέφους εξαιτίας της διαχείρισης, του συντονισμού και της συμπεριφοράς των χρηστών (Goyal, 2014).

3. **Δημόσιο νέφος (Public cloud):** Η δημόσια υποδομή νέφους παρέχεται για ανοιχτή χρήση σε ένα ευρύ κοινό. Η ιδιοκτησία, η διαχείριση και η λειτουργία του δημοσίου νέφους δύναται να ανατεθεί σε διάφορες οντότητες, όπως επιχειρήσεις, ακαδημαϊκά ιδρύματα, κυβερνητικές υπηρεσίες ή συνδυασμούς όλων των προαναφερόμενων ενδιαφερομένων. Η υποδομή ενός δημόσιου νέφους βρίσκεται στις εγκαταστάσεις του παρόχου του και περιλαμβάνει συστήματα δικτύων, διακομιστές, συσκευές αποθηκευτικού χώρου και κέντρα δεδομένων όπου στεγάζονται όλα τα παραπάνω. Οι υπηρεσίες του δημόσιου νέφους διατίθενται μέσω του Διαδικτύου, επιτρέποντας στους χρήστες να αξιοποιούν πόρους και εφαρμογές από οπουδήποτε (Mell and Grance, 2011a). Το δημόσιο νέφος διαθέτει προηγμένα συστήματα αντιγράφων ασφαλείας και αποκατάστασης προσφέροντας την δυνατότητα στους χρήστες του νέφους να έχουν πρόσβαση στα δεδομένα τους σχεδόν οποιαδήποτε χρονικό διάστημα της ημέρας. Οι περισσότεροι πάροχοι του δημοσίου νέφους προσφέρουν τεχνική υποστήριξη όλο το εικοσιτετράωρο, επτά ημέρες την εβδομάδα. Ένα ακόμη σημαντικό πλεονέκτημα στο δημόσιο νέφους είναι η δυνατότητα κλιμάκωσης των πόρων του νέφους κατ' απαίτηση, δηλαδή είτε αύξηση είτε μείωση των πόρων του νέφους ανάλογα με τις εκάστοτε ανάγκες και απαιτήσεις του καταναλωτή του νέφους. Η υιοθέτηση του δημοσίου υπολογιστικού νέφους προσφέρει σημαντικά οικονομικά οφέλη σε μια επιχείρηση, καθώς η επιχείρηση δεν χρειάζεται να μπει στην διαδικασία σπατάλης χρημάτων για καινούργιο εξοπλισμό ή συντήρηση του υπάρχοντος, αφού όλες τις παραπάνω ευθύνες τις αναλαμβάνει εξολοκλήρου ο πάροχος του νέφους. Η ανοιχτή πρόσβαση σε ένα ευρύ κοινό που προσφέρεται από το δημόσιο νέφος όμως εγείρει πολλά θέματα σχετικά με την ασφάλεια και την ιδιωτικότητα των χρηστών (Goyal, 2014), ιδιαίτερα διότι η επιφάνεια επιθέσεων είναι πολύ μεγαλύτερη σε σχέση με άλλα είδη νέφους.
4. **Υβριδικό νέφος (Hybrid cloud):** Η υβριδική υποδομή νέφους είναι σύνθετη, συνδυάζοντας δύο ή περισσότερα υπολογιστικά νέφη (ιδιωτικό, δημόσιο, κοινοτικό). Το κάθε υποκείμενο υπολογιστικό νέφος σε αυτή την υποδομή διατηρεί την αυτονομία του, αλλά χρησιμοποιεί τυποποιημένη τεχνολογία, η οποία επιτρέπει την επικοινωνία και την μεταφορά δεδομένων και υπολογισμών μεταξύ των υποκείμενων αυτών νεφών. Επομένως, μέσω της τεχνολογίας αυτής εξασφαλίζεται η φορητότητα των δεδομένων και υπολογισμών σε ένα υβριδικό νέφος. Για παράδειγμα, η υπερχείλιση νέφους (cloud bursting) είναι μια στρατηγική που επιτρέπει στις επιχειρήσεις να επεκτείνουν δυναμικά την υπολογιστική τους ισχύ σε ένα δημόσιο υπολογιστικό νέφος, όταν η ιδιωτική τους υποδομή (δηλαδή το ιδιωτικό τους νέφος) υπερφορτώνεται. Η υπερχείλιση νέφους μπορεί να είναι χρήσιμη για την εξισορρόπηση φορτίου του δικτύου μίας επιχείρησης κατά τη διάρκεια αιχμών ζήτησης και για την διαχείριση των απρόβλεπτων αυξήσεων στην κυκλοφορία του συστήματος μέσω της δυναμικής κλιμάκωσης των πόρων του υπολογιστικού νέφους (Mell and Grance, 2011a). Το υβριδικό νέφος προσφέρει τα οφέλη του κόστους και της κλιμακωσιμότητας του

δημοσίου νέφους, ενώ παράλληλα προσφέρει την ασφάλεια και τον έλεγχο ενός ιδιωτικού νέφους. Το υβριδικό νέφος μειώνει τα έξοδα για υποδομή του υπάρχοντος νέφους, βελτιώνει την κατανομή πόρων για προσωρινά έργα (έργα που πρέπει να εκτελεστούν σε ένα καθορισμένο χρονικό διάστημα και έχουν ανάγκη από προσωρινούς πόρους και υποδομές, όπως για παράδειγμα ερευνητικά προγράμματα) με την χρήση του δημοσίου νέφους, παρέχει την ικανότητα της ταχείας κλιμάκωσης των πόρων και αυξάνει την ευελιξία της οργάνωσης, επιτρέποντας την αξιοποίηση τόσο των δημόσιων όσο και των ιδιωτικών νεφών. Τα πιο σημαντικό μειονεκτήματα του υβριδικού νέφους είναι η αυξημένη πολυπλοκότητα διαχείρισης και η ανησυχία για την ασφάλεια των δεδομένων καθώς μετακινούνται μεταξύ ιδιωτικού και δημόσιου νέφους (δηλαδή των υποκείμενων νεφών), (Goyal, 2014).

2.3 Fog Computing

2.3.1 Ορισμός

Μέχρι το 2030, ο αριθμός των συνδεδεμένων IoT συσκευών στον κόσμο θα βρίσκεται μεταξύ 25 και 125 δισεκατομμυρίων (Wilson, 2020). Επομένως, η μεταφορά όλων των δεδομένων από όλες τις συνδεδεμένες συσκευές για επεξεργασία στο νέφος θα χρειαστεί τεράστια ποσά εύρους ζώνης πέρα αυτών που υποστηρίζονται από το υπολογιστικό νέφος, το οποίο αποτελεί μια περιορισμένη κεντρικοποιημένη υποδομή (Naha *et al.*, 2018). Σύμφωνα με τη Cisco, ο υπολογισμός ομίχλης επεκτείνει το υπολογιστικό νέφος, ώστε να είναι πιο κοντά στα IoT πράγματα που παράγουν και ενεργούν με βάση τα δεδομένα και άρα να επιτύχει υψηλότερο εύρος, όπως επίσης και αρκετά χαμηλή καθυστέρηση (Wilson, 2020).

Συμφώνα με τον οργανισμό NIST, ο Ομιχλώδης Προγραμματισμός (Fog Computing) είναι οριζόντιο, φυσικό ή εικονικό υπολογιστικό μοντέλο διαχείρισης πόρων, το οποίο βρίσκεται ανάμεσα σε έξυπνες τερματικές συσκευές και παραδοσιακά υπολογιστικά νέφη ή κέντρα δεδομένων. Ο Ομιχλώδης Προγραμματισμός υποστηρίζει εφαρμογές με αυστηρές απαιτήσεις στην καθυστέρηση, ενώ παρέχει τα οφέλη της πανταχού παρούσας, κλιμακούμενης, διαβαθμισμένης και κατανεμημένης υποδομής. Οι κόμβοι ομίχλης μπορούν να οργανωθούν σε συστάδες είτε κάθετα (για να υποστηρίξουν απομόνωση μεταξύ των διαφορετικών εφαρμογών για λόγους ασφάλειας), είτε οριζόντια (υιοθετώντας μια ομοσπονδιακή δομή που επιτρέπει την κατανομή του φόρτου εργασίας) (Iorga *et al.*, 2017). Η παραπάνω προσέγγιση καθιστά τον Ομιχλώδη Προγραμματισμό ελκυστικό για ένα ευρύ φάσμα εφαρμογών, αφού μπορεί να προσφέρει λύσεις σε ένα πλήθος πεδίων, από το Διαδίκτυο των Πραγμάτων έως κα την υγειονομική περίθαλψη.

Εκτός από τον παραπάνω ορισμό, πολλοί άλλοι ερευνητές έχουν ορίσει τον ομιχλώδη προγραμματισμό με διαφορετικούς τρόπους, όπως τους εξής:

- Ο υπολογισμός ομίχλης είναι μια εξαιρετικά εικονικοποιημένη πλατφόρμα που παρέχει υπηρεσίες υπολογισμού, αποθήκευσης και δικτύωσης μεταξύ των IoT συσκευών και των

κέντρων δεδομένων του παραδοσιακού υπολογιστικού νέφους. Οι IoT συσκευές, εκ φύσεως, βρίσκονται στην άκρη του δικτύου, δηλαδή σε διάφορες τοποθεσίες, συχνά απομακρυσμένες, δυσπρόσιτες ή με περιορισμένη σύνδεση στο Διαδίκτυο (Bonomi *et al.*, 2012). Αντί να χρησιμοποιηθούν τα κέντρα δεδομένων του υπολογιστικού νέφους, δημιουργούνται καινούργια μικρότερα κέντρα δεδομένων (micro datacenter (MDC), τα οποία τυπικά βρίσκονται στην άκρη του δικτύου αλλά όχι πάντα (Bonomi *et al.*, 2012), (Aazam and Huh, 2015). Αυτά τα MDC μειώνουν δραστικά τον χρόνο που απαιτείται για την αποστολή και λήψη δεδομένων από τις IoT συσκευές (Bonomi *et al.*, 2012).

- Το Fog computing είναι ένα σενάριο όπου ένας τεράστιος αριθμός ετερογενών (ασύρματων και μερικές φορές αυτόνομων) πανταχού παρών και αποκεντρωμένων συσκευών επικοινωνούν και δυνητικά συνεργάζονται μεταξύ τους και με το δίκτυο για την εκτέλεση εργασιών αποθήκευσης και επεξεργασίας χωρίς την παρέμβαση τρίτων μερών. Οι εργασίες αυτές μπορεί να αφορούν την υποστήριξη βασικών λειτουργιών του δικτύου ή νέων υπηρεσιών και εφαρμογών που εκτελούνται σε ένα sandboxed[1] περιβάλλον. Οι κάτοχοι συσκευών που διαθέτουν σημαντικό αριθμό συσκευών, όπως πάροχοι υποδομής ή οργανισμοί, μισθώνουν μέρος των συσκευών τους για να φιλοξενήσουν ένα ευρύ φάσμα υπηρεσιών ομιχλώδη προγραμματισμού, πράγμα το οποίο προσφέρει μια σειρά από οφέλη, τόσο οικονομικά όσο και τεχνολογικά (Vaquero and Rodero-Merino, 2014). Για παράδειγμα, ένας οργανισμός με αχρησιμοποίητους πόρους στον αποθηκευτικό του χώρο, μπορεί να τους μισθώσει σε μια εταιρεία ομιχλώδους προγραμματισμού, δημιουργώντας με αυτό τον τρόπο μία νέα πηγή εσόδων για αυτόν.
- Το Fog computing είναι μια κατανεμημένη υπολογιστική πλατφόρμα όπου το μεγαλύτερο μέρος της επεξεργασίας δεδομένων πραγματοποιείται από εικονικοποιημένες ή μη εικονικοποιημένες συσκευές. Συνδέεται επίσης με το υπολογιστικό νέφος για επεξεργασία χωρίς καθυστέρηση και τη μακροπρόθεσμη αποθήκευση χρήσιμων δεδομένων, λειτουργώντας ως ενδιάμεσος σταθμός μεταξύ των χρηστών και του νέφους (Naha *et al.*, 2018).

Επομένως, ο ομιχλώδης προγραμματισμός είναι ένα είδος πλατφόρμας κατανεμημένης υπολογιστικής, η οποία επιτρέπει την επεξεργασία των δεδομένων να γίνεται πιο κοντά στις συσκευές όπου παράχθηκαν, ενώ παράλληλα ενσωματώνει το υπολογιστικό νέφος για πιο βαριές εργασίες. Έτσι, ο ομιχλώδης προγραμματισμός δημιουργεί τις κατάλληλες προϋποθέσεις για ένα υπολογιστικό περιβάλλον υψηλής απόδοσης, όπου ο χρόνος απόκρισης παίζει καθοριστικό ρόλο (Naha *et al.*, 2018).

[1] Ένα sanboxed περιβάλλον είναι ένας μηχανισμός ασφάλειας των πληροφοριακών συστημάτων και αφορά την απομόνωση λογισμικού ή δεδομένων σε ένα ελεγχόμενο περιβάλλον, αποτρέποντας την διάδοση τυχών επιπτώσεων (αστοχίες συστήματος ή τα τρωτά σημεία λογισμικού) ή τροποποιήσεων στο υπόλοιπο σύστημα (Wikipedia, 2024), (Goldberg *et al.*, 1996).

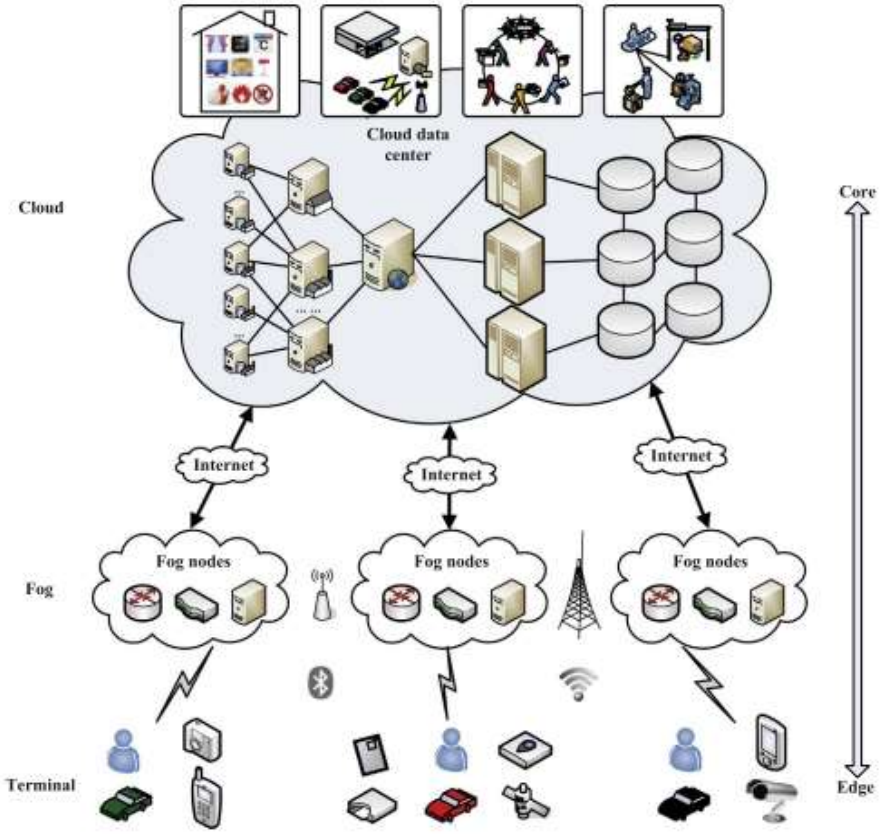
2.3.2 Η αρχιτεκτονική του ομιχλώδους προγραμματισμού

Ο ομιχλώδης προγραμματισμός προτάθηκε για πρώτη φορά από τη Cisco το 2012. Η αυξανόμενη ζήτηση για εφαρμογές πραγματικού χρόνου σε IoT περιβάλλοντα, καθώς και η απαίτηση για εξοικονόμηση ενέργειας στα παραδοσιακά κέντρα δεδομένων δημιούργησε την ανάγκη για τον ομιχλώδη προγραμματισμό (Weng *et al.*, 2021). Η ιεραρχική αρχιτεκτονική του Ομιχλώδους Προγραμματισμού αποτελείται από τα τρία επίπεδα που αναλύονται παρακάτω:

1. **Τερματικό επίπεδο (Terminal Layer)**
   Το τερματικό επίπεδο περιλαμβάνει τους τελικούς χρήστες και τις τελικές συσκευές. Αποτελείται από διάφορες συσκευές IoT, όπως αισθητήρες, κινητά τηλέφωνα, έξυπνα οχήματα, έξυπνες κάρτες, αναγνώστες κ.α. (Weng *et al.*, 2021). Όλες οι παραπάνω συσκευές είναι ευρέως γεωγραφικά κατανεμημένες και παίζουν καθοριστικό ρόλο στη συλλογή χαρακτηριστικών δεδομένων από φυσικά αντικείμενα ή γεγονότα (Alzoubi *et al.*, 2020). Τα συλλεχθέντα δεδομένα στη συνέχεια διαβιβάζονται στο επόμενο επίπεδο (επίπεδο Ομίχλης) για επεξεργασία και αποθήκευση (Weng *et al.*, 2021).
2. **Επίπεδο Ομίχλης (Fog Layer)**
   Το επίπεδο ομίχλης βρίσκεται κοντά στο τερματικό επίπεδο και αποτελείται από μεγάλο αριθμό κατανεμημένων κόμβων ομίχλης (fog nodes). Οι κόμβοι ομίχλης αποτελούνται από δικτυακό εξοπλισμό (κινητό ή στατικό) με μεγαλύτερη χωρητικότητα αποθήκευσης και υπολογιστική ισχύ σε σύγκριση με τις δυνατότητες των συσκευών του τερματικού επιπέδου. Ουσιαστικά, το επίπεδο ομίχλης λειτουργεί ως ενδιάμεσος σταθμός μεταξύ του τερματικού επιπέδου και του επιπέδου νέφους. Το επίπεδο ομίχλης παρέχει πολλές υπηρεσίες και ικανότητες ανάλυσης σε πραγματικό χρόνο στα δεδομένα των συσκευών του Διαδικτύου των Πραγμάτων (IoT). Επιπλέον, το επίπεδο ομίχλης συμβάλλει στην εικονικοποίηση. Οπότε, επιτρέπει την υποστήριξη των πολλαπλών μισθωτών[2] (multi-tenant virtualization), βελτιώνει τους υπολογισμούς, την αποθήκευση και τον διαμοιρασμό πόρων, ενώ παράλληλα απομονώνει τα δεδομένα και τις εφαρμογές IoT. Η ισχύς υπολογισμού σε αυτό το επίπεδο μειώνει το φορτίο επεξεργασίας στους περιορισμένους πόρους των συσκευών IoT και βοηθά στη μεταφορά των πιο απαιτητικών υπολογισμών στους διακομιστές νέφους (cloud servers). Οι κόμβοι ομίχλης συνδέονται με το κέντρο δεδομένων νέφους, ενισχύοντας ακόμη περισσότερο τις δυνατότητες του υπολογισμού και αποθήκευσης που προσφέρονται στις IoT συσκευές. (Alzoubi *et al.*, 2020)
3. **Επίπεδο Νέφους (Cloud Layer)**
   Το επίπεδο νέφους αποτελείται από πολλούς διακομιστές και συσκευές αποθήκευσης υψηλής απόδοσης. Σκοπός του είναι να παρέχει διάφορες υπηρεσίες έξυπνων εφαρμογών, όπως έξυπνο σπίτι, έξυπνες μεταφορές, έξυπνο εργοστάσιο και έξυπνη περίθαλψη. Το στρώμα νέφους διαθέτει ισχυρές δυνατότητες υπολογισμού και αποθήκευσης για να υποστηρίξει μια ευρεία γκάμα υπολογιστικών αναλύσεων και αποθήκευσης μεγάλου όγκου δεδομένων (Weng *et al.*, 2021). Σε αντίθεση με την παραδοσιακή αρχιτεκτονική υπολογιστικού νέφους, όπου όλα τα δεδομένα και οι εργασίες αποστέλλονται αποκλειστικά

[2] Η εικονοποίηση επιτρέπει την υποστήριξη των πολλαπλών μισθωτών (multi-tenant) διότι μπορεί να δημιουργεί απομονωμένα περιβάλλοντα (tenants) (π.χ. ένα για κάθε πελάτη) σε έναν μόνο φυσικό διακομιστή (Zenarmor, 2024)

στο κεντρικό νέφος, το επίπεδο νέφους στο υπολογισμό ομίχλης, δεν διαχειρίζεται όλες τις εργασίες υπολογισμού και αποθήκευσης παρά μόνο τις απαιτητικές. Για αυτές τις ανατιθέμενες εργασίες, το υπολογιστικό νέφος οργανώνεται κατάλληλα για την αποδοτική εκτέλεσή τους. Ειδικότερα, σύμφωνα με το φορτίο ζήτησης, οι κεντρικές μονάδες του νέφους (cloud core modules) διαχειρίζονται και προγραμματίζονται αποδοτικά μέσω ορισμένων στρατηγικών ελέγχου, με σκοπό τη βελτιστοποίηση της χρήσης των πόρων του νέφους (Hu *et al.*, 2017).



Εικόνα 4 - Η ιεραρχική αρχιτεκτονική τρίων επιπέδων του Fog Computing. Πηγή: (Hu et al., 2017)

2.3.3 Τα χαρακτηριστικά του ομιχλώδους προγραμματισμού

Οι υπηρεσίες του ομιχλώδους προγραμματισμού βρίσκονται στην άκρη του δικτύου, δηλαδή κοντά στις τερματικές συσκευές. Λόγω της εγγύτητας των τελικών συσκευών, το μοντέλο του ομιχλώδους προγραμματισμού επιφέρει σημαντικά πλεονεκτήματα έναντι των παραδοσιακών μοντέλων νεφοϋπολογιστικής (Rahman and Chuah, 2018). Κύριο χαρακτηριστικό του ομιχλώδους προγραμματισμού είναι η χρήση των κόμβων ομίχλης, οι οποίοι βρίσκονται κοντά στους τελικούς χρήστες έτσι ώστε τα δεδομένα από τις IoT συσκευές να αποθηκεύονται, να μεταδίδονται και να διαχειρίζονται με μεγαλύτερη ευκολία στο αμέσως επόμενο επίπεδο στην προαναφερόμενη αρχιτεκτονική (Ni *et al.*, 2017).

Παρακάτω αναλύονται τα βασικότερα χαρακτηριστικά του ομιχλώδους προγραμματισμού (δείτε Εικόνα 5):

- **Επίγνωση τοποθεσίας (Location awareness)**
  Η τοποθεσία των κόμβων ομίχλης μπορεί να εντοπιστεί αυτόματα με άμεσο ή έμμεσο τρόπο, έχοντας ως σκοπό την παροχή προσωποποιημένων υπηρεσιών υψηλής ποιότητας στις συσκευές στην άκρη του δικτύου. Ο Ομιχλώδης Προγραμματισμός εστιάζει σε τοπικές IoT εφαρμογές, οι οποίες παρέχονται μόνο σε συσκευές που βρίσκονται στις περιοχές όπου είναι εγκατεστημένοι οι κόμβοι ομίχλης. Επομένως, κάθε κόμβος γνωρίζει την τοποθεσία του (φυσική και λογική / σχετική σε σχέση με τους υπολοίπους), ενώ η τοποθεσία των τελικών συσκευών γίνεται γνωστή με έμμεσο τρόπο, βάσει των κόμβων ομίχλης με τους οποίους επικοινωνούν (Ni *et al.*, 2017). Η πληροφορία της τοποθεσίας αξιοποιείται για την παροχή premium υπηρεσιών χαμηλής καθυστέρησης (λόγω της εγγύτητας με την τελική συσκευή), βοηθώντας με αυτό τον τρόπο στον καλύτερο σχεδιασμό προσαρμοσμένων εφαρμογών στις ανάγκες του χρήστη και του περιβάλλοντος της συσκευής (Patel and Patel, 2021).
- **Χαμηλή καθυστέρηση (Low latency)**
  Οι κόμβοι ομίχλης μπορούν να λάβουν αποφάσεις και να παρέχουν υπηρεσίες με βάση τα τοπικά δεδομένα, χωρίς να απαιτείται η συνεχόμενη χρήση μια υπολογιστικής πλατφόρμας νέφους (Ni *et al.*, 2017). Αυτό σημαίνει ότι οι κόμβοι ομίχλης μπορούν να επεξεργάζονται αιτήματα πολύ γρήγορα, γιατί βρίσκονται κοντά στις τελικές συσκευές (Kaviyazhiny, Bala and Gowri, 2021). Όταν μια τελική συσκευή υποβάλει ένα αίτημα, οι κοντινοί κόμβοι ομίχλης μπορεί να ανταποκριθούν γρήγορα, να αναλύσουν τα δεδομένα και να εκτελέσουν τις απαραίτητες υπολογιστικές εργασίες σχεδόν αμέσως. Επομένως, η εγγύτητα των κόμβων ομίχλης στις τερματικές συσκευές μειώνει τη δικτυακή καθυστέρηση και έτσι συμβάλλει στην επιτάχυνση των υπολογιστικών εργασιών και την ανάλυση των αιτημάτων σε σχέση με την επιτέλεση αυτών στο επίπεδο νέφους (Das and Inuwa, 2023), (Kaviyazhiny, Bala and Gowri, 2021).
- **Κινητικότητα (Mobility)**
  Η υποστήριξη κινητικότητας διαδραματίζει ζωτικό ρόλο για ορισμένες εφαρμογές ομίχλης ως προς την ενίσχυση της άμεσης επικοινωνίας με τις κινητές συσκευές που τις καταναλώνουν μέσω της χρήσης πρωτοκόλλων δικτύου. Για παράδειγμα, το πρωτόκολλο διαχωρισμού Cisco Locator/ID[3] χρησιμοποιεί ένα κατανεμημένο σύστημα καταλόγου για τον διαχωρισμό της μοναδικής ταυτότητας μιας κινητής συσκευής (host identity) που είναι συνδεδεμένη στο διαδίκτυο από την ταυτότητα της τοποθεσίας (site identity) όπου βρίσκεται η κινητή συσκευή. Ο παραπάνω διαχωρισμός επιταχύνει τον εντοπισμό κινητών συσκευών και την παροχή σχετικών υπηρεσιών και εφαρμογών σε αυτές, καθιστώντας τον ιδανικό για εφαρμογές με υψηλή διαθεσιμότητα και αξιοπιστία, όπως η φωνητική

[3] Το πρωτόκολλο διαχωρισμού CISCO Locator/ID (Cisco Locator ID Separation Protocol - LISP) χωρίζει την ταυτότητα μιας συσκευής (Endpoint Identifier - EID) από τη θέση της στο δίκτυο (Routing Locator - RLOC) χρησιμοποιώντας διάφορες τεχνικές όπως χαρτογράφησης και ενθυλάκωσης. Ο κύριος στόχος του είναι να αντιμετωπίσει το πρόβλημα της κλιμακωσιμότητας στη δρομολόγηση του Διαδικτύου που αντιμετωπίζει το παραδοσιακό πρωτόκολλο δρομολόγησης Border Gateway Protocol - BGP). (Cisco, 2024), (NetwrokLessons, 2024)

επικοινωνία και η ροή βίντεο (Rahman and Chuah, 2018). Χάρις το χαρακτηριστικό της κινητικότητας και της κατανεμημένης προσέγγισης του ομιχλώδους προγραμματισμού επιτρέπεται η ανάλυση και η επεξεργασία των δεδομένων να γίνεται όσο τον δυνατόν πιο κοντά στον πελάτη, χωρίς να είναι απαραίτητη η συνεχομένη αποστολή δεδομένων σε κεντροποιημένα κέντρα δεδομένων (Weng *et al.*, 2021).

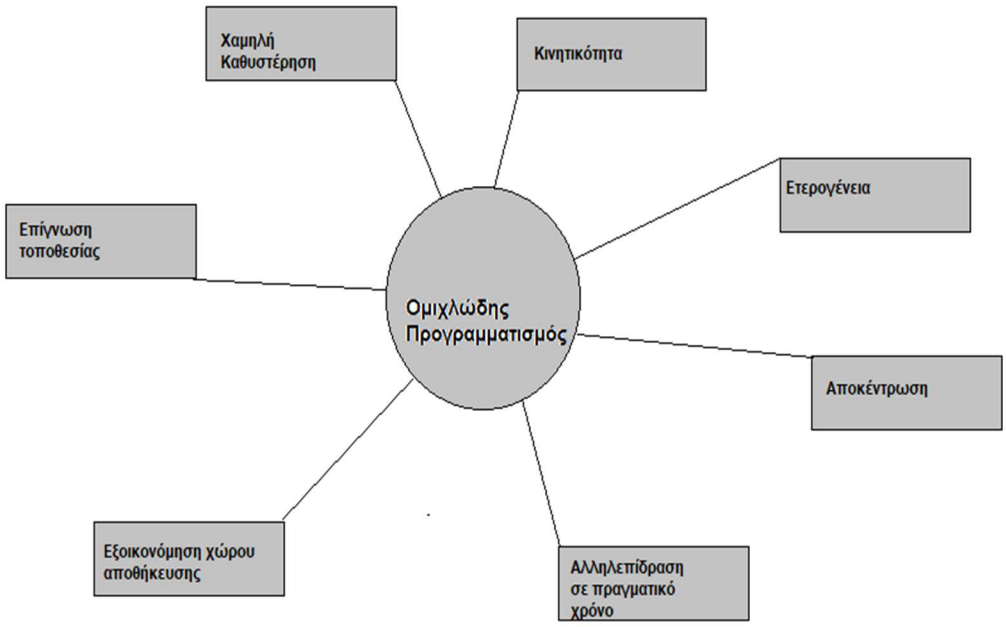
- **Ετερογένεια (Heterogeneity)**
  Η ετερογένεια στον ομιχλώδη προγραμματισμό οφείλεται στην χρήση διαφορετικών συσκευών, δικτυακών πρωτοκόλλων, λειτουργικών συστημάτων και λογισμικών. Οι εφαρμογές έχουν απαιτήσεις που δεν μπορούν να καλυφθούν μόνο από έναν κόμβο ομίχλης. Επιπλέον, η ετερογένεια του περιβάλλοντος επιβάλλει την ανάγκη για την σχεδίαση ειδικών κόμβων ομίχλης, οι οποίοι θα μπορούν να προσαρμόζονται στις ιδιαίτερες απαιτήσεις κάθε περίπτωσης. Επομένως, συναντάμε διάφορα είδη κόμβων ομίχλης, όπως υψηλών επιδόσεων διακομιστές (high-performance servers), διακομιστές αιχμής (edge servers), πύλες δικτύου (gateways), σημεία πρόσβασης (access point) και σταθμούς βάσης (base stations). Το υλικό των ομιχλωδών πλατφόρμων διαθέτει διαφορετικά επίπεδα υπολογιστικής και αποθηκευτικής ικανότητας, ενώ μπορεί να εκτελέσει μια ποικιλία λειτουργικών συστημάτων, καθώς και εφαρμογές λογισμικού. Επιπλέον, οι πλατφόρμες του ομιχλώδους προγραμματισμού υποστηρίζουν την λειτουργία της εικονικοποίησης, επιτρέποντας την δημιουργία και εκμετάλλευση εικονικών κόμβων. Η λειτουργία της εικονικοποίησης στις πλατφόρμες του ομιχλώδους προγραμματισμού προσφέρει πολλά πλεονεκτήματα, όπως την βελτιστοποίηση της διαχείρισης των πόρων, την αυξημένη κλιμακωσιμότητα, την ασφάλεια και τη μείωση του κόστους. Συνεπώς, καθίσταται αναγκαία για την αποτελεσματικότερη και αποδοτικότερη λειτουργία του ομιχλώδους προγραμματισμού καθώς και για την αντιμετώπιση της ετερογένειας. Τέλος, θα πρέπει να σημειώσουμε πως η ετερογένεια δημιουργεί διαφορές προκλήσεις στην διαλειτουργικότητα των δικτυών σε ένα ομιχλώδης περιβάλλον, καθώς απαιτούνται μηχανισμοί για την ομαλή λειτουργία και την ανταλλαγή δεδομένων μεταξύ τους (Weng *et al.*, 2021).
- **Αποκέντρωση (Decentralization)**
  Η αρχιτεκτονική του ομιχλώδους προγραμματισμού είναι αποκεντρωμένη, δηλαδή δεν υπάρχει ένας κεντρικός διακομιστής για την διαχείριση υπολογιστικών πόρων και υπηρεσιών. Η αυτόματη οργάνωση και η συνεργασία των κόμβων ομίχλης επιτρέπουν την ανάπτυξη ευέλικτων και αποδοτικών συστημάτων για εφαρμογές Διαδικτύου των Πραγμάτων (IoT) που λειτουργούν σε πραγματικό χρόνο (Rahman and Chuah, 2018). Η αυτόματη οργάνωση των κόμβων ομίχλης επιτυγχάνεται με την βοήθεια αλγορίθμων αυτό-οργάνωσης, οι οποίοι είναι βασισμένοι σε διαφορές τεχνικές μηχανικής μάθησης. Οι αλγόριθμοι αυτό-οργάνωσης επιτρέπουν στους κόμβους ομίχλης να παίρνουν αποφάσεις μόνοι τους, χωρίς την ύπαρξη κάποιου κεντρικού ελέγχου και να αυτοματοποιούν διάφορες διαδικασίες που αφορούν την τοπολογία του δικτύου, την ανακατανομή των πόρων και την ανάκαμψη σφαλμάτων (Karagiannis and Schulte, 2021).
- **Αλληλεπίδραση σε πραγματικό χρόνο (Real time interaction)**
  Ο ομιχλώδης προγραμματισμός υποστηρίζει την αλληλεπίδραση σε πραγματικό χρόνο και όχι μόνο την επεξεργασία κατά δεσμίδες (batch processing, δηλαδή την διαδικασία επεξεργασίας ενός συνόλου δεδομένων) λόγω της απλότητας, της ευελιξίας, της

συνεργατικότητας και της απόδοσης του (Rahman and Chuah, 2018), (WordReference, 2024). Η επεξεργασία κατά δεσμίδες μπορεί να είναι ωφέλιμη σε ορισμένες περιπτώσεις (π.χ. μηχανική μάθηση, επεξεργασία εικόνας και βίντεο) όμως τείνει να είναι πιο περιπλοκή και λιγότερο ευέλικτη (Rahman and Chuah, 2018).

Παρόλα αυτά συνεχίζεται να υποστηρίζεται και να γίνονται προσπάθειες για την βελτίωση της. Από την άλλη μεριά, η υποστηριζόμενη επεξεργασία σε πραγματικό χρόνο περιλαμβάνει την επαυξημένη πραγματικότητα, το παιχνίδι και την επεξεργασία ροής σε πραγματικό χρόνο. (Rahman and Chuah, 2018)

- **Εξοικονόμηση χώρου αποθήκευσης (Storage space saving)**

  Ο ομιχλώδης προγραμματισμός είναι μία από τις καλύτερες επιλογές για την αποφυγή μεταφοράς ακατάλληλων ή μη σχετιζόμενων δεδομένων σε ολόκληρο το δίκτυο. Με αυτό τον τρόπο, εξοικονομείται χώρος αποθήκευσης και θα μειώνεται η καθυστέρηση, οδηγώντας σε ένα πιο αποδοτικό και ευέλικτο σύστημα διαχείρισης δεδομένων (Rahman and Chuah, 2018). Επίσης, ο ομιχλώδης προγραμματισμός μειώνει τον όγκο δεδομένων που εν τέλει θα αποθηκευτούν στο τρίτο επίπεδο, δηλαδή το υπολογιστικό νέφος.



Εικόνα 5 - Τα κύρια χαρακτηριστικά του ομιχλώδους προγραμματισμού

2.3.4 Οι εφαρμογές του ομιχλώδους προγραμματισμού

Οποιαδήποτε υπολογιστική οντότητα βρίσκεται κοντά στο άκρο του δικτύου, συμπεριλαμβανομένων των διακομιστών που διαχειρίζονται οι χρήστες, των σημείων πρόσβασης δικτύου, των δρομολογητών και των πυλών, μπορεί να χρησιμοποιηθεί για την ανάπτυξη περιβαλλόντων ομιχλώδους προγραμματισμού. Από την άποψη της αρχιτεκτονικής του δικτύου, το μοντέλο υπολογιστικού νέφους είναι μια κεντρικοποιημένη αρχιτεκτονική ελέγχου. Από την άλλη πλευρά, ο ομιχλώδης υπολογισμός αποτελεί μια κατανεμημένη αρχιτεκτονική δικτύου τριών επιπέδων, η οποία επεκτείνει και συμπληρώνει τις υπηρεσίες του υπολογιστικού νέφους. Ένα

περιβάλλον ομίχλης μπορεί να συνδυάσει διάφορους IoT αισθητήρες, υπηρεσίες τοποθεσίας, την ασύρματη μετάδοση δεδομένων και διάφορες άλλες τεχνολογίες με σκοπό την δημιουργία ποικίλων εφαρμογών, οι οποίες έχουν σχεδιαστεί με βάση την αρχιτεκτονική του ομιχλώδους προγραμματισμού. Παρακάτω αναλύονται οι βασικές εφαρμογές του ομιχλώδους προγραμματισμού που συναντάμε σε διαφόρους τομείς της καθημερινότητας μας (Weng *et al.*, 2021):

- **Έξυπνες πόλεις**
  Ένα περιβάλλον ομιχλώδους προγραμματισμού είναι ιδιαίτερα κατάλληλο για εφαρμογές έξυπνων πόλεων, όπως η ειδοποίηση για αστικούς κινδύνους, μέσω της ανατροφοδότησης δεδομένων και της απάντησης σε πραγματικό χρόνο. Παραδείγματος χάριν, κατά την προσπάθεια ανάπτυξης ενός συστήματος υποστήριξης αποφάσεων για πλημμύρες, εγκαθίστανται πολλοί κόμβοι ομίχλης σχηματίζοντας ένα δίκτυο ομιχλώδους προγραμματισμού, οι οποίοι χρησιμοποιούνται για τη συλλογή δεδομένων σε πραγματικό χρόνο από το σύστημα ύδρευσης μιας έξυπνης πόλης και την έγκαιρη προειδοποίηση και σήμανση συναγερμού σε περίπτωση πλημμύρας (Weng *et al.*, 2021).
- **Ιατρική περίθαλψη**
  Οι Rahman και Chuah (2018) υπογραμμίζουν δύο σημαντικές προκλήσεις που αντιμετωπίζουν οι υπηρεσίες και οι εφαρμογές υγείας: η αργή απόκριση και η ασφάλεια των προσωπικών δεδομένων των ασθενών. Η υιοθέτηση της τεχνολογίας του ομιχλώδους προγραμματισμού στον τομέα της υγείας μπορεί να βελτιώσει την ποιότητα και την αποτελεσματικότητα των συστημάτων υγειονομικής περίθαλψης. Για παράδειγμα, το FAST είναι ένα σύστημα παρακολούθησης πτώσεων για ενηλικιωμένα άτομα, το οποίο αξιοποιεί την υπηρεσία της κατανεμημένης ανάλυσης δεδομένων του ομιχλώδους προγραμματισμού, καθώς και αλγόριθμους πρόβλεψης πτώσεων για την έγκαιρη ανίχνευση και πρόληψη πτώσεων, συμβάλλοντας στην προστασία της υγείας και της ευημερίας των ηλικιωμένων (Hu *et al.*, 2017), (Cao *et al.*, 2015), (Rehman *et al.*, 2013).
- **Έξυπνες μεταφορές**
  Το δίκτυο VANET (Vehicular Ad Hoc Network) εξασφαλίζει την αποτελεσματικότητα, την ασφάλεια και την ευκολία στην οδήγηση μέσω της ανταλλαγής πολύτιμων πληροφοριών (Rehman *et al.*, 2013). Επίσης, το δίκτυο VANET χρησιμοποιείται για κοινή χρήση περιεχομένου (διαφήμιση και ψυχαγωγία) και για και υπηρεσίες διάδοσης πληροφοριών, όπως λειτουργίες έκτακτης ανάγκης (φυσικές καταστροφές και τρομοκρατικές επιθέσεις). Ωστόσο, οι νέες εφαρμογές μεταφοράς, όπως η επαυξημένη πραγματικότητα και η αυτόνομη οδήγηση, οι οποίες επιβάλλουν πολύπλοκες λειτουργίες αποθήκευσης και επεξεργασίας δεδομένων, απαιτούν υψηλότερο επίπεδο τόσο αποθήκευσης δεδομένων όσο και υπολογιστικών και επικοινωνιακών δυνατοτήτων.
  Προς τον σκοπό αυτό, προτάθηκε ένα νέο είδος αρχιτεκτονικής υπολογισμού που ονομάζεται VFC (Vehicular Fog Computing, (Οχηματικός Ομιχλώδης Προγραμματισμός)) για να καλύψει αυτές τις απαιτήσεις, συμπεριλαμβανομένης της κινητικότητας, της επίγνωσης θέσης και της χαμηλής καθυστέρησης (Weng *et al.*, 2021). Το δίκτυο κινητών οχημάτων (vehicular network), αποτελεί μια αναδυομένη κατηγορία κινητών δικτύων, άρρηκτα συνδεδεμένη με το Διαδίκτυο των Πραγμάτων. Το δίκτυο κινητών οχημάτων διευκολύνει την επικοινωνία μεταξύ των οχημάτων, των σημείων πρόσβασης και άλλων

αντικειμένων μέσω του V2X (Vehicle-to-Everything) για την ανταλλαγή πληροφοριών σε πραγματικό χρόνο. Βασικά χαρακτηριστικά του παραπάνω δικτύου αποτελούν η επίγνωση της τοποθεσίας, η ασύρματη συνδεσιμότητα, η ταχύτερη επεξεργασία, η χαμηλή καθυστέρηση, η αλληλεπίδραση σε πραγματικό χρόνο και η κινητικότητα. Για να ανταποκριθεί ένα δίκτυο κινητών οχημάτων σε αυτές τις απαιτήσεις, πρέπει να τοποθετηθεί ένας μεγάλος αριθμός κόμβων επεξεργασίας κοντά στα οχήματα, επιτρέποντας την επικοινωνία μέσω ασύρματων συνδέσμων χαμηλής καθυστέρησης. Ο ομιχλώδης προγραμματισμός αποτελεί το πιο κατάλληλο μοντέλο επικοινωνίας για δίκτυα κινητών οχημάτων λόγω των πλεονεκτημάτων (π.χ. χαμηλή καθυστέρηση ανταλλαγής δεδομένων, αξιόπιστη λειτουργία δικτύου κ.α.) που προσφέρει σε σύγκριση με το υπολογιστικό νέφος (Firdhous, Ghazali and Hassan, 2014).

- **Έξυπνο δίκτυο ηλεκτρικής ενέργειας (Smart grid)**

  Ένα έξυπνο δίκτυο ηλεκτρικής ενέργειας (smart grid) αποτελεί ένα δίκτυο ηλεκτρικής ενέργειας επόμενης γενιάς, το οποίο υπόσχεται ότι θα φέρει επανάσταση στον τρόπο διαχείρισης και διανομής ηλεκτρικής ενέργειας. Ένα έξυπνο δίκτυο ηλεκτρικής ενέργειας περιέχει γραμμές μεταφοράς ηλεκτρικής ενέργειας, υποσταθμούς, έξυπνους μετασχηματιστές, έξυπνους μετρητές κ.α. Επίσης, το έξυπνο δίκτυο ηλεκτρικής ενέργειας χρησιμοποιεί αμφίδρομες ροές ισχύος και δεδομένων για τη δημιουργία ενός αυτοματοποιημένου και κατανεμημένου δικτύου διανομής ηλεκτρικής ενέργειας. Επιπλέον, το έξυπνο δίκτυο ηλεκτρικής ενέργειας προσφέρει την δυνατότητα στους πάροχους υπηρεσιών και στους πελάτες να μπορούν παρακολουθούν και να ελέγχουν την τιμολόγηση, την παραγωγή και την χρέωση της κατανάλωσης (των πελατών) σε πραγματικό χρόνο. Ουσιαστικά, δημιουργείται ένα περιβάλλον μεγάλων δεδομένων (big data environment), όπου εκατομμύρια έξυπνοι μετρητές είναι τοποθετημένοι στα σπίτια των καταναλωτών και παράγουν έναν μεγάλο όγκο δεδομένων. Για την αποτελεσματική διαχείριση του τεραστίου όγκου δεδομένων από ένα έξυπνο δίκτυο ηλεκτρικής ενέργειας, χρησιμοποιούνται συλλέκτες ομίχλης (fog collectors) τοποθετημένοι κοντά στα σπίτια των καταναλωτών. Οι συλλέκτες ομίχλης συλλέγουν, επεξεργάζονται και φιλτράρουν τα δεδομένα, στέλνοντας μόνο τις σημαντικές πληροφορίες σε ένα κέντρο δεδομένων του υπολογιστικού νέφους για περαιτέρω ανάλυση και μακροχρόνια αποθήκευση (Rahman and Chuah, 2018).

- **Βιομηχανικό Διαδίκτυο των Πραγμάτων**

  Η Βιομηχανία 4.0 (Industry 4.0) αναφέρεται στην εποχή του μετασχηματισμού της βιομηχανίας που επιτρέπει τον αυτοματισμό και την ανταλλαγή δεδομένων στις τεχνολογίες και τις διαδικασίες παραγωγής. Οι εφαρμογές του Βιομηχανικού Διαδικτύου Πραγμάτων (Industrial Internet of Things - IIoT) χρειάζονται υψηλούς ρυθμούς δεδομένων, εξαιρετικά χαμηλή καθυστέρηση, τοπική αποθήκευση, επεξεργασία σε πραγματικό χρόνο και αξιοπιστία (Basir *et al.*, 2019). Η εφαρμογή του Ομιχλώδους Προγραμματισμού στο Βιομηχανικό Διαδίκτυο των Πραγμάτων μπορεί να διαμορφώσει κατάλληλα τα μηχανήματα, τους αισθητήρες, τους ενεργοποιητές και τις πύλες παραγωγής σε ένα δίκτυο ομίχλης (fog network) για τη βελτίωση της αποδοτικότητας της παραγωγής (Weng *et al.*, 2021). Επιπλέον, το IIoT μπορεί να προσφέρει πολλά οφέλη, όπως είναι η αποκεντρωμένη επεξεργασία δεδομένων, η γρήγορη λήψη αποφάσεων σε πραγματικό χρόνο, η ασφάλεια,

το μειωμένο κόστος, η αυξημένη ευελιξία, καθώς και η ανθεκτικότητα σε βλάβες του δικτύου (Chowdhury and Raut, 2019).

- **Πολυμεσικές εφαρμογές**
  Οι νέες εφαρμογές πολυμέσων υψηλής ποιότητας, όπως τα κατανεμημένα διαδραστικά παιχνίδια, οι πλατφόρμες με βίντεο υπηρεσίες κατ' απαίτηση και ροής (streaming) απαιτούν υψηλές ταχύτητες δεδομένων με χαμηλή καθυστέρηση, αστάθεια και απώλεια πακέτων. Για να επιτευχθούν οι υψηλές ταχύτητες δεδομένων είναι αναγκαίο οι παραπάνω εφαρμογές να τρέχουν όσο πιο κοντά γίνεται στο σημείο όπου βρίσκονται οι τελικοί χρήστες. Τα κέντρα δεδομένων του υπολογιστικού νέφους μπορεί να βρίσκονται διάσπαρτα οπουδήποτε στον κόσμο και η φυσική τους τοποθεσία είναι γνωστή. Ωστόσο, αυτά τα κέντρα δεδομένων, παρόλο που είναι διάσπαρτα, δεν μπορούν πάντοτε να βρίσκονται κοντά στους τελικούς χρήστες, γεγονός που μπορεί να οδηγήσει σε αυξημένη καθυστέρηση στην παροχή των σχετικών υπηρεσιών. Επομένως, ο ομιχλώδης προγραμματισμός αποτελεί την πρακτική λύση για πολυμεσικές εφαρμογές, ώστε να επιτευχθεί ο στόχος της μέγιστης απόδοσης που μπορούν να προσφέρουν τέτοιου είδους εφαρμογές. (Firdhous, Ghazali and Hassan, 2014)
- **Πλαίσιο Δικτύωσης Κεντρικής Πληροφορίας**
  Στο Διαδίκτυο των Πάντων (Internet of Everything (IoE)) σε συνδυασμό με τον ομιχλώδη προγραμματισμό οι υπάρχουσες διευθύνσεις IP μπορεί να αντικατασταθούν με ονομασίες, χρησιμοποιώντας το πλαίσιο Δικτύωσης Κεντρικής Πληροφορίας (Information Centric Networking (ICN) με βελτιωμένους μηχανισμούς αποθήκευσης. Οι κόμβοι ομίχλης μπορούν να διαχειριστούν την μνήμη αποθήκευσης με δίκαιο τρόπο με την βοήθεια αποδοτικότερων αλγορίθμων αποθήκευσης, όπως ο αλγόριθμός δέντρου Steiner (Khan, Parkinson and Qin, 2017). Ειδικότερα κατά την διαδικασία της αποθήκευσης, οι κόμβοι ομίχλης παράγουν ένα δέντρο Steiner, το οποίο προσπαθεί να ελαχιστοποιήσει το συνολικό βάρος του μονοπατιού με την εύρεση του συντομότερου μονοπατιού στο δέντρο, έτσι ώστε να μειωθεί το κόστος αποθήκευσης των πόρων (Su *et al.*, 2015).
- **Αλλές εφαρμογές στον ομιχλώδη προγραμματισμό**
  Οι κόμβοι ομίχλης εκτελούν διάφορες εργασίες σχετικά την ανάκτηση (fetching), την συνένωση (combining) και την εκτέλεση (executing) του περιεχομένου από διαφορές ιστοσελίδες ταυτόχρονα, βελτιώνοντας με αυτό τον τρόπο την απόδοση του δικτύου και μειώνοντας τον χρόνο απόκρισης των ιστοσελίδων, αφού μπορούν να εκτελεστούν σε έναν κόμβο ομίχλης αντί για έναν διακομιστή. Επιπλέον, οι κόμβοι ομίχλης έχουν την δυνατότητα να διακρίνουν τους χρήστες βάσει των MAC διευθύνσεων τους ή των cookies τους, να παρακολουθούν τα αιτήματα των χρηστών, να αποθηκεύουν προσωρινά αρχεία στην μνήμη (cache file) και να καθορίζουν την κατάσταση του τοπικού δικτύου. Βάση των αποτελεσμάτων έρευνας, τα συστήματα του ομιχλώδους προγραμματισμού φαίνεται να έχουν μειώσει την καθυστέρηση πρόβλεψης (prediction latency) από 5 δευτερόλεπτα σε 1.5 δευτερόλεπτα ενώ ο χρόνος καθυστέρησης της εμφάνισης της σελίδας έχει μειωθεί από τα 8 δευτερόλεπτα στα 3 δευτερόλεπτα. Επιπλέον, έχει μειωθεί και η ταχύτητα με την οποία μεταφέρονται τα δεδομένα μέσα στο διαδίκτυο από 75 Kbps σε 10 Kbps. (Khan, Parkinson and Qin, 2017)

2.3.5 Διαφορές ανάμεσα στο υπολογιστικό νέφος και τον ομιχλώδη προγραμματισμό

Το υπολογιστικό νέφος και ο ομιχλώδης προγραμματισμός αποτελούν δύο βασικές αρχιτεκτονικές υπολογισμού που προσφέρουν λύσεις για την αποθήκευση, επεξεργασία και διαχείριση δεδομένων. Αν και οι παραπάνω αρχιτεκτονικές μοιράζονται ομοιότητες ως προς την υλοποίηση των εικονικών τους συστημάτων και την κατ' απαίτηση διάθεση πόρων τους, υπάρχει μια βασική διάφορα: η τοποθεσία τους. Ο ομιχλώδης προγραμματισμός υλοποιείται πολύ πιο κοντά στους τελικούς χρήστες σε σύγκριση με το υπολογιστικό νέφος. Στην παρούσα ενότητα της διπλωματικής εργασίας θα εμβαθύνουμε στις ομοιότητες και τις διαφορές του υπολογιστικού νέφους και του ομιχλώδους προγραμματισμού, εστιάζοντας στις τεχνικές τους διαφορές και τις επιπτώσεις τους σε διάφορες παραμέτρους. (Firdhous, Ghazali and Hassan, 2014)

Ο ομιχλώδης προγραμματισμός ως ιδανική λύση για ασύρματα δίκτυα αισθητήρων σε ένα IoT περιβάλλον

Τα ασύρματα δίκτυα αισθητήρων έχουν χρησιμοποιηθεί ευρέως σε πολλές εφαρμογές ενός IoT περιβάλλοντος. Τα ασύρματα δίκτυα αισθητήρων περιλαμβάνουν κόμβους χαμηλής κατανάλωσης ισχύος, χαμηλού εύρους ζώνης και με περιορισμένες δυνατότητες επεξεργασίας, οι οποίοι είναι κατανεμημένοι σε μεγάλες γεωγραφικές περιοχές. Επιπλέον, τα ασύρματα δίκτυα αισθητήρων πρέπει να υποστηρίζονται από συστήματα με χαμηλή καθυστέρηση, επίγνωση της τοποθεσίας τους και την ευρεία κατανεμημένη κατανομή τους για κατάλληλη επεξεργασία και διανομή των δεδομένων. Ο ομιχλώδης προγραμματισμός από την αρχιτεκτονική φύση του ταιριάζει περισσότερο στις απαιτήσεις των ασύρματων δικτύων από ότι το υπολογιστικό νέφος. (Firdhous, Ghazali and Hassan, 2014)

Η σημασία της ελαχιστοποίησης των «αλμάτων» για την βελτίωση της ασφάλειας και της ακεραιότητας των δεδομένων στο διαδίκτυο

Η ασφάλεια και η ακεραιότητα των δεδομένων αποτελούν δύο από τα πιο σημαντικά χαρακτηριστικά που απαιτούνται από πολλές εφαρμογές του διαδικτύου. Όσο περισσότερο χρόνο ταξιδεύουν τα πακέτα δεδομένων μέσα στο διαδίκτυο, υπάρχει μεγαλύτερη πιθανότητα να διακοπεί η επικοινωνία και επομένως να παραβιαστεί η ακεραιότητα των πακέτων. Επομένως, είναι πάντα επιθυμητό να υπάρχουν λίγα άλματα (hops) μεταξύ των πελατών και των διακομιστών. (Firdhous, Ghazali and Hassan, 2014)

Οι διάφορες στην ασφάλεια μεταξύ του ομιχλώδους προγραμματισμού και του υπολογιστικού νέφους

Η σύγκριση της ασφάλειας μεταξύ του υπολογιστικού νέφους και του ομιχλώδους προγραμματισμού δεν είναι απλή και εξαρτάται από διάφορους παράγοντες. Το υπολογιστικό νέφος είναι μια κεντρικοποιημένη υποδομή, η οποία υιοθετεί τις βέλτιστες πρακτικές στην ασφάλεια και αυστηρά μέτρα ασφάλειας που υλοποιούνται από τον πάροχο. Αντιθέτως, ο καθορισμός των μέτρων ασφάλειας είναι πολύπλοκος στον Ομιχλώδη Προγραμματισμό. Ο χρήστης φέρει μεγαλύτερη

ευθύνη για την ασφάλεια, καθώς και η αποκεντρωμένη φύση του ομιχλώδους υπολογισμού δυσχεραίνει την υλοποίηση ομοιόμορφων μέτρων ασφάλειας σε όλα τα επίπεδα. Επιπλέον, όσον αναφορά τον ομιχλώδη υπολογισμό, υπάρχει το ζήτημα πως χρησιμοποιούνται πιο ελαφριά πρωτόκολλα που δεν έχουν σχεδιαστεί ειδικά για την ασφάλεια. (Atlam, Walters and Wills, 2018)

Από τα παραπάνω προκύπτει ότι ο ομιχλώδης προγραμματισμός ανταποκρίνεται καλύτερα στις ανάγκες των χρηστών και μπορεί να προσαρμοστεί στα χαρακτηριστικών των αναδυόμενών υπολογιστικών και επικοινωνιακών μοντέλων σε σχέση με τα παραδοσιακά υπολογιστικά νέφη. Ωστόσο, η υλοποίηση ενός συστήματος ομιχλώδους προγραμματισμού σε μεγάλη κλίμακα φέρνει μαζί τις προκλήσεις όσον αφορά το κόστος, τους πόρους και την ασφάλεια. Τα παραδοσιακά συστήματα του υπολογιστικού νέφους θα συνεχίσουν να παίζουν σημαντικό ρόλο για εργασίες υψηλού επιπέδου. Συνεπώς, ο ομιχλώδης προγραμματισμός και το υπολογιστικό νέφος αναμένεται να συνυπάρχουν και να αλληλοσυμπληρώνονται στο μέλλον, εξυπηρετώντας ένα ευρύ φάσμα αναγκών και απαιτήσεων. Στον Πίνακα 1 φαίνονται συνοπτικά οι διαφορές μεταξύ του υπολογιστικού νέφους και του ομιχλώδους προγραμματισμού. (Firdhous, Ghazali and Hassan, 2014)

Πίνακας 1 - Οι διαφορές μεταξύ του υπολογιστικού νέφους και του ομιχλώδους προγραμματισμού. Πηγή: (Firdhous, Ghazali and Hassan, 2014), (Atlam, Walters and Wills, 2018)

Απαιτήσεις	**Υπολογιστικό νέφος**	**Ομιχλώδης Προγραμματισμός**
Καθυστέρηση	Υψηλή	Χαμηλή
Τοποθεσία των κόμβων διακομιστών	Κεντρικοποιημένη	Στη άκρη ενός τοπικού δικτύου
Απόσταση μεταξύ του πελάτη και του διακομιστή	Μεγάλη	Μικρή
Μέτρα Ασφάλειας	Μπορεί να οριστούν και να εγκαθιδρυθούν	Δύσκολο να οριστούν
Επιθέσεις στα δεδομένα κατά την διάρκεια της μεταφοράς τους μέσα στο δίκτυο	Υψηλή πιθανότητα	Μέτρια πιθανότητα
Επίγνωση τοποθεσίας	Όχι	Ναι
Γεωγραφική κατανομή	Κεντρικοποιημένη	Αποκεντρωμένη
Αριθμός κόμβων διακομιστών	Από λίγοι έως παρά πολλοί (ανάλογα, με την τοποθεσία, την επένδυση και το είδος του νέφους)	Από λίγοι έως παρά πολλοί (ανάλογα με την τοποθεσία και την επένδυση)
Υποστήριξη κινητικότητας	Περιορισμένη	Υποστηρίζεται
Αλληλεπίδραση σε πραγματικό χρόνο	Εν μέρει	Υποστηρίζεται

2.4 Απαιτήσεις ασφάλειας στον ομιχλώδη προγραμματισμό

Η εμπιστευτικότητα (confidentiality) της μετάδοσης και της αποθήκευσης των δεδομένων, η ακεραιότητα (integrity) και η διαθεσιμότητα (availability) των δεδομένων αποτελούν τις τρεις θεμελιώδεις απαιτήσεις ασφάλειας των πληροφοριακών συστημάτων. Επίσης, οι τρεις αυτές θεμελιώδεις απαιτήσεις ασφάλειας αποτελούν βασικές προϋποθέσεις για την ασφάλεια και την λειτουργικότητα των δικτυών νέας γενιάς, τα οποία χαρακτηρίζονται από αυξημένες απαιτήσεις διασύνδεσης και αυτόματης επικοινωνίας, όπως είναι το Διαδίκτυο των Πραγμάτων. Η εμπιστευτικότητα εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες των IoT συσκευών, όπως οι κάτοχοι των δεδομένων ή οι εξουσιοδοτημένοι εκπρόσωποι τους, μπορούν να έχει πρόσβαση σε αυτά. Αυτό ισχύει ακόμη και όταν τα δεδομένα μεταφέρονται σε κόμβους ομίχλης για επεξεργασία ή αποθήκευση. Με αυτόν τον τρόπο, αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση κατά την μετάδοση ή λήψη δεδομένων μεταξύ του τερματικού επιπέδου, του επίπεδου ομίχλης και του επιπέδου νέφους, καθώς και όταν τα δεδομένα αποθηκεύονται στα κέντρα δεδομένων ομίχλης ή νέφους. Μέσω της κρυπτογράφησης, μετατρέποντας τα δεδομένα σε μη αναγνωρίσιμη μορφή, μπορεί να επιτευχθεί η εμπιστευτικότητα. (Alzoubi *et al.*, 2020)

Η ακεραιότητα εγγυάται ότι τα δεδομένα που παρέχονται είναι σωστά χωρίς παραμορφώσεις και αποτρέπει την τροποποίηση ή την παραμόρφωση των αποθηκευμένων δεδομένων από μη εξουσιοδοτημένα μέρη (Alzoubi *et al.*, 2020). Αυτό επιτυγχάνεται μέσω της εφαρμογής μηχανισμών ελέγχου κατά την μεταφορά και την αποθήκευση, οι οποίοι διασφαλίζουν ότι τα δεδομένα παραμένουν ακέραια. Επιπλέον, η χρήση κρυπτογραφικών τεχνικών συμβάλουν στην προστασία της ακεραιότητας, αναγνωρίζοντας ή αποτρέποντας οποιαδήποτε προσπάθεια μη εξουσιοδοτημένης τροποποίησης των δεδομένων (Farhadi *et al.*, 2020).

Η διαθεσιμότητα των δεδομένων διασφαλίζει ότι τα δεδομένα είναι διαθέσιμα οποτεδήποτε και προσπελάσιμα από οπουδήποτε, αλλά παίζει και κρίσιμο ρόλο στην αποτελεσματική λειτουργία των συστημάτων (Alzoubi *et al.*, 2020), (Farhadi *et al.*, 2020). Για παράδειγμα, σε εφαρμογές όπως είναι το βιομηχανικό διαδίκτυο των πραγμάτων, τα δεδομένα που λαμβάνονται από μία IoT συσκευή μπορεί να αξιοποιηθούν για την ανάλυση και την αποστολή εντολών σε άλλες IoT συσκευές σε μια γραμμή παραγωγής του εργοστασίου. Εάν η διαθεσιμότητα των δεδομένων των IoT συσκευών παραβιαστεί, αυτό ενδέχεται να οδηγήσει στην παραβίαση της σωστής λειτουργίας ολοκλήρου του συστήματος παραγωγής (Farhadi *et al.*, 2020).

Για να επιτευχθούν οι παραπάνω απαιτήσεις ασφάλειας στον ομιχλώδη υπολογισμό θα πρέπει να εφαρμοστούν διάφορα μέτρα ή μηχανισμοί (π.χ. έλεγχος ταυτότητας), τεχνικές κρυπτογράφησης, διαδικασίες και στρατηγικές ασφάλειας. Οι συγγραφείς Alzoubi κ.α. (2020) χωρίζουν τις απαιτήσεις ασφάλειας στον ομιχλώδη υπολογισμό σε τρεις κατηγορίες:

- Υπηρεσίες δικτύου και επικοινωνίας σε ομιχλώδη περιβάλλοντα (Fog-based network services and communication)

- Επεξεργασία δεδομένων σε ομιχλώδη περιβάλλοντα (Fog-based data processing)
- Η ιδιωτικότητα των IoT συσκευών σε ομιχλώδη περιβάλλοντα (IoT devices privacy)

2.4.1 Υπηρεσίες δικτύου και επικοινωνίας σε ομιχλώδη περιβάλλοντα

Οι κόμβοι ομίχλης εντοπίζονται σε ή επικοινωνούν με μικρά σε μέγεθος κέντρα δεδομένων, τα οποία έχουν περιορισμένες δυνατότητες αποθήκευσης και υπολογιστικής ισχύς σχέση με ένα υπολογιστικό νέφος. Η κατηγορία «Υπηρεσίες δικτύου και επικοινωνίας σε ομιχλώδη περιβάλλοντα» παρέχει βασικές λειτουργίες δικτύωσης, επικοινωνίας και διαχείρισης. Αυτές οι υπηρεσίες διευκολύνουν την επικοινωνία μεταξύ των συσκευών που ανήκουν τόσο στο υπολογιστικό νέφος όσο και στο Διαδίκτυο των Πραγμάτων, ενώ παράλληλα διασφαλίζουν την ομαλή λειτουργία των κόμβων ομίχλης. (Alzoubi *et al.*, 2020)

Ειδικότερα, ο ομιχλώδης υπολογισμός χρησιμοποιείται ως μεσολαβητής μεταξύ του υπολογιστικού νέφους και των IoT συσκευών, διευκολύνοντας διαφορές λειτουργίες επικοινωνίας, όπως η προώθηση ή δρομολόγηση πακέτων και η συλλογή δεδομένων από τις δύο πλευρές. Ένας κόμβος ομίχλης συλλέγει διάφορα δεδομένα από τις IoT συσκευές και στην συνέχεια είτε τα επεξεργάζεται είτε τα στέλνει στο υπολογιστικό νέφος μετά από μια αρχική προεπεξεργασία (aggregation) ώστε να είναι μικρότερα σε μέγεθος και πιο διαχειρίσιμα. Επίσης, οι κόμβοι ομίχλης διαθέτουν τοπικούς διακομιστές και υπολογιστικούς πόρους επιτρέποντας την επεξεργασία δεδομένων IoT συσκευών σε πραγματικό χρόνο, βοηθώντας στη λήψη αποφάσεων σε εφαρμογές ευαίσθητες στο χρόνο, όπως η υγειονομική περίθαλψη και τα συστήματα φαναριών. (Alzoubi *et al.*, 2020)

Για να καλυφθούν οι απαιτήσεις ασφάλειας των υπηρεσιών δικτύου και επικοινωνίας του ομιχλώδους προγραμματισμού, θα πρέπει να εφαρμοστούν συστήματα για το έλεγχο αυθεντικοποίησης και πρόσβασης, την ανίχνευση κακόβουλου λογισμικού στους κόμβους ομίχλης και την προώθηση πακέτων, να σχεδιαστούν ελαφριά αλλά ασφαλή πρωτόκολλα επικοινωνίας, καθώς και να γίνουν εκμεταλλεύσιμες οι δυνατότητες της εικονικοποίησης και της ανοχής σφαλμάτων. (Alzoubi *et al.*, 2020)

Παρακάτω αναφέρονται οι βασικότερες απαιτήσεις ασφάλειας που τίθενται για τις υπηρεσίες δικτύου και επικοινωνίας σε ομιχλώδη περιβάλλοντα συμφώνα με τους Alzoubi κ.α. (2020):

Αυθεντικοποίηση (Authentication)

Η αυθεντικοποίηση είναι η διαδικασία επιβεβαίωσης της ταυτότητας μιας IoT συσκευής ενός χρήστη του Ομιχλώδους Προγραμματισμού. Ο Ομιχλώδης Προγραμματισμός χρησιμοποιεί την διαδικασία της αυθεντικοποίησης με τέτοιο τρόπο ώστε οι χρήστες να μπορούν να χρησιμοποιούν τις συσκευές τοπικά χωρίς να είναι απαραίτητη η συχνή επικοινωνία με τους διακομιστές του υπολογιστικού νέφους. Η τοπική επαλήθευση της ταυτότητας κάθε IoT συσκευής που συνδέεται στο δίκτυο αποτελεί θεμελιώδης απαίτηση για την ενίσχυση της ασφάλειας σε περιβάλλοντα Ομιχλώδης Προγραμματισμού. Επιπλέον, ένας χρήστης του συστήματος ομιχλώδους

προγραμματισμού θα πρέπει να μπορεί να αυθεντικοποιηθεί με ασφάλεια πριν του επιτραπεί η είσοδος στο σύστημα ή σε δεδομένα. (Alzoubi *et al.*, 2020)

Έλεγχος Πρόσβασης (Access Control)

Ο έλεγχος πρόσβασης χρησιμοποιεί στρατηγικές ελέγχου για την εξασφάλιση της ασφάλειας και του απορρήτου των δεδομένων σε περιβάλλοντα ομιχλώδη προγραμματισμού. Καθορίζει ποιος μπορεί να έχει πρόσβαση στους πόρους ενός ομιχλώδους περιβάλλοντος καθώς και ποιες ενέργειες είναι σε θέση να εκτελέσει, όπως ανάγνωση ή τροποποίηση των δεδομένων. Ένα σύστημα ελέγχου πρόσβασης διασφαλίζει ότι ένας ή περισσότεροι κόμβοι ομίχλης είναι υπεύθυνοι για την εξουσιοδότηση IoT συσκευών. (Alzoubi *et al.*, 2020)

Συνήθως, στα παραδοσιακά κεντρικοποιημένα συστήματα ο έλεγχος πρόσβασης συχνά ορίζεται για έναν ολόκληρο τομέα, επιτρέποντας σε έναν κεντρικό διακομιστή να διαχειρίζεται όλες τις εξουσιοδοτήσεις. Ωστόσο, σε περιβάλλοντα ομιχλώδη προγραμματισμού λόγω της κατανεμημένης φύσης τους, υλοποιείται με κρυπτογραφικές τεχνικές (π.χ. κρυπτογραφημένη επικοινωνία) (Alzoubi *et al.*, 2020). Αυτές οι τεχνικές εξασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητά των δεδομένων, καθώς τα δεδομένα μεταφέρονται μεταξύ των κόμβων ομίχλης, προστατεύοντας τα από μη εξουσιοδοτημένη πρόσβαση και τυχόν αλλοιώσεις. Επομένως, η χρήση της κρυπτογραφίας είναι απαραίτητη για να διατηρηθεί η ασφάλεια σε ένα περιβάλλον όπου δεν υπάρχει ένα κεντρικό σημείο ελέγχου (Aleisa, Abuhussein and Sheldon, 2020).

Η κατανεμημένη φύση των ομιχλωδών περιβαλλόντων ουσιαστικά απαιτεί έναν πιο εκλεπτυσμένο έλεγχο πρόσβασης με σκοπό να ενισχύσει την ασφάλεια και την αποτελεσματικότητα του συστήματος, ενώ παράλληλα περιορίζει την πιθανότητα παρεμβολών και επιθέσεων (Aleisa, Abuhussein and Sheldon, 2020).

Σχεδίαση Ελαφριών Πρωτόκολλων (Light – Weight Protocol Design)

Με την υιοθέτηση ελαφριών πρωτοκόλλων επικοινωνίας οι προγραμματιστές μπορούν να αναπτύξουν εφαρμογές επικοινωνιών, οι οποίες εξασφαλίζουν την αποτελεσματική ανταλλαγή δεδομένων μεταξύ των IoT συσκευών και των κόμβων ομίχλης σε πραγματικό χρόνο. Ωστόσο, η ασφάλεια των ελαφριών πρωτόκολλων επικοινωνίας πρέπει οπωσδήποτέ να λαμβάνεται υπόψη ως απαραίτητη απαίτηση, και όχι απλά ως προαιρετική επιλογή. Κάποια από τα υπάρχοντα πρωτόκολλα, ενδέχεται να παρουσιάζουν ευπάθειες σε κυβερνοεπιθέσεις, θέτοντας σε κίνδυνο την ασφάλεια των δεδομένων και των πόρων του συστήματος. Οι ευπάθειες αυτές μπορεί να προκύπτουν για τους εξής λόγους: (α) από λανθασμένο σχεδιασμό ή / και υλοποίηση των πρωτοκόλλων, που οδηγεί σε κενά ασφάλειας, (β) από την σχεδίαση των πρωτοκόλλων χωρίς να λαμβάνεται επαρκώς υπόψιν η ασφάλεια, με αποτέλεσμα να υπάρχουν ανεπαρκή μέτρα προστασίας για την αντιμετώπιση των απειλών. (Alzoubi *et al.*, 2020)

Η αποτελεσματική αντιμετώπιση αυτών των ζητημάτων απαιτεί προσεκτική προσέγγιση στον σχεδιασμό και την υλοποίηση των πρωτοκόλλων, με έμφαση στην ασφάλεια από την αρχή. Για την

μεγιστοποίηση της απόδοσης του χρόνου που απαιτείται να ταξιδέψουν τα δεδομένα μεταξύ των IoT συσκευών και των κόμβων ομίχλης κρίνεται αναγκαία η σωστή επιλογή του καταλλήλου πρωτοκόλλου επικοινωνίας, το οποίο θα πρέπει να συνδυάζει αποτελεσματικά χαρακτηριστικά απόδοσης και να μπορεί να ενσωματώνει διαφορές πρακτικές ασφάλειας, λαμβάνοντας υπόψη τις ανάγκες της εφαρμογής και τους περιορισμούς της εκάστοτε συσκευής, έτσι ώστε να διασφαλιστεί η ακεραιότητα των δεδομένων και η ασφάλεια του συστήματος. (Alzoubi *et al.*, 2020)

Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDS)

Τα συστήματα ανίχνευσης εισβολών (IDS) μπορούν να προβλέψουν, να ανιχνεύσουν και να προειδοποιούν τον διαχειριστή του συστήματος σε περίπτωση που εντοπιστεί κάτι ύποπτο σε ένα σύστημα του Ομιχλώδους Προγραμματισμού, όπως οι κακόβουλοι ιοί ή οι επιθέσεις τύπου δούρειου ίππου (trojan attacks) (Alzoubi *et al.*, 2020). Ένα κοινό χαρακτηριστικό όλων των IDS είναι ότι δεν μπορούν να παρέχουν απόλυτη ακρίβεια. Ένα IDS μπορεί να εντοπίσει ψευδώς θετικά αποτελέσματα, δηλαδή κατά την διαδικασία της ταυτοποίησης μια κανονική κίνηση του δικτύου να χαρακτηριστεί λανθασμένα ως επιβλαβής. Από την άλλη πλευρά, ενδέχεται μια κακόβουλη δραστηριότητα να θεωρείται λανθασμένα ως σωστή, δηλαδή να χαρακτηρίζεται ως ψευδές αρνητικό αποτέλεσμα (Chang *et al.*, 2022).

Επομένως, εφόσον είναι αδύνατο να εξαλειφθούν όλα τα ψευδώς θετικά και τα ψευδώς αρνητικά αποτελέσματα, το καλύτερο που μπορεί να γίνει είναι να ελαχιστοποιηθούν όσο το δυνατόν περισσότερο (Chang *et al.*, 2022). Επιπλέον, οι προσπάθειες παράκαμψης των μηχανισμών ασφάλειας μπορεί να προέρχονται από εξωτερικούς ή εσωτερικούς χρήστες. Αυτό δημιουργεί την επιτακτική ανάγκη να δημιουργηθούν πιο αποτελεσματικά και αποδοτικά συστήματα ανίχνευσης εισβολών, τα οποία θα πρέπει να εγκατασταθούν στα κατάλληλα σημεία ενός περιβάλλοντος ομιχλώδους προγραμματισμού για την τεκμηρίωση υπαρκτών απειλών, καθώς και την ενίσχυση των παλαιών συστημάτων ασφάλειας (Abbasi and Shah, 2017).

Διαχείριση Εμπιστοσύνης (Trust Management)

Ένα σύστημα διαχείρισης εμπιστοσύνης στο ομιχλώδες περιβάλλον επιδιώκει να εξασφαλίζει ότι όλες οι οντότητες που αλληλοεπιδρούν και ανταλλάσσουν δεδομένα στο περιβάλλον αυτό είναι αξιόπιστες σε βαθμό που ταιριάζει με τις συγκεκριμένες συνθήκες και την κρισιμότητα των δεδομένων που πρέπει να επεξεργαστούν ή να τροποποιηθούν. Η υιοθέτηση διαφορετικών επίπεδων ασφάλειας μεταξύ των κόμβων ομίχλης είναι μια απαραίτητη απαίτηση ασφάλειας για κάθε ομιχλώδης περιβάλλον, αφού συμβάλλει στην διασφάλιση της ασφάλειας και της ακεραιότητας των δεδομένων. Επίσης, τα διαφορετικά επίπεδα ασφάλειας σε ένα ομιχλώδες περιβάλλον μπορεί να προσφέρουν πολλά οφέλη, όπως βελτιωμένη κατανομή των πόρων, καλύτερη κλιμακωσιμότητα και ευελιξία στο σύστημα. Τέλος, σε ένα ομιχλώδες περιβάλλον, η εμπιστοσύνη θα πρέπει να είναι μια αμφίδρομη διαδικασία μεταξύ των κόμβων ομίχλης και των IoT συσκευών, αφού η εμπιστοσύνη διασφαλίζει την ομαλή συνεργασία μεταξύ των κόμβων ομίχλης και των IoT συσκευών για την ανταλλαγή δεδομένων, μειώνοντας ως ένα βαθμό τον κίνδυνο της ανάπτυξης κακόβουλης δραστηριότητας. (Alzoubi *et al.*, 2020)

Οι κόμβοι ομίχλης θα μπορούσαν να επικυρώνονται από το υπολογιστικό νέφος. Ωστόσο αυτό μπορεί να εγείρει ανησυχίες σχετικά με την εμπιστευτικότητα και την ασφάλεια των δεδομένων, καθώς το υπολογιστικό νέφος μπορεί να ανήκει σε τρίτα μέρη. Επομένως, η αντιμετώπιση των κακόβουλων κόμβων συνδέεται άμεσα με την διαχείριση εμπιστοσύνης, η οποία μπορεί να αναδείξει την εσκεμμένη κακόβουλη συμπεριφορά των κόμβων ώστε αυτή να αποκλείεται από το ομιχλώδες δίκτυο. Η καλύτερη δυνατή λύση σε αυτή την περίπτωση είναι η επικύρωση να πραγματοποιείται συνεργατικά και κατανεμημένα από το περιβάλλον ομίχλης, ενισχύοντας έτσι την εμπιστοσύνη και την αξιοπιστία του συστήματος. (Alzoubi *et al.*, 2020)

Αντιμετώπιση κακόβουλων κόμβων ομίχλης (Malicious Fog Nodes Confronting)

Ένας κακόβουλος κόμβος ομίχλης είναι ένας μη νόμιμος κόμβος, ο οποίος προσποιείται πως είναι νόμιμος ώστε να παραπλανήσει τους χρήστες να συνδεθούν σε αυτόν, καθώς και άλλους κόμβους, οι οποίοι θα δοκιμάσουν να συνεργαστούν με αυτό τον κόμβο, με κίνδυνο διαρροής των δεδομένων / πληροφοριών και υπολογισμών. Επίσης, ένας κακόβουλος κόμβος ομίχλης αποτελεί σοβαρή απειλή για όλες τις ιδιότητες/απαιτήσεις ασφάλειας του Ομιχλώδους Προγραμματισμού. Επιπλέον, οι κακόβουλοι κόμβοι ομίχλης λόγω της επιβάρυνσης που μπορεί να προκαλέσουν εσκεμμένα στο δίκτυο μπορεί να οδηγήσουν σε μείωση της απόδοσης της πλατφόρμας του Ομιχλώδους Υπολογισμού. Επιπρόσθετα, μπορούν να δημιουργούν πίσω πόρτες (backdoor) ή να διευκολύνουν εσωτερικές επιθέσεις που έχουν ως σκοπό να βλάψουν τα προσωπικά δεδομένα των τελικών χρηστών του συστήματος. (Alzoubi *et al.*, 2020)

Η διαχείριση της εμπιστοσύνης, όπως αναφέρθηκε προηγουμένως, μπορεί να χρησιμοποιηθεί για τον εντοπισμό των κακόβουλων κόμβων και τον αποκλεισμό τους από το περιβάλλον ομίχλης.

Εικονικοποίηση (Virtualization)

Η συγκέντρωση όλων των εικονικών μηχανών σε ένα κοινό εικονικοποιημένο περιβάλλον, των κόμβων ομίχλης, καθώς και η αποκεντρωμένη φύση του ομιχλώδους προγραμματισμού μπορεί να προκαλέσουν αρνητικές συνέπειες στους χρήστες, τα δεδομένα και τις υπηρεσίες ενός συστήματος ομιχλώδους προγραμματισμού. Για παράδειγμά, μια κακόβουλη εικονική μηχανή μπορεί να πραγματοποιήσει τροποποιήσεις ή να πάρει τον έλεγχο του υποκείμενου υλικού και λογισμικού ενός κόμβου ομίχλης, έχοντας ως σκοπό να εξαπλώσει επιθέσεις στο υπόλοιπο περιβάλλον ομίχλης. Γνωστές επιθέσεις εικονικοποιήσης αποτελούν οι επιθέσεις στον υπερεπόπτη (hypervisor attacks), οι επιθέσεις πλευρικού καναλιού (slide channel attacks) και οι επιθέσεις βασισμένες σε εικονικές μηχανές (VM-based attacks) (Alzoubi *et al.*, 2020).

Μια από τις βασικές απαιτήσεις ασφάλειας της εικονικοποίησης (του ομιχλώδους προγραμματισμού αλλά και της νεφο-υπολογιστικής) είναι η βελτίωση της απομόνωσης των πόρων σε φυσικό και λογικό επίπεδο, έτσι ώστε να αποτραπεί η αλληλεπίδραση μεταξύ των εικονικών μηχανών και η παρεμβολή μιας κακόβουλης εικονικής μηχανής στους πόρους μια άλλης, μειώνοντας έτσι την πιθανότητα εμφάνισης επιθέσεων σε ολόκληρο το σύστημα. Επίσης, είναι απαραίτητη η σκλήρυνση του υπερεπόπτη και των εικονικών μηχανών για την προστασία

ολόκληρου του ομιχλώδους περιβάλλοντος από κακόβουλες επιθέσεις και τη διασφάλιση της ασφάλειας των δεδομένων του συστήματος (Κρητικός, 2023).

Ανοχή Σφαλμάτων (Fault tolerance)

Σε περίπτωση παρουσίασης δυσλειτουργιών σε μεμονωμένους αισθητήρες, δίκτυα, πλατφόρμες υπηρεσιών ή εφαρμογές, τα συστήματα του ομιχλώδους προγραμματισμού οφείλουν να συνεχίσουν κανονικά την λειτουργία τους. Το παραπάνω είναι μια σημαντική απαίτηση ασφάλειας σχετικά με τον ομιχλώδη προγραμματισμό που μπορεί να οδηγήσει σε ομιχλώδη συστήματα με αυξημένη ανθεκτικότητα σε βλάβες, μειώνοντας παράλληλα τον χρόνο διακοπής λειτουργίας του συστήματος και βελτιώνοντας την εμπειρία χρήστη (Alzoubi *et al.*, 2020).

2.4.2 Επεξεργασία δεδομένων σε ομιχλώδη περιβάλλοντα

Η προσωρινή αποθήκευση στον Ομιχλώδη Προγραμματισμό (Transient Storage for Fog) είναι η δυνατότητα των κόμβων ομίχλης να κρατούν προσωρινά τα συλλεχθέντα δεδομένα των IoT συσκευών για ένα μικρό χρονικό διάστημα, συνήθως μία με δύο ώρες. Εκτός από την προσωρινή αποθήκευση των πιο συχνά χρησιμοποιούμενων δεδομένων των χρηστών στους κόμβους ομίχλης, προσφέρεται η δυνατότητα της γρήγορης ενημέρωσης των δεδομένων με ευέλικτο και αποτελεσματικό τρόπο. Επίσης, τα κέντρα δεδομένων του ομιχλώδους προγραμματισμού υποστηρίζουν την λειτουργία της εικονικοποίησης, επιτρέποντας με αυτό τον τρόπο την πιο αποδοτική χρήση των πόρων. Αυτό διασφαλίζει την εξισορρόπηση του φορτίου (load balancing) ώστε όλοι οι κόμβοι να έχουν ένα καλό επίπεδο χρήσης. Με αυτό τον τρόπο, αποφεύγεται η υπερφόρτωση ενός μικρού αριθμού πόρων, που θα μπορούσε να οδηγήσει σε μείωση της απόδοσης ή αύξησης της φθοράς τους, ενώ παράλληλα επιτυγχάνεται η βέλτιστη κατανομή του φορτίου σε όλο το σύστημα. Επιπλέον, οι IoT συσκευές επωφελούνται από την βοήθεια των κόμβων ομίχλης, οι οποίοι αναλαμβάνουν την υλοποίηση εργασιών (επεξεργασίας και φιλτραρίσματος δεδομένων) εκ μέρους του υπολογιστικού νέφους, έτσι ώστε να μεταφορτώνονται λιγότερα δεδομένα στις IoT συσκευές ή στους διακομιστές του υπολογιστικού νέφους. (Alzoubi *et al.*, 2020)

Παρακάτω αναλύονται οι απαιτήσεις ασφάλειας σχετικά με την επεξεργασία δεδομένων σε ομιχλώδη περιβάλλοντα με βάση τους Alzoubi et al (2020):

Η ταυτοποίηση, συλλογή και ακεραιότητα των δεδομένων (Data identification, aggregation, and integrity)

Οι IoT συσκευές έχουν την ικανότητα να συλλέγουν συνεχώς πληροφορίες από ένα IoT περιβάλλον, αλλά δεν είναι σε θέση να αναγνωρίσουν και να διακρίνουν τα σημαντικά από τα ασήμαντα δεδομένα από τον τεράστιο όγκο δεδομένων που παράγονται. Στην συνέχεια τα δεδομένα στέλνονται από τις IoT συσκευές για περαιτέρω επεξεργασία και αποθήκευση στους κόμβους ομίχλης. (Alzoubi *et al.*, 2020)

Ωστόσο, η αποθήκευση των δεδομένων στους κόμβους ομίχλης δημιουργεί ποικίλα προβλήματα. Ένα από τα κυριότερα προβλήματα είναι ότι οι χρήστες χάνουν τον έλεγχο των δεδομένων τους όταν αυτά διατηρούνται στους κόμβους ομίχλης, καθώς ελλοχεύει ο κίνδυνος να τροποποιηθούν ή να χαθούν τα δεδομένα των χρηστών χωρίς την γνώση ή την συγκατάθεση τους. Επίσης, η τροποποίηση των δεδομένων μπορεί να τα κάνει αγνώριστα και έτσι ο χρήστης-ιδιοκτήτης τους να μην μπορεί να ανιχνεύσει πως είναι δικά του. Άρα μπορεί να χαθεί η ιδιοκτησία των δεδομένων. (Alzoubi *et al.*, 2020)

Ακόμη άλλο ένα κρίσιμο ζήτημα είναι η κρυπτογράφηση των δεδομένων πριν την αποστολή τους στους κόμβους ομίχλης, έτσι ώστε τα δεδομένα να παραμένουν προστατευμένα από μη εξουσιοδοτημένη πρόσβαση (Alzoubi *et al.*, 2020).

Τέλος, μετά την τοπική επεξεργασία που υφίστανται τα δεδομένα από τους κόμβους ομίχλης, τα επεξεργασμένα δεδομένα συγχωνεύονται σε μια ενιαία μορφή. Η συγχώνευση των δεδομένων από διαφορετικούς κόμβους εμπεριέχει κινδύνους για την ακεραιότητα των δεδομένων, ιδιαίτερα εφόσον κάποιοι από αυτούς είναι κακόβουλοι. (Alzoubi *et al.*, 2020)

Κατανομή δεδομένων (Data distribution)

Τα δεδομένα πρέπει να κρυπτογραφηθούν πριν αυτά αποσταλούν στους κόμβους ομίχλης για λόγους ασφάλειας και διατήρησης του απόρρητου των χρηστών στον Ομιχλώδη Προγραμματισμό. Ωστόσο, δημιουργούνται προβλήματα σχετικά με το διαμοιρασμό των κρυπτογραφημένων δεδομένων, αφού ο κάτοχος των δεδομένων δεν μπορεί να μοιραστεί τα δεδομένα αυτά εφόσον το επιθυμεί με άλλους νόμιμους χρήστες, οι οποίοι δεν μπορούν να τα αποκρυπτογραφήσουν, εφόσον δεν γνωρίζουν το κλειδί της κρυπτογράφησης, ώστε έπειτα να τα αξιοποιήσουν Βέβαια, υπάρχει περίπτωση στο κλειδί αυτό να μπορεί να διανεμηθεί στους χρήστες αυτούς, αλλά μπορούν να προκληθούν πολλά ζητήματα ασφάλειας. (Alzoubi *et al.*, 2020)

Το πρώτο ζήτημα αφορά την ανάγκη χρήσης κρυπτογράφησης με δημόσιο κλειδί (public-key encryption) για την διασφάλιση υψηλότερου επιπέδου ασφάλειας. Παρά την ισχυρή προστασία που προσφέρει αυτή η μέθοδος, εντούτοις παρουσιάζει υψηλές υπολογιστικές απαιτήσεις και ενδέχεται να επιφέρει σημαντικό φόρτο σε ομιχλώδη περιβάλλοντα, γεγονός που περιορίζει την αποτελεσματικότητα και την αξιοποίηση των δεδομένων σε τέτοιες συνθήκες. (Alzoubi *et al.*, 2020)

Από την άλλη πλευρά, αν χρησιμοποιηθεί συμμετρική κρυπτογράφηση (symmetric-key encryption), το πρόβλημα είναι η ασφαλής διανομή του κλειδιού, γεγονός που σημαίνει ότι όλοι οι χρήστες που έχουν το κλειδί θα έχουν πρόσβαση σε όλα τα δεδομένα και όχι μόνο σε ένα μέρος αυτών, όπως επιθυμεί ο κάτοχος των δεδομένων. (Alzoubi *et al.*, 2020)

Προστασία δεδομένων και αναζήτηση (Data protection and search)

Οι IoT συσκευές δεν διαθέτουν κάποια λειτουργία, η οποία να μπορεί να διακρίνει τα ευαίσθητα δεδομένα των χρηστών πριν αυτά αποσταλούν στους κόμβους ομίχλης. Επομένως, την παραπάνω αρμοδιότητα την αναλάβουν οι κόμβοι ομίχλης, οι οποίοι πρέπει να είναι σε θέση να μπορούν να αναγνωρίσουν ποια είναι τα ευαίσθητα δεδομένα για να τα προστατεύσουν. Ένα σημαντικό ζήτημα αποτελεί η χρήση διαφορετικών λέξεων-κλειδιών για την αναζήτηση των δεδομένων των χρηστών στον ομιχλώδη προγραμματισμό και στο υπολογιστικό νέφος. Αυτό συμβαίνει επειδή τα δεδομένα που έχουν υποστεί επεξεργασία στους κόμβους ομίχλης (ή στις εικονικές μηχανές του νέφους) ενδέχεται να μην εμπεριέχουν τις αρχικές λέξεις-κλειδιά. Επομένως, η αναζήτηση μπορεί να γίνει πιο δύσκολη λόγω της αφαίρεσης ή τροποποίησης των λέξεων-κλειδιών. Συνεπώς, η αναζήτηση των δεδομένων θα πρέπει να γίνει με διαφορετικό τρόπο. (Alzoubi *et al.*, 2020)

Επιπλέον, με βάση το προηγούμενο ζήτημα της κατανομής δεδομένων, τίθεται το πρόβλημα της αναζήτησης σε κρυπτογραφημένα δεδομένα, καθώς πρέπει να βρεθεί μια μέθοδος εντοπισμού των δεδομένων που θα αξιοποιηθούν, χωρίς την ανάγκη αποκρυπτογράφησης όλων των δεδομένων εκ των προτέρων. Προφανώς, η ανάκτηση όλων των δεδομένων με βάση κάποιο διαμοιρασμένο κλειδί δεν είναι η αποδοτική και η κατάλληλη λύση. Συνεπώς, θα πρέπει να υποστηριχθεί η αναζήτηση των δεδομένων όντας σε κρυπτογραφημένη μορφή. Εδώ πρέπει να τονίσουμε πως είναι σημαντικό τα δεδομένα να παραμείνουν κρυπτογραφημένα στους κόμβους ομίχλης, καθώς οι πάροχοι αυτών των κόμβων μπορεί να είναι περίεργοι και να θελήσουν να δουν ή ακόμη να εκμεταλλευτούν τα δεδομένα αυτά. Για αυτό και πρέπει να παραμείνουν σε αυτή τη μορφή, η οποία είναι βολική, διότι δεν χρειάζεται επιπλέον επεξεργασία για την μεταφορά τους στους αιτούντες πρόσβαση σε αυτά. (Alzoubi *et al.*, 2020)

Για να επιτραπεί η αναζήτηση κρυπτογραφημένων δεδομένων οι ιδιοκτήτες τους πρέπει να δημιουργήσουν ένα ευρετήριο ασφάλειας (secure index) κατά την διάρκεια της αποστολής των δεδομένων στους κόμβους ομίχλης. Στην ουσία, το ευρετήριο ασφάλειας μοιάζει με έναν κατάλογο με κρυπτογραφημένες ετικέτες, οι οποίες περιγράφουν τα δεδομένα χωρίς να αποκαλύπτουν το πραγματικό τους περιεχόμενο. Κάθε τέτοια κρυπτογραφημένη ετικέτα «δείχνει» στα δεδομένα που την εμπεριέχουν, επιτρέποντας στους ιδιοκτήτες των δεδομένων να μπορούν να πραγματοποιήσουν αναζήτηση στα δεδομένα τους χωρίς να είναι αναγκαία η αποκρυπτογράφηση τους. (Alzoubi *et al.*, 2020)

Με παρόμοια λογική μπορεί να γίνεται και η πρόσβαση στα δεδομένα από άλλους χρήστες που έχουν δικαίωμα πρόσβασης σε αυτά. Οι χρήστες αυτοί θα μπορούν να χρησιμοποιούν ένα κλειδί για την παραγωγή κρυπτογραφημένης μορφής των λέξεων-κλειδιών που τους ενδιαφέρει κι έπειτα θα πραγματοποιούν τη σχετική αναζήτηση. Μόλις τα απαραίτητα δεδομένα φθάσουν σε αυτούς, τότε θα μπορούν να τα αποκρυπτογραφήσουν (π.χ. με το ίδιο κλειδί εφόσον εφαρμόζεται συμμετρική κρυπτογράφηση).

Προφανώς, το ζήτημα της τροποποίησης των (κρυπτογραφημένων) δεδομένων όταν είναι αποθηκευμένα σε έναν κόμβο ομίχλης αγγίζει και τον προαναφερόμενο τρόπο αναζήτησης, διότι

εφόσον οι λέξεις-κλειδιά δεν ισχύουν πλέον, θα πρέπει να γίνει τροποποίηση του ευρετηρίου ασφάλειας.

Διανομή περιεχομένου (Content Distribution)

Όσον αναφορά την διαδικασία της διανομής περιεχομένου πρέπει να καθοριστεί ένας κανονισμός πλαισίου σχετικά με τον έλεγχο της διανομής του περιεχομένου που έχει ως επίκεντρο την προστασία των προσωπικών δεδομένων των χρηστών. Πιο συγκεκριμένα, θα πρέπει να καθοριστεί ποιος έχει το δικαίωμα να διαμοιράζεται περιεχόμενο και τι τύπος περιεχομένου επιτρέπεται να διαμοιράζεται με βάση συγκεκριμένους κανόνες και μέτρα ασφάλειας. Κατά την διάρκεια εγγραφής νέων χρηστών σε υπηρεσίες διανομής περιεχομένου, το μυστικό κλειδί που χρησιμοποιείται για την διανομή περιεχομένου πρέπει να ανανεώνεται ή να ενημερώνεται ώστε να αποτρέπεται η πρόσβαση τους σε προηγούμενο περιεχόμενο (Alzoubi *et al.*, 2020).

Ανάλυση μεγάλων δεδομένων (Big data analysis)

Η αποκεντρωμένη ανάλυση των μεγάλων δεδομένων κατ' απαίτηση λαμβάνει χωρά στους κόμβους ομίχλης και είναι απαραίτητη για IoT εφαρμογές που απαιτούν άμεση ανταπόκριση, λήψη γρήγορων αποφάσεων και ενεργειών. Η διαδικασία της ανάλυσης των μεγάλων δεδομένων παίζει καθοριστικό ρόλο για την επιτυχία και την αποτελεσματική λειτουργία των εφαρμογών του Ομιχλώδους Προγραμματισμού, αλλά ταυτόχρονα αντιμετωπίζει πολλές δυσκολίες και προκλήσεις. Οι κόμβοι ομίχλης μπορούν να χρησιμοποιηθούν ως προσωρινοί καταλύτες για την προσωρινή αποθήκευση διάφορων δεδομένων από πολλές IoT συσκευές. Εξαιτίας της προσωρινής αποθήκευσης τα ευαίσθητα δεδομένα θα πρέπει να εντοπιστούν πριν την αποστολή τους στους διάφορους κόμβους ομίχλης, ώστε να μειωθεί η πολυπλοκότητα της επεξεργασίας των συλλεχθέντων δεδομένων. (Alzoubi *et al.*, 2020)

Υποβοηθούμενος υπολογισμός (Aided computation)

Οι κόμβοι ομίχλης δύναται να εκτελέσουν πολύπλοκες υπολογιστικές εργασίες (π.χ. ασφαλείς υπολογισμούς με την χρήση ανασφαλών βοηθητικών συσκευών, όπως αισθητήρες, μικροελεγκτές ή κινητές συσκευές) για λογαριασμό των IoT συσκευών, έτσι ώστε να βελτιωθεί η υπολογιστική πολυπλοκότητα των υπολογισμών που εκτελούνται σε αυτές τις IoT συσκευές. Κατά την διαδικασία διάθεσης δεδομένων σε κόμβους ομίχλης για την εκτέλεση συγκεκριμένων εργασιών ενδέχεται να υπάρξει αποκάλυψη ευαίσθητων πληροφοριών, όπως η αποκάλυψη μυστικών κλειδιών του χρήστη. Επομένως, η έλλειψη πλήρους ελέγχου από τους χρήστες στα δεδομένα τους σε ομιχλώδη περιβάλλοντα μπορεί να οδηγήσει σε σημαντικά ζητήματα απορρήτου και ασφάλειας. Άρα, είναι ζωτικής σημασίας να ληφθούν υπόψη αυτά τα ζητήματα κατά το σχεδιασμό και την εφαρμογή λύσεων στα ομιχλώδη περιβάλλοντα έτσι ώστε διασφαλιστεί η προστασία των δεδομένων των χρηστών. (Alzoubi *et al.*, 2020)

Επαληθεύσιμος υπολογισμός (Verifiable computation)

Ο επαληθεύσιμος υπολογισμός[4] ενεργοποιεί την ανάθεση υπολογιστικών πόρων σε κόμβους ομίχλης, ενώ παράλληλα παρέχει μηχανισμό επαλήθευσης για την ορθότητα των υπολογισμών που εκτελούνται στους κόμβους ομίχλης σε αυτούς. Ωστόσο, η επαλήθευση της ακεραιότητας των αποτελεσμάτων που επιστρέφονται από τους κόμβους ομίχλης αποτελεί διαφορετικό ζήτημα από την εγγύηση της ορθότητας της επαλήθευσης. Η ακεραιότητα επικεντρώνεται στη διασφάλιση ότι τα δεδομένα δεν έχουν αλλοιωθεί ή παραποιηθεί κατά την μεταφορά τους. Αντίθετα, η ορθότητα της επαλήθευσης αφορά την ακρίβεια με την οποία αξιολογείται αν ο υπολογισμός εκτελέστηκε σωστά. Επομένως, απαιτείται περαιτέρω ερευνά για την ενσωμάτωση μηχανισμών ελέγχου σφαλμάτων στους αλγορίθμους υπολογισμού που ανατίθενται στους κόμβους ομίχλης (Alzoubi *et al.*, 2020).

Εγκληματολογία (Forensics)

Κάθε επίθεση αφήνει πίσω της ίχνη, τα οποία μπορεί να χρησιμοποιηθούν για την ανάλυση, ώστε να εξαχθούν κρίσιμες πληροφορίες για την κατανόηση της επίθεσης και την ταυτοποίηση των επιτιθεμένων και των μεθόδων τους. Η εγκληματολογία του ομιχλώδους προγραμματισμού σχετίζεται εν μέρει με την εγκληματολογία του υπολογιστικού νέφους. Επομένως, θα μπορούσαν να υιοθετηθούν εγκληματολογικές προσεγγίσεις από το υπολογιστικό νέφος. Με αυτό τον τρόπο, η ανάκτηση αποδεικτικών στοιχείων που σχετίζονται με περιστατικά κακόβουλων επιθέσεων που αφορούν τις υπηρεσίες του ομιχλώδους προγραμματισμού μπορεί να αποτελέσει ένα πολύτιμο εργαλείο για την εξασφάλιση της ομαλής λειτουργίας του περιβάλλοντος του ομιχλώδους προγραμματισμού. (Alzoubi *et al.*, 2020)

Όμως, ένα ομιχλώδες περιβάλλον παρουσιάζει ορισμένες προκλήσεις. Ειδικότερα, οι περιορισμένοι υπολογιστικοί πόροι στους κόμβους ομίχλης σε συνδυασμό με την κατανεμημένη φύση των κόμβων αυτών επηρεάζουν την ικανότητα συλλογής, αποθήκευσης, ανάλυσης και προστασίας των δεδομένων, διότι απαιτείται αρκετός χρόνος και ταχύτητα για την αναζήτηση και την ανάκτηση των πληροφοριών από τους κόμβους ομίχλης, καθιστώντας δύσκολη την εξαγωγή κρίσιμων πληροφοριών από αποδεικτικά στοιχεία. Επομένως, οι προαναφερόμενες προσεγγίσεις πρέπει να ενημερωθούν ώστε να μπορούν να είναι εφαρμόσιμες σε τέτοια περιβάλλοντα. (Alzoubi *et al.*, 2020)

2.4.3 Ιδιωτικότητα των προσωπικών δεδομένων στον ομιχλώδη προγραμματισμό

Μια IoT συσκευή μπορεί να διαμοιράσει το μοναδικό χαρακτηριστικό της, την πληροφορία της τοποθεσίας της συσκευής και διάφορα δεδομένα που έχει συλλέξει με κόμβους ομίχλης, οι οποίοι με την σειρά τους μοιράζονται αυτά τα δεδομένα με άλλους κόμβους ή τα στέλνουν στο

[4] Ο επαληθεύσιμος υπολογισμός δίνει την δυνατότητα σε ένα υπολογιστικό σύστημα να αναθέτει την εκτέλεση μιας συνάρτησης σε άλλους, ενδεχομένως μη αξιόπιστους, εξωτερικούς υπολογιστικούς πόρους, διατηρώντας παράλληλα την δυνατότητα επαλήθευσης της ορθότητας των αποτελεσμάτων. Οι εξωτερικοί αυτοί πόροι εκτελούν τον υπολογισμό της συνάρτησης και επιστρέφουν το αποτέλεσμα συνοδευόμενο από μια απόδειξη που πιστοποιεί ότι ο υπολογισμός εκτελέστηκε σωστά (Wikipedia, 2024).

υπολογιστικό νέφος για επεξεργασία. Επιπλέον, η εξέταση του μοτίβου του τρόπου λειτουργίας μια IoT συσκευής μπορεί να λειτουργήσει σαν "δακτυλικό αποτύπωμα", αποκαλύπτοντας διαφορές πληροφορίες σχετικά με τον χρήστη της IoT συσκευής. Για παράδειγμα, οι έξυπνοι μετρητές μπορεί να χρησιμοποιηθούν για την εξαγωγή συμπερασμάτων για την καθημερινή ρουτίνα που μπορεί να έχει ο ιδιοκτήτης του σπιτιού, παραβιάζοντας έμμεσα την ιδιωτικότητα του. (Alzoubi *et al.*, 2020)

Για να διασφαλιστεί πλήρως η ιδιωτικότητα των προσωπικών δεδομένων των συσκευών (και των χρηστών που τις κατέχουν) του ομιχλώδους προγραμματισμού πρέπει να ληφθούν υπόψη τέσσερις τύποι απαιτήσεων, οι οποίοι αναλύονται παρακάτω (Alzoubi *et al.*, 2020):

Απόρρητο δεδομένων (Data privacy)

Η διασφάλιση της εμπιστευτικότητας των δεδομένων αποτελεί κρίσιμο ζήτημα, αφού τα δεδομένα πρέπει να διατηρούνται απόρρητα ακόμη και από νόμιμους χρήστες, οι οποίοι προσπαθούν να αποκτήσουν πρόσβαση σε δεδομένα πέραν τον αρμοδιοτήτων τους. Επίσης, άλλο ένα σημαντικό ζήτημα είναι η παράνομη πρόσβαση σε βάσεις δεδομένων, η οποία μπορεί να προκαλέσει σοβαρούς κινδύνους (π.χ. απώλεια δεδομένων, παραβίαση δεδομένων, αναπαραγωγή δεδομένων και κοινή χρήση των δεδομένων) στα δεδομένα του συστήματος του ομιχλώδους προγραμματισμού. Επιπλέον, τα ευαίσθητα δεδομένα μπορεί να διαρρεύσουν (από το επίπεδο των βάσεων δεδομένων ή των εφαρμογών) λόγω επιτυχών διαδικτυακών επιθέσεων. Τέτοιες επιθέσεις περιλαμβάνουν, εκχύσεις SQL (SQL injection), cross-site scripting, cross-site request forgery (CSRF ή πλαστογράφηση αιτήματος μεταξύ ιστοτόπων) και πειρατείες συνόδων/λογαριασμών (session/account). (Alzoubi *et al.*, 2020)

Ιδιωτικότητα ταυτότητας (Identity privacy)

Μία βασική πρόκληση αποτελεί η προστασία της ταυτότητας του χρήστη, η οποία πρέπει να εξασφαλίζεται ακόμα και σε περιπτώσεις όπου οι αντίπαλοι (είτε αυτοί είναι χρήστες, κόμβοι ομίχλης, ή πάροχοι υπηρεσιών νέφους) έχουν πρόσβαση στα δεδομένα παρότι μπορεί να είναι ειλικρινείς και να ακολουθούν τους κανόνες του συστήματος, ενδέχεται να είναι περίεργοι στην προσπάθεια τους να αποκαλύψουν την ταυτότητα του χρήστη μέσω της ανάλυσης των δεδομένων που δημιουργούνται κατά την διαδικασία ελέγχου της ταυτοποίησης. Οι φορείς που αναλαμβάνουν την διαδικασία της ταυτοποίησης αναγκαστικά αποκτούν πρόσβαση σε ένα υποσύνολο των προσωπικών δεδομένων που σχετίζονται με την ταυτότητα του χρήστη. Ωστόσο, το ζήτημα δεν είναι το γεγονός ότι ο φορέας γνωρίζει κάποιες πληροφορίες, όσο ο βαθμός στον οποίο μπορεί να αναλύσει και να συνδυάσει τα δεδομένα με άλλες πηγές πληροφοριών για να αποκαλύψει την πλήρη ταυτότητα του χρήστη. Η πρόκληση λοιπόν αφορά την ανάγκη ανάπτυξης μηχανισμών που θα επιτρέπουν την επαλήθευση της ταυτότητας χωρίς να αποκαλύπτουν περισσότερες πληροφορίες από όσες είναι απαραίτητες για την παροχή της εκάστοτε υπηρεσίας. Επίσης, μια σημαντική πρόκληση αποτελεί η συνεργασία των πολλών επιπέδων σε περιβάλλοντα ομίχλης, όπου δημιουργούνται καινούργια ζητήματα ασφάλειας σχετικά με την διαχείριση τόσο της διαδικασίας ταυτοποίησης όσο και των δεδομένων ταυτοποίησης των χρηστών των περιβαλλόντων ομίχλης, αφού οι συσκευές και οι υπηρεσίες αλληλοεπιδρούν σε διαφορετικά επίπεδα ιεραρχίας. (Alzoubi *et al.*, 2020)

Ιδιωτικότητα τοποθεσίας (Location privacy)

Μια βασική πρόκληση αποτελεί η εξασφάλιση του απορρήτου της τοποθεσίας ενός χρήστη σε περιβάλλοντα όπου αν και οι αντίπαλοι ακολουθούν το πρωτόκολλο ασφάλειας του συστήματος έχουν την «περιέργεια» να αποκτήσουν πρόσβαση σε ιδιωτικές πληροφορίες σχετικά με την τοποθεσία του χρήστη. Οι αντίπαλοι μπορεί να είναι άλλοι χρήστες, είτε οι ίδιοι οι κόμβοι ομίχλης, είτε πάροχοι υπηρεσιών νέφους, είτε κυβερνήσεις, είτε ακόμη και εσωτερικοί επιτιθέμενοι που έχουν πρόσβαση στο σύστημα. Επίσης, μια πρόκληση αποτελεί ο μη διαχωρισμός της ταυτότητας της συσκευής του χρήστη από τα στοιχεία της τοποθεσίας του κατά την διάρκεια της μεταφοράς πληροφοριών μέσα στο περιβάλλον ομίχλης. Αυτό έχει ως αποτέλεσμα να υπάρχει ο κίνδυνος να αποκαλυφθούν διαφορές ευαίσθητες πληροφορίες (π.χ. καθημερινές διαδρομές, συχνές τοποθεσίες, επισκέψεις σε συγκεκριμένα καταστήματα ή χώρους, πληροφορίες σχετικά με την προσωπική κατάσταση του χρήστη κ.α.) σχετικά με τον χρήστη κατά την διάρκεια της αποστολής των δεδομένων είτε στους κόμβους ομίχλης είτε στο υπολογιστικό νέφος. Επομένως, θα πρέπει να εξασφαλιστεί ότι αν και παρέχονται προσωποποιημένες υπηρεσίες με βάση την τοποθεσία του χρήστη, αυτές δεν οδηγούν σε ταυτοποίηση του χρήστη ή σε διαρροή ευαίσθητων πληροφοριών, όπως οι καθημερινές διαδρομές. Είναι προφανές επίσης ότι θα πρέπει να γίνεται φιλτράρισμα των πληροφοριών, ώστε να μην διαχέονται ταυτόχρονα η ταυτότητα και η τοποθεσία κατά μήκος του δικτύου ή του περιβάλλοντος. (Alzoubi *et al.*, 2020)

Ιδιωτικότητα χρήσης (Usage privacy)

Μια βασική πρόκληση αποτελεί η διασφάλιση του απορρήτου χρήσης των IoT συσκευών από άτομα ή οντότητες, όπως χάκερ, ερευνητές ασφάλειας, εταιρείες ή ακόμα και άλλες συνδεδεμένες συσκευές, που μπορεί να μην έχουν κακές προθέσεις, αλλά είναι «περίεργα» και επιδιώκουν να αποκτήσουν πρόσβαση σε δεδομένα των IoT συσκευών έχοντας ως σκοπό να εξάγουν ευαίσθητες πληροφορίες. Αυτές οι οντότητες μπορεί να εντοπίζονται είτε στο φυσικό χώρο όπου βρίσκονται οι συσκευές, είτε σε απομακρυσμένες τοποθεσίες, αξιοποιώντας την πρόσβαση μέσω του διαδικτύου. Επίσης, η παρακολούθηση της συχνότητας της αποστολής δεδομένων στους κόμβους ομίχλης είναι ένα κρίσιμο ζήτημα, καθώς ελλοχεύει ο κίνδυνος να αποκαλυφθούν σημαντικές πληροφορίες και μοτίβα χρήσης, σχετικά με το πως συγκεκριμένοι χρήστες αλληλοεπιδρούν με ένα σύστημα, εφαρμογή ή υπηρεσία που βρίσκεται σε ένα περιβάλλον ομίχλης. Για παράδειγμα, η ανάλυση αυτών των δεδομένων θα μπορούσε να αποκαλύψει τις συνήθειες χρήσης ή άλλες λεπτομέρειες που συνδέονται άμεσα με τη συμπεριφορά και τις προτιμήσεις ενός χρήστη, θέτοντας σε κίνδυνο την ιδιωτικότητα του. (Alzoubi *et al.*, 2020)

3 *Μεθοδολογία της διπλωματικής εργασίας*

3.1 Ερευνητικά ερωτήματα

Στην παρούσα διπλωματική εργασία πραγματοποιήθηκε μια συστηματική ανασκόπηση της βιβλιογραφίας έχοντας ως σκοπό την αξιολόγηση των υφιστάμενων τρωτοτήτων και κίνδυνων που υπάρχουν σε περιβάλλοντα Ομιχλώδη Προγραμματισμού αλλά και επιθέσεων που εκμεταλλεύονται αυτές τις τρωτότητες, καθώς και των μεθόδων και των εργαλείων που χρησιμοποιούνται για την αντιμετώπιση των επιθέσεων αυτών. Τα κύρια ερωτήματα που επιδιώκει να απαντήσει η διπλωματική εργασία που εξετάζουμε είναι:

- E1: *Ποιες κατηγορίες επιθέσεων και τρωτοτήτων υπάρχουν στον Ομιχλώδη Προγραμματισμό και ποια είναι τα κύρια χαρακτηριστικά τους;*
- E2: *Ποιες μέθοδοι έχουν προταθεί για τον εντοπισμό, την αποτροπή και την αντίδραση σε επιθέσεις που στοχεύουν σε περιβάλλοντα Ομιχλώδη Προγραμματισμού;*
- E3: *Πως κατηγοριοποιούνται οι μέθοδοι για την αντιμετώπιση των επιθέσεων σε περιβάλλοντα Ομιχλώδη Προγραμματισμού*;
- E4: *Πως συγκρίνονται οι μέθοδοι για την αντιμετώπιση των επιθέσεων σε περιβάλλοντα Ομιχλώδη Προγραμματισμού;*
- E5: *Ποιες προκλήσεις και ανοιχτά ζητήματα υπάρχουν στον τομέα της ασφάλειας των περιβαλλόντων του Ομιχλώδους Προγραμματισμού, αλλά και ποιες ερευνητικές κατευθύνσεις μπορούν να υιοθετηθούν για την αντιμετώπιση αυτών των προκλήσεων;*

3.2 Τρόπος αναζήτησης

Για να επιτευχθεί με επιτυχία η ολοκλήρωση της βιβλιογραφικής ανασκόπησης της διπλωματικής εργασίας χρειάστηκε να ακολουθηθεί μια σειρά από βήματα. Σε πρώτη φάση, αντί για μεμονωμένες αναζητήσεις υιοθετήθηκε ένα μοτίβο επερώτησης που κάλυπτε όλες τις πιθανές περιπτώσεις. Το μοτίβο αυτό περιλάμβανέ τα εξής μέρη:

- *τα χαρακτηριστικά ασφάλειας*: "security | privacy "
- *το αντικείμενο προς ασφάλιση*: "fog && (computing | environment | node | application)"
- *τις ιδιότητες ή όρους ασφάλειας*, όπως "threats | vulnerabilities | weaknesses | risks | attacks | measures | countermeasures | solutions | methods | techniques | prevention | detection | prolepsis | impeding | obstruction | spotting | identification | diagnosis"

Το μοτίβο αυτό εφαρμόστηκε ανάλογα με τις ιδιαιτερότητες τους σε παρά πολλές αξιόπιστες και ευρέως χρησιμοποιούμενες επιστημονικές βάσεις δεδομένων, όπως το Google Scholar, Web of Science, Research Gate, IEEE Xplore για τον εντοπισμό κατάλληλων επιστημονικών άρθρων.

3.3 Φιλτράρισμα εντοπισμένων άρθρων

Κατά την διάρκεια της αναζήτησης εντοπίστηκε μια πληθώρα άρθρων, τόσο από περιοδικά όσο και από πρακτικά συνεδρίων σχετικά με το θέμα που πραγματεύεται η παρούσα διπλωματική εργασία. Στην συνέχεια χρησιμοποιήθηκαν αυστηρά κριτήρια επιλογής ή απόρριψης και ποιότητας για το φιλτράρισμά των άρθρων, τα οποία αναφέρονται παρακάτω:

Κριτήρια αποδοχής

- *Τύπος άρθρου:* Προτιμήθηκαν άρθρα από επιστημονικά περιοδικά, πρακτικά συνεδρίων, κεφάλαια βιβλίων, βιβλία και διδακτορικές διατριβές εξασφαλίζοντας μια πιο ολοκληρωμένη οπτική στο πεδίο του Ομιχλώδους Προγραμματισμού, αλλά και στην ενίσχυση της εγκυρότητας της παρούσας αναφοράς.
- *Έτος δημοσίευσης:* Επιλέχτηκαν άρθρα που δημοσιευτήκαν μετά το 2013, επειδή εκείνη την περίοδο πρωτοεμφανίστηκε ο όρος του ομιχλώδους προγραμματισμού, διασφαλίζοντας έτσι την επικαιρότητα των άρθρων προς ανάλυση.
- *Συνάφεια με το αντικείμενο της ανασκόπησης:* Επιλέχθηκαν επιστημονικά άρθρα που εξετάζουν θέματα ασφάλειας και ιδιωτικότητας στον ομιχλώδη προγραμματισμό.

Κριτήρια απόρριψης

- *Μέγεθος άρθρου:* Απορρίφθηκαν άρθρα μικρής έκτασης (short papers), τα οποία δεν περιείχαν επαρκή ανάλυση και δεδομένα.
- *Γλώσσα δημοσίευσης:* Απορρίφθηκαν άρθρα, τα οποία ήταν γραμμένα σε άλλες γλώσσες εκτός των αγγλικών ή των ελληνικών εξαιτίας της δυσκολίας στην κατανόηση και την αξιολόγηση τους.

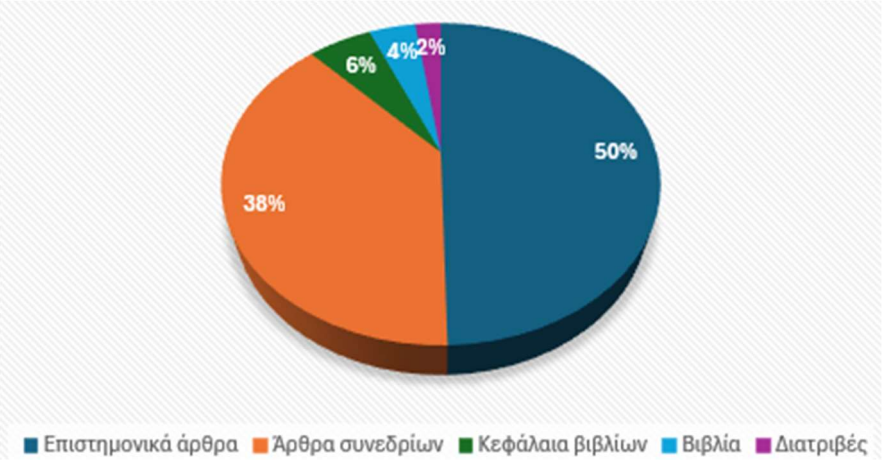
Κριτήρια Ποιότητας

- *Αξιολόγηση συνεισφοράς:* Απορρίφθηκαν άρθρα, τα οποία δεν παρουσίαζαν επουσιώδη ευρήματα και δεν τεκμηρίωναν τα αποτελέσματα τους.
- *Κατανόηση:* Απορρίφθηκαν επιστημονικές πηγές και άρθρα, τα οποία ήταν δυσνόητα ή παρουσίαζαν συντακτικές ή γλωσσικές ατέλειες σε μεγάλο βαθμό.

3.4 Ποσοτική ανάλυση

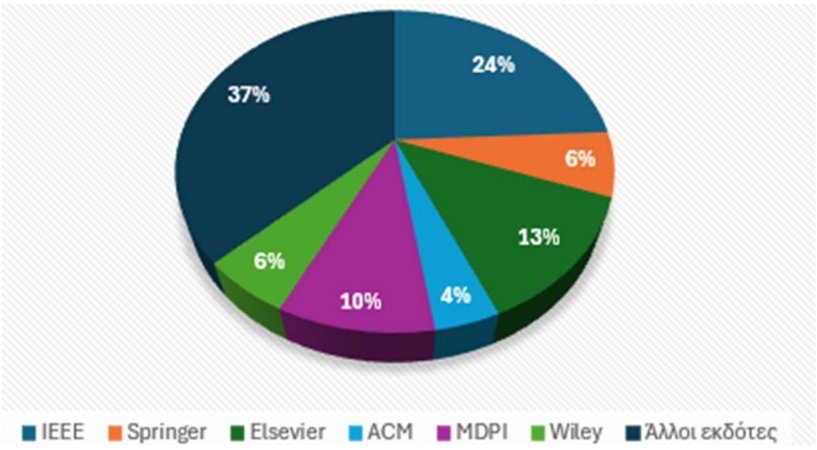
Να σημειώσουμε ότι ο αρχικός αριθμός των άρθρων που εντοπιστήκαν ήταν 434 και μέσω της εφαρμογής του φιλτραρίσματος με την βοήθεια των κριτηρίων επιλεξιμότητας ο αριθμός αυτός μειώθηκε δραματικά στα 145 άρθρα (αυτό αντιστοιχεί σε 33,44 % όποτε έγινε φιλτράρισμα του

66,56 % των άρθρων). Επίσης, 49,60 % των άρθρων ήταν επιστημονικά περιοδικά, το 38,34 % των άρθρων ήταν από συνέδριο, το 5,64 % από κεφάλαια βιβλίων, το 4,14 % ήταν βιβλία και το 2,28 % αφορούσε διπλωματικές διατριβές.



Εικόνα 6 - Γράφημα για την κατανομή των άρθρων ανά είδος

Το 24,19 % των άρθρων έχουν δημοσιευτεί από την IEEE, το 6,45 % των άρθρων είναι δημοσιευμένα από το Springer, το 12,90 % των άρθρων είναι δημοσιευμένα από το Elsevier, το 4,03 % των άρθρων έχουν δημοσιευτεί από ACM, το 9,68 % των άρθρων έχουν δημοσιευτεί από MDPI, το 5,65 % από το Wiley και το 37,10 % από άλλους εκδότες. Η παραπάνω μεθοδολογία που ακολουθήθηκε, βοήθησε στον εντοπισμό σχετικών επιστημονικών άρθρων, θέτοντας τα θεμέλια για μια εμπεριστατωμένη και ολοκληρωμένη βιβλιογραφική ανασκόπηση.



Εικόνα 7 - Γραφική παράσταση με το ποσοστό των άρθρων ανά εκδότη που χρησιμοποιήθηκαν στην διπλωματική εργασία

4 *Τρωτότητες, επιθέσεις & επιπτώσεις επιθέσεων στον ομιχλώδη προγραμματισμό*

4.1 Εισαγωγή

Ο ομιχλώδης προγραμματισμός θεωρείται μια επέκταση του υπολογιστικού νέφους, και ως εκ τούτου είναι αναπόφευκτο ότι ορισμένα ζητήματα ασφάλειας και ιδιωτικότητας που κληρονομηθήκαν από το υπολογιστικό νέφος δεν θα σταματήσουν να υπάρχουν. Επομένως, οι υπάρχουσες λύσεις του υπολογιστικού νέφους ενδεχομένως να μπορούσαν να αντιμετωπίσουν πολλά ζητήματα ασφάλειας του ομιχλώδους προγραμματισμού, αλλά λόγω των ιδιαιτέρων χαρακτηριστικών (π.χ. υποστήριξη κινητικότητας, ετερογένεια) του ομιχλώδους προγραμματισμού γεννιούνται νέες προκλήσεις σχετικά με την ασφάλεια και την ιδιωτικότητα των περιβαλλόντων ομίχλης. Αυτές οι προκλήσεις ενδέχεται να επηρεάσουν την ενσωμάτωση του ομιχλώδους προγραμματισμού σε ένα περιβάλλον IoT. Επομένως, η επίλυση αυτών των θεμάτων είναι απαραίτητη για την προώθηση της ευρείας αποδοχής και χρήσης του ομιχλώδους προγραμματισμού σε IoT εφαρμογές, διασφαλίζοντας ταυτόχρονα την ασφάλεια και την ιδιωτικότητα των χρηστών. (Alrawais *et al.*, 2017)

Με βάση την παραπάνω ανάλυση, ο σκοπός του κεφαλαίου αυτού είναι να αναλύσει όλα αυτά τα ζητήματα ασφάλειας στον ομιχλώδη προγραμματισμό. Η ανάλυση πραγματοποιείται ανά είδος ζητήματος (τρωτότητες, επιθέσεις και επιπτώσεις επιθέσεων) σε ξεχωριστές ενότητες. Το κεφάλαιο κλείνει με την παράθεση πραγματικών επιθέσεων που έχουν πραγματοποιηθεί σε ομιχλώδη περιβάλλοντα.

4.2 Τρωτότητες

Οι τρωτότητες αποτελούν κεντρικό ζήτημα που μπορεί να επηρεάσει την ασφάλεια και την ακεραιότητα των συστημάτων του ομιχλώδους προγραμματισμού. Οι τρωτότητες αποτελούν αδυναμίες που, εάν δεν αντιμετωπιστούν, μπορούν να γίνουν εκμεταλλεύσιμες από επιτιθέμενους για την εκτέλεση κακόβουλων ενεργειών. Στο πλαίσιο του ομιχλώδους προγραμματισμού οι τρωτότητες μπορούν να χωριστούν σε τρεις βασικές κατηγορίες ανάλογα με το επίπεδο που τις επιδεικνύει: στο επίπεδο της συσκευής, στο επίπεδο της επικοινωνίας και στο επίπεδο των υπηρεσιών. Πιο συγκεκριμένα, οι τρωτότητες στο επίπεδο της συσκευής αφορούν τα φυσικά και

λογικά περιουσιακά στοιχεία, όπως είναι η μνήμη, ο κώδικας του λειτουργικού συστήματος και τα δεδομένα. Στο επίπεδο της επικοινωνίας, εξετάζονται οι τρωτότητες που σχετίζονται με την επικοινωνία μεταξύ των κόμβων και του νέφους, ενώ στο επίπεδο υπηρεσιών εξετάζονται οι τρωτότητες που επηρεάζουν την διαθεσιμότητα των υπηρεσιών, καθώς και την προστασία των δεδομένων και της ιδιωτικότητας των χρηστών. (Farhadi *et al.*, 2020)

4.2.1 Τρωτότητες στο επίπεδο της συσκευής

Η ανάλυση των τρωτών σημείων σε επίπεδο συσκευής του ομιχλώδους προγραμματισμού αποσκοπεί στην κατανόηση των αδυναμιών που υπάρχουν σε κάθε μεμονωμένο κόμβο. Αυτές οι αδυναμίες μπορεί να αφορούν τόσο τις φυσικές όσο και τις λογικές ιδιότητες του κόμβου (Farhadi *et al.*, 2020).

4.2.1.1 Τρωτότητες σε φυσικά περιουσιακά στοιχεία

Παρόλο που τα μοντέλα απειλής συχνά υποθέτουν ότι οι επιτιθέμενοι δεν έχουν άμεση φυσική πρόσβαση σε IoT συσκευές, η πραγματικότητα είναι τελείως διαφορετική, ειδικά για περιφερειακά δίκτυα. Η φυσική πρόσβαση παραμένει μια σημαντική ανησυχία, καθώς επιτρέπει στους επιτιθέμενους να στοχεύσουν άμεσα στην μνήμη των συσκευών. Η μνήμη ενός κόμβου θεωρείται ως κύριος στόχος για επιθέσεις, λόγω της φύσης της και των δεδομένων που αποθηκεύει. Οι κυριότερες κατηγορίες απειλών στην μνήμη περιλαμβάνουν την ανάγνωση, την εγγραφή και την αντιγραφή αποθηκευμένων δεδομένων, επιτρέποντας στους επιτιθέμενους να αποκτήσουν πρόσβαση σε ευαίσθητές πληροφορίες, να αλλοιώσουν την λειτουργία της συσκευής ή να δημιουργήσουν αντίγραφα για περαιτέρω ανάλυση. (Farhadi *et al.*, 2020)

Οι τρωτότητες στα φυσικά περιουσιακά στοιχεία δεν περιορίζονται μόνο στην μνήμη των IoT συσκευών. Αντίθετα, υπάρχουν τρωτότητες και σε άλλα είδη υλικού, όπως είναι οι επεξεργαστές και, τα διάφορα φυσικά σημεία πρόσβασης καθώς και στα πλαίσια υλικού (hardware framework) που μπορεί να ενσωματώνονται σε αυτές τις συσκευές. Οι τρωτότητες αυτές μπορεί να οφείλονται σε κατασκευαστικές ή σχεδιαστικές ατέλειες. (Farhadi *et al.*, 2020)

Παρακάτω αναλύουμε μια σειρά από τέτοιες τρωτότητες.

Τρωτότητες σε επίπεδο τσιπ (Chip-Level Vulnerabilities)

Οι τρωτότητες σε επίπεδο τσιπ συνδέονται συχνά με αδυναμίες που ενδέχεται να υπάρχουν στους επεξεργαστές ή στα chipsets (σύνολο από τσιπς που συνδέονται με τον επεξεργαστή). Οι τρωτότητες αυτές δεν περιορίζονται μόνο στις παραδοσιακές υπολογιστικές συσκευές, όπως είναι οι υπολογιστές και οι φορητοί υπολογιστές, αλλά ισχύουν και για τους κόμβους ομίχλης. Το φάντασμα (Spectre) και η κατάρρευση (Meltdown) είναι δύο κλασικά παραδείγματα τρωτοτήτων στο επιπέδο τσιπ (Mishra and Yadav, 2020). Το φάντασμα εκμεταλλεύεται την λειτουργία «εκτέλεση υπό συνθήκη (speculative execution)» των επεξεργαστών, δηλαδή μιας τεχνικής για την βελτίωση των επιδόσεων των επεξεργαστών, επιτρέποντας σε έναν κακόβουλό χρήστη να παρακάμψει τους μηχανισμούς ασφάλειας έτσι ώστε να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα από άλλα προγράμματα (Wikipedia, 2024). Η τεχνική αυτή επιτρέπει στους επεξεργαστές

να προβλέπουν και να εκτελούν οδηγίες πρόωρα για να βελτιώσουν την απόδοση του συστήματος. Αλλά η τεχνική αυτή μπορεί να γίνει εκμεταλλεύσιμη κυρίως μέσω επιθέσεων πλευρικού καναλιού (side-channel attacks) και ειδικότερα επιθέσεων χρονισμού κρυφής μνήμης (cache timing attacks) για να εξαχθεί κρίσιμη πληροφορία (όπως κρυπτογραφικά κλειδιά) από διεργασίες, εφαρμογές ή τον πυρήνα του λειτουργικό συστήματος (ΛΣ).

Η κατάρρευση, από την άλλη πλευρά, επιτρέπει την άμεση, μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα σε περιορισμένες περιοχές της μνήμης του συστήματος παραβιάζοντας την απομόνωση μεταξύ των διάφορων εφαρμογών και του συστήματος (Graz University of Technology, 2018). Η εκμετάλλευση της ευπάθειας πραγματοποιείται μέσω δημιουργίας συνθήκης ανταγωνισμού μεταξύ της πρόσβασης στη μνήμη και του ελέγχου προνομίων / δικαιωμάτων ενώ η εξαγωγή των ευαίσθητων δεδομένων γίνεται μέσω επιθέσεων πλευρικού καναλιού.

Και οι δύο προαναφερόμενες τρωτότητες εκμεταλλεύονται σχεδιαστικά προβλήματα της αρχιτεκτονικής της CPU, ειδικότερα τον μηχανισμό «εκτέλεσης υπό συνθήκη», τα οποία οποίες επιτρέπουν την πρόσβαση σε δεδομένα που υπό κανονικές συνθήκες θα έπρεπε να είναι προστατευμένα (Mishra and Yadav, 2020). Η μόνη διάφορα τους έγκειται στο γεγονός πως η κατάρρευση σπάει την απομόνωση μεταξύ εφαρμογών και του πυρήνα ενώ το φάντασμα σπάει την απομόνωση μεταξύ διαφορετικών εφαρμογών ή διεργασιών.

Τρωτότητες στο firmware

Οι ευπάθειες του firmware (υλικολογισμικού) είναι ένα κρίσιμο ζήτημα για την ασφάλεια των κόμβων ομίχλης, καθώς το firmware αποτελεί ένα λογισμικό χαμηλού επιπέδου που εξασφαλίζει τη σωστή λειτουργία των κόμβων ομίχλης. Συχνά οι αδυναμίες στο υλικό των συσκευών (π.χ. IoT συσκευές) επηρεάζουν και το firmware, το οποίο με τη σειρά του μπορεί να μην έχει σχεδιαστεί, υλοποιηθεί ή ασφαλιστεί σωστά. Οι αδυναμίες στο firmware συνηθώς προκύπτουν από ελλείψεις κατά την φάση του σχεδιασμού, όπως η έμφαση στην απόδοση αντί στην ασφάλεια, από την ανεπαρκή δοκιμή, την εξάρτηση από legacy κώδικα με τρωτά σημεία και την υψηλή πολυπλοκότητα της λειτουργικότητας σε συσκευές με περιορισμένους πόρους, γεγονός που οδηγεί σε προγραμματιστικά λάθη. Επίσης, οι διαδικασίες ενημέρωσης του firmware μπορεί να είναι περιορισμένες, μη αυτοματοποιημένες και ανασφαλείς, ενώ από αυτές τις διαδικασίες μπορεί να λείπουν βασικά χαρακτηριστικά ασφάλειας, όπως ο έλεγχος πρόσβασης, ή αυθεντικοποίηση, η υποστήριξη ψηφιακής υπογραφής ή η αποθήκευση του firmware σε κρυπτογραφημένη μορφή. (Katbi, Hammad and Ksantini, 2023)

Παραδείγματος χάριν, πολλές IoT συσκευές μπορεί να λειτουργούν ξεπερασμένο (outdated) ή μη ασφαλές firmware που δεν έχει διορθωθεί (unpatched) ως προς τα ζητήματα ασφάλειας που έχουν εντοπιστεί σε αυτό. Αδυναμίες έχουν επίσης εντοπιστεί στο UEFI (Untified Extensible Firmware Interface), σε bootloaders, σε BMCs (Baseboard Management Controllers) και σε υλικολογισμικό περιφερειακών συσκευών, όπως προσαρμογείς δικτύου και ελεγκτές αποθήκευσης. Συνεπώς, το πρόβλημα μετατίθεται δυνητικά και σε κόμβους ομίχλης. (Katbi, Hammad and Ksantini, 2023)

Οι παραπάνω αδυναμίες καθιστούν ευάλωτο το υλικολογισμικό σε επιθέσεις (π.χ. DoS, Mirai botnet), καθώς οι εισβολείς μπορούν να εκμεταλλευτούν τα κενά ασφάλειας για να εισάγουν κακόβουλο κώδικά ή να παρακάμψουν τα συστήματα ασφάλειας. Οι επιθέσεις αυτές μπορούν να οδηγήσουν σε σοβαρές συνέπειες, όπως είναι η απώλεια των δεδομένων, η διακοπή των λειτουργιών του συστήματος του ομιχλώδους προγραμματισμού ή την παραβίαση της ιδιωτικότητας των χρηστών. (Katbi, Hammad and Ksantini, 2023)

Τρωτότητα διαρροής ηλεκτρικού φορτιού στην δυναμική μνήμη τυχαίας προσπέλασης (Dynamic Random Access Memory – DRAM)

Η τρωτότητα διαρροής ηλεκτρικού φορτιού αναφέρεται στην απώλεια του αποθηκευμένου ηλεκτρικού φορτίου στους πυκνωτές των κελιών DRAM, η οποία συμβαίνει με την πάροδο του χρόνου και μπορεί να οδηγήσει σε απώλεια δεδομένων. Αυτή η τρωτότητα εξαρτάται από τον χρόνο διατήρησης κάθε κελιού, δηλαδή την περίοδο κατά την οποία το κελί μπορεί να διατηρήσει τα δεδομένα χωρίς να απαιτείται ανανέωση (refresh). Η τρωτότητα διαρροής ηλεκτρικού φορτιού στην DRAM επηρεάζεται από φαινόμενα, όπως είναι η εξάρτηση από το μοτίβο των δεδομένων (data pattern dependence), όπου η διατήρηση του ηλεκτρικού φορτιού ενός κελιού επηρεάζεται από τα δεδομένα που είναι αποθηκευμένα σε γειτονικά κελιά. Επιπλέον, η μεταβλητότητα του χρόνου διατήρησης καθιστά δύσκολη την πρόβλεψη της συμπεριφοράς των κελιών, καθώς ο χρόνος διατήρησης μπορεί να μεταβάλλεται απρόβλεπτα με την πάροδο του χρόνου, περιπλέκοντας την εκτίμηση των απαιτήσεων και αυξάνοντας την πιθανότητα απώλειας. Οι επιτιθέμενοι εκμεταλλεύονται αυτή την τρωτότητα και μπορεί να την χρησιμοποιήσουν για να εκτελέσουν επιθέσεις, όπως είναι η επίθεση σφυρί (rowhammer attack). (Liu *et al.*, 2013)

Τρωτότητες στην διαταραχή μνήμης μέσω ηλεκτρομαγνητικών εκπομπών (Disturbing memory by electromagnetic emissions)

Αυτή η τρωτότητα αφορά την ευπάθεια της μνήμης των συσκευών σε διαταραχές που προκύπτουν από ηλεκτρομαγνητικές εκπομπές και απαιτείται φυσική πρόσβαση για να συμβεί. Η ύπαρξή της υποδηλώνει ότι οι συσκευές μπορεί να είναι επιρρεπείς σε αλλοιώσεις των δεδομένων ή στην απώλεια δεδομένων λόγω φυσικών παρεμβολών, καθιστώντας αναγκαία την θωράκιση τους από τέτοιες εκπομπές. (Farhadi *et al.*, 2020)

4.2.1.2 Τρωτότητες σε λογικά περιουσιακά στοιχεία

Τα κύρια λογικά περιουσιακά στοιχεία είναι ο κώδικας και τα δεδομένα. Ο κώδικας μπορεί να ανήκει στο λειτουργικό σύστημα (OS), στον ενορχηστρωτή δοχείων (container orchestrator, όπως το Docker) ή στο δοχείο (container). Κάθε ένας από τους αναφερόμενους τύπους κώδικα έχει και διαχειρίζεται τα αντίστοιχα δεδομένα του. Στην περίπτωση που υποστηρίζεται η εικονικοποίηση των κόμβων, είναι πιθανό να υπάρχει ένας υπερεπόπτης (hypervisor), ο οποίος μπορεί να ενέχει κινδύνους για τρωτότητες, τόσο στον ίδιο τον υπερεπόπτη όσο και στις εικονικές μηχανές που αυτός διαχειρίζεται. Οι τρωτότητες στα λογικά περιουσιακά στοιχεία αφορούν τρεις ιδιότητες: την

ακεραιότητα, την διαθεσιμότητα και την εμπιστευτικότητα. Παρακάτω αναφέρονται οι τρωτότητες που εμφανίζονται σε αυτά τα στοιχεία (Farhadi *et al.*, 2020):

Πρόσβαση στη μνήμη μέσω των θυρών του κόμβου ομίχλης (access to the memory using the Fog node's ports)

Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις θύρες επικοινωνίας του κόμβου ομίχλης, οι οποίες λειτουργούν σε επίπεδο συστήματος, για να αποκτήσουν πρόσβαση στη μνήμη του. Αυτή η τρωτότητα οφείλεται είτε στην έλλειψη ελέγχου πρόσβασης, είτε στην εκτέλεση ανασφαλών υπηρεσιών στις θύρες επικοινωνίας. Η πρόσβαση στη μνήμη του κόμβου ομίχλης επιτρέπει στους επιτιθέμενους να διαβάσουν, να τροποποιήσουν ή ακόμα και να δημιουργήσουν αντίγραφα της μνήμης. Αυτό μπορεί να οδηγήσει σε πιο σοβαρές επιθέσεις, όπως η δημιουργία ψεύτικων κόμβων ομίχλης. (Farhadi *et al.*, 2020)

Τρωτότητες στις συσχετίσεις δεδομένων (data correlations vulnerabilities)

Στα περιβάλλοντα ομίχλης όπου υπάρχει ανταλλαγή μεγάλου όγκου δεδομένων, η σωστή διαχείριση των συσχετίσεων μεταξύ των ευαίσθητών δεδομένων και μη δεδομένων είναι ζωτικής σημασίας. Αν δεν υπάρχει μια τέτοια διαχείριση, τότε είναι δυνατή η αποκάλυψη ευαίσθητων δεδομένων ή ακόμα και η ταυτότητα των χρηστών μέσω σχετικών επιθέσεων. (Zhang, 2019)

Τρωτότητες στα APIs και στις διεπαφές

Τα APIs και οι διεπαφές χρησιμοποιούνται για την επικοινωνία μεταξύ των κόμβων ομίχλης με άλλες συσκευές ή εφαρμογές του ομιχλώδους προγραμματισμού. Οι διεπαφές και τα APIs μεταξύ των συστημάτων είναι ευάλωτα σε τρωτότητες (σχεδίασης, προγραμματιστικές) αν δεν ελέγχονται σωστά. Οι πιο σημαντικές τρωτότητες είναι ο ανεπαρκής έλεγχος αυθεντικοποίησης, η ανεπαρκής επικύρωση εισόδου και η ασθενής κρυπτογράφηση. Οι επιτιθέμενοι μπορούν να τις εκμεταλλευτούν για να εισάγουν κακόβουλο κώδικα έτσι ώστε να αποκτήσουν πρόσβαση σε δεδομένα ή υπηρεσίες. (Farhadi *et al.*, 2020)

Έλλειψη εκλεπτυσμένου ελέγχου πρόσβασης

Η έλλειψη εκλεπτυσμένου ελέγχου πρόσβασης (fine-grained access control) στον ομιχλώδη προγραμματισμό μπορεί να οδηγήσει σε σοβαρά ζητήματα ασφάλειας. Αυτή η έλλειψη σημαίνει ότι το σύστημα δεν εφαρμόζει λεπτομερείς κανόνες για το ποιος μπορεί να έχει να δικαιώματα πρόσβασης σε συγκεκριμένους πόρους ή λειτουργίες του συστήματος του ομιχλώδους προγραμματισμού. Η ανάγκη για εκλεπτυσμένο έλεγχο πρόσβασης προκύπτει από το γεγονός ότι ο ομιχλώδης προγραμματισμός αποτελείται από πολλούς διασκορπισμένους κόμβους ομίχλης, οι οποίοι διαχειρίζονται πολλά δεδομένα και αλληλοεπιδρούν με εφαρμογές που βρίσκονται κοντά στους τελικούς χρήστες. Τα παραδοσιακά συστήματα ελέγχου πρόσβασης, όπως το RBAC, δεν επαρκούν σε ομιχλώδη περιβάλλοντα, καθώς δεν λαμβάνουν υπόψιν μεταβαλλόμενες συνθήκες, όπως η τοποθεσία ή η συσκευή του χρήστη, οι οποίες είναι κρίσιμες για την ασφάλεια του συστήματος. Έτσι, για να διασφαλιστεί η ασφάλεια, είναι απαραίτητο να εξετάζονται επιπλέον περιβαλλοντικά στοιχεία και ιδιότητες των χρηστών, όπως για παράδειγμα η ανάγκη περιορισμού

πρόσβασης του χρήστη όταν αυτός συνδέεται από μια μη ασφαλή συσκευή ή ένα επικίνδυνο δίκτυο. Αν δεν υπάρχει σωστή διαχείριση και έλεγχος του για το ποιος μπορεί να έχει δικαίωμα πρόσβασης στο σύστημα του ομιχλώδους προγραμματισμού, τότε μη εξουσιοδοτημένοι χρήστες μπορούν να αποκτήσουν πρόσβαση σε ευαίσθητές πληροφορίες ή να αλληλοπιδράσουν με κρίσιμες λειτουργίες του συστήματος. (Popoola *et al.*, 2024)

Ειδικές τρωτότητες εφαρμογών (Application Specific Vulnerabilities)

Οι τρωτότητες που δημιουργούνται κατά την ανάπτυξη μιας εφαρμογής ή εν γένει ενός λογισμικού μπορούν να αξιοποιηθούν από επιτιθέμενους σε μεταγενέστερο χρόνο. Η ανάπτυξη λογισμικού που δεν πληροί τα πρότυπα ασφάλειας ή δεν ακολουθεί τις βέλτιστες πρακτικές μπορεί να δημιουργήσει σημεία αδυναμίας, μέσω των οποίων οι επιτιθέμενοι έχουν την δυνατότητα να διεισδύσουν στο σύστημα και να εκμεταλλευτούν τις αδυναμίες του λογισμικού αυτού. (Puthal *et al.*, 2019)

Τρωτότητες ακεραιότητας στον κώδικα του λογισμικού (Vulnerabilities to software code integrity)

Τρωτότητες μπορεί να υπάρχουν σε διάφορα είδη λογισμικού που χρησιμοποιούνται στον ομιχλώδη προγραμματισμό, όπως το λειτουργικό σύστημα, τους ενορχηστρωτές και τα δοχεία. Η ανεπίσημη ή μη εξουσιοδοτημένη έκδοση (δηλαδή μια έκδοση που δεν εκδίδεται από τον επίσημο οργανισμό άλλα από τρίτα μέρη που ενδέχεται να μην είναι εμπιστευτικά) του λειτουργικού συστήματος ή η εγκατάσταση εφαρμογών και ενορχηστρωτών από αναξιόπιστες πηγές μπορεί να θέσει σε κίνδυνο την ακεραιότητα του κώδικα του λειτουργικού συστήματος. Αυτή η κατάσταση είναι κρίσιμη, γιατί μπορεί να οδηγήσει σε αναξιόπιστα συστήματα και πιθανές επιθέσεις. Παρόμοια προβλήματα μπορούν να προκληθούν από την χρήση κακόβουλων ενημερώσεων. (Farhadi *et al.*, 2020)

Εάν ο κώδικας του ενορχηστρωτή παραβιαστεί, μπορεί να θέσει σε κίνδυνο ολόκληρο το σύστημα διαχείρισης των δοχείων. Ειδικότερα, ο επιτιθέμενος μπορεί να εκτελέσει μη εξουσιοδοτημένες ενέργειες, όπως η διαγραφή των δεδομένων ή η εκτέλεση κακόβουλου κώδικα. Επίσης, ο ενορχηστρωτής ενδέχεται να σταματήσει να λειτουργεί σωστά, προκαλώντας την διακοπή υπηρεσιών που διαχειρίζεται. Επιπλέον, ο επιτιθέμενος μπορεί να συλλέξει ευαίσθητες πληροφορίες από το σύστημα του ομιχλώδους προγραμματισμού. (Farhadi *et al.*, 2020)

Τα παραπάνω μπορεί να συμβούν λόγω της χρήσης ανεπίσημων ή παλαιών εκδόσεων του ενορχηστρωτή. Όμως, ενδέχεται να συμβούν και για διάφορους λόγους, όπως είναι η εκτέλεση ανασφαλών ή κακόβουλων δοχείων, που μπορεί να επηρεάσει την ακεραιότητα του συστήματος. Επίσης, η χρήση ανασφαλών πρόσθετων (plugins) στον ενορχηστρωτή μπορεί να χρησιμοποιηθεί σε παραβιάσεις ασφάλειας. (Farhadi *et al.*, 2020)

Ένα άλλο ζήτημα είναι η εκτέλεση των δοχείων με ριζικά (root) δικαιώματα, καθώς ένα κακόβουλο ή παραβιασμένο δοχείο με τέτοια δικαιώματα μπορεί να αποκτήσει πρόσβαση σε κρίσιμα αρχεία ή πόρους του συστήματος, επηρεάζοντας την ακεραιότητα του κώδικα του ενορχηστρωτή αλλά και όλου του συστήματος. Επιπλέον, η μη ασφαλής πρόσβαση στο API του ενορχηστρωτή (π.χ.

Docker), χωρίς την κατάλληλη αυθεντικοποίηση και εξουσιοδότηση, μπορεί να επιτρέψει σε επιθεωρητές να πραγματοποιήσουν μη εξουσιοδοτημένες ενέργειες. Τέλος, το volume mapping / mounting, όπου διαμοιράζονται αρχεία του συστήματος με τα δοχεία, αποτελεί σημαντική τρωτότητα, καθώς ένα κακόβουλο ή παραβιασμένο δοχείο μπορεί να θέσει σε κίνδυνο την ακεραιότητα των δεδομένων και του κώδικα του Docker. (Farhadi *et al.*, 2020)

Ο κώδικας των δοχείων περιλαμβάνει διεπαφές (interfaces) και APIs που ενδεχομένως να είναι προσβάσιμα εκτός του κόμβου ομίχλης, οπότε μπορεί να αποτελέσει στόχο απομακρυσμένων επιθέσεων, ιδιαιτέρα σε περιβάλλοντα που υποστηρίζουν την πολλαπλή μίσθωση (multi-tenancy). Οι επιτιθέμενοι μπορεί να εκμεταλλευτούν αδυναμίες σε αυτά τα APIs για να αποκτήσουν πρόσβαση στα δοχεία, να τροποποιήσουν τον κώδικα τους ή να εκτελέσουν κακόβουλο κώδικα. Συνεπώς, υπάρχει κίνδυνος όχι μόνο για την ακεραιότητα του κώδικα του δοχείου, άλλα και για την μετατροπή του δοχείου σε κακόβουλο, το οποίο ενδεχομένως να χρησιμοποιηθεί ως μέσο και για άλλες επιθέσεις. Ειδικότερα, υπάρχουν περιπτώσεις όπου η μη επαρκής απομόνωση των δοχείων ή η εκτέλεση ενός (κακόβουλου) δοχείου με διαχειριστικά δικαιώματα μπορεί να επηρεάσουν την ακεραιότητα του κώδικα ενός δοχείου στόχου αλλά και του ίδιου του συστήματος (φιλοξενίας). Επομένως, οι τρωτότητες ακεραιότητας στον κώδικα του δοχείου δεν εξαρτάται μόνο από τον ίδιο τον κώδικα του, αλλά και από το περιβάλλον στο οποίο εκτελείται και από τις αλληλεπιδράσεις του με άλλα συστήματα (Farhadi *et al.*, 2020)

Τρωτότητες εμπιστευτικότητας στον κώδικα των δοχείων (Vulnerabilities to container code confidentiality)

Η προστασία του κώδικα των δοχείων είναι ζωτικής σημασίας για την ασφάλεια των συστημάτων του ομιχλώδους προγραμματισμού έτσι ώστε να αποφευκτούν οι τρωτότητες εμπιστευτικότητας στον κώδικα του δοχείου. Εάν οι επιτιθέμενοι αποκτήσουν πρόσβαση σε αυτόν τον κώδικα, μπορούν να τον αντιγράψουν, να τον τροποποιήσουν προς επίτευξη δικών τους σκοπών ή να σχεδιάζουν πιο αποτελεσματικά μια επίθεση που εκμεταλλεύεται τις τρωτότητες του κώδικα αυτού, θέτοντας σε κίνδυνο την ασφάλεια ολοκλήρου του συστήματος (Farhadi *et al.*, 2020). Μια από τις πιο γνωστές τρωτότητες σχετίζεται με την διαρροή του πηγαίου κώδικα μέσα στις εικόνες των δοχείων. Αυτό συμβαίνει όταν δεν χρησιμοποιούνται τεχνικές όπως είναι τα πολλαπλά στάδια κατασκευής (multi-stage builds), κατά την δημιουργία των εικόνων. Σε αυτή την περίπτωση, ο πηγαίος κώδικας παραμένει μέσα στην εικόνα και αν η εικόνα είναι δημόσια διαθέσιμη, τότε οποιοσδήποτε μπορεί να αποκτήσει πρόσβαση σε αυτήν. Βέβαια, ακόμα, και όταν χρησιμοποιούνται πολλαπλά στάδια κατασκευής, υπάρχει ο κίνδυνος να εξαχθεί ο πηγαίος κώδικας μέσω τεχνικών ανάστροφης μηχανικής (reverse engineering). Επιπλέον, ακόμη και αν οι εικόνες των δοχείων είναι ιδιωτικές υπάρχουν παρά πολύ κίνδυνοι, όπως είναι το κλέψιμο ή το μάντεμα των διαπιστευτηρίων (αν δεν χρησιμοποιούνται ισχυροί κωδικοί ή ασφαλή κανάλια επικοινωνίας ή πρωτόκολλα κατά την αυθεντικοποίηση) από κάποιον κακόβουλο χρήστη για την πρόσβαση στο αποθετήριο όπου αποθηκεύονται οι εικόνες. Μια επιπλέον τρωτότητα αφορά τη χρήση μη ασφαλών καναλιών κατά την μεταφορά των εικόνων (π.χ. από ένα αποθετήριο εικόνων σε έναν κόμβο ομίχλης) έτσι ώστε το περιεχόμενο των εικόνων (και άρα των ενδεχομένων και ο πηγαίος κώδικάς των δοχείων) να γίνει ορατό από ενδιάμεσους επιτιθέμενους. (Brady *et al.*, 2020).

Αδύναμα δικαιώματα πρόσβασης σε αρχεία του συστήματος (weak file system permissions)

Τα αδύναμα δικαιώματα πρόσβασης σε αρχεία του συστήματος μπορούν να δημιουργήσουν σοβαρά κενά ασφάλειας στο λειτουργικό σύστημα, σε μια εικονική μηχανή ή ένα δοχείο. Όταν τα δικαιώματα πρόσβασης σε κρίσιμα αρχεία του συστήματος δεν είναι σωστά καθορισμένα τότε μη εξουσιοδοτημένοι χρήστες μπορεί να αποκτήσουν πρόσβαση σε αυτά τα αρχεία, τα οποία κανονικά θα έπρεπε να προστατεύονται. Αυτό μπορεί να επιτρέψει την ανάγνωση, την τροποποίηση ή ακόμη και την διαγραφή σημαντικών δεδομένων ή αρχείων που σχετίζονται με την λειτουργία του συστήματος. Τέτοιες παραβιάσεις μπορούν να διαταράξουν την σωστή λειτουργία του συστήματος, θέτοντας σε κίνδυνο την ακεραιότητα του συστήματος, καθώς οι αλλαγές στα βασικά αρχεία του συστήματος μπορεί να οδηγήσουν σε δυσλειτουργίες, αστάθεια ή ακόμη και την πλήρη κατάρρευση του συστήματος. (Juggernaut Pentesting Blog, 2024)

Τρωτότητες στα δεδομένα (Data vulnerabilities)

Η ακεραιότητα των δεδομένων του λειτουργικού συστήματος (τα οποία βρίσκονται σε αρχεία και στην κύρια μνήμη) σε έναν κόμβο ομίχλης δεν πρέπει να εξαρτάται μόνο από το σύνολο των καθορισμένων κανόνων πρόσβασης (έλεγχος πρόσβασης αρχείων & φακέλων) (οπότε το ζήτημα εδώ είναι να έχουμε σωστούς κανόνες πρόσβασης), αλλά και από την κατάλληλη απομόνωση των πόρων μνήμης και τη χρήση σχετικών μηχανισμών προστασίας, έτσι ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση στην στοίβα και σε αλλά κρίσιμα σημεία της μνήμης. Τα δεδομένα του λειτουργικού συστήματος περιλαμβάνουν ένα ευρύ φάσμα πολύτιμων πληροφοριών, όπως είναι οι διευθύνσεις επιστροφής στη στοίβα, ο δείκτης στοίβας και οι δείκτες των πλαισίων στην στοίβα, τα οποία αποτελούν μόνο παραδείγματα δεδομένων που ανήκουν στο τμήμα της στοίβας του λειτουργικού συστήματος. Δεν είναι εύκολο να καθοριστεί πόσα ακριβώς δεδομένα του λειτουργικού συστήματος θα πρέπει να προστατευθούν. (Farhadi *et al.*, 2020)

Εάν το λειτουργικό σύστημα δεν είναι ενημερωμένο, τότε είναι πιο ευάλωτο σε τρωτότητες εμπιστευτικότητας των δεδομένων του λειτουργικού συστήματος και άρα στη διεξαγωγή σχετικών επιθέσεων. Επίσης, αν δεν υπάρχει κατάλληλος έλεγχος πρόσβασης είναι πιο εύκολο να γίνει διαρροή εμπιστευτικών δεδομένων από μη εξουσιοδοτημένους χρήστες. Η μη κρυπτογράφηση τέτοιων δεδομένων είναι ακόμη ένα ζήτημα, το οποίο επηρεάζει την εμπιστευτικότητα. Ειδικότερα, ακόμη και αν υπάρχει κατάλληλος έλεγχος πρόσβασης, σε περίπτωση διείσδυσης σε ένα σύστημα και απόκτησης διαχειριστικής πρόσβασης, τα εμπιστευτικά δεδομένα θα διαρρεύσουν. Συνεπώς, αν δεν είναι κρυπτογραφημένα, τότε η διαρροή θα είναι επιτυχής, διότι το περιεχόμενο των δεδομένων θα είναι άμεσα ορατό. Τα εμπιστευτικά δεδομένα μπορεί να είναι ευαίσθητα / προσωπικά δεδομένα χρηστών καθώς και κλειδιά του λειτουργικού συστήματος (OS keys). (Farhadi *et al.*, 2020)

Υπάρχουν δύο κατηγόριες κλειδιών λειτουργικού συστήματος: τα κλειδιά προϊόντος / ενεργοποίησης (product / activation keys) και τα κλειδιά αυθεντικοποίησης ή διαπιστευτήρια (authentication keys /credentials). Τα κλειδιά προϊόντος / ενεργοποίησης χρησιμοποιούνται για την ενεργοποίηση ενός λειτουργικού συστήματος. Σε περίπτωση διαρροής των κλειδιών προϊόντος /

ενεργοποίησης, το μόνο που μπορεί να κάνει ένας επιτιθέμενος είναι να χρησιμοποιήσει αυτό το κλειδί για να ενεργοποιήσει παράνομα ένα λειτουργικό σύστημα. Τα κλειδιά αυθεντικοποίησης ή διαπιστευτήρια μπορεί να σχετίζονται με την πρόσβαση σε υποσυστήματα, εφαρμογές ή υπηρεσίες. Για παράδειγμα, εάν κάποιος ξεχάσει τα διαπιστευτήρια του σε μια εικόνα εικονική μηχανή ή σε ένα δοχείο (container) και αυτά δεν είναι κρυπτογραφημένα, τότε ένας επιτιθέμενος μπορεί να τα δει και να τα χρησιμοποιήσει για την διείσδυση σε ένα σύστημα ή υπηρεσία στο σύστημα έτσι ώστε να το / την εκμεταλλευτεί. (Farhadi *et al.*, 2020)

Οι τρωτότητες ακεραιότητας στα δεδομένα του ενορχηστρωτή είναι πανομοιότυπες με τις τρωτότητες δεδομένων του λειτουργικού συστήματος, αλλά αφορούν μονάχα τον ενορχηστρωτή. Αν αυτά τα δεδομένα αλλοιωθούν μπορεί να προκύψουν σοβαρά προβλήματα στο σύστημα του ομιχλώδους προγραμματισμού. Ειδικότερα, ο ενορχηστρωτής μπορεί να λάβει λανθασμένες αποφάσεις σχετικά με την διαχείριση των πόρων, οδηγώντας σε απώλεια χρόνου ή χρημάτων, αλλά και σε ζητήματα διαθεσιμότητας και απόδοσης των υπηρεσιών και των εφαρμογών που εκτελούνται στους πόρους που διαχειρίζεται. Η αλλοίωση των δεδομένων μπορεί να προκαλέσει αστάθεια στο σύστημα, με αποτέλεσμα να υπάρχουν διακοπές λειτουργίας του συστήματος, ή ακόμα και να οδηγήσει και στην απώλεια των δεδομένων. Επιπλέον, εάν τα δεδομένα του ενορχηστρωτή περιέχουν ευαίσθητες πληροφορίες, η αλλοίωση τους μπορεί να οδηγήσει σε παραβιάσεις ασφάλειας και ιδιωτικότητας. Τέλος, ισχύουν και ορισμένες τρωτότητες που αναφέρθηκαν στις τρωτότητες ακεραιότητας στον κώδικα του λογισμικού, όπως για παράδειγμα οι ανεπίσημες εκδόσεις του ενορχηστρωτή. (Farhadi *et al.*, 2020)

Σε περιβάλλοντα που υποστηρίζουν την πολλαπλή μίσθωση οι χρήστες συχνά μοιράζονται τον ίδιο κόμβο ομίχλης, γεγονός που δημιουργεί διάφορες τρωτότητες ακεραιότητας στα δεδομένα του δοχείου. Πρώτα από όλα, μια σημαντική τρωτότητα είναι οι περιοχές αποθήκευσης, οι οποίες είναι εύκολα προσβάσιμες και μπορεί να συνδεθούν με κρίσιμους φακέλους των δοχείων, επιτρέποντας έτσι σε οποιοδήποτε χρήστη να έχει μη εξουσιοδοτημένη πρόσβαση στα δοχεία αυτά. Επίσης, οι τρωτότητες των APIs και των διεπαφών (που προσφέρονται μέσω των δοχείων) μπορεί να εκθέσουν τα δεδομένα σε μη εξουσιοδοτημένους χρήστες, επιτρέποντας την διαρροή τους ή την μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, εάν τα δοχεία λειτουργούν με διαχειριστικά ή προνομιούχα δικαιώματα ή δεν υπάρχει κατάλληλη απομόνωση μεταξύ τους, τότε αυτό μπορεί να δώσει την δυνατότητα σε ένα δοχείο να έχει πρόσβαση σε ένα άλλο δοχείο χωρίς την απαραίτητη εξουσιοδότηση. Όλα τα παραπάνω, δεν οδηγούν μόνο σε μη εξουσιοδοτημένη πρόσβαση σε δεδομένα που μπορεί να είναι ευαίσθητα, αλλά μπορεί να οδηγούν και σε επηρεασμό της ακεραιότητας τους ή ακόμη και στην απώλεια τους. Επιπλέον, η έκθεση δοχείων μπορεί να οδηγήσει σε ζητήματα ακεραιότητας δεδομένων και στο ίδιο το σύστημα (φιλοξενίας, όπως είναι ένας κόμβος ομίχλης). (Farhadi *et al.*, 2020)

Τρωτότητες στην εφοδιαστική αλυσίδα (supply chain vulnerabilities)

Η εφοδιαστική αλυσίδα ενός λογισμικού, είτε αφορά το λειτουργικό σύστημα, είτε τον ενορχηστρωτή δοχείων, είτε τα δοχεία, μπορεί να παρουσιάζει τρωτότητες αν δεν υπάρχουν αυστηροί μηχανισμοί ελέγχου για την γνησιότητα των ενημερώσεων του λογισμικού ή του

firmware. Τέτοιες τρωτότητες επιτρέπουν στους επιτιθέμενους να εισάγουν κακόβουλο λογισμικό μέσω τροποποιημένων ή μη εγκεκριμένων ενημερώσεων, παραβιάζοντας με αυτό τον τρόπο την ακεραιότητα όχι μόνο του λειτουργικού συστήματος, αλλά και των άλλων κρίσιμων στοιχείων της υποδομής, όπως ο ενορχηστρωτής δοχείων ή τα δοχεία. (Rupanetti and Kaabouch, 2024)

4.2.2 Τρωτότητες στο επίπεδο επικοινωνίας

Μια πλατφόρμα ομιχλώδους προγραμματισμού μπορεί να θεωρηθεί ως ένα «δικτυωμένο σύστημα», όπου πολλαπλοί κόμβοι ομίχλης αλληλοεπιδρούν μεταξύ τους ή με το επίπεδο του νέφους. Από αυτή την οπτική γωνία, τα περιουσιακά στοιχεία μπορούν να χωριστούν σε δύο κύριες κατηγορίες: επικοινωνία από ομίχλη σε ομίχλη (Fog-to-Fog communication) και την επικοινωνία από την ομίχλη στο νέφος (Fog-to-Cloud communication). Το κανάλι επικοινωνίας είτε μεταξύ των ίδιων των κόμβων ομίχλης είτε μεταξύ ενός κόμβου ομίχλης και το επίπεδο του νέφους, θεωρείται ως περιουσιακό στοιχείο. Επίσης, μια IP διεύθυνση ενός κόμβου ομίχλης θεωρείται και αυτή ως περιουσιακό στοιχείο, αφού χρησιμοποιείται ως μέσο αναγνώρισης, ταυτοποίησης και πρόσβασης στα συστήματα του ομιχλώδους προγραμματισμού. Η ακεραιότητα και η αυθεντικότητα των διευθύνσεων IP των κόμβων ομίχλης είναι δύο ιδιότητες αυτού του περιουσιακού στοιχειού. Παρακάτω στις δύο υποενότητες της παρούσας ενότητας αναλύονται οι τρωτότητες που υπάρχουν στο επίπεδο επικοινωνίας του ομιχλώδους προγραμματισμού, οι οποίες χωρίζονται με βάση το είδος του περιουσιακού στοιχείου που αφορούν σε: (α) τρωτότητες στο κανάλι επικοινωνίας και (β) τρωτότητες στη διεύθυνση οντοτήτων. (Farhadi *et al.*, 2020)

4.2.2.1 Τρωτότητες στο κανάλι / μέσο επικοινωνίας

Από την μια μεριά, η επικοινωνία από ομίχλη σε ομίχλη περιλαμβάνει όλη την εσωτερική επικοινωνία μεταξύ των κόμβων ομίχλης. Σε εφαρμογές όπου οι IoT συσκευές είναι κινητές, ο ενορχηστρωτής μπορεί να χρειαστεί να μεταφέρει τον κώδικα και τα δεδομένα της εφαρμογής από έναν κόμβο ομίχλης σε έναν άλλο κόμβο ομίχλης, έτσι ώστε να διατηρηθεί η εγγύτητα μεταξύ της εκάστοτε IoT συσκευής και του κόμβου ομίχλης που την εξυπηρετεί. Από την άλλη πλευρά, ο ομιχλώδης προγραμματισμός μπορεί να θεωρηθεί ως επέκταση του υπολογιστικού νέφους, το οποίο ενσωματώνει επιπροσθέτους πόρους που βρίσκονται πλησιέστερα στις IoT συσκευές και τους τελικούς χρήστες. Αυτό σημαίνει ότι πρέπει να υπάρχει επικοινωνία μεταξύ του επιπέδου ομίχλης και του επιπέδου νέφους, γνώστη ως επικοινωνία από Ομίχλη σε Νέφος (Fog-to-Cloud communication), η οποία είναι απαραίτητη για την σωστή λειτουργία και τον συγχρονισμό των δεδομένων και των υπηρεσιών που παρέχονται από το επίπεδο του νέφους και το επίπεδο της ομίχλης. (Farhadi *et al.*, 2020)

Δεδομένου ότι τα δεδομένα μεταφέρονται μεταξύ των στοιχείων μέσω του καναλιού επικοινωνίας, υπάρχει ο κίνδυνος αλλοιώσεων των δεδομένων, υποκλοπής ή ακόμη και απώλειας των δεδομένων κατά την μεταφορά τους στο κανάλι. Επομένως, το κανάλι επικοινωνίας πρέπει να διασφαλίζει την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των δεδομένων. Η ακεραιότητα των δεδομένων απαιτεί ότι τα δεδομένα που λαμβάνονται στον κόμβο προορισμού πρέπει να είναι

ακριβώς τα ίδια με αυτά που εστάλησαν από τον κόμβο πηγής, καθώς οποιαδήποτε παραβίαση της ακεραιότητας θα μπορούσε να επηρεάσει της διαδικασίες υπολογισμού ή λήψης αποφάσεων. Η εμπιστευτικότητα διασφαλίζει ότι τα δεδομένα είναι προσβάσιμα μόνο από την πηγή και τον νόμιμο αποδέκτη, κάτι που είναι ιδιαίτερα σημαντικό όταν τα δεδομένα περιέχουν ευαίσθητες πληροφορίες, όπως για παράδειγμα σε έναν απομακρυσμένο σύστημα υγειονομικής περίθαλψης, όπου η πρόσβαση πρέπει να περιορίζεται μόνο στον γενικό ιατρό του χρήστη. Τέλος, η διαθεσιμότητα εξασφαλίζει ότι τα δεδομένα είναι πάντα διαθέσιμα στον νόμιμο αποδέκτη τους, κάτι που είναι κρίσιμο για βιομηχανικές εφαρμογές ενός εργοστασίου, όπου τα δεδομένα πρέπει να είναι διαθέσιμα συνεχώς και άμεσα στους νόμιμους χρήστες ή το σύστημα έτσι ώστε να εξασφαλίζεται η ομαλή και η αποδοτική λειτουργία του εργοστασίου. (Farhadi *et al.*, 2020)

Οι τρωτότητες που σχετίζονται με το κανάλι επικοινωνίας μπορεί να περιλαμβάνουν (Farhadi *et al.*, 2020):

Έλλειψη μηχανισμών ασφάλειας στο κανάλι επικοινωνίας

Αναφέρεται στην ικανότητα να διασφαλίζεται ότι τα μηνύματα που μεταφέρονται μεταξύ των κόμβων ομίχλης δεν έχουν τροποποιηθεί κατά την διάρκεια της μεταφοράς τους, είτε σκόπιμα είτε ακούσια. Χωρίς επαρκείς μηχανισμούς ασφάλειας που να διασφαλίζουν την ακεραιότητα των μηνυμάτων κατά την μεταφορά, κακόβουλες οντότητες μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση με σκοπό να αλλάξουν το περιεχόμενο των μηνυμάτων. Αυτή η τρωτότητα μπορεί να οδηγήσει σε επιθέσεις τροποποίησης (των μηνυμάτων) (*modification attack*) (Cagalj, *et al.*, 2006).

Όταν τα μηνύματα δεν κρυπτογραφούνται κατά την διάρκεια της αποστολής τους, επιτρέπεται σε κακόβουλους χρήστες να παρακολουθούν την επικοινωνία και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες. Αυτή η τρωτότητα μπορεί να οδηγήσει σε επιθέσεις υποκλοπής (eavesdropping). (Al Harbi, Halabi, and Bellaiche, 2020)

Χρήση μη ισχυρής κρυπτογράφησης

Ακόμα και αν υπάρχει κρυπτογράφηση, η χρήση αδύναμων αλγορίθμων ή αδύναμων κλειδιών κρυπτογράφησης μπορεί να διευκολύνει τους επιτιθέμενους να αποκωδικοποιήσουν τα μηνύματα και να υποκλέψουν δεδομένα. Αυτή η τρωτότητα μπορεί να οδηγήσει σε επιθέσεις υποκλοπής. (Al Harbi, Halabi, and Bellaiche, 2020)

Μη κατάλληλα πρωτόκολλα

Χρησιμοποιούμενα πρωτόκολλα (επικοινωνίας) που δεν έχουν σχεδιαστεί με γνώμονα την ασφάλεια ή έχουν σχεδιαστικά προβλήματα ή έχουν υλοποιηθεί εσφαλμένα ή ατελώς οδηγούν επίσης σε προβλήματα όπως τα προαναφερόμενα (π.χ. η υποκλοπή ή τροποποίηση των δεδομένων). Να σημειωθεί εδώ πως σε περιβάλλοντα ομίχλης όπου υπάρχουν περιορισμοί πόρων, η έμφαση στη σχεδίαση πρωτοκόλλων κατά το παρελθόν γινόταν με γνώμονα την απόδοση και την κατανάλωση ενέργειας και όχι την ασφάλεια. Συνεπώς, η τρωτότητα αυτή μπορεί να θεωρηθεί σχεδόν αναπόφευκτη σε τέτοια περιβάλλοντα. (Riggs *et al.*, 2023)

Ένα τρανταχτό παράδειγμα σχεδιαστικών ατελειών σε πρωτόκολλα επικοινωνίας αφορά το πρωτόκολλο TCP και ειδικότερα τον τρόπο διαχείρισης που αυτό πραγματοποιεί σε ημιτελείς συνδέσεις SYN. Ένας επιτιθέμενος στέλνει έναν μεγάλο αριθμό SYN πακέτων χωρίς να έχει ολοκληρώσει την σύνδεση, δηλαδή χωρίς να στέλνει το τελικό ACK και έτσι το σύστημα διατηρεί συνεχώς πόρους για αυτές τις ημιτελείς συνδέσεις, με αποτέλεσμα να εξαντλούνται οι διαθέσιμοι πόροι του. Ως αποτέλεσμα, η διαθεσιμότητα του συστήματος να ελαχιστοποιείται και δεν μπορεί να ικανοποιήσει αιτήματα νόμιμων χρηστών. Συνεπώς, αυτή η αδυναμία της διαχείρισης των SYN αιτήσεων μπορεί να αποτελέσει την βάση για την πραγματοποίηση επιθέσεων, όπως είναι η επίθεση τύπου άρνησης υπηρεσίας (Denial of Service - DoS), όπως είναι η επίθεση πλημμυρίσματος πακέτων SYN (SYN flooding). (De Vivo *et al.*, 1999)

Επιπλέον, ένα ακόμη σημαντικό (σχεδιαστικό) ζήτημα αφορά το πρωτόκολλο NTP, το οποίο επιτρέπει την διενέργεια πολλαπλών επερωτήσεων που οδηγούν σε μεγάλες απαντήσεις. Με βάση αυτή την «ατέλεια» είναι δυνατόν να γίνει επίθεση ενίσχυσης (amplification attack), άλλο ένα είδος επίθεσης DoS. (De Vivo *et al.*, 1999)

Αδυναμίες του λειτουργικού συστήματος

Ορισμένα λειτουργικά συστήματα μπορεί να μην έχουν σχεδιαστεί για να αντιμετωπίζουν αποδοτικά «δύσμορφα πακέτα» ή κακόβουλα πακέτα. Η ανικανότητα του λειτουργικού συστήματος να διαχειριστεί τα κακόβουλα πακέτα μπορεί να προκαλέσει επιβράδυνση ή ακόμα και κατάρρευση των υπηρεσιών του συστήματος του ομιχλώδους προγραμματισμού. Αυτή η τρωτότητα μπορεί να οδηγήσει σε επιθέσεις (D)DoS. (Farhadi *et al.*, 2020).

Τρωτότητες στα πρωτόκολλα δρομολόγησης

Οι τρωτότητες των πρωτοκόλλων δρομολόγησης αποτελούν σοβαρό κίνδυνο για την ασφάλεια των δικτύων του ομιχλώδους προγραμματισμού, καθώς ενδέχεται να προκύπτουν από λάθη σχεδίασης ή υλοποίησης ή από σχεδίαση που δεν λαμβάνει επαρκώς υπόψη την ασφάλεια. Η έλλειψη αυθεντικοποίησης και εξουσιοδότησης μεταξύ των κόμβων μπορεί να επιτρέψει σε επιτιθέμενούς να εισάγουν ψευδή δεδομένα δρομολόγησης. Επίσης, η μη χρήση κρυπτογράφησης κατά την ανανέωση των δρομολογήσεων αυξάνει τον κίνδυνο υποκλοπής ή αλλοίωσης των δεδομένων. Επιπλέον, η έλλειψη προκαθορισμένων ρυθμίσεων ασφάλειας μπορεί να επιτρέψει στους επιτιθέμενους να χειραγωγήσουν την διαδρομή των δεδομένων παρακάμπτοντας τους μηχανισμούς ασφάλειας. Αυτό μπορεί να οδηγήσει σε υποκλοπή ή αλλοίωσης των δεδομένων ή ακόμα και σε πλήρη διακοπή της επικοινωνίας, με αποτέλεσμα την αποτροπή πρόσβασης σε κρίσιμές υπηρεσίες. (Katal and Sethi, 2022)

Τρωτότητες στον τρόπο λειτουργίας των φυσικών καναλιών

Οι φυσικοί τρόποι επικοινωνίας (π.χ. ραδιοκύματα, οπτικές ίνες) μπορεί να αποκαλύψουν (ευαίσθητες) πληροφορίες απλά με την παρατήρηση τους. Αυτό σημαίνει ότι ένας εισβολέας μπορεί να «ακούσει» τι συμβαίνει στο δίκτυο χωρίς να έχει άμεση πρόσβαση σε αυτό. Στην συνέχεια, αυτές οι εξαγόμενες πληροφορίες από τους επιτιθέμενους μπορούν να αναλυθούν για να αποκαλύψουν

ευαίσθητα δεδομένα ή πρότυπα λειτουργίας. Ένα χαρακτηριστικό παράδειγμα είναι η υποκλοπή οπτικών ινών (fiber tapping) όπου ένας επιτιθέμενος μπορεί να συνδέσει μια συσκευή παρακολούθησης στις ίνες χωρίς να διακόψει τη ροή των δεδομένων, αποκτώντας πρόσβαση σε ευαίσθητες πληροφορίες. (Katal and Sethi, 2022)

Τρωτότητες στα πρωτοκόλλα κρυπτογράφησης

Οι τρωτότητες στα πρωτόκολλα κρυπτογράφησης προκύπτουν από λανθασμένες εφαρμογές ή εφαρμογές στους κανόνες και τις διαδικασίες που καθορίζουν τη χρήση κρυπτογραφικών αλγορίθμων και τη διαχείριση ασφαλούς επικοινωνίας. Αυτές οι αδυναμίες μπορεί να επιτρέψουν σε μη εξουσιοδοτημένα άτομα να αποκρυπτογραφήσουν τα δεδομένα και να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες. (Riggs *et al.*, 2023)

Τρωτότητες ανεπαρκούς απομόνωσης του μέσου επικοινωνίας

Η έλλειψη επαρκούς απομόνωσης του μέσου επικοινωνίας αποτελεί μια σημαντική πύλη εισόδου για τους επιτιθέμενους Μέσω της παρεμβολής στις επικοινωνίες, οι επιτιθέμενοι μπορούν να αλλοιώσουν τα δεδομένα, να υποκλέψουν δεδομένα και να οδηγήσουν σε επιθέσεις έκχυσης κακόβουλου λογισμικού. (Alzoubi *et al.*, 2020)

4.2.2.2 Τρωτότητες στην διεύθυνση οντοτήτων

Χρήση μη ισχυρών μεθόδων αυθεντικοποίησης

Η τρωτότητας της χρήσης μη ισχυρών μεθόδων αυθεντικοποίησης των κόμβων ομίχλης αναφέρεται στην αδυναμία επαλήθευσης με ισχυρό και κατάλληλο τρόπο των ταυτοτήτων των κόμβων ομίχλης. Αυτή η κατάσταση μπορεί να οδηγήσει σε κινδύνους για την αξιοπιστία και την ασφάλεια της επικοινωνίας, όπως είναι η διαρροή ευαίσθητων δεδομένων, η υποκλοπή δεδομένων και η δρομολόγηση των δεδομένων σε ψεύτικους κόμβους. Επίσης, η τρωτότητα αυτή μπορεί να οδηγήσει σε επιθέσεις, όπως είναι η επίθεση των ψεύτικων διευθύνσεων. (Farhadi et al., 2020)

Τρωτότητες που σχετίζονται με δυναμικές διευθύνσεις

Οι δυναμικές διευθύνσεις μπορεί να γίνουν εκμεταλλεύσιμες από επιτιθέμενους, επιτρέποντάς τους να παρακολουθούν ή να παραβιάζουν την επικοινωνία μέσω τεχνικών, όπως η υποκλοπή ή η πειρατεία της ροής δεδομένων (Κρητικός, 2023).

Απουσία ελέγχου στις αιτήσεις απόκτησης διευθύνσεων

Χωρίς επαρκή έλεγχο στις αιτήσεις για απόκτηση διευθύνσεων, μπορούμε να οδηγηθούμε σε υπερφόρτωση του διαθέσιμου χώρου διευθύνσεων, με αποτέλεσμα την εξάντληση των διαθέσιμων διευθύνσεων και την αδυναμία παροχής νέων για συσκευές στο δίκτυο (Κρητικός, 2023).

Χρήση στατικών διευθύνσεων

Η χρήση στατικών διευθύνσεων καθιστά το δίκτυο πιο ευάλωτο σε επιθέσεις, καθώς αυτές οι διευθύνσεις είναι εύκολα ανιχνεύσιμες και ενδέχεται να γίνουν στόχοι για επιτιθέμενους που επιθυμούν να εκμεταλλευτούν την αναγνωσιμότητα τους (Κρητικός, 2023).

4.2.3 Τρωτότητες στο επίπεδο υπηρεσιών

Ο ομιχλώδης προγραμματισμός προορίζεται να παρέχει υπηρεσίες στους χρήστες του, οπότε οι κρίσιμες ιδιότητες που διασφαλίζουν την αξιόπιστη παροχή αυτών των υπηρεσιών πρέπει να αναγνωριστούν ως βασικά περιουσιακά στοιχεία για την διασφάλιση της αδιάλειπτης και της αξιόπιστης λειτουργίας αυτών των υπηρεσιών. Από αυτή την προοπτική του επιπέδου υπηρεσίας, η ασφάλεια των υπηρεσιών, η προστασία της ιδιωτικότητας των χρηστών και η ασφάλεια των ιδιωτικών / ευαίσθητων δεδομένων τους αποτελούν τους πρωταρχικούς περιουσιακούς στόχους που πρέπει οπωσδήποτε να εξασφαλιστούν. (Farhadi *et al.*, 2020)

Η διαθεσιμότητα της υπηρεσίας αναφέρεται στην ικανότητα ενός συστήματος να παρέχει τις υπηρεσίες του συνεχώς και χωρίς διακοπές. Στο πλαίσιο του ομιχλώδους προγραμματισμού, όπου οι υπηρεσίες παρέχονται μέσω μιας κατανεμημένης υποδομής, η διαθεσιμότητα αποτελεί κρίσιμο παράγοντα. Ο ομιχλώδης προγραμματισμός παρέχει υπηρεσίες σε IoT συσκευές και στο υπολογιστικό νέφος. Ορισμένες από τις εφαρμογές που βασίζονται σε αυτές τις υπηρεσίες, όπως οι εφαρμογές παρακολούθησης της υγείας, είναι ιδιαίτερα ευαίσθητές σε διακοπές ή διαταραχές της υπηρεσίας. Σε αυτή την περίπτωση, οποιαδήποτε επίθεση άρνησης υπηρεσίας που στέλνει πολλαπλά περιττά αιτήματα στις υπηρεσίες ομίχλης θα απειλήσει την διαθεσιμότητα της υπηρεσίας για τα πραγματικά αιτήματα. Εκτός από την διαθεσιμότητα, η ακεραιότητα των υπηρεσιών καθώς και η ασφάλεια των δεδομένων που διαχειρίζονται μπορεί να επιδραστεί από σχετικές τρωτότητες στο επίπεδο των υπηρεσιών ή των στατικών τους μερών. (Farhadi *et al.*, 2020)

Η ενότητα 4.2.3 αφορά την κατηγοριοποίηση των τρωτοτήτων που ενδέχεται να υπάρχουν στο σύστημα και διαχωρίζεται σε τέσσερα κύρια μέρη, τα οποία αντιπροσωπεύουν τα βασικά συστατικά του συστήματος: το λογισμικό, τις υπηρεσίες, τα άτομα και τα δεδομένα. Παρακάτω αναλύεται η δομή της:

- ***Τρωτότητες Λογισμικού (Ενότητα 4.2.3.1):*** Αυτή η υποενότητα επικεντρώνεται στις τρωτότητες του λογισμικού που χρησιμοποιείται στο σύστημα. Αναλύονται θέματα όπως σφάλματα προγραμματισμού, χρήση ευπαθών βιβλιοθηκών, και προβλήματα που προκύπτουν από την ανεπαρκή ενημέρωση ή συντήρηση του λογισμικού.
- ***Τρωτότητες στις Υπηρεσίες (Ενότητα 4.2.3.2):*** Αυτή η υποενότητα εξετάζει τις τρωτότητες που αφορούν τις υπηρεσίες του συστήματος, όπως τα λειτουργικά και τεχνικά χαρακτηριστικά που προσφέρουν οι διάφορες εφαρμογές και υπηρεσίες. Εστιάζει σε ευπάθειες που μπορεί να προκύψουν από σφάλματα στον σχεδιασμό, την υλοποίηση ή τη συντήρηση των υπηρεσιών.

- ***Τρωτότητες που σχετίζονται με τα Άτομα (Ενότητα 4.2.3.3):*** Εδώ αναλύονται οι τρωτότητες που αφορούν τους χρήστες και τα άτομα που αλληλεπιδρούν με το σύστημα. Αυτές μπορεί να προκύπτουν από ανθρώπινους παράγοντες, όπως αδύναμοι κωδικοί, λάθος χειρισμός δεδομένων ή επιθέσεις κοινωνικής μηχανικής (social engineering).
- ***Τρωτότητες Δεδομένων / Ιδιωτικότητας (Ενότητα 4.2.3.4):*** Αυτή η υποενότητα εξετάζει τις τρωτότητες που σχετίζονται με την ασφάλεια των δεδομένων, όπως απώλεια, μη εξουσιοδοτημένη πρόσβαση ή αλλοίωση των δεδομένων, καθώς και ζητήματα προστασίας ιδιωτικότητας και συμμόρφωσης με κανονισμούς.

4.2.3.1 Λογισμικού

Τρωτότητες λόγω έλλειψης εκλεπτυσμένων ελέγχων πρόσβασης

Η απουσία αποτελεσματικών μηχανισμών εκλεπτυσμένου ελέγχου πρόσβασης επιτρέπει στους χρήστες με περιορισμένα δικαιώματα να εκτελούν ενέργειες που υπερβαίνουν το επιτρεπτό επίπεδο πρόσβασης τους. Επίσης, η έλλειψη διαχωρισμού δικαιωμάτων και η απουσία καταλόγων ελέγχου πρόσβασης (Access Control List - ACLs) ενισχύουν περαιτέρω τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης. (Aleisa, Abuhussein and Sheldon, 2020)

Τρωτότητες λόγω μη συχνών επιδιορθώσεων στο λογισμικό της υπηρεσίας

Η παράλειψη εφαρμογής ενημερώσεων ασφάλειας και επιδιορθώσεων αφήνει τις υπηρεσίες εκτεθειμένες σε νέες τρωτότητες και επιθέσεις. (An et al., 2022)

Τρωτότητες λόγω της χρήσης τρωτού λογισμικού για την υλοποίηση των υπηρεσιών

Η χρήση παλαιών ή μη ενημερωμένων εκδόσεων λογισμικού / εξαρτήσεων με γνωστές ευπάθειες αποτελεί μια σημαντική πηγή κινδύνου για την ασφάλεια του συστήματος. Οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις ευπάθειες για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και να προκαλέσουν σοβαρή ζημία στο σύστημα του ομιχλώδους προγραμματισμού και άρα και στη διαθεσιμότητα του. (Alzoubi et al., 2020)

4.2.3.2 Υπηρεσιών

Τρωτότητες σε ακατάλληλα ή μη ασφαλή πρωτόκολλα αυθεντικοποίησης και εξουσιοδότησης

Η έλλειψη ισχυρών μηχανισμών αυθεντικοποίησης και εξουσιοδότησης αποτελεί σοβαρή τρωτότητα για τα συστήματα του ομιχλώδους προγραμματισμού. Επιπλέον, υπάρχουν τρωτότητες που σχετίζονται με την εξουσιοδότηση, όπως η εφαρμογή χαλαρών πολιτικών πρόσβασης και η κακή διαμόρφωση των πρωτοκόλλων εξουσιοδότησης. Επιπρόσθετα, η λανθασμένη ή ανεπαρκής διαχείρισης σύνοδών, η χρήση ανασφαλών καναλιών επικοινωνίας και η εφαρμογή βέλτιστων πρακτικών ασφάλειας, όπως η αρχή του ελάχιστου δικαιώματος (least privilege) και η σωστή διαχείριση της λήξης των tokens, αυξάνουν τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης. (Riggs *et al.*, 2023)

Τρωτότητες λόγω έλλειψης μηχανισμών ανοχής σφαλμάτων

Η απουσία μηχανισμών που επιτρέπουν στο σύστημα να συνεχίσει να λειτουργεί παρά τα σφάλματα αυξάνει την πιθανότητα διακοπής των υπηρεσιών σε περίπτωση αποτυχίας του συστήματος του ομιχλώδους προγραμματισμού. (Alzoubi *et al.*, 2020)

Τρωτότητες λόγω μη ασφαλών APIs και διεπαφών υπηρεσιών

Τα μη ασφαλή APIs και διεπαφές υπηρεσιών μπορούν να γίνουν στόχος επιθέσεων επιτρέποντας με αυτό τον τρόπο την εκμετάλλευση των υπηρεσιών του συστήματος του ομιχλώδους προγραμματισμού ή την υποκλοπή των δεδομένων του συστήματος. (Farhadi *et al.*, 2020)

Τρωτότητες λόγω ανασφαλών μηχανισμών ανακάλυψης και σύνθεσης υπηρεσιών για νέες υπηρεσίες

Η δυνατότητα προσθήκης νέων υπηρεσιών στο σύστημα του ομιχλώδους προγραμματισμού εισάγει νέους κινδύνους ασφάλειας, Η έλλειψη επαλήθευσης της ταυτότητας και της αξιοπιστίας των νέων υπηρεσιών μπορεί να επιτρέψει την εισαγωγή κακόβουλων εφαρμογών στο σύστημα του ομιχλώδους προγραμματισμού. Επίσης, η ελλιπής σύνθεση υπηρεσιών και η έλλειψη επικύρωσης της σύνθεσης μπορεί να δημιουργήσει προβλήματα διαθεσιμότητας σύνθετων υπηρεσιών & εφαρμογών καθώς και άλλα κενά ασφάλειας. (Farhadi *et al.*, 2020)

Τρωτότητες λόγω έλλειψης κατάλληλου συστήματος διαχείρισης εμπιστοσύνης

Η έλλειψη διαχείρισης εμπιστοσύνης δημιουργεί ένα ευάλωτο περιβάλλον ομίχλης, όπου τα ευαίσθητα δεδομένα των χρηστών εκτίθενται σε σοβαρούς κίνδυνους (κατά τη μεταφορά τους ή όταν αποστέλλονται σε κακόβουλους κόμβους για αποθήκευση ή επεξεργασία), όπως είναι η μη εξουσιοδοτημένη πρόσβαση, η διαρροή των δεδομένων και η κακή χρήση των ευαίσθητων δεδομένων (Saad, 2018).

Τρωτότητες στην έλλειψη επαλήθευσης υπηρεσιών

Η δυνατότητα προσθήκης νέων υπηρεσιών στο σύστημα του ομιχλώδους προγραμματισμού εισάγει νέους κινδύνους ασφάλειας, Η έλλειψη επαλήθευσης της ταυτότητας και της αξιοπιστίας των νέων υπηρεσιών μπορεί να επιτρέψει την εισαγωγή κακόβουλων εφαρμογών στο σύστημα του ομιχλώδους προγραμματισμού. (Farhadi *et al.*, 2020)

Τρωτότητες λόγω μη ασφαλούς διαδικασίας μετανάστευσης υπηρεσιών

Η ανεπαρκής κρυπτογράφηση των δεδομένων κατά την μεταφορά τους από τον έναν κόμβο ομίχλης σε έναν άλλον, καθώς και η απουσία μηχανισμών επαλήθευσης της ακεραιότητας των δεδομένων και του κώδικα αυξάνουν τον κίνδυνο διαρροής ή αλλοίωσης των δεδομένων και του κώδικα μιας υπηρεσίας κατά την διάρκεια της μετανάστευσης τους. (Aguzzi *et al.*, 2020)

4.2.3.3 Ατόμων

Τρωτότητες λόγω ανθρώπινων σφαλμάτων

Τα άτομα, ειδικά αν δεν έχουν εκπαιδευθεί σωστά και επαρκώς, μπορεί να κάνουν λάθη που μπορεί να προκαλέσουν σημαντικά προβλήματα ασφάλειας σε ένα σύστημα, όπως ένα σύστημα ομιχλώδους προγραμματισμού. Για παράδειγμα, οι διαχειριστές μπορεί να σβήσουν κατά λάθος αρχεία συστήματος ή να διαμορφώσουν λανθασμένα μηχανισμούς/υπηρεσίες ασφάλειας. Οι λειτουργοί (operators) μπορεί να διαμορφώσουν λανθασμένα ή με μη ασφαλή τρόπο υπηρεσίες/εφαρμογές ομιχλώδους προγραμματισμού. Τέλος, εν γένει, οι χρήστες είναι ευάλωτοι σε ψυχολογική χειραγώγηση στα πλαίσια επιθέσεων κοινωνικής μηχανικής, πράγμα το οποίο μπορεί να οδηγήσει σε διαρροές ευαίσθητων δεδομένων και σε μη εξουσιοδοτημένη πρόσβαση σε ένα ομιχλώδες περιβάλλον.

4.2.3.4 Δεδομένων / Ιδιωτικότητας

Η ιδιωτικότητα των χρηστών είναι η ικανότητα να διατηρούνται ιδιωτικές οι πληροφορίες που σχετίζονται με το κάθε άτομο, εκτός από τις περιπτώσεις που έχει συμφωνηθεί τα δεδομένα αυτά να κοινοποιούνται σε νόμιμους προορισμούς δεδομένων. Μια από τις σημαντικότερες απαιτήσεις των υπηρεσιών είναι η προστασία της ιδιωτικότητας, ιδιαιτέρα στο πλαίσιο του IoT, το οποίο συχνά έχει πρόσβαση σε προσωπικές πληροφορίες. Επομένως, η ιδιωτικότητα των χρηστών αποτελεί ένα άλλο περιουσιακό στοιχείο του επιπέδου υπηρεσίας. Η ιδιωτικοτήτα χωρίζεται σε τρείς κατηγορίες: την ιδιωτικότητα της τοποθεσίας, την ιδιωτικότητα της ταυτότητας, την ιδιωτικότητα χρήσης και την ιδιωτικότητα προσωπικών δεδομένων. (Farhadi *et al.*, 2020)

Τρωτότητες στην ιδιωτικότητα της τοποθεσίας των χρηστών μέσω των κόμβων ομίχλης

Καθώς οι κόμβοι ομίχλης συνήθως παρέχουν υπηρεσίες σε κοντινούς χρήστες, η γνώση της τοποθεσίας ενός κόμβου ομίχλης αποκαλύπτει την κατά προσέγγιση τοποθεσία των IoT συσκευών που είναι συνδεδεμένες σε αυτόν και συνεπώς και των χρηστών του συστήματος του ομιχλώδους προγραμματισμού. Οι τρωτότητες που προκύπτουν από την αποκάλυψη της τοποθεσίας των κόμβων ομίχλης περιλαμβάνουν την έκθεση της ιδιωτικότητας των χρηστών και της τοποθεσίας των IoT συσκευών τους. Αν και η ίδια η τοποθεσία του χρήστη ενδέχεται να μην προκαλεί άμεση διαρροή άλλων ευαίσθητων δεδομένων, η συσχέτιση αυτής της τοποθεσίας με άλλες πληροφορίες (όπως το ιστορικό του χρήστη) μπορεί να επιτρέψει σε κακόβουλους τρίτους να αποκτήσουν πρόσβαση σε προσωπικά ή ευαίσθητα δεδομένα. Για παράδειγμα, η τοποθεσία μιας IoT συσκευής που είναι συνδεδεμένη με έναν κόμβο ομίχλης μπορεί να αποκαλύψει συχνές επίσκεψης του χρήστη της IoT συσκευής σε κέντρα απεξάρτησης ή άλλες ευαίσθητες τοποθεσίες, δηλαδή ενδέχεται να οδηγήσει σε αποκάλυψη προσωπικών πληροφοριών. Επομένως, είναι σημαντικό να διατηρείται η τοποθεσία των κόμβων ιδιωτική. (Farhadi *et al.*, 2020)

Τρωτότητες στην προστασία των προσωπικών δεδομένων

Μια άλλη τρωτότητα αφορά την προστασία των προσωπικών δεδομένων των χρηστών, τα οποία μπορεί να διαρρεύσουν λόγω παράνομης εισδοχής στους λογαριασμούς που αυτοί έχουν σε σχετικές ομιχλώδεις εφαρμογές. Για να γίνει μια εγκατάσταση εφαρμογών στον κόμβο ομίχλης χρησιμοποιούνται κωδικοί πρόσβασης που είναι κωδικοποιημένοι είτε εισηγμένοι στον πηγαίο κώδικα με ορατό τρόπο ή είτε εν γένει διαθέσιμοι στο κοινό. Αυτό μπορεί να συμβεί κυρίως σε

εφαρμογές ανοιχτού κώδικα που είναι διαθέσιμες στο Διαδίκτυο. Καθώς οι χρήστες ενδέχεται να μην αλλάζουν τους κωδικούς πρόσβασης που είναι «κωδικοποιημένοι», πολλές εφαρμογές μπορεί να αποτελούν εύκολο στόχο για τους επιτιθέμενους. (Farhadi *et al.*, 2020)

Τρωτότητες στις υπηρεσίες λόγω έλλειψης ανωνυμοποίησης

Υπάρχουν περιπτώσεις όπου ο χρήστης θέλει να παραμένει ανώνυμος κατά την χρήση μιας υπηρεσίας. Για παράδειγμα, οι χρήστες μιας υπηρεσίας, η οποία βοηθά τα άτομα με εθισμό στα ναρκωτικά, μπορεί να επιθυμούν να παραμείνουν ανώνυμοι. Από την άλλη πλευρά, εάν η υπηρεσία γίνει μέρος του δημοσίου συστήματος, όπως ένα σύστημα δημόσιας διοίκησης, ενδέχεται να χρειαστεί να έχει πρόσβαση στην πραγματική ταυτότητα των χρηστών. Εφόσον, ένας χρήστης παρέχει την ταυτότητα του στο σύστημα για να καταχωρηθεί σε αυτήν την υπηρεσία, το δημόσιο σύστημα θα πρέπει να διασφαλίσει ότι αυτή η ταυτότητα δεν θα κοινοποιηθεί ή χρησιμοποιηθεί για άλλους σκοπούς πέραν από το συμφωνηθέν πλαίσιο και την παροχή της υπηρεσίας. Ωστόσο, η έλλειψη ισχυρών τεχνικών ανωνυμοποίησης αποτελεί σημαντική τρωτότητα και αν δεν εφαρμοστούν κατάλληλες τεχνικές, μπορεί να αποκαλυφθεί η ταυτότητα του χρήστη. Αυτό μπορεί να γίνει, π.χ. εφόσον η υπηρεσία επιτρέπει την επερώτηση των δεδομένων της ή τα εξάγει για ερευνητικούς σκοπούς σε ερευνητές ή ερευνητικά ιδρύματα. Ακόμη και αν τα δεδομένα είναι ανωνυμοποίημενα, η αδυναμία εξάλειψης των συσχετίσεων μεταξύ των προσωπικών και μη δεδομένων μπορεί να οδηγήσει στην έμμεση ή άμεση αποκάλυψη των προσωπικών δεδομένων των χρηστών του συστήματος του ομιχλώδους προγραμματισμού (Sarwar, et al., 2021). Επιπλέον, η αποθήκευση προσωπικών δεδομένων του χρήστη σε κόμβους ομίχλης σε μη κρυπτογραφημένη μορφή αποτελεί μια σοβαρή τρωτότητα για τα συστήματα, καθώς αυξάνει τον κίνδυνο διαρροής τους. Αυτό το πρόβλημα μπορεί να συμβεί τόσο στο επίπεδο του IoT όσο και στο επίπεδο του νέφους. (Farhadi *et al.*, 2020)

Στο παραπάνω παράδειγμα, ακόμη και τα απλά ονόματα του χρήστη μπορεί να θεωρηθούν περιουσιακά στοιχεία και πρέπει να προστατευτούν. Εάν μια υπηρεσία χρησιμοποιεί τοπικούς κόμβους ομίχλης, οι οποίοι είναι δημόσια γνωστοί ότι ανήκουν σε μια συγκεκριμένη υπηρεσία, ακόμη και η παρακολούθηση των δεδομένων από μια συσκευή του χρήστη μέχρι τον κόμβο ομίχλης θα μπορούσε να απειλήσει την ιδιωτικότητα ενός χρήστη. Σε αυτήν την περίπτωση, το πρόβλημα δεν αφορά τα δεδομένα που στέλνει ο χρήστης, αλλά και τον τρόπο αποστολής τους. Αν η ροή δεδομένων μεταξύ των IoT συσκευών και των κόμβων ομίχλης δεν είναι κρυπτογραφημένη, αυτό μπορεί να απειλήσει την ιδιωτικότητα του χρήστη. Αν και η ύπαρξη μιας ροής δεδομένων είναι απαραίτητη για την επικοινωνία και την λειτουργία των υπηρεσιών, ο τρόπος με τον οποίο μεταφέρονται τα διαπιστευτήρια του χρήστη για την αυθεντικοποίηση σε μια υπηρεσία είναι κρίσιμος για την ασφάλεια και την προστασία των προσωπικών δεδομένων. (Farhadi *et al.*, 2020)

Τρωτότητες μοτίβων ροής δεδομένων

Ένας επιτιθέμενος είναι σε θέση να αναλύσει το μοτίβο ροής των δεδομένων του χρήστη χρησιμοποιώντας τους κόμβους ομίχλης ή το νέφος, έτσι ώστε να κάνει κάποιες προβλέψεις σχετικά με τις συνήθειες του χρήστη. Η τρωτότητα ανάλυσης ροής δεδομένων έγκειται στο ότι η ανάλυση αυτών των μοτίβων μπορεί να οδηγήσει στην έκθεση προσωπικών πληροφοριών και συμπεριφορών

του χρήστη, επιτρέποντας στον επιτιθέμενο να εξάγει ευαίσθητα δεδομένα και να εκμεταλλευτεί τις συνήθειες του χρήστη για κακόβουλους σκοπούς. (Farhadi *et al.*, 2020)

Έλλειψη ασφαλών και κατάλληλων μηχανισμών αντιγράφων ασφαλείας

Η έλλειψη ασφαλών και κατάλληλων μηχανισμών αντιγράφων ασφαλείας αποτελεί τρωτότητα που μπορεί να εκθέτει τα ευαίσθητα δεδομένα σε σοβαρούς κίνδυνους, όπως είναι η απώλεια των δεδομένων και η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητα δεδομένα (Farhadi *et al.*, 2020).

Μη συμμόρφωση με νομικά πλαίσια και κανονισμούς

Η μη συμμόρφωση με νομικά πλαίσια και κανονισμούς, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), συνιστά τρωτότητα που μπορεί να οδηγήσει σε σοβαρές συνέπειες, όπως είναι οι νομικές κυρώσεις και η απώλεια της εμπιστοσύνης των χρηστών, καθώς τα προσωπικά δεδομένα δεν προστατεύονται με επαρκή τρόπο μέσω του ομιχλώδους προγραμματισμού (Seth, Najana and Ranjan, 2024).

Στον παρακάτω πίνακα φαίνονται συγκεντρωτικά όλες οι τρωτότητες της Ενότητας 4.2 της παρούσας διπλωματικής εργασίας.

Πίνακας 2 - Τρωτότητες στον ομιχλώδη προγραμματισμό

Επίπεδο	**Κατηγορία**	**Τρωτότητες**
Συσκευής	Φυσικά περιουσιακά στοιχεία	Τρωτότητες σε επίπεδο τσιπ Firmware Διαρροής ηλεκτρικού φορτιού στην DRAM Διαταραχή μνήμης μέσω ηλεκτρομαγνητικών εκπομπών
	Λογικά περιουσιακά στοιχεία	Πρόσβαση στη μνήμη μέσω των θυρών του κόμβου ομίχλης Συσχετίσεις δεδομένων APIs και στις διεπαφές Έλλειψη εκλεπτυσμένου ελέγχου πρόσβασης Ειδικές τρωτότητες εφαρμογών Ακεραιότητας στον κώδικα του λογισμικού Εμπιστευτικότητας στον κώδικα των δοχείων Αδύναμα δικαιώματα πρόσβασης σε αρχεία του συστήματος Δεδομένα

		Εφοδιαστική αλυσίδα
Επικοινωνίας	Τρωτότητες στο κανάλι / μέσω επικοινωνίας	Έλλειψη μηχανισμών ασφάλειας στο κανάλι επικοινωνίας Χρήση μη ισχυρής κρυπτογράφησης Μη κατάλληλα πρωτόκολλα Αδυναμίες του λειτουργικού συστήματος Τρωτότητες στα πρωτόκολλα δρομολόγησης Τρωτότητες στον τρόπο λειτουργίας των φυσικών καναλιών Ανεπαρκής απομόνωση του μέσου επικοινωνίας Πρωτοκόλλα κρυπτογράφησης
	Τρωτότητες στην διεύθυνση οντοτήτων	Χρήση μη ισχυρών μεθόδων αυθεντικοποίησης των κόμβων ομίχλης Δυναμικές διευθύνσεις Απουσία ελέγχου στις αιτήσεις απόκτησης διευθύνσεων Χρήση στατικών διευθύνσεων
Υπηρεσίες	Λογισμικού	Έλλειψη εκλεπτυσμένων ελέγχων πρόσβασης Μη συχνών επιδιορθώσεων στο λογισμικό της υπηρεσίας Χρήση τρωτού λογισμικού για την υλοποίηση των υπηρεσιών
	Υπηρεσιών	Ακατάλληλα ή μη ασφαλή πρωτόκολλα αυθεντικοποίησης και εξουσιοδότησης Έλλειψη μηχανισμών ανοχής σφαλμάτων Μη ασφαλή APIs και διεπαφές υπηρεσιών Ανασφαλείς μηχανισμοί ανακάλυψης και σύνθεσης υπηρεσιών για νέες υπηρεσίες Έλλειψη κατάλληλου συστήματος διαχείρισης εμπιστοσύνης Μη ασφαλής διαδικασία μετανάστευσης υπηρεσιών
	Άτομα	Ανθρώπινα σφάλματα
	Δεδομένων/ Ιδιωτικότητας	Ιδιωτικότητα της τοποθεσίας των χρηστών μέσω των κόμβων ομίχλης

		Προστασία των προσωπικών δεδομένων και στους κωδικούς πρόσβασης Τρωτότητες στις υπηρεσίες λόγω έλλειψης ανωνυμοποίησης Μοτίβων ροής δεδομένων Έλλειψη ασφαλών και κατάλληλων μηχανισμών αντιγράφων ασφαλείας Μη συμμόρφωση με νομικά πλαίσια και κανονισμούς

4.3 Είδη Επιθέσεων

Οι επιθέσεις στον ομιχλώδη προγραμματισμό κατηγοριοποιούνται σε έξι κατηγορίες (Khan, Parkinson and Qin, 2017):

- Επιθέσεις εικονικοποίησης (Virtualization attacks)
- Επιθέσεις ασφάλειας ιστού (Web security attacks)
- Επιθέσεις σχετικά με την επικοινωνία εντός ή εκτός του οργανισμού / επιχείρησης (Internal/external communication attacks)
- Επιθέσεις ασύρματης επικοινωνίας (Wireless communication attacks)
- Επιθέσεις ασφάλειας δεδομένων (Data security attacks)
- Επιθέσεις κακόβουλου λογισμικού (Malware attacks)

4.3.1 Επιθέσεις εικονικοποίησης

Η εκτεταμένη χρήση εικονικοποιημένων περιβαλλόντων στον ομιχλώδη προγραμματισμό προσφέρει πολλά οφέλη, όπως ευελιξία και αποδοτικότητα, αλλά προκαλεί ένα πλήθος τρωτοτήτων ασφάλειας που προκύπτουν από την κοινόχρηστη τεχνολογία (shared technology), εξαιτίας του διαμοιρασμού των πόρων του ομιχλώδους περιβάλλοντος, οι οποίοι είναι προσπελάσιμοι από πολλούς χρήστες ταυτόχρονα, αυξάνοντας με αυτό τον τρόπο την πιθανότητα εμφάνισης ευπαθειών και επιθέσεων. Αυτές οι τρωτότητες μπορεί να πηγάζουν από διάφορούς παράγοντες, όπως κενά ασφάλειας που μπορεί να υπάρχουν στο λογισμικό του υπερόπτη (hypervisor), από την ανεπαρκή απομόνωση μεταξύ των εικονικών μηχανών (VMs), την ύπαρξη πλευρικών καναλιών (side-channel attack) κ.α. Για παράδειγμα, ένας υπερεπόπτης με κενά ασφάλειας μπορεί να αποτελέσει στόχο εκμετάλλευσης από επιτήδειους, αφού αποτελεί μοναδικό σημείο αποτυχίας (single point of failure). Αυτό σημαίνει πως εφόσον ο υπερόπτης παρουσιάσει κάποια τρωτότητα που γίνει εκμεταλλεύσιμη από μια επίθεση, τότε όλες οι εικονικές μηχανές που εξαρτώνται από αυτόν θα επηρεαστούν, οδηγώντας στη κατάρρευση της πλατφόρμας του ομιχλώδους προγραμματισμού στον κόμβο-θύμα. (Khan, Parkinson and Qin, 2017)

Στον ομιχλώδη προγραμματισμό, περαιτέρω εικονικοποίηση (στο επίπεδο του λειτουργικού συστήματος) μπορεί να επιτευχθεί με την χρήση των δοχείων (containers), βοηθώντας στην αποτελεσματικότερη διαχείριση των πόρων που χρησιμοποιούνται από τις εφαρμογές και στην αύξηση της ασφάλειας λόγω της χρήσης δύο επιπέδων εικονικοποίησης. Η δημιουργία δοχείων πραγματοποιείται στα κέντρα δεδομένων του ομιχλώδους προγραμματισμού βοηθώντας στην μείωση της κατανάλωσης ενέργειας του συστήματος, του αποθηκευτικού χώρου και του κόστους. Σε αντίθεση με τις εικονικές μηχανές, που απαιτούν την εκτέλεση ολοκλήρων λειτουργικών συστημάτων, τα δοχεία μοιράζονται τον ίδιο πυρήνα του λειτουργικού συστήματος, μειώνοντας έτσι την ανάγκη για επιπλέον υπολογιστική ισχύ και αποθηκευτικό χώρο, γεγονός που οδηγεί σε μικρότερη κατανάλωση ενέργειας. Τα δοχεία επιτρέπουν την αποδοτικότερη αξιοποίηση των πόρων, μειώνοντας την υπερφόρτωση του συστήματος. Επιπλέον, τα δοχεία προσφέρουν ταχύτερη εκκίνηση και τερματισμό των εφαρμογών σε σύγκριση με τις παραδοσιακές εικονικές μηχανές. Τέλος, τα δοχεία επιτρέπουν την ταχεία κλιμάκωση μιας εφαρμογής. (Mahadevappa and Murugesan, 2021)

Το Docker είναι η πιο δημοφιλής πλατφόρμα ανοιχτού λογισμικού για την ανάπτυξη των δοχείων εξαιτίας των πολλών πλεονεκτημάτων που προσφέρει, όπως της κλιμακωσιμότητας, φορητότητας, πυκνότητας (density) (των δοχείων σε σχέση με τις εικονικές μηχανές) και της άμεσης παράδοσης (rapid delivery). Ωστόσο, οι εφαρμογές των δοχείων μπορούν να αποκτούν άμεση πρόσβαση και να επικοινωνούν με τους πυρήνες φιλοξενίας (host kernel) (ενός λειτουργικού συστήματος). Όποτε, εφόσον ένας επιτιθέμενος εκμεταλλευτεί κάποιο κενό ασφάλειας σε αυτή την επικοινωνία, μπορεί να αποκτήσει πρόσβαση στον πυρήνα, γεγονός που ενδέχεται να επιτρέψει πρόσβαση και σε άλλα δοχεία στο ίδιο σύστημα, καθώς όλα μοιράζονται τον ίδιο πυρήνα. Κατά τη διάρκεια αυτής της διαδικασίας, οι επιτιθέμενοι μπορούν να επιτεθούν στα δοχεία των εφαρμογών του κόμβου φιλοξενίας, να ελέγξουν τα δεδομένα στα δοχεία ή να αποκτήσουν πρόσβαση στη μηχανή Docker (docker engine) (δηλαδή την μηχανή υπεύθυνη για την διαχείριση και ενορχήστρωσή των δοχείων). Για να επιτύχουν τον παραπάνω στόχο, οι επιτιθέμενοι μπορεί να πραγματοποιήσουν διάφορες επιθέσεις μέσω του διαδικτύου ή που να αφορούν αποκλειστικά και μονό τα δοχεία, όπως επιθέσεις άρνησης υπηρεσίας (DoS), κακόβουλου λογισμικού (malware), παραποίησης ταυτότητας (spoofing), δημιουργία μολυσμένης εικόνας δοχείου (infected container image), η οποία μπορεί να οδηγήσει στην δημιουργίας κακόβουλων δοχείων που ενδέχεται να επιτεθούν σε άλλα δοχεία, στην μηχανή Docker ή και στον πυρήνα, χειρισμού δικαιωμάτων (handling privileges) μέσω του πυρήνα, επίθεσης απόδρασης από δοχείο (container escape attack), αιωρούμενου αποθηκευτικού χώρου (dangling volume), επιθέσεις shell shock, καθώς και δημιουργίας ή εκμετάλλευσης υπαρχουσών backdoors. (Mahadevappa and Murugesan, 2021)

4.3.1.1 Είδη επιθέσεων σχετικά με την εικονικοποίηση στον ομιχλώδη προγραμματισμό

Αιωρούμενος αποθηκευτικός χώρος (Dangling volume)

Τα ενεργά δοχεία αποθηκεύουν τα δεδομένα σε ένα εγγράψιμο στρώμα δοχείου (writeable container layer), το όποιο αποθηκεύει τις τροποποιήσεις και τα δεδομένα που δημιουργούνται κατά την εκτέλεση ενός δοχείου. Όταν διαγράφεται ένα δοχείο, το εγγράψιμο στρώμα δοχείου διαγράφεται επίσης. Ωστόσο, χρησιμοποιώντας μια δέσμευση (bind mount) και τους αποθηκευτικούς χώρους (volumes), τα δεδομένα μπορούν να παραμείνουν ακόμη και μετά την διαγραφή των δοχείων. Η δέσμευση λειτουργεί με την προσάρτηση αρχείων (mounting a file) ή καταλόγου από το σύστημα φιλοξενίας (host) στα δοχεία. Όταν μια εφαρμογή εκτελείται σε πολλαπλά δοχεία (containers) και τα δοχεία δεν έχουν αφαιρεθεί μετά την παύση τους, π.χ. μέσω της εντολής «docker system / prune», τότε ο επιτιθέμενος μπορεί υπό συγκεκριμένες προϋποθέσεις να έχει πρόσβαση στα δεδομένα οποιουδήποτε από αυτά τα δοχεία. Οι προϋποθέσεις αυτές περιλαμβάνουν την απόκτηση ριζικών δικαιωμάτων στο σύστημα, την εκμετάλλευση ευπαθειών για την διαφυγή περιβάλλοντος δοχείου (container escape) (οπότε ο επιτιθέμενος αποκτά πρόσβαση και ενδεχομένων στον πυρήνα), την ύπαρξη κοινόχρηστου ή αποθηκευτικού χώρου που είναι προσβάσιμος από όλα τα δοχεία (και άρα του επιτιθέμενου), ή την περίπτωση όπου ο αποθηκευτικός χώρος ενός δοχείου έχει δεσμευθεί σε άλλο δοχείο (όπως του επιτιθέμενου). Να πούμε βέβαια πως κατά ορισμό, ένας αποθηκευτικός χώρος είναι αιωρούμενος όταν δεν χρησιμοποιείται από εκτελέσιμα δοχεία. Άρα, αν και οι τελευταίες δύο περιπτώσεις δεν αφορούν αιωρούμενους χώρους, ουσιαστικά μπορεί να αφορούν οποιοδήποτε χρησιμοποιούμενο χώρο. (Mahadevappa and Murugesan, 2021)

Επιθέσεις Shellshock και δημιουργίας εικόνων μέσω πίσω πόρτας (Shellshock and backdooring images)

Η εικόνα ενός δοχείου αναπτύσσονται πάνω από μια βασική εικόνα από ένα δημόσιο αποθετήριο (όπως το Docker Hub). Αν όμως αυτές οι εικόνες βάσης δεν είναι εμπιστευτικές ή δεν παρέχονται από αξιόπιστες πηγές, ενδέχεται να περιέχουν κακόβουλο κώδικα πίσω πόρτας. Για παράδειγμα, μια τέτοια εικόνα μπορεί να δημιουργηθεί από έναν επιτιθέμενο ώστε να παρέχεται μια γνωστή χρήσιμη υπηρεσία (π.χ. servlet container, όπως ο Tomcat, ή μίνι λειτουργικού συστήματος) προς τους προγραμματιστές. Η εικόνα αυτή ενδέχεται να έχει έγκυρη υπογραφή ώστε να φαίνεται ασφαλής. Όταν οι προγραμματιστές χρησιμοποιούν αυτή την μολυσμένη εικόνα για να δημιουργήσουν τις εικόνες των εφαρμογών τους, το κακόβουλο λογισμικό πίσω πόρτας ενσωματώνεται αυτόματα στον κώδικα των εφαρμογών τους. Αυτό προφανώς θα έχει άμεσες αρνητικές συνέπειες μόλις τα δοχεία των εφαρμογών δημιουργηθούν από τις εικόνες τους, επιτρέποντας ουσιαστικά τους επιτιθέμενους να συνδεθούν στα δοχεία και να διενεργήσουν κακόβουλες ενέργειες. Είναι σημαντικό να σημειωθεί ότι κάποιες εικόνες (βάσης), όπως αυτές που αφορούν συστήματα βάσεων δεδομένων, μπορούν να εκτελούνται άμεσα ως συστατικά μιας εφαρμογής. Οπότε δεν χρειάζεται να ενσωματωθούν στον κώδικα του συστατικού μας εφαρμογής για να εκτελεστούν. (Mahadevappa and Murugesan, 2021)

Παρομοίως, η επίθεση shellshock είναι μια μορφή εκτέλεσης οποιουδήποτε κώδικα, άρα και κακόβουλου, που μπορεί να οδηγήσει σε διάφορες δυσάρεστες συνέπειες. Ειδικότερα, μέσω μιας τέτοιας επίθεσης μπορεί να γίνει μη εξουσιοδοτημένη πρόσβαση στα αρχεία του δοχείου και στον κώδικα του με αντίκτυπο στην ακεραιότητα και εμπιστευτικότητά τους. Αν συνδυαστεί με μια επίθεση διαφυγής (περιβάλλοντος) δοχείου (container escape), τότε ο κακόβουλος χρήστης από

ριζικός χρήστης του δοχείου μπορεί να γίνει διαχειριστής του συστήματος φιλοξενίας. Η επίθεση αυτή είναι δυνατή εφόσον χρησιμοποιούνται περιβάλλοντα Bash (ειδικά για διεπαφές γραμμής εντολών), τα οποία είναι τρωτά λόγω ελλιπούς ελέγχου στις τιμές των μεταβλητών περιβάλλοντος. Με αυτό τον τρόπο, το πέρασμα κακόβουλου κώδικα σε μεταβλητή περιβάλλοντος μπορεί να οδηγήσει στην εκτέλεση του. (Mahadevappa and Murugesan, 2021)

Επίθεση πλευρικού καναλιού (side-channel attack)

Η επίθεση πλευρικού καναλιού είναι ένας τρόπος για τους επιτιθέμενους να αποκτήσουν πρόσβαση σε δεδομένα ή πληροφορίες, εκμεταλλευόμενοι τα φυσικά φαινόμενα που παράγονται στο επίπεδο των κόμβων ομίχλης ή στο περιβάλλον τους από τους μικροεπεξεργαστές και άλλα είδη συσκευών κατά την κανονική λειτουργία τους, με στόχο την αποκόμιση ευαίσθητων πληροφοριών. Αυτές οι πληροφορίες μπορεί να αφορούν τα δεδομένα που επεξεργάζεται ο υπολογιστής, τους αλγορίθμους που χρησιμοποιεί, κρυπτογραφικά κλειδιά που ενδέχεται να εμπλέκονται, τις δραστηριότητες που πραγματοποιεί ένας χρήστης, κ.α. (Standaert, 2010)

Για παράδειγμα, οι μικροεπεξεργαστές καταναλώνουν ενέργεια και χρόνο για να εκτελέσουν τις διεργασίες τους, αλλά παράλληλα μπορεί να εκπέμπουν ηλεκτρομαγνητική ακτινοβολία, να αποβάλουν θερμότητα ή να παράγουν κάποιο θόρυβο. Αυτά τα φυσικά φαινόμενα δεν είναι τυχαία, αλλά σχετίζονται άμεσα με τις εντολές που εκτελεί ο επεξεργαστής και τα δεδομένα που επεξεργάζεται. Έτσι οι διακυμάνσεις στην κατανάλωση ενέργειας, στον χρόνο εκτέλεσης και στην ακτινοβολία που εκπέμπεται μπορούν να παρέχουν ενδείξεις για το ποια δεδομένα επεξεργάζονται ή ποιοι αλγόριθμοι χρησιμοποιούνται. Οι επιτιθέμενοι μπορούν να αναλύσουν αυτές τις μετρήσεις για να εξάγουν ευαίσθητες πληροφορίες, όπως κρυπτογραφικά κλειδιά ή συγκεκριμένα δεδομένα που επεξεργάζεται το σύστημα εκείνη την στιγμή. (Standaert, 2010)

Άλλα παραδείγματα επιθέσεων πλευρικού καναλιού τις *επιθέσεις στην κρυφή μνήμη*, όπου ένας εισβολέας μπορεί να εκμεταλλευτεί τον κοινόχρηστο χώρο μνήμης μεταξύ των εφαρμογών για να αποσπάσει πληροφορίες και τις *επιθέσεις μέσω της ανάλυσης της κατανάλωσης ισχύος ή χρονισμού,* που επιτρέπουν την διαρροή των δεδομένων μέσω φυσικών χαρακτηριστικών ενός συστήματος (Standaert, 2010)

Για να διασφαλιστεί η ιδιωτικότητα των δεδομένων στο υπολογιστικό νέφος, οι χρήστες συνήθως κρυπτογραφούν τα ευαίσθητα δεδομένα τους πριν τα μεταφορτώσουν στο νέφος. Ωστόσο, οι παραδοσιακές τεχνικές κρυπτογράφησης δεν υποστηρίζουν την κατάργηση διπλοτύπων δεδομένων (data deduplication). Η τεχνική της κατάργησης διπλότυπων δεδομένων μπορεί να μειώσει σημαντικά το κόστος για το αποθηκευτικό χώρο του υπολογιστικού νέφους εξαλείφοντας τα διπλότυπα δεδομένα και διατηρώντας ένα αντίγραφο κάθε φορά. Η κρυπτογράφηση με κλειδί μηνύματος (MLE) υποστηρίζει την τεχνική κατάργησης διπλότυπων δεδομένων και χρησιμοποιεί κρυπτογραφικά κατακερματισμένες τιμές των μηνυμάτων ως κλειδιά κρυπτογράφησης. (Lu *et al.*, 2021)

Η MLE είναι ευάλωτη σε επιθέσεις πλευρικού καναλιού, όπως η *επίθεση προσωρινής αποθήκευσης κλειδιού (key-cache attack)*. Η αποθήκευση του κλειδιού MLE μπορεί να πραγματοποιείται σε διάφορες τοποθεσίες του συστήματος, όπως είναι η μνήμη RAM ή η κρυφή μνήμη που δεν είναι επαρκώς προστατευμένες. Για παράδειγμα, ένας κακόβουλος χρήστης μπορεί να κρυφακούει μέσω ενός πλευρικού καναλιού για να αποκτήσει πρόσβαση σε δεδομένα του συστήματος, έτσι ώστε κλέψει το κλειδί MLE. Επίσης, ακόμα και αν η πρόσβαση του επιτιθέμενου στο σύστημα έχει αφαιρεθεί, εάν ο επιτιθέμενος έχει καταφέρει να ανακτήσει το κλειδί MLE πριν ή ακόμα και μετά την αφαίρεση της πρόσβασης του από το σύστημα, μπορεί να το χρησιμοποιήσει για να αποκρυπτογραφήσει τα δεδομένα τοπικά, εκτός του συστήματος, εφόσον έχει ήδη στην κατοχή του τα αντίστοιχα κρυπτογραφικά αρχεία. Επομένως, η επίθεση της προσωρινής αποθήκευσης ενδέχεται να προκαλέσει προβλήματα στην διαρροή προσωπικών δεδομένων των χρηστών. Προφανώς, και μπορεί να εκτελεστεί σε περιβάλλοντα ομίχλης. (Lu *et al.*, 2021)

Επίθεση διαφυγής δοχείων (Container escape attack)

Ο μηχανισμός εικονικοποιήσης των δοχείων χρησιμοποιεί διάφορες τεχνολογίες, όπως τον χώρο ονομάτων (namespaces) και τις ομάδες ελέγχου (cgroups) για την απομόνωση των διεργασιών και των πόρων τους (ενός δοχείου) τους στον υπολογιστή / κόμβο φιλοξενίας (το κεντρικό σύστημα που φιλοξένει τα δοχεία), αρά και από τα άλλα δοχεία (Mahadevappa and Murugesan, 2021). Ωστόσο, όταν εκτελείται κάποιος εξειδικευμένος κώδικας εκμετάλλευσης (exploit code) του πυρήνα μέσα στο δοχείο, μπορεί να προκαλέσει την κατάρρευση ολοκλήρου του υπολογιστή ή ακόμα και να αναβαθμίσει τα δικαιώματα του χρήστη σε δικαιώματα διαχειριστή, αποκτώντας έτσι πλήρη έλεγχο του υπολογιστή αυτού. Αυτό συμβαίνει είτε λόγω ανεπαρκούς απομόνωσης του δοχείου από τον κεντρικό πυρήνα του συστήματος είτε λόγω εκμετάλλευσης των τρωτών σημείων που υπάρχουν στον ίδιο τον πυρήνα (Jian and Chen, 2017). Η παραπάνω επίθεση ονομάζεται επίθεση διαφυγής δοχείων. Υπάρχουν δύο τύποι διαφυγής: (α) η εναλλαγή χώρων ονομάτων (namespace switching) και (β) η τροποποίηση κοινής μνήμης (shared memory modification), (Mahadevappa and Murugesan, 2021).

Η επίθεση απόδρασης εναλλαγής χώρων ονομάτων αποτελεί έναν σοβαρό κίνδυνο για την ασφάλεια των δοχείων (containers) του Linux, η οποία πραγματοποιείται μέσω της δομής task_struct. Η δομή task_struct αποτελεί ένα θεμελιώδες στοιχείο που περιγράφει μια ενεργή διεργασία (process) στον πυρήνα του Linux (Jian and Chen, 2017). Η δομή task_struct περιλαμβάνει πληροφορίες σχετικά με την διεργασία που εκτελείται κάθε φορά, το αναγνωριστικό της διεργασίας που εκτελείται (PID), τον γονέα της διεργασίας (real parent) και δείκτες σε άλλες δομές, όπως την fs_struct και την ns_proxy, οι οποίες περιέχουν πληροφορίες για το χώρο των ονομάτων, όπως απεικονίζονται στον παρακάτω κώδικα (Mahadevappa and Murugesan, 2021):

```
struct task_struct {
        ... pid_t pid;
         struct task_struct __rcu *real_parent;
         struct fs_struct *fs;
```

```
        /* namespaces */
        struct nsproxy *nsproxy;
... }
```

Ο παραπάνω ορισμός της προαναφερόμενης δομής εξηγεί πως η επίθεση απόδρασης εναλλαγής ονομάτων εκμεταλλεύεται την δομή task_struct, έτσι ώστε η κακόβουλη διεργασία να αποδράσει από το δοχείο. Στην ουσία, η κακόβουλη διεργασία «μιμείται» μια διεργασία του υπολογιστή φιλοξενίας, αντιγράφοντας πληροφορίες από την γονική διεργασία στον υπολογιστή αυτό. Μέσω της μεθόδου της «swich task namespaces», η κακόβουλη διεργασία υιοθέτει το χώρο ονομάτων του υπολογιστή, αποκτώντας πρόσβαση στους πόρους του. (Mahadevappa and Murugesan, 2021)

Η επίθεση απόδρασης μέσω της τροποποίησης κοινής μνήμης ή dirty cow ή copy-on-write είναι μια πολύ γνωστή επίθεση σχετικά με τα δοχεία του Linux. Το Dirty COW εκμεταλλεύεται μια ευπάθεια στο σύστημα αρχείων του μηχανήματος φιλοξενίας για να επιτρέψει στον επιτιθέμενο να τροποποιήσει δεδομένα σε ένα αρχείο, ακόμη και αν ο χρήστης που εκτελεί το πρόγραμμα δεν έχει τα απαραίτητα δικαιώματα. Πρέπει να σημειωθεί ότι για να γίνει δυνατή η πρόσβαση στο αρχείο από το δοχείο (container), το αρχείο αυτό θα πρέπει να έχει γίνει mount στο δοχείο. Αν δεν έχει γίνει mount, το αρχείο δεν θα είναι ορατό μέσα στο δοχείο. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτήν την τροποποίηση για να αποκτήσει ριζική πρόσβαση στο σύστημα, μέσω του λογαριασμού του διαχειριστή του συστήματος, δηλαδή του χρήστη με τα υψηλότερα δικαιώματα στο σύστημα. (Mahadevappa and Murugesan, 2021)

Δηλητηριασμός εικόνων (Image poisoning)

Το image poisoning σε δοχεία αφορά την περίπτωση όπου κακόβουλοι χρήστες δημιουργούν και δημοσιεύουν δηλητηριασμένες εικόνες δοχείων (container images) σε αποθετήρια. Δεδομένου ότι οι εικόνες δοχείων μπορούν να δημιουργηθούν από οποιονδήποτε, οι επιτιθέμενοι έχουν τη δυνατότητα να εισάγουν κακόβουλες εικόνες στα αποθετήρια, τα οποία στη συνέχεια χρησιμοποιούν άλλοι χρήστες. Αυτό μπορεί να οδηγήσει σε ποικιλία επιθέσεων, όπως εκτέλεση κακόβουλου κώδικα ή κλοπή δεδομένων, από τους χρήστες που θα κατεβάσουν και θα εκτελέσουν αυτές τις εικόνες. Ειδικά όταν η διαδικασία δημιουργίας και αποθήκευσης των εικόνων δεν είναι αυστηρά ελεγχόμενη, η χρήση κακόβουλων εικόνων δοχείων γίνεται σημαντική απειλή για την ασφάλεια. (Syed, Fernandez and Silva, 2017)

Άρνηση Υπηρεσίας (DoS -Denial of Service)

Οι επιθέσεις DoS (Denial of Service) μπορούν να επηρεάσουν σοβαρά την απόδοση των δοχείων (containers). Ένας επιτιθέμενος μπορεί να αναγκάσει ένα δοχείο να καταναλώνει υπερβολικούς πόρους, όπως CPU ή μνήμη, προκαλώντας εξάντληση των πόρων σε όλο το σύστημα και επηρεάζοντας άλλα δοχεία στο ίδιο μηχάνημα. Αυτό μπορεί να οδηγήσει σε συνολική κατάρρευση του συστήματος ή να εμποδίσει τη λειτουργία άλλων εφαρμογών. (Wong *et al.*, 2023)

Διαφυγή εικονικής μηχανής (VM escape)

Η διαοφυγή εικονικής μηχανής είναι μια επίθεση όπου ο επιτιθέμενος χρησιμοποιεί κακόβουλο κώδικα που επιτρέπει στο φιλοξενούμενο λειτουργικό σύστημα να εκμεταλλευτεί τρωτότητες του υπερεπόπτη (hypervisor), δηλαδή του λογισμικού που διαχειρίζεται τις εικονικές μηχανές (VMs), ώστε να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε αυτόν και κατά επέκταση και στις εικονικές μηχανές που αυτός διαχειρίζεται. Επομένως, ο κεντρικός στόχος αυτής της επίθεσης είναι η παραβίαση του υπερεπόπτη, με αποτέλεσμα την πρόσβαση στους κοινούς πόρους που μοιράζονται οι άλλες εικονικές μηχανές στον ίδιο φυσικό διακομιστή. Ωστόσο, μπορεί το φιλοξενούμενο λειτουργικό σύστημα έχει την ευχέρεια να εκτελέσει εντολές στο υποκείμενο σύστημα φιλοξενίας. Επομένως, στόχος μπορεί να είναι και το τελευταίο. Αυτό μπορεί να έχει ως αποτέλεσμα την ενδεχόμενη παραβίαση του συστήματος αρχείων, των διεπαφών δικτύωσης και της φυσικής αποθήκευσης. Η βασική αρχή είναι η «απόδραση» από το περιβάλλον της εικονικής μηχανής, επιτρέποντας στον επιτιθέμενο να εκμεταλλευτεί τον υπερεπόπτη ή / και το τοπικό σύστημα ή το φυσικό μηχάνημα φιλοξενίας. Σε περίπτωση αποτυχίας του υπερεπόπτη, οι συνέπειες είναι σοβαρές, καθώς όλες οι εικονικές μηχανές που υποστηρίζονται από αυτόν ενδέχεται να διακοπούν. Συνεπώς, η επίθεση της διαφυγής της εικονικής μηχανής επιδιώκει την απόκτηση του πλήρους ελέγχου του εικονικού περιβάλλοντος παρακάμπτοντας τους υπάρχοντες μηχανισμούς απομόνωσης μεταξύ των εικονικών μηχανών. (Sane, Niang and Fall, 2018)

Επίθεση στον υπερεπόπτη (Hypervisor attack)

Η επίθεση υπερεπόπτη εκμεταλλεύεται τρωτότητες που ενδέχεται να υπάρχουν στον υπερεπόπτη, επιτρέποντας στους επιτιθέμενους να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε όλες τις εικονικές μηχανές που διαχειρίζεται ο υπερεπόπτης. Σε αντίθεση με την επίθεση διαφυγής εικονικής μηχανής, η οποία στοχεύει στην διαφυγή από την εικονική μηχανή σε άλλες VMs ή στο φυσικό σύστημα φιλοξενίας, η επίθεση στον υπερεπόπτη επικεντρώνεται στην ίδια υποδομή που διαχειρίζεται και ελέγχει τις εικονικές μηχανές. Αυτή η διαδικασία μπορεί να έχει σοβαρές συνέπειες, συμπεριλαμβανομένου της διαρροής των δεδομένων και της διακοπή των υπηρεσιών, υπονομεύοντας με αυτό τον τρόπο την συνολική ασφάλεια και την ακεραιότητα του εικονικού περιβάλλοντος (Fiveable, 2024). Οι επιτιθέμενοι θεωρούν τον υπερεπόπτη ως έναν ελκυστικό στόχο, καθώς ο υπερεπόπτης μπορεί να έχει την πρόσβαση και την εξουσία να διαχειρίζεται τόσο τις εικονικές μηχανές όσο και τους φυσικούς πόρους του υπολογιστικού συστήματος, δίνοντας έτσι την δυνατότητα στους επιτιθέμενους να επηρεάζουν και να ελέγχουν ολόκληρο το σύστημα. Παραδείγματα γνωστών επιθέσεων που εκμεταλλεύονται τον υπερεπόπτη είναι το hypejacking, το BLUEPILL, το Vitriol, το SubVir και το DKSM που ανήκουν στην κατηγορία των VM-Based Rootkits. Τα VM-Based Rootkits έχουν την δυνατότητα είτε να εισάγουν έναν κακόβουλο υπερεπόπτη δυναμικά είτε να τροποποιήσουν έναν υπάρχοντα υπερεπόπτη, επιτρέποντας στους επιτιθέμενους να αποκτήσουν τον πλήρη έλεγχο του φόρτου εργασίας του συστήματος. Σε ορισμένους υπερεπόπτες, όπως ο Xen, υπάρχει μια προνομιούχα εικονική μηχανή (Privileged VM) που λειτουργεί ως διαχειριστική διεπαφή για τον έλεγχο των άλλων εικονικών μηχανών. Αυτή η προνομιούχα εικονική μηχανή αποτελεί επίσης έναν πιθανό στόχο για τους επιτιθέμενους αφού μπορούν να εκμεταλλευτούν τα τρωτά σημεία που τυχόν υπάρχουν σε αυτήν για να αποκτήσουν

πρόσβαση στον υπερεπόπτη ή στις άλλες εικονικές μηχανές (Ibrahim, Hamlyn-Harris and Grundy, 2016).

Επίθεση μετανάστευσης εικονικής μηχανής (VM migration attack)

Η επίθεση μετανάστευσης εικονικών μηχανών είναι μια μορφή κυβερνοεπίθεσης στον ομιχλώδη προγραμματισμό που εκμεταλλεύεται την διαδικασία μετανάστευσης (migration) των εικονικών μηχανών αναμεσά σε φυσικές συσκευές του δικτύου ομίχλης. Σε περίπτωση υπερφόρτωσης μιας φυσικής συσκευής / κόμβου που εκτελεί πολλές εικονικές μηχανές, κάποιες από αυτές τις εικονικές μηχανές ενδέχεται να χρειαστεί να μεταφερθούν σε άλλες συσκευές για να αποτραπεί η υπερφόρτωση και να διασφαλιστεί η συνεχής λειτουργία του συστήματος. Κατά τη διάρκεια της μετανάστευσης, οι εικονικές μηχανές διασχίζουν το δίκτυο, εκθέτοντας τα δεδομένα τους σε κινδύνους υποκλοπής από άλλες εικονικές μηχανές / ενδιάμεσους στο ίδιο δίκτυο, εφόσον αυτά δεν κρυπτογραφούνται. Ο επιτιθέμενος, χρησιμοποιώντας των προσαρμογέα της εικονικής μηχανής του σε ακατάσχετη λειτουργία (promiscuous mode), μπορεί να συλλέξει πακέτα δεδομένων και να υποκλέψει ευαίσθητες πληροφορίες, όπως τα κρυπτογραφικά κλειδιά, τα πιστοποιητικά ή τα διαπιστευτήρια, τα οποία στη συνέχεια να τα χρησιμοποιήσει για πρόσβαση στην μεταναστευόμενη εικονική μηχανή. (Zimba and Chama, 2018)

Ο επιτιθέμενος μπορεί επίσης να οδηγήσει σε μετανάστευση μιας εικονικής μηχανής εκεί που αυτός επιθυμεί. Αυτό μπορεί να επιτευχθεί μέσω επιθέσεων DoS, ώστε να υπερφορτωθούν οι πόροι και να επιβληθεί η μετανάστευση της εικονικής μηχανής προς εκείνο το μέρος της υποδομής που «βολεύει» τον επιτιθέμενο. Μόλις ξεκινήσει η μετανάστευση, ο επιτιθέμενος συλλέγει τα δεδομένα και τα φιλτράρει για πολύτιμες πληροφορίες, οι οποίες μπορεί να χρησιμοποιηθούν για περαιτέρω επιθέσεις ή για πρόσβαση σε άλλες εικονικές μηχανές στο δίκτυο. Αν η συσκευή προορισμού στην μετανάστευση είναι υπό τον έλεγχο του επιτιθέμενου, τότε ουσιαστικά αυτός μπορεί να αποκτήσει άμεση πρόσβαση στις εικονικές μηχανές που μεταναστεύουν εκεί. Αυτή η επίθεση επηρεάζει την εμπιστευτικότητα, την διαθεσιμότητα και την ακεραιότητα των υπηρεσιών του ομιχλώδους προγραμματισμού. (Zimba and Chama, 2018)

4.3.2 Επιθέσεις ασφάλειας ιστού

Ο ομιχλώδης προγραμματισμός είναι μια νέα αναδυομένη τεχνολογία, η οποία χρησιμοποιείται για την αντιμετώπιση των συνεχόμενων αυξανομένων απαιτήσεων και των καθυστερήσεων (latency) των σύγχρονων εφαρμογών και υπηρεσιών ιστού, αλλά και των δικτυακών υπηρεσιών. Η φόρτωση μιας ιστοσελίδας, η οποία μπορεί να αποτελείται από εικόνες, υπολογιστικά φύλλα (style sheets), σενάρια (scripts), ανακατευθύνσεις (redirection) κ.α., απαιτεί πολλαπλά αιτήματα HTTP αμφίδρομης επικοινωνίας με έναν κεντρικό διακομιστή, οδηγώντας με αυτό τον τρόπο στην αύξηση του φόρτου και της καθυστέρησης του δικτύου. (Khan, Parkinson and Qin, 2017)

Εκτός από μια τέτοια επίθεση, υπάρχει μια πληθώρα άλλων επιθέσεων που μπορούν να στοχεύσουν ένα ομιχλώδες περιβάλλον μέσω του διαδικτύου. Ορισμένες από αυτές τις επιθέσεις αναλύονται παρακάτω.

4.3.2.1 Είδη επιθέσεων δικτυακών εφαρμογών στον ομιχλώδη προγραμματισμό

Έκχυση SQL (SQL Injection)

Η έκχυση SQL αποτελεί τον πιο σημαντικό τύπο ευπάθειας σε συστήματα βάσεων δεδομένων διαδικτυακών εφαρμογών (που ενδέχεται να εκτελούνται σε ομιχλώδη περιβάλλοντα). Ειδικότερα, αν δεν γίνεται σωστή επικύρωση των δεδομένων που εισάγει ο χρήστης, η εφαρμογή γίνεται ευάλωτη σε επιθέσεις έκχυσης SQL, επιτρέποντας μη εξουσιοδοτημένη πρόσβαση και τροποποίηση της υποκείμενης βάσης δεδομένων (Khan, Parkinson and Qin, 2017). Σε αυτή την επίθεση, ο εισβολέας ενσωματώνει σε απεσταλμένα δεδομένα μιας δικτυακής εφαρμογής, η οποία δεν εφαρμόζει επικύρωση δεδομένων, κακόβουλα κομμάτια κώδικα SQL, τα οποία ενοποιούνται με κανονικά ερωτήματα SQL που δημιουργεί η εφαρμογή στα πλαίσια ικανοποίησης της τρέχουσας αίτησης χρήστη. Το τροποποιημένο ερώτημα SQL που ενσωματώνει κακόβουλα μέρη στέλνεται στον διερμηνέα της βάσης δεδομένων προς άμεση εκτέλεση, διότι ο διερμηνέας εκτελεί μόνο εντολές κώδικα χωρίς να μπορεί να τις επεξεργαστεί. Με αυτόν τον τρόπο, ο επιτιθέμενος εξαπατά τον διερμηνέα, ο οποίος αναγκάζεται να εκτελέσει τις ανεπιθύμητες εντολές, δίνοντας το δικαίωμα πρόσβασης στον εισβολέα ώστε να μπορεί να τροποποιήσει ή να διαγράψει δεδομένα που υπάρχουν στην SQL βάση δεδομένων ή να αποκαλύψει ευαίσθητα δεδομένα. Στην χειρότερη περίπτωση, μια επίθεση έκχυσης SQL μπορεί να αξιοποιήσει την μη εξουσιοδοτημένη πρόσβαση στη βάση δεδομένων, ώστε να εξαπλωθεί και να προκαλέσει ζημία και σε άλλα διασυνδεμένα συστήματα με αυτήν (π.χ. μέσω κλοπής διαπιστευτηρίων χρηστών), παρακάμπτοντας μέτρα ασφάλειας, όπως είναι τα τείχη προστασίας (firewalls) (Azarkasb and Khasteh, 2023).

Cross-site scripting (XSS)

Η επίθεση XSS ανήκει στην υποκατηγορία επιθέσεων HTML έκχυσης (HTML injection). Αυτές οι επιθέσεις εκμεταλλεύονται ευπάθειες σε ιστοσελίδες ή εφαρμογές επιτρέποντας με αυτό τον τρόπο στους επιτιθέμενους να εκχέουν κακόβουλο κώδικα HTML ή JavaScript σε ιστοσελίδες, ο οποίος εκτελείται όταν οι ιστοσελίδες αυτές προβάλλονται από άλλους χρήστες. Μια επίθεση XSS μπορεί να χρησιμοποιηθεί από επιτιθέμενους για διάφορους σκοπούς (Azarkasb and Khasteh, 2023), (Khan, Parkinson and Qin, 2017):

1. Για την κλοπή των cookies ενός χρήστη, τα οποία περιέχουν πληροφορίες σύνδεσης, επιτρέποντας στους επιτιθέμενους να αποκτήσουν πρόσβαση σε λογαριασμούς χρηστών (cookie hijacking).
2. Για την μεταφόρτωση και εκτέλεση κακόβουλου κώδικα στο υπολογιστή του χρήστη μέσω εκμετάλλευσης τρωτοτήτων στο πρόγραμμα περιήγησης από κακόβουλα scripts που έχουν ενσωματωθεί στην αντίστοιχη ιστοσελίδα που επισκέπτεται ο χρήστης (drive-by attacks).
3. Για την ανακατεύθυνση των χρηστών σε κακόβουλες ιστοσελίδες (malicious redirections).

4. Για την τροποποίηση του περιεχόμενου της ιστοσελίδας με την εμφάνιση παραπλανητικών ή επιβλαβών πληροφοριών. Αυτό μπορεί να έχει να έχει ως αποτέλεσμα την εξαπάτηση των χρηστών ώστε να αποκαλυφθούν δεδομένα (π.χ. διαπιστευτήρια) ή να κάνουν κλικ σε κακόβουλους συνδέσμους (links).
5. Για την μη εξουσιοδοτημένη απευθείας πρόσβαση σε ευαίσθητα δεδομένα, όπως κωδικούς πρόσβασης και ευαίσθητες πληροφορίες (insecure direct object references).

Επίθεση πλαστογράφησης αιτήματος μεταξύ ιστοτόπων (cross-site request forgery - CSRF)

Στην επίθεση πλαστογράφησης αιτήματος μεταξύ ιστοτόπων, ο τελικός χρήστης αναγκάζεται να υποβάλει μια μη εξουσιοδοτημένη εντολή σε έναν ιστότοπτο, χωρίς ο ίδιος να το γνωρίζει ή να το εγκρίνει. Η αίτηση δημιουργείται και αποστέλλεται μέσω κακόβουλης ιστοσελίδας που εκμεταλλεύεται την αυθεντικοποίηση του χρήστη στον στόχο ιστοτόπο, συνήθως μέσω κρυμμένων αιτημάτων HTTP (όπως GET ή POST), τα οποία εκτελούνται αυτόματα στο παρασκήνιο χωρίς την άμεση γνώση ή συναίνεση του χρήστη (Kaviyazhiny, Bala and Gowri, 2021). Η επίθεση εκμεταλλεύεται την ύπαρξη ενεργών συνεδρίων (sessions) και αυθεντικοποιητικών στοιχείων (authentication tokens), όπως τα cookies, τα οποία χρησιμοποιούνται για την αναγνώριση / αυθεντικοποίηση του χρήστη. Έτσι, ακόμα και αν ο χρήστης αγνοεί μια τέτοια επίθεση, το πρόγραμμα περιήγησης αναγνωρίζει την «παράνομη» αίτηση ως έγκυρη, επειδή τα αυθεντικοποίημενα στοιχεία στέλνονται αυτόματα με κάθε αίτηση, όπως συμβαίνει όταν ο χρήστης είναι ήδη συνδεδεμένος σε έναν ιστότοπο. Αυτή η διαδικασία μπορεί να επιτρέψει στον επιτιθέμενο να εκτελεί ανεπιθύμητες ενέργειες, όπως να υποχρεώσει την ιστοσελίδα να πραγματοποιήσει χρηματικές συναλλαγές, την αποστολή προσωπικών δεδομένων κτλ., χωρίς την γνώση ή την συναίνεση του χρήστη. Για παράδειγμα, ένας χρήστης που είναι συνδεδεμένος στον τραπεζικό του λογαριασμό μπορεί, χωρίς να το αντιληφθεί, να πραγματοποιήσει μια πληρωμή μέσω μιας κακόβουλης ιστοσελίδας, η οποία υποβάλει κρυφά ένα αίτημα στον τραπεζικό διακομιστή, αξιοποιώντας τα ενεργά διαπιστευτήρια αυθεντικοποίησης του. Συχνά η CSRF επίθεση και η XSS επίθεση συγχέονται, όμως πρόκειται για διαφορετικές επιθέσεις. Στην XSS επίθεση ο επιτιθέμενος αξιοποιεί την εισαγωγή κακόβουλου κώδικα για να εκμεταλλευτεί τον χρήστη (ουσιαστικά τα δεδομένα του ή για να πραγματοποιεί ενέργειες εκ μέρους του) και έχει ως στόχο το πρόγραμμα περιήγησης του θύματος (δηλαδή έχει ως στόχο τον client μία web εφαρμογής), ενώ στην CSRF επίθεση ο επιτιθέμενος εκμεταλλεύεται την σύνδεση του χρήστη με τον ιστότοπο για να στείλει αιτήματα χωρίς να χρειάζεται να εισάγει κακόβουλο κώδικα, αλλά βασίζεται στο γεγονός ότι ο χρήστης είναι ήδη αυθεντικοποιήμενος, η αίτηση εκτελείται στο όνομα του χρήστη και έχει ως στόχο την εκτέλεση του αιτήματος στον διακομιστή μιας web εφαρμογής. (Mao, Li and Molloy, 2009)

Επίθεση πλημμύρας HTTP (HTTP flood)

Μια επίθεση πλημμύρας HTTP είναι ένας τύπος επίθεσης (D)DoS. Κατά την διάρκεια μιας τέτοιας επίθεσης, ένας επιτιθέμενος κατακλύζει τους στοχευμένους διακομιστές εφαρμογών με αιτήματα π.χ. HTTP GET ή HTTP POST. Τα πολυάριθμα αυτά αιτήματα αναγκάζουν τα νήματα σύνδεσης (connection threads) των διακομιστών να δεσμεύσουν πόρους του συστήματος προκείμενου να επεξεργαστούν τα αιτήματα αυτά. Τα αιτήματα αυτά μπορεί είτε να προέρχονται από μία πηγή είτε

πολλαπλές (π.χ. ένα botnet). Στην δεύτερη περίπτωση, η επίθεση γίνεται ακόμα πιο ισχυρή, οδηγώντας στην εξάντληση των πόρων των διακομιστών εφαρμογών, ενώ προφανώς είναι πιο δύσκολη στην αναχαίτηση της. Επομένως, η διαθεσιμότητα των διακομιστές εφαρμογών μειώνεται στο ελάχιστο, φθάνοντας σε κατάσταση άρνησης υπηρεσίας των νόμιμών χρηστών του συστήματος. Σημειώνεται εδώ πως επειδή οι κόμβοι ομίχλης είναι περιορισμένοι σε πόρους, μια τέτοια επίθεση μπορεί άνετα να τους θέσει εκτός λειτουργίας (ανάλογα βέβαια με το είδος τους), εξαντλώντας για παράδειγμα την ενέργεια τους. (Radware, 2024)

Η Slowloris είναι μια εναλλακτική επίθεση πλημμυρίσματος HTTP μπορεί να επιτρέψει σε έναν μόνο υπολογιστή να καταρρίψει έναν διακομιστή, πλημμυρίζοντας τον με ατελή HTTP αιτήματα, χωρίς να χρησιμοποιεί μεγάλο εύρος ζώνης. Η Slowloris υλοποιείται δημιουργώντας πολλαπλές συνδέσεις προς τον διακομιστή και στέλνοντας μόνο τις HTTP κεφαλίδες, χωρίς να ολοκληρώνεται πότε το κάθε HTTP αίτημα. Αυτό καταλαμβάνει όλες τις διαθέσιμες θέσεις / ουρά συνδέσεων του διακομιστή, εμποδίζοντας νέες συνδέσεις και οδηγώντας έτσι σε επίθεση DoS. Η Slowloris χρησιμοποιεί ελάχιστους πόρους και είναι δύσκολο να ανιχνευθεί. (Imperva, 2024)

Κοινωνική Μηχανική (Social Engineering)

Οι επιτιθέμενοι αποκτούν σημαντικές πληροφορίες από τους χρήστες, δημιουργώντας σχέσεις φιλίας μαζί τους ή χειραγωγώντας τους ψυχολογικά και αργότερα χρησιμοποιούν αυτές τις πληροφορίες με κακόβουλο τρόπο (π.χ. για να συνδεθούν σε εφαρμογή / υπηρεσία του νέφους εκ μέρους του θύματος). Η επίθεση ψαρέματος (phishing attack) είναι ένα είδος επίθεσης κοινωνικής μηχανικής. Στην επίθεση ψαρέματος (phishing attack), η διεύθυνση email της κύριας αρχής χρησιμοποιείται για την απόκτηση διαπιστευτηρίων και την διαρροή ευαίσθητων δεδομένων. Στην επίθεση ψαρέματος οι επιτιθέμενοι στέλνουν ψεύτικα μηνύματα που φαίνονται να προέρχονται από αξιόπιστους φορείς, όπως τράπεζες, με σκοπό να εξαπατήσουν τους χρήστες και να τους οδηγήσουν να αποκαλύψουν ευαίσθητες πληροφορίες. Όταν οι χρήστες καταχωρούν τα δεδομένα τους σε ψεύτικες ιστοσελίδες, οι επιτιθέμενοι αποκτούν τα διαπιστευτήριά τους και μπορούν να αποκτήσουν πρόσβαση σε προσωπικούς λογαριασμούς ή να κλέψουν δεδομένα (Puthal *et al.*, 2019). Άλλο ένα είδος κοινωνικής μηχανικής μηχανής είναι το spear-phishing. Αυτή είναι μια στοχευμένη μορφή ηλεκτρονικού ψαρέματος όπου οι επιτιθέμενοι χρησιμοποιούν προσωπικές πληροφορίες των χρηστών για να κάνουν το μήνυμα να φαίνεται πιο προσποιημένο και αξιόπιστο (Krombholz *et al.*, 2015).

Πειρατεία Συνεδρίας (session hijacking)

Η πειρατεία συνεδρίας είναι μια επίθεση στον κυβερνοχώρο, κατά την οποία ο επιτιθέμενος αποκτά μη εξουσιοδοτημένη πρόσβαση σε μια ενεργή συνεδρία μεταξύ ενός χρήστη και ενός διακομιστή. Αυτό συμβαίνει όταν ο επιτιθέμενος κλέβει ή προβλέπει το αναγνωριστικό συνεδρίας (session token), το οποίο χρησιμοποιείται για τα ταυτοποίησή τον χρήστη κατά την διάρκεια της επικοινωνίας. Μόλις ο επιτιθέμενος αποκτήσει το αναγνωριστικό συνεδρίας, μπορεί να εκτελέσει ενέργειες στον διακομιστή σαν να ήταν ο νόμιμος χρήστης. Ο επιτιθέμενος ενδέχεται να χάσει την πρόσβαση όταν λήξει η συνεδρία. (Okta, 2024)

Ορισμένες από της μεθόδους για την πραγματοποίηση της πειρατείας συνεδρίας περιλαμβάνουν (Okta, 2024) :

- *Session fixation:* Ο επιτιθέμενος στέλνει ένα κατάλληλα κατασκευασμένο αναγνωριστικό συνεδρίας μέσω ενός συνδέσμου. Όταν ο χρήστης κάνει κλικ σε αυτόν, ο επιτιθέμενος αποκτά πρόσβαση στην συνεδρία.
- *Session side-jacking:* Ο επιτιθέμενος παγιδεύει την μη κρυπτογραφημένη κυκλοφορία δεδομένων μεταξύ του χρήστη και του διακομιστή, συχνά σε δημόσια δίκτυα Wi-Fi.
- *Session sniffing:* Ο επιτιθέμενος παρακολουθεί την κυκλοφορία του δικτύου για να αποσπάσει αναγνωριστικά συνεδρίας που αποστέλνονται χωρίς κρυπτογράφηση.

Πειρατεία λογαριασμού (account hijacking)

Η πειρατεία λογαριασμού αναδεικνύεται ως ένα μείζον ζήτημα ασφάλειας σε επίπεδο δικτύου του ομιχλώδους προγραμματισμού (Qureshi *et al.*, 2023). Η πειρατεία λογαριασμού αναφέρεται στην παράνομη κατάληψη ενός ολόκληρου λογαριασμού χρήστη, κατά την οποία ο επιτιθέμενος κλέβει τα διαπιστευτήρια του χρήστη, όπως κωδικούς πρόσβασης για να παραβιάσει τον λογαριασμό του και να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα ή να εκτελέσει μη εξουσιοδοτημένες ενέργειες εκ μέρους του χρήστη-θύματος (Archana Lisbon and Kavitha, 2017). Η παράνομη κατάληψη ενός λογαριασμού χρήστη μπορεί να οδηγήσει σε οικονομικές απώλειες, ζητήματα ιδιωτικότητας, ενώ ταυτόχρονα ενδέχεται να επιφέρει ευρύτερες συνέπειες, όπως η απώλεια της εμπιστοσύνης του χρήστη στο σύστημα που έχει δεχτεί την επίθεση, με αποτέλεσμα την αποφυγή της περαιτέρω χρήσης του, εκτός και αν η ευθύνη της επίθεσης βαραίνει τον ίδιο τον χρήστη, όπως στην περίπτωση που διέρρευσαν οι κωδικοί του από προσωπικό λάθος. (Qureshi *et al.*, 2023).

Cryptojacking

Το cryptojacking είναι η διαδικασία κατά την οποία οι επιτιθέμενοι χρησιμοποιούν χωρίς άδεια την υπολογιστική ισχύ του θύματος για να εξορύξουν κρυπτονομίσματα. Αυτό επιτυγχάνεται μέσω κακόβουλου λογισμικού που εγκαθίσταται σε μια συσκευή (π.χ. μέσω drive-by εκφορτώσεων) ή μέσω XSS scripts, τα οποία φορτώνονται όταν ο χρήστης επισκέπτεται μια μολυσμένη ιστοσελίδα. Οι επιτιθέμενοι τοποθετούν τον κακόβουλο κώδικα εξόρυξης σε ιστοσελίδες διαφημίσεις ή ακόμα και σε νόμιμες εφαρμογές, ενώ ο κώδικας ενεργοποιείται αυτόματα όταν οι χρήστες αλληλοεπιδρούν με αυτές. Ένα παράδειγμα κακόβουλου κώδικα που χρησιμοποιείται για το cryptojacking αφορά τη χρήση βιβλιοθηκών, όπως η Coinhive, οι οποίες μπορούν να φορτωθούν εύκολα σε ιστοσελίδες ή να εκτελεστούν απευθείας σε συσκευές (π.χ. η Coinhive διαθέτει CLI προς αυτό τον σκοπό). Όταν ο κώδικας εξόρυξης ενεργοποιηθεί, το σύστημα του θύματος αρχίζει να εκτελεί υπολογιστικές διεργασίες που απαιτούνται για την εξόρυξη κρυπτονομισμάτων. Κατά την διάρκεια αυτής της διαδικασίας, οι πόροι (CPU / GPU) και η ηλεκτρική ενέργειά του χρησιμοποιείται έντονα, χωρίς το θύμα να το γνωρίζει. Τα αποτελέσματα αυτών των υπολογισμών, τα λεγόμενα «hashes» αποστέλλονται στον επιτιθέμενο, ο οποίος λαμβάνει τα κρυπτονομίσματα (π.χ. Monero) ως αντάλλαγμα για την εκμετάλλευση των πόρων του θύματος. Το cryptojacking έχει σημαντικές επιπτώσεις, καθώς επιβαρύνει το σύστημα του θύματος, προκαλώντας αργή απόδοση και υψηλή κατανάλωση ενέργειας. Παράλληλα, είναι δύσκολο να ανιχνευτεί, επειδή δεν προκαλεί

άμεσα ζημιές στο σύστημα. Αντίθετα, λειτουργεί αθόρυβα και μπορεί να παραμείνει αόρατο για μεγάλο χρονικό διάστημα, επιτρέποντας στους επιτιθέμενους να συνεχίσουν να εκμεταλλεύονται το σύστημα του θύματος για μεγάλα χρονικά διαστήματα. (Tekiner *et al.*, 2021)

4.3.3 Επιθέσεις σχετικά με την επικοινωνία εντός ή εκτός του οργανισμού / επιχείρησης

Στον ομιχλώδη προγραμματισμό οι υπολογιστικοί πόροι και οι υπηρεσίες μεταφέρονται κοντά στην άκρη του δικτύου με σκοπό την βελτίωση της απόδοσης και της απόκρισης τους. Όμως, προκύπτουν κάποια σημαντικά ζητήματα ασφάλειας, τόσο εσωτερικά όσο και εξωτερικά που αφορούν την επικοινωνία ενός οργανισμού. Είναι σημαντικό να τονίσουμε ότι οι επιθέσεις επικοινωνίας μπορεί να είναι παρόμοιες και να συμβαίνουν είτε εσωτερικά είτε εξωτερικά σε έναν οργανισμό, με αποτελέσματα να έχουν ανάλογες επιπτώσεις στην ασφάλεια των συστημάτων του. (Khan, Parkinson and Qin, 2017)

Τα εσωτερικά ζητήματα επικοινωνίας αναφέρονται στις προκλήσεις και τα προβλήματα που αντιμετωπίζουν οι οργανισμοί και τα άτομα κατά την επικοινωνία μεταξύ τους, επηρεάζοντας με αρνητικό τρόπο την ομαλή λειτουργία και την ασφάλεια του οργανισμού. Τα εσωτερικά ζητήματα επικοινωνίας μπορούν να χωριστούν σε δύο κατηγορίες: στους ανεπαρκείς κανόνες / πολιτικές (inefficient rules / policies) και στον ελλιπή έλεγχο πρόσβασης (poor access control). Οι ανεπαρκείς κανόνες και πολιτικές μπορούν να οδηγήσουν σε ασάφειες και στην ελλιπή κατανόηση των διαδικασιών από τους εργαζομένους, κάτι που αυξάνει τον κίνδυνο για εσφαλμένη διαχείριση των συστημάτων, την μη ασφαλή διαμόρφωση υπηρεσιών και την παραβίαση των πρωτοκόλλων ασφάλειας. Αυτό μπορεί να δημιουργήσει κενά ασφάλειας που θα μπορούσαν να εκμεταλλευτούν οι κυβερνοεγκληματίες, οδηγώντας σε παραβιάσεις προσωπικών δεδομένων ή σε κυβερνοεπιθέσεις. (Khan, Parkinson and Qin, 2017)

Εκτός από τις εσωτερικές απειλές που οφείλονται σε φαινόμενα privilege escalation και right abuse, υπάρχουν και άλλοι τύποι επικοινωνιακών επιθέσεων που πρέπει να ληφθούν υπόψιν, όπως οι επιθέσεις ενδιάμεσου (Man-in-the-middle) και η παραβίαση επαγγελματικών email (business email compromise). Αυτές οι επιθέσεις ενδέχεται να προκύψουν και να επηρεάσουν σοβαρά την ασφάλεια, καθώς και την ακεραιότητα των οργανισμών. (Khan, Parkinson and Qin, 2017)

Από την άλλη πλευρά, ο φτωχός έλεγχος πρόσβασης μπορεί να επιτρέψει στους χρήστες να αποκτήσουν πρόσβαση σε δεδομένα και πόρους που κανονικά δεν θα έπρεπε. Αυτό αυξάνει τον κίνδυνο για την κλοπή ευαίσθητων δεδομένων, αλλά και την πιθανότητα *επιθέσεων κλιμάκωσης δικαιωμάτων (privilege escalation),* όπου οι χρήστες με χαμηλά δικαιώματα (συμπεριλαμβανομένου ενός επιτιθέμενου που έχει κατορθώσει να διεισδύσει στο σύστημα) καταφέρνουν να αποκτήσουν (ριζική) πρόσβαση σε κρίσιμες λειτουργίες του συστήματος. Αυτό μπορεί να οδηγήσει σε τροποποίηση ή διαγραφή σημαντικών αρχείων, την ανάπτυξη κακόβουλης δραστηριότητας και την εκμετάλλευση πόρων του οργανισμού για περαιτέρω επιθέσεις.

Ειδικότερα, στο πλαίσιο συστημάτων και κόμβων, η έλλειψη αυστηρών πολιτικών πρόσβασης ή οι κακοσχεδιασμένες πολιτικές μπορεί να οδηγήσουν σε μη ασφαλή διαμόρφωση των συστημάτων και των υπηρεσιών, επιτρέποντας στους επιτιθέμενους να εκμεταλλευτούν τρωτότητες που προκύπτουν από την ανασφαλή διαχείριση και να ξεκινήσουν επιθέσεις που θέτουν σε κίνδυνο ολόκληρο το σύστημα. Επίσης, η έλλειψη αυστηρών πολιτικών πρόσβασης ή οι κακοσχεδιασμένες πολιτικές μπορεί να οδηγήσουν σε *επιθέσεις κατάχρησης δικαιωμάτων (rights abuse)* όπου εσωτερικοί χρήστες, εκμεταλλευόμενοι τα πλούσια (πέραν του δέοντος) δικαιώματα τους μπορούν να προσπελάσουν ιδιωτικές πληροφορίες άλλων χρηστών ή να εκτελέσουν ορισμένες «κακόβουλες» ενέργειες προς ικανοποίηση των στόχων τους (π.χ. κλείσιμο ή καταστροφή υπηρεσιών ή διακομιστών, εκτέλεση επιθέσεων σε άλλους οργανισμούς με πηγή τον τρέχοντα, κ.α.) (Khan, Parkinson and Qin, 2017).

Στα εξωτερικά ζητήματα επικοινωνίας, τα δεδομένα που μεταδίδονται από και προς ένα δίκτυο του ομιχλώδους προγραμματισμού είναι ευάλωτα σε επιθέσεις, όπως είναι η υποκλοπή (eavesdropping) και η αλλοίωση των δεδομένων (Khan, Parkinson and Qin, 2017). Πιο συγκεκριμένα, με την υποκλοπή ένας κακόβουλος χρήστης μπορεί να παρακολουθεί την επικοινωνία που λαμβάνει χώρα σε ένα κανάλι επικοινωνίας, καταγράφοντας τα δεδομένα που μεταδίδονται μεταξύ των συσκευών και των κόμβων ομίχλης και αποκτώντας με αυτό τον τρόπο πρόσβαση σε ευαίσθητες πληροφορίες που αφορούν τον χρήστη (Alwakeel, 2021). Αξιοποιώντας τις πληροφορίες που αποκτήθηκαν μέσω της διαδικασίας της υποκλοπής, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε μη εξουσιοδοτημένους πόρους και υπηρεσίες, είτε αυτοί βρίσκονται στο περιβάλλον του ομιχλώδους προγραμματισμού, είτε στο τοπικό περιβάλλον της επιχείρησης. Η πρόσβαση αυτή μπορεί να οδηγήσει σε παραβιάσεις ασφάλειας και επιθέσεις που υπονομεύουν την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των υπολογιστικών πόρων και δεδομένων του οργανισμού, ανεξαρτήτως του περιβάλλοντος στο όποιο βρίσκονται. Άλλες επιθέσεις που σχετίζονται με τα εξωτερικά ζητήματα επικοινωνίας είναι οι επιθέσεις ενδιάμεσου (man-in-the-middle attacks). (Khan, Parkinson and Qin, 2017).

Παρακάτω αναλύουμε ορισμένες από τις πιο σημαντικές επιθέσεις στο επίπεδο της επικοινωνίας. Πολλές από αυτές τις επιθέσεις μπορούν να συμβούν τόσο εντός όσο και εκτός ενός οργανισμού, οπότε μπορεί να αφορούν την εσωτερική ή εξωτερική επικοινωνία του οργανισμού αυτού.

Business email compromise

Η Business email compromise ή BEC είναι μια εξελιγμένη μορφή κυβερνοεπίθεσης, η οποία εκμεταλλεύεται την κοινωνική μηχανική για να εξαπατήσει επιχειρήσεις η οργανισμούς. Σε αντίθεση με άλλες μορφές κυβερνοεπιθέσεων δεν βασίζονται τόσο σε τεχνικές αδυναμίες των συστημάτων ασφάλειας, αλλά κυρίως στην εκμετάλλευση της ανθρώπινης εμπιστοσύνης και της οργάνωσης των επιχειρησιακών διαδικασιών. Στην κλασική μορφή της, οι επιτιθέμενοι χρησιμοποιούν παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου που φαίνεται να προέρχονται από αξιόπιστους αποστολείς, όπως ανώτερα στελέχη ή σημαντικούς επιχειρησιακούς συνεργάτες, με σκοπό να παραπλανήσουν τους υπάλληλούς και να τους πείσουν να εκτελέσουν ενέργειες (όπως η μεταφορά χρημάτων ή την αποκάλυψη ευαίσθητων πληροφοριών). Επίσης, μια

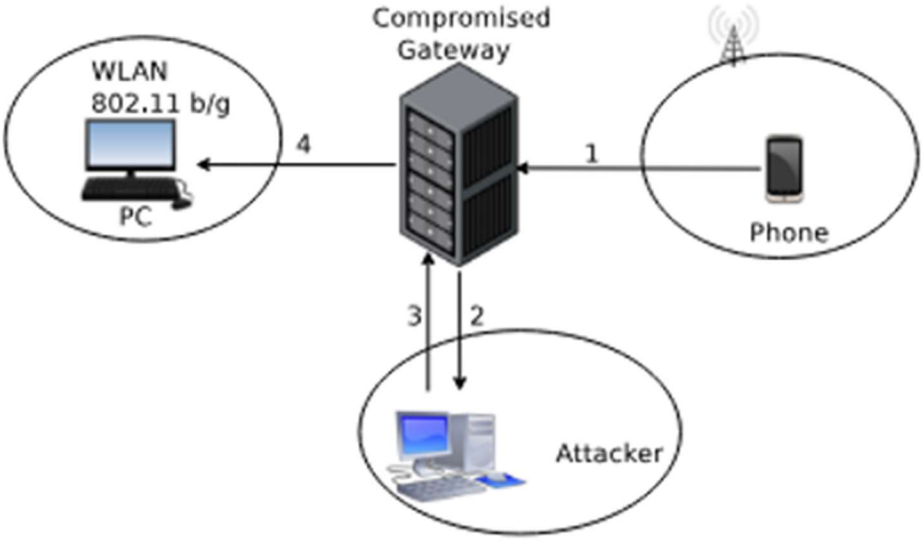
επίθεση BEC εκμεταλλεύεται καταστάσεις όπου οι ανώτεροι υπάλληλοι είναι απασχολημένοι ή εκτός γραφείου , ώστε οι υπάλληλοι να μην μπορούν να επαληθεύσουν άμεσα την αυθεντικότητα του αιτήματος, κάνοντας τους πιο πιθανό να πέσουν στην παγίδα. Ακόμα, πολλοί επιτιθέμενοι χρησιμοποιούν δωρεάν πλατφόρμες ηλεκτρονικού ταχυδρομείου, όπως το Gmail και το Yahoo, για να κάνουν τις επιθέσεις BEC πιο δύσκολες να ανιχνευτούν. Εκτός από τις οικονομικές απώλειες, οι επιθέσεις BEC μπορούν να προκαλέσουν σοβαρή ζημία στην φήμη και την αξιοπιστία μιας εταιρείας, καθώς οι εμπιστευτικές πληροφορίες που διαρρεύσουν μπορούν να χρησιμοποιηθούν σε νέες επιθέσεις ή ακόμη και για να εκβιάσουν την επιχείρηση. (Al-Musib *et al.*, 2023)

Επίθεση ενδιάμεσου (Man-in-the-Middle - MitM)

Μία επίθεση ενδιάμεσου αποτελεί ένα είδος κυβερνοεπίθεσης στην οποία ο επιτιθέμενος παρεμβάλλεται κρυφά μεταξύ των οντοτήτων που επικοινωνούν ήδη ή πρόκειται να επικοινωνήσουν. Ο επιτεθέντος εκμεταλλεύεται το υπάρχον σενάριο επικοινωνίας ή ένα που αναμένεται να πραγματοποιηθεί. Με αυτό τον τρόπο, ο επιτιθέμενος παραπλανά τις οντότητες που επικοινωνούν ή πρόκειται να επικοινωνήσουν ώστε να θεωρούν ότι η επικοινωνία τους παραμένει ασφαλής και αδιάλειπτη. Σε ορισμένες περιπτώσεις, η επικοινωνία μπορεί να ξεκινήσει από τον επιτιθέμενο, όταν αυτός προσποιείται ότι είναι ένα από τα μέρη της επικοινωνίας. Οι χρήστες του συστήματος πιστεύουν ότι τα δεδομένα τους ανταλλάσσονται απευθείας με τους νόμιμους παραλήπτες χωρίς κάποια παρεμβολή ή υποκλοπή. (Alwakeel, 2021).

Μέσω μιας επίθεσης MitM, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες χρηστών χωρίς να έχουν επίγνωση της παραβίασης (Alwakeel, 2021). Η επίθεση ενδιάμεσου μπορεί να προκαλέσει σοβαρά προβλήματα στα συστήματα του ομιχλώδους προγραμματισμού. Στον ομιχλώδη προγραμματισμό μια πύλη (gateway) μπορεί να λειτουργήσει ως κόμβος ομίχλης, ο οποίος μπορεί να παραβιαστεί ή να αντισταθεί από έναν εικονικό. Στην παρακάτω εικόνα απεικονίζεται ένα σενάριο όπου οι χρήστες με τα έξυπνα κινητά τηλεφωνά τους στέλνουν δεδομένα στον κόμβο ομίχλης. (Nath *et al.*, 2018)

Ωστόσο, οι κόμβοι ομίχλης μπορεί να παραβιαστούν, επιτρέποντας στους επιτιθέμενους να αποκτήσουν πρόσβαση στα δεδομένα που διέρχονται από αυτούς. Στην συνέχεια, οι επιτιθέμενοι, έχοντας αποκτήσει πρόσβαση στα δεδομένα μέσω της παραβίασης των κόμβων ομίχλης, τροποποιούν τα δεδομένα και τα επαναπροωθούν μέσω αυτών των κόμβων. Ως αποτέλεσμα, οι κόμβοι ομίχλης μεταδίδουν λανθασμένα δεδομένα ή δεδομένα που έχει παραβιαστεί η ακεραιότητά τους στους χρήστες, θέτοντας έτσι σε κίνδυνο τόσο τις συσκευές των χρηστών όσο και τους κόμβους ομίχλης. Η χρήση ενός μη ασφαλούς καναλιού επικοινωνίας δημιουργεί ένα περιβάλλον ευάλωτο σε επιθέσεις, καθώς ο επιτιθέμενος / ενδιάμεσος μπορεί να παρεμβάλλεται στην επικοινωνία και να προσποιείται οποιοδήποτε από τα δύο άκρα της επικοινωνίας, επιβαρύνοντας έτσι τόσο τις συσκευές όσο και τους κόμβους ομίχλης. Επιπλέον, οι κίνδυνοι δεν περιορίζονται μόνο στην κλοπή ή την τροποποίηση των δεδομένων. Ο επιτιθέμενος μπορεί να προσποιηθεί το θύμα σε υπηρεσίες και να εκτελέσει κακόβουλες ενέργειες εις βάρος του, όπως η καταστροφή των δεδομένων, η πραγματοποίηση παραγγελιών χρησιμοποιώντας τα στοιχεία διεύθυνσης του θύματος ή την μεταφορά χρημάτων σε λογαριασμούς του επιτιθέμενου. (Nath *et al.*, 2018)



Εικόνα 8 - Η επίθεση ενδιαμέσου στον ομιχλώδη προγραμματισμό, Πηγή: (Nath et al., 2018).

Επίθεση αναπαραγωγής (Replay attack)

Σε αυτή την επίθεση, ένας επιτιθέμενος καταγράφει τα πακέτα δεδομένων που μεταδίδονται στο δίκτυο και στην συνέχεια τα αναπαράγει, έτσι ώστε να τα ξαναστείλει. Η επανάληψη των παλιών πακέτων μπορεί να παραβιάσει τους μηχανισμούς επαλήθευσης του δικτύου, καθώς επιτρέπει στον επιτιθέμενο να αποκτήσει πρόσβαση σε περιορισμένες περιοχές του συστήματος (Puthal *et al.*, 2019). Αυτό του είδους οι επιθέσεις εμφανίζονται συχνά όταν οι κωδικοί πρόσβασης μεταδίδονται χωρίς κρυπτογράφηση με πρωτοκολλά, όπως το PPP (point to point protocol), POP3 (Post Office Protocol 3) και το Telnet. Αν οι επιθέσεις αναπαραγωγής δεν ανιχνευθούν μπορούν να προκαλέσουν πολλά προβλήματα, όπως οι πολλαπλές ανεπιθύμητες κλήσεις, διακοπές στην ροή του ήχου ή ακόμη και υπερβολική αύξηση των συμμετεχόντων σε κλήσεις πολλαπλών ατόμων. Μια παραλλαγή της επίθεσης αναπαραγωγής είναι η «αντιγραφή και η επικόλληση (cut-and-paste attack)» όπου ο επιτιθέμενος αντιγράφει ένα μέρος ενός πακέτου που κατέγραψε και το συνδυάζει με ένα νέο πακέτο (Johnston, 2015).

Επίθεση αναπαραγωγής κόμβων (node replication attack)

Σε μια επίθεση αναπαραγωγής κόμβων (node replication ή clone node attack) ένας επιτιθέμενος πρώτα συλλαμβάνει έναν νόμιμο κόμβο από το δίκτυο. Στη συνέχεια, χρησιμοποιώντας ειδικά εργαλεία, ο επιτιθέμενος εξάγει τα εμπιστευτικά στοιχεία του κόμβου, όπως τα αναγνωριστικά (IDs), τα δεδομένα και τα κρυπτογραφικά κλειδιά. Με τα στοιχεία αυτά ο επιτιθέμενος δημιουργεί κλωνοποιημένους κόμβους (clones) και τους εισάγει σε στρατηγικά σημεία του δικτύου με στόχο την υποκλοπή δεδομένων, την διατάραξή της λειτουργίας του δικτύου ή την πραγματοποίηση άλλων κακόβουλων ενεργειών. Επίσης, ο επιτιθέμενος μπορεί να αποσυνδέσει τον αρχικό νόμιμο κόμβο από το δίκτυο και να χρησιμοποιήσει τους κλωνοποιημένους κόμβους για να αποφύγει την ανίχνευση ή και την αφαίρεση αυτών των κλώνων από το σύστημα. Μια επίθεση αναπαραγωγής κόμβων είναι πιο εύκολο να ανιχνευθεί σε στατικά δίκτυα του ομιχλώδους προγραμματισμού, όπου

οι κόμβοι δεν μετακινούνται, καθώς οι θέσεις τους είναι σταθερές και έτσι μπορούμε να δούμε αν το ίδιο αναγνωριστικό ID ανήκει σε περισσότερους από έναν κόμβους. Αντίθετα, στα κινητά δίκτυα του ομιχλώδους προγραμματισμού είναι πιο δύσκολο να ανιχνευθούν κλωνοποιημένοι κόμβοι, καθώς αν βρεθεί το ίδιο αναγνωριστικό (ID) σε δύο διαφορετικά μέρη του δικτύου, δεν σημαίνει απαραίτητα ότι πρόκειται για κλώνο, καθώς ο κόμβος μπορεί απλώς να έχει μετακινηθεί από ένα σημείο σε ένα άλλο. (Numan *et al.*, 2020)

Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας (Distributed Denial of service attack - DDoS)

Η DDoS επίθεση είναι μια επίθεση που εξαπολύεται εναντίον ενός θύματος (συνήθως ενός εξυπηρετητή ή στην τρέχουσα περίπτωση ενός κόμβου ομίχλης) με την βοήθεια ενός μεγάλου αριθμού μηχανών, οι οποίες είναι γνωστές ως μηχανές ζόμπι (zombie machines) ή bot. Τα εν λόγω συστήματα (μηχανές ζόντι) μολύνονται με κακόβουλο κώδικα ή παραβιάζονται από τον δράστη της επίθεσης. Έπειτα, τα συστήματα αυτά ελέγχονται και συντονίζονται κεντρικά από τον εισβολέα ώστε να ξεκινήσει μια επίθεση στο μηχάνημα του θύματος με σκοπό να μειώσει τη διαθεσιμότητα του ως προς τους νόμιμους χρήστες του. (Chaudhary, Bhushan and Gupta, 2018)

Σε ένα περιβάλλον ομίχλης, μια επίθεση DDoS έχει ως σκοπό να διαταράξει την φυσιολογική λειτουργία ενός περιβάλλοντος ομίχλης, απαρτιζόμενο από μια σειρά από κόμβους ομίχλης, έχοντας ως στόχο να το κατακλύσει με μια πληθώρα αιτήσεων πρόσβασης. Σε πρώτη φάση, ο εισβολέας προσπαθεί να αποκτήσει τον έλεγχο ενός μεγάλου αριθμού από IoT συσκευές που βρίσκονται στο τερματικό επίπεδο του ομιχλώδους προγραμματισμού μέσω της εισαγωγής κακόβουλων προγραμμάτων, όπως είναι οι δούρειοι ίπποι (trojans) και οι ιοί. Εφόσον πλέον οι μολυσμένες συσκευές των χρηστών ελέγχονται με επιτυχία από τον εισβολέα, αυτός τις χρησιμοποιεί για να στείλει ένα τεράστιο αριθμό παράνομων αιτήσεων προς τους κόμβους ομίχλης δημιουργώντας μια επίθεση DDoS (An *et al.*, 2018).

Γνώστες DDoS επιθέσεις σε αυτό το επίπεδο αποτελούν επιθέσεις που βασίζονται στο πρωτόκολλο, σε δύσμορφα πακέτα, πλημμυρίσματος, ανάκλασης και ενίσχυσης. Οι επιθέσεις που βασίζονται στο πρωτόκολλο εκμεταλλεύονται σχεδιαστικές αδυναμίες ή αδυναμίες υλοποίησης ενός πρωτοκόλλου. Στην περίπτωση του πρωτοκόλλου TCP, η επίθεση SYN εκμεταλλεύεται τη διαδικασία χειραψίας στο πρωτόκολλο αυτό, στέλνοντας πολλαπλές αιτήσεις SYN με λανθασμένες πηγές προέλευσης. Το θύμα έπειτα θα προσπαθήσει να δημιουργήσει συνδέσεις με τις πηγές αυτές. Αυτό θα οδηγήσει στο γέμισμα της ουράς TCP του θύματος οπότε το θύμα δεν θα μπορεί πλέον να εξυπηρετεί τους νόμιμους πελάτες. Στην περίπτωση του πρωτοκόλλου IP, στέλνονται πακέτα IP / ping με πολύ μεγαλύτερο μέγεθος από το αναμενόμενο. Επειδή το λειτουργικό σύστημα του θύματος δεν γνωρίζει πως να χειριστεί αυτά τα πακέτα, «κρασάρει» ή επανεκινείται. (An *et al.*, 2018).

Τα δύσμορφα πακέτα έχουν περιεχόμενο που δημιουργεί προβλήματα στο σύστημα του θύματος. Συνήθως, το πρωτόκολλο εκμετάλλευσης είναι το IP. Αλλά υπάρχουν δύο διαφορετικές περιπτώσεις εκμετάλλευσης: (α) χρήση ίδιας διεύθυνσης πηγής και προορισμού – το λειτουργικό σύστημα δεν γνωρίζει πως να χειριστεί ένα τέτοιο πακέτο IP και κρασάρει & (β) χρήση όλων των

επιλογών σε ένα IP πακέτο – αυτό οδηγεί σε μεγάλη καθυστέρηση επεξεργασίας του πακέτου και προφανώς αν ένας μεγάλος αριθμός από τέτοια πακέτα σταλούν, τότε θα «γονατίσει» το σύστημα του θύματος. (Kumarasamy and Gowrishankar, 2012).

Στις επιθέσεις πλημμυρίσματος, οι επιτιθέμενοι στέλνουν έναν μεγάλο αριθμό πακέτων στο θύμα, καταναλώνοντας το διαθέσιμο εύρος ζώνης του δικτύου. Αυτό αφορά τη χρήση πρωτοκόλλων όπως UDP ή ICMP. Στις επιθέσεις ανάκλασης ο επιτιθέμενος χρησιμοποιεί πολλά ενδιάμεσα συστήματα που έχει θέσει υπό τον έλεγχό του, όπου το δίκτυο των συστημάτων αυτών έχει διαμορφωθεί ώστε να ανακλά / προωθεί ψευδείς αιτήσεις προς τον εξυπηρετητή-θύμα. Τέλος, οι επιθέσεις πλημμυρίσματος είναι παρόμοιες με τις επιθέσεις ανάκλασης αλλά είναι πιο αφόρητες. Σε αυτές τις επιθέσεις χρησιμοποιούνται πρωτόκολλα, όπως το NTP, τα οποία επιτρέπουν την διενέργεια επερωτήσεων που οδηγούν σε πολύ μεγάλες απαντήσεις. Συνεπώς, εφόσον πραγματοποιηθούν ταυτόχρονα πολλές τέτοιες επερωτήσεις, θα υπερσυμφορηθεί το σύστημα-στόχος. (Kumarasamy and Gowrishankar, 2012).

Πλαστοπροσωπία DNS (DNS Spoofing)

Η πλαστοπροσωπία DNS (DNS Spoofing ή DNS cache poisoning) είναι μια επίθεση όπου οι επιτιθέμενοι παραποιούν την κρυφή μνήμη του DNS για να παρέχουν λανθασμένες διευθύνσεις IP. Όταν ένας χρήστης προσπαθεί να επισκεφτεί μια ιστοσελίδα, ο φυλλομετρητής του ζήτα από τον εξυπηρετητή DNS την αντίστοιχη διεύθυνση IP. Αν η κρυφή μνήμη έχει δηλητηριαστεί, τότε ο εξυπηρετητής DNS επιστρέφει μια λανθασμένη διεύθυνση IP. Έτσι οι χρήστες ανακατευθύνονται σε ιστοσελίδες με κακόβουλο λογισμικό ή ψεύτικες εκδόσεις κανονικών ιστοσελίδων που μοιάζουν με τις κανονικές. Η πλαστοπροσωπία DNS συνήθως εκμεταλλεύεται το γεγονός ότι το DNS πρωτόκολλο δεν επαληθεύει την αυθεντικότητα των απαντήσεων που λαμβάνονται από DNS εξυπηρετητές, επιτρέποντας στους επιτιθέμενους να εισάγουν κακόβουλα δεδομένα στην κρυφή μνήμη του DNS. (Cloudflare, 2024)

4.3.4 Επιθέσεις ασύρματης επικοινωνίας

4.3.4.1 Εισαγωγή

Το μεγαλύτερο μέρος της επικοινωνίας στον ομιχλώδη πραγματοποιείται μέσω ασύρματων η μη συνδεδεμένων δικτύων. Τα δεδομένα μεταδίδονται μέσω των δικτύων αυτών για να φτάσουν στον προορισμό τους. Πριν φτάσουν στον τελικό προορισμό, μπορεί να προκύψουν πολλές απειλές και ζητήματα δικτυακής ασφάλειας, ιδιαίτερα όσον αφορά την ασύρματη επικοινωνία. (Kaviyazhiny, Bala and Gowri, 2021)

Η ασφάλεια του ασύρματου δικτύου σε ομιχλώδη περιβάλλοντα είναι ζωτικής σημασίας, καθώς μια επίθεση σε έναν κόμβο ομίχλης ή μια τελική συσκευή μπορεί να επηρεάσει ολόκληρη τη λειτουργία του δικτύου και να προκαλέσει σοβαρές βλάβες στο περιβάλλον ομίχλης, θέτοντας σε κίνδυνο τα δεδομένα και τις υπηρεσίες των χρηστών. Για παράδειγμα, ένας επιτιθέμενος μπορεί να

εκμεταλλευτεί μια παραβίαση σε μια τελική συσκευή για να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα ή να χρησιμοποιήσει τη συσκευή ως σημείο εισόδου για περαιτέρω επιθέσεις σε άλλους κόμβους του δικτύου, προκαλώντας σοβαρές διακοπές στις υπηρεσίες και θέτοντας σε κίνδυνο την ασφάλεια του περιβάλλοντος ομίχλης. (Ramakanth and Kumar, 2019)

Η εγκαθίδρυση και η διατήρηση της εμπιστοσύνης στον ομιχλώδη προγραμματισμό είναι κρίσιμη για την εξασφάλιση της ακεραιότητας, της διαθεσιμότητας και του απορρήτου των δεδομένων. Η εμπιστοσύνη είναι μια διαδικασία αμφίδρομης αλληλεπίδρασης μεταξύ ενός κόμβου και μιας συσκευής προκειμένου να διασφαλιστεί μια υψηλού επιπέδου ασφάλειας επικοινωνίας και συνεργασίας μεταξύ τους. Η ασφαλής επικοινωνία αποτελεί τη βάση μιας αξιόπιστης σχέσης μεταξύ των συσκευών. Ορισμένα βασικά θέματα της εμπιστοσύνης της ασύρματης επικοινωνίας στον ομιχλώδη προγραμματισμό περιλαμβάνουν την εμπιστοσύνη στην αυθεντικοποίηση του κόμβου, που αναφέρεται στη διαδικασία επαλήθευσης της αυθεντικοποίησης των κόμβων ομίχλης για να διασφαλιστεί ότι μόνο οι αξιόπιστοι κόμβοι συμμετέχουν στην επικοινωνία. Επιπλέον, η εμπιστοσύνη στην ακεραιότητα των δεδομένων είναι κρίσιμη για την διασφάλιση ότι τα δεδομένα παραμένουν αμετάβλητα και δεν παραβιάζονται κατά την μεταφορά τους. Η εμπιστοσύνη στον έλεγχο της πρόσβασης είναι επίσης απαραίτητη, εξασφαλίζοντας ότι μόνο οι εξουσιοδοτημένοι κόμβοι, στο πλαίσιο μιας εφαρμογής ή υπηρεσίας, μπορούν να επικοινωνούν μεταξύ τους, αποτρέποντας έτσι την μη εξουσιοδοτημένη πρόσβαση. Η εμπιστοσύνη στην κρυπτογράφηση εστιάζει στην αξιοπιστία των μεθόδων κρυπτογράφησης που προστατεύουν τα δεδομένα κατά την μεταφορά τους, ενώ εμπιστοσύνη στη διαχείριση των ταυτοτήτων αφορά στην ακρίβεια και την αξιοπιστία των ταυτοτήτων των κόμβων ομίχλης, αλλά και στον τρόπο διαχείρισης τους. Τέλος, η εμπιστοσύνη σε μηχανισμούς πλεονασμού και εφεδρείας εστιάζει στην αξιοπιστία των μηχανισμών που διασφαλίζουν την συνεχή διαθεσιμότητα των υπηρεσιών. (Murkomen, 2023)

Παίρνοντας τα κατάλληλα μετρά ασφάλειας για την προστασία του ασύρματου δικτύου του ομιχλώδους προγραμματισμού μπορεί να επιτευχθεί η ασφαλής και η αξιόπιστη επικοινωνία μεταξύ των κόμβων ομίχλης και των τελικών χρηστών, καθώς και μεταξύ των κόμβων ομίχλης. Αυτό δημιουργεί συνολικά μια ασφαλής υποδομή ασύρματης επικοινωνίας που παρέχει τόσο ασφάλεια όσο και εμπιστοσύνη για το ομιχλώδης περιβάλλον, προστατεύοντας το δίκτυο και τα δεδομένα που διακινούνται από τυχόν επιθέσεις. (Ramakanth and Kumar, 2019).

Στην ενότητα 4.3.4.2 ακολουθεί η ανάλυση των πιο σημαντικών επιθέσεων που αφορούν την ασύρματη επικοινωνία σε ομιχλώδη περιβάλλοντα.

4.3.4.2 Είδη επιθέσεων σχετικά με την ασφάλεια της ασύρματης επικοινωνίας στον ομιχλώδη προγραμματισμό

Επίθεση παραποίησης (tampering attack)

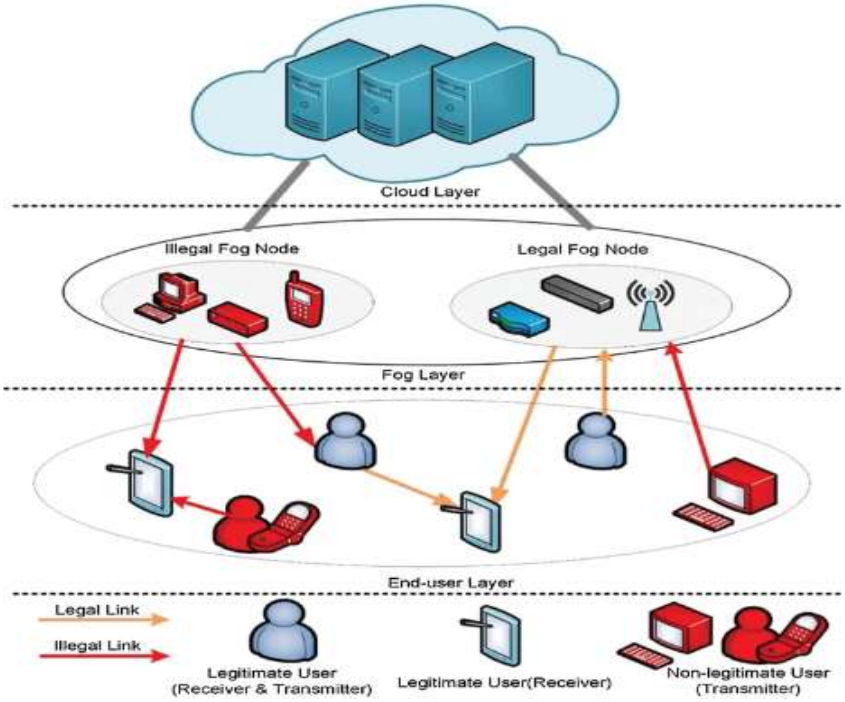
Η επίθεση παραποίησης είναι μια μορφή κυβερνοεπίθεσης κατά την οποία οι επιτιθέμενοι ενδέχεται να προχωρήσουν σε κακόβουλες ενέργειες, όπως είναι η τροποποίηση, η καθυστέρηση και η αποπομπή των μεταδιδόμενων δεδομένων, προκειμένου να υποβαθμίσουν και να διαταράξουν την απόδοση και την αποτελεσματικότητα της (ασύρματης) επικοινωνίας του ομιχλώδους προγραμματισμού. Τις περισσότερες φορές, η ανίχνευση των επιθέσεων παραποίησης καθίσταται εξαιρετικά δύσκολο να πραγματοποιηθεί από τους αναλυτές ασφάλειας ή τα συστήματα ανίχνευσης εισβολών, καθώς η κινητικότητα των χρηστών και οι συνθήκες του ασύρματου δικτύου μπορούν να προκαλέσουν αναμενόμενες καθυστερήσεις και αποτυχίες στην μετάδοση των δεδομένων. Επομένως, είναι δύσκολο να εντοπιστεί αν το πρόβλημα, όπως η αποτυχία μετάδοσης, οφείλεται σε κανονικές αλληλεπιδράσεις μεταξύ κόμβων ή σε επιθέσεις παραποίησης. (Aljumah and Ahanger, 2018)

Επίθεση εμπλοκής (jamming attack)

Η επίθεση εμπλοκής περιλαμβάνει το μπλοκάρισμα του καναλιού επικοινωνίας μεταξύ του αποστολέα και του παραλήπτη ή την διαφθορά του περιεχομένου των μηνυμάτων με ανεπιθύμητες ραδιοσυχνότητες (Kaviyazhiny, Bala and Gowri, 2021). Στόχος των εισβολέων είναι να αποτρέψουν τους νόμιμούς χρήστες να έχουν πρόσβαση σε ένα αξιόπιστο και αποδοτικό μέσο μετάδοσης, καθιστώντας τους έτσι ανίκανους να χρησιμοποιήσουν τις υπηρεσίες δικτύου με επιθυμητό τρόπο (Alwakeel, 2021). Η επίθεση εμπλοκής αποτελεί μια μορφή επίθεσης DoS, η οποία διακόπτει την μετάδοση των δεδομένων και αποτελεί σημαντική πρόκληση για τα ασύρματα δίκτυα δεδομένων (Kaviyazhiny, Bala and Gowri, 2021).

Ενεργή πλαστοπροσωπία (active impersonation)

Η ενεργή πλαστοπροσωπία (δείτε Εικόνα 9) ή επίθεσή μίμησης είναι ένας ύπουλος τύπος κυβερνοεπίθεσης και δύσκολος στην ανίχνευση του σε ένα σύστημα, όπου ένας επιτιθέμενος μιμείται μία ψεύτικη ταυτότητα μίας νόμιμης συσκευής, σημείου πρόσβασης ή οντότητας σε ένα δίκτυο. Η ενεργή πλαστοπροσωπία αποτελεί ένα παρακλάδι της επίθεσης ενδιάμεσου, διότι η παραποίηση της ταυτότητας γίνεται ενεργά και με συνεχή τρόπο ενώ στοχεύει στην υποκλοπή ή τροποποίηση των δεδομένων που ανταλλάσσονται μεταξύ συσκευών στα ασύρματα δίκτυα των ομιχλωδών περιβαλλόντων. Η επίθεση αυτή εκμεταλλεύεται έγκυρα διαπιστευτήρια νόμιμων οντοτήτων / συσκευών, ή τεχνικές εξαπάτησης (όπως ARP spoofing), καθώς και αδυναμίες πρωτοκόλλων, όπως WPA2, WEP, και Bluetooth, για να αποφύγει την διαδικασία αυθεντικοποίησης. Στον ομιχλώδη προγραμματισμό, η ενεργή πλαστοπροσωπία μπορεί να διαταράξει την επικοινωνία μεταξύ των κόμβων ομίχλης και των τερματικών συσκευών, προκαλώντας εσφαλμένη επικοινωνία, κλοπή δεδομένων ή ακόμη και διακοπή της παρεχόμενης υπηρεσίας (Pakmehr et al., 2023). Άλλες επιθέσεις που ανήκουν στην οικογένεια των επιθέσεων ενεργής πλαστοπροσωπίας είναι: η κλωνοποίηση συσκευής (device cloning), τα ψευδή σημεία πρόσβασης / σταθμοί βάσης, τα deauth μηνύματα και η επίθεση κακόβουλου διδύμου σημείου πρόσβασης (evil twin) (Κρητικός, 2023).



Εικόνα 9 - Επίθεση πλαστοπροσωπίας στον ομιχλώδη προγραμματισμό, Wan et al., 2021)

Επίθεση κακόβουλου διδύμου σημείου πρόσβασης (evil twin): είναι μια επίθεση σε ανοιχτά δίκτυα Wi-Fi όπου ένας επιτιθέμενος δημιουργεί ένα ψεύτικο σημείο πρόσβασης (access point) που μιμείται ένα Wi-Fi δίκτυο που έχει χρησιμοποιήσει ο χρήστης στο παρελθόν. Ο χρήστης συνδέεται αυτόματα στο ψεύτικο δίκτυο χωρίς να το γνωρίζει, δίνοντας στον επιτιθέμενο την δυνατότητα να υποκλέψει τα δεδομένα που στέλνει ο χρήστης ή να εισάγει κακόβουλο λογισμικό. Η επίθεση αξιοποιεί λίστες προτιμώμενων δικτύων, που επιτρέπουν την αυτόματη επανασύνδεση σε γνωστά δίκτυα, χωρίς να ελέγχουν αν το δίκτυο είναι γνήσιο ή κακόβουλο. (Gonzales *et al.*, 2010)

Κλωνοποίηση συσκευής (*device cloning):* είναι η μη εξουσιοδοτημένη αντιγραφή των χαρακτηριστικών ταυτότητας (π.χ. IMEI, MAC διεύθυνση) μιας κινητής συσκευής (π.χ. κινητό τηλέφωνο, συσκευή δικτύωσης, RFID ετικέτες) που χρησιμοποιούνται για τη δημιουργία αντιγράφου ή τη μίμηση της αρχικής συσκευής. Στο πλαίσιο της ασφάλειας εφαρμογών, η κλωνοποίηση συσκευών επιτρέπει σε κακόβουλους παράγοντες να πλαστογραφούν τον ιδιοκτήτη της αρχικής συσκευής, οδηγώντας ενδεχομένως σε κλοπή ταυτότητας και απάτη (π.χ. κακόβουλες δοσοληψίες). Εκτός από την απάτη, άλλες επιπτώσεις περιλαμβάνουν την κλοπή δεδομένων και την διατάραξη της λειτουργίας του ασύρματου δικτύου. (Promon, 2024)

Deauth μηνύματα: τα μηνύματα αυτά χρησιμοποιούνται στο πρωτόκολλο IEEE 802.11 για να τερματίσουν την σύνδεση ενός χρήστη σε ένα ασύρματο δίκτυο Wi-Fi. Επειδή τα μηνύματα αυτά δεν είναι κρυπτογραφημένα, οι επιτιθέμενοι μπορούν να τα πλαστογραφήσουν και να αναγκάσουν τις συσκευές να αποσυνδεθούν, χρησιμοποιώντας εργαλεία, όπως το aireplaying. Οι επιθέσεις με deauth μηνύματα συνήθως στοχεύουν στη διακοπή της σύνδεσης των χρηστών ή στην υποκλοπή

δεδομένων μέσω ψεύτικων δικτύων Wi-Fi. Επιπλέον, μπορεί να δημιουργήσουν συνθήκες άρνησης υπηρεσίας διότι μπορεί να εξαναγκάζουν μια συσκευή να προσπαθεί συνεχώς να συνδεθεί στο ασύρματο δίκτυο, καταναλώνοντας σημαντικούς πόρους. Τέλος, μπορεί να οδηγήσουν στην υποκλοπή δεδομένων μέσω ψεύτικων δικτύων Wi-Fi (evil twin) ή επιθέσεων επαναγκατάστασης κλειδιού (key reinstallation attacks) κατά την επανεκκίνηση της σύνδεσης. (Arora, 2018)

Επιθέσεις Κατάταξης (Rank attack)

Το πρωτόκολλο δρομολόγησης για δίκτυα χαμηλής ισχύος και απώλειας (Routing Protocol for Low Power and Lossy Networks - RPL) είναι ένα θεμελιώδης πρωτόκολλο δρομολόγησης και υποστηρίζει το 6LoWPAN, επιτρέποντας την αποτελεσματική διασύνδεση των IoT συσκευών σε δίκτυα χαμηλής ισχύος. Η επίθεση κατάταξης (rank attack) είναι μια επίθεση που στοχεύει στο χαρακτηριστικό της κατάταξης (rank) του πρωτοκόλλου RPL. Το χαρακτηριστικό αυτό είναι ζωτικής σημασίας για το πρωτόκολλο RPL, καθώς καθορίζει την σχέση μεταξύ των κόμβων του δικτύου και την απόσταση τους από ένα ριζικό κόμβο ή τον κόμβο παραλήπτη ενός μηνύματος. Με αυτό τον τρόπο διασφαλίζεται η βέλτιστη δρομολόγηση και η αποφυγή δημιουργίας βρόγχων στους κόμβους του δικτύου. Στην επίθεση αυτή, οι επιτιθέμενοι εκμεταλλεύονται την κατάταξη των κόμβων, είτε αλλάζοντας την κατάταξη τους είτε παραβιάζοντας τους κανόνες επεξεργασίας των πληροφοριών κατάταξης. Για παράδειγμα, οι κακόβουλοι κόμβοι μπορεί να παρέχουν εσφαλμένη τιμή για την κατάταξή τους, γεγονός που θα υποβαθμίσει την απόδοση του δικτύου, αυξάνοντας την καθυστέρηση και δημιουργώντας περισσότερα μηνύματα ελέγχου (control overhead), καθώς και γενικότερα υποβάθμιση του δικτύου. Επιπλέον, η επίθεση είναι δύσκολο να ανιχνευτεί, ειδικότερα όταν οι επιτιθέμενοι δεν αλλάζουν άμεσα με τις τιμές κατάταξής τους, αλλά επηρεάζουν τον τρόπο με τον οποίο το πρωτόκολλο RPL επεξεργάζεται αυτές τις πληροφορίες, παρακάμπτοντας έτσι τις παραδοσιακές μεθόδους προστασίας, όπως η κρυπτογράφηση. (Le *et al.*, 2013)

Επίθεση Sybil (Sybil attack)

Η επίθεση Sybil πραγματοποιείται όταν επιτιθέμενος δημιουργεί πολλές ψεύτικες ταυτότητες σε ένα δίκτυο, προκειμένου να παραπλανήσει το σύστημα. Αυτές οι ψεύτικες ταυτότητες ονομάζονται κόμβοι Sybil. Ειδικότερα, στην επίθεση αυτή, ο επιτιθέμενος χρησιμοποιώντας έναν μόνο κόμβο μπορεί να δημιουργεί πολλές ταυτότητες, κάνοντας το δίκτυο να πιστέψει ότι υπάρχουν παρά πολλοί κόμβοι, επιτρέποντας με αυτό τον τρόπο να παρακάμψει μηχανισμούς ασφάλειας του δικτύου (Chen and Yang, 2012). Επιπλέον, λόγω της ψευδαίσθησης ύπαρξης επιπλέον κόμβων που ελέγχονται από τον επιτιθέμενο, ο επιτιθέμενος μπορεί να επηρεάσει προς δικό του όφελος τις αποφάσεις που αφορούν τη λειτουργία του δικτύου, όπως τη δρομολόγηση μηνυμάτων, τη διενέργεια ψηφοφοριών και την επικύρωση δοσοληψιών. Η επίθεση αυτή έχει ως αποτέλεσμα να μπλοκάρεται η δυνατότητα επιλογής του πιο αποτελεσματικού συνδέσμου ή της πιο βέλτιστης διαδρομής, καθώς οι ψευδείς ταυτότητες επηρεάζουν την λήψη αποφάσεων του δικτύου. Αυτό μπορεί να οδηγήσει σε μείωση της αποδοτικότητας του δικτύου, σε αύξηση της καθυστέρησης του δικτύου, ή ακόμα και σε πλήρη αποτυχία του συστήματος σε ορισμένες περιπτώσεις. Σε ορισμένες περιπτώσεις, η επίθεση Sybil μπορεί να είναι το εφαλτήριο έναυσμα για τη διενέργεια άλλων επιθέσεων, όπως άρνησης υπηρεσίας ή ενδιάμεσου. (Puthal *et al.*, 2019)

Επίθεση άρνησης υπηρεσίας βάση διαδρομής (Path based DoS)

Έχουμε κατακλυσμό των κόμβων (αισθητήρων) κατά μήκος συγκεκριμένων μονοπατιών με την εισαγωγή επαναλαμβανόμενων και ψευδών πακέτων. Αυτή η επίθεση οδηγεί σε εξάντληση των μπαταριών, των πόρων του δικτύου και μειώνει την διαθεσιμότητα των υπηρεσιών του συστήματος. Η επίθεση υλοποιείται μέσω εκμετάλλευσης αδυναμιών στα πρωτόκολλα δρομολόγησης ή στους μηχανισμούς χειρισμού μονοπατιών, οι οποίες οδηγούν σε υπερβολική επεξεργασία και άρα δέσμευση πόρων, αδύναμη λογική δρομολόγησης και λανθασμένη επικύρωση μονοπατιών. (Puthal *et al.*, 2019)

Επίθεση Sniffing

Οι επιτιθέμενοι χρησιμοποιούν τεχνικές παρακολούθησης (sniffing) για να εξάγουν σημαντικά δεδομένα, όπως κωδικούς πρόσβασης, ηλεκτρονικά μηνύματα και FTP αρχεία. Πολλά (ασύρματα) πρωτόκολλα στο δίκτυο είναι ευάλωτα στην παρακολούθηση. (Puthal *et al.*, 2019)

Επίθεση σύλληψης κόμβου (node capture attack)

Η επίθεση σύλληψης κόμβου είναι μία από τις πιο επικίνδυνες απειλές για ασύρματα δίκτυα αισθητήρων (WSN), επειδή ο επιτιθέμενος μπορεί να αποκτήσει φυσική πρόσβαση σε έναν ή περισσότερους κόμβους του δικτύου (π.χ. λόγω ανεπάρκειας των φυσικών μέτρων ελέγχου πρόσβασης). Αρχικά, ο επιτιθέμενος «συλλαμβάνει» έναν ή περισσότερους κόμβους (αισθητήρων) από το φυσικό τους περιβάλλον. Αυτό σημαίνει ότι ο επιτιθέμενος είτε αφαιρεί τους κόμβους από την φυσική τους τοποθεσία είτε μπορεί να παραβιάσει τους κόμβους επί τόπου, ώστε να αποκτήσει τον πλήρη έλεγχο τους και να κλέψει σημαντικές πληροφορίες από την μνήμη τους, όπως τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται για την ασφαλή επικοινωνία. Με αυτά τα κλειδιά, ο επιτιθέμενος μπορεί να υποκλέψει και να αποκωδικοποιήσει την επικοινωνία στο δίκτυο, δηλαδή να παρακολουθεί και να επεμβαίνει στα δεδομένα που ανταλλάσσονται. Επίσης, μπορεί να τροποποιήσει το λογισμικό ή το υλικό των συλλαμβανόμενων κόμβων για να τους χρησιμοποιήσει σε επιθέσεις που θα επηρεάσουν ακόμη περισσότερο τους κόμβους αυτούς ή να προκαλέσει σοβαρές ζημίες στο δίκτυο π.χ. διαταραχή λειτουργίας δικτύου). Με αυτό τον τρόπο, η επίθεση σύλληψης κόμβου καταστρέφει την εμπιστευτικότητα και την ακεραιότητα του ασυρμάτου δικτύου κάνοντας το ευάλωτο σε περαιτέρω επιθέσεις. (Butani, Shukla and Silakari, 2014)

Επίθεση μαύρης τρύπας (Blackhole attack)

Ο επιτιθέμενος εισάγει έναν κακόβουλο κόμβο στο δίκτυο και εκμεταλλεύεται αδυναμίες πρωτοκόλλων δρομολόγησης ώστε να δημιουργείται μια παραπλανητική πληροφορία δρομολόγησης, δημιουργώντας τη ψευδαίσθηση πως είναι μέρος της πιο σύντομης διαδρομής. Με αυτό τον τρόπο, όλα τα πακέτα δεδομένων ανακατευθύνονται προς αυτό τον κόμβο, ο οποίος λειτουργεί ως προς μία μαύρη τρύπα. Διότι είτε εν τέλει αυτός δεν είναι προσβάσιμος (οπότε τα πακέτα «χάνονται» κατά μήκος του μονοπατιού) είτε αποπέμπει τα πακέτα που καταλήγουν σε αυτόν. Αυτό μπορεί να προκαλέσει συμφόρηση στο δίκτυο, καθώς και απώλεια πακέτων και άρα δεδομένων. (Puthal *et al.*, 2019)

Σε ένα δίκτυο υπολογιστών, μια μαύρη τρύπα (blackhole) αναφέρεται σε έναν κόμβο ή δρομολογητή που είναι μη προσβάσιμος, με αποτέλεσμα τα πακέτα που αποστέλλονται σε αυτόν να απορρίπτονται χωρίς να ειδοποιείται ο αποστολέας. Επιπλέον, δεν αποστέλνονται μηνύματα σφάλματος (π.χ. ICMP destination unreachable), επομένως ο αποστολέας δεν γνωρίζει την απώλεια δεδομένων. Σε μια στατική δρομολόγηση, η μαύρη τρύπα παραμένει μέχρι να αποκατασταθεί ο δρομολογητής ή να προσαρμοστούν οι πίνακες δρομολόγησης. Σε μια δυναμική δρομολόγηση, η μαύρη τρύπα προσομοιώνει ένα έγκυρο μονοπάτι και απορρίπτει τα πακέτα χωρίς να ειδοποιείται για την αποτυχία το δίκτυο. Σε αυτή την περίπτωση, οι υπόλοιποι δρομολογητές δεν ανιχνεύουν το πρόβλημα αμέσως, διότι δεν αποστέλλονται μηνύματα σφάλματος και τα δεδομένα χάνονται (The Network Encyclopedia, 2024).

Επίθεση σκουλικότρυπας (wormhole)

Σε αυτήν την επίθεση ένας επιτιθέμενος δημιουργεί μια «σήραγγα» μεταξύ δύο σημείων στο δίκτυο μέσω της οποίας μπορεί να μεταφέρονται πακέτα δεδομένων. Αυτή η σήραγγα μπορεί να χρησιμοποιηθεί για να παρακάμψει τους κανονικούς δρομολογητές και να κατευθύνει τα πακέτα σε έναν επιλεγμένο προορισμό (π.χ. έναν άλλο κόμβο), ο οποίος συνήθως ελέγχεται από τον επιτιθέμενο ή από τον συνεργάτη του (Puthal *et al.*, 2019). Ο προορισμός έπειτα αποστέλλει τα πακέτα που λαμβάνει, δίνοντας τη ψευδαίσθηση πως είναι μέρος της πιο σύντομης διαδρομής για αυτά. Τα αποτελέσματα της επίθεσης αυτής είναι η κλοπή των δεδομένων (εφόσον πάντα καταλήγουν σε συγκεκριμένο προορισμό που ελέγχεται από τον επιτιθέμενο) καθώς και η αποπομπή ή καθυστέρηση στην αποστολή πακέτων. Επιπλέον, η επίθεση αυτή μπορεί να οδηγήσει στη διενέργεια άλλων επιθέσεων, όπως είναι οι επιθέσεις μαύρης τρύπας και επιλεγμένης προώθησης (Κρητικός, 2023).

Επίθεση πλημμυρίσματος Hello (Hello-Flood attack)

Ο επιτιθέμενος πλημμυρίζει το κανάλι με ψευδή πακέτα δεδομένων για να ξεγελάσει τους κόμβους ώστε να νομίζουν πως είναι γείτονας τους (π.χ. χρησιμοποιώντας έναν κόμβο με μεγάλη ισχύ), ακόμη και αν βρίσκεται αρκετά μακριά τους. Αυτό προκαλεί σύγχυση στο δίκτυο και μπορεί να οδηγήσει σε σημαντική απώλεια δεδομένων ή πακέτων, διότι αυτά θα αποστέλλονται στο κενό, δηλαδή σε ένα μη προσβάσιμο κόμβο. (Puthal *et al.*, 2019)

Πλημμύρα Αναγνωρίσεων (Acknowledge Flooding)

Η επίθεση αυτή έχει δύο εκδοχές. Στην πρώτη εκδοχή, οι επιτιθέμενοι κατακλύζουν τους κόμβους με περιττά μηνύματα επιβεβαίωσης, έχοντας ως αποτέλεσμα την υπερβολική κατανάλωση των πόρων των κόμβων και σημαντικές καθυστερήσεις στην μετάδοση των δεδομένων. (Puthal *et al.*, 2019)

Στην δεύτερη εκδοχή, οι επιτιθέμενοι στέλνουν ψευδείς πληροφορίες όσον αφορά τις επιβεβαιώσεις (acknowledgements) στο επίπεδο των ζεύξεων για πακέτα που προορίζονται για γειτονικούς κόμβους, με αποτέλεσμα να ξεγελάσουν έναν κόμβο ότι μια αδύναμη ζεύξη είναι διαθέσιμη ή ότι

ένας πεθαμένος / απενεργοποιημένος κόμβος είναι ζωντανός. Αυτό έχει ως αποτέλεσμα την δημιουργία καθυστερήσεων στην αποστολή των πακέτων, την επαναποστολή των πακέτων και την απώλεια δεδομένων. (Κρητικός, 2023)

4.3.5 Επιθέσεις ασφάλειας δεδομένων

Η ασφάλεια των δεδομένων αποτελεί θεμελιώδες ζήτημα για τα συστήματα του ομιχλώδους προγραμματισμού. Η προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση κατά την διαδικασία της επεξεργασίας τους στους κόμβους ομίχλης είναι απαραίτητη. Επιπροσθέτως, κατά τη διαδικασία της επεξεργασίας, το μέγεθος, η δομή και η εγκυρότητα των δεδομένων, δύναται να υποστούν τροποποιήσεις. Εξίσου σημαντικός είναι ο έλεγχός της αξιοπιστίας των κόμβων ομίχλης, τους οποίους διαχειρίζονται διαφορετικοί πάροχοι και άτομα, καθώς τα δεδομένα υφίσταται επεξεργασίας σε αυτούς, ώστε να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητας των δεδομένων (Ramakanth and Kumar, 2019).

Παρακάτω παραθέτουμε ορισμένα συχνά είδη επιθέσεων που σχετίζονται με την ασφάλεια των δεδομένων στον ομιχλώδη προγραμματισμό.

Επίθεση Oracle

Η επίθεση oracle είναι ένας τύπος κυβερνοεπίθεσης που εκμεταλλεύεται πληροφορίες που αποκαλύπτονται μέσω της ανατροφοδότησης από το σύστημα, όπως σφάλματα ή η εγκυρότητα της προσθήκης ενός padding (συμπληρώματος) σε ένα κρυπτογραφικό μήνυμα. Ο όρος «oracle» αναφέρεται σε ένα σύστημα, το οποίο όταν δέχεται κάποιο αίτημα (π.χ. στα πλαίσια μιας επίθεσης), παρέχει κάποια ανατροφοδότηση πέρα από τα άμεσα δεδομένα σε ένα καθαρό κείμενο (π.χ. επεξηγητικά μηνύματα σφάλματος, τα οποία περιλαμβάνουν ευαίσθητες πληροφορίες, όπως ονόματα χρηστών και κωδικούς πρόσβασης ή και ενδεχομένως όλη τη στοίβα λαθών), όπου ο επιτιθέμενος μπορεί να τα χρησιμοποιήσει για να εξάγει περαιτέρω ευαίσθητες πληροφορίες. Όταν χρησιμοποιούνται συσκευές υλικού ως πηγή ανατροφοδότησης, η επίθεση μπορεί να θεωρηθεί ένας τύπος επίθεσης πλευρικού καναλιού (side-channel attack). Με την εκμετάλλευση της ελάχιστης ανατροφοδότησης από το σύστημα μέσω των μηνυμάτων για σφάλματα, τις διαφορές χρόνου ή των ενδείξεων συμπεριφοράς, οι επιτιθέμενοι μπορούν να συγκεντρώσουν πολύτιμες πληροφορίες. Για παράδειγμα, η στοίβα λαθών μπορεί να αποκαλύψει τρωτότητες μη ελέγχου δεδομένων εισόδου που μπορούν να διευκολύνουν μια επίθεση υπερχείλισης στοίβας, η οποία με τη σειρά της μπορεί να επιτρέψει την έκχυση κακόβουλου λογισμικού, όπως λυτρισμικού (ransomware), η τη διενέργεια επιθέσεων άρνησης υπηρεσίας. Ως ένα άλλο παράδειγμα, η παροχή κρυπτογραφικής ανατροφοδότησης μπορεί να επιτρέψει στον επιτιθέμενο σταδιακά με βάση τα κατάλληλα αιτήματα να εξάγει το κλειδί της κρυπτογράφησης, πράγμα το οποίο είναι καταστροφικό και μπορεί να οδηγήσει στην διαρροή ευαίσθητων δεδομένων (Packetlabs, 2024)

Οι επιθέσεις oracle συχνά σχετίζονται με κρυπτογραφία και αποτελούν απειλή, καθώς οι επιτιθέμενοι μπορούν να αξιοποιήσουν ακόμη και μικρή ανατροφοδότηση για να ανασυνθέσουν το

κρυπτογραφικό κλειδί ή να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Κάποια γνωστά παραδείγματα κρυπτογραφικών επιθέσεων oracle είναι:

- *Padding Oracle Attack*: Οι επιτιθέμενοι εκμεταλλεύονται την ανατροφοδότηση από το σύστημα σχετικά με την εγκυρότητα του padding σε κρυπτογραφημένα μηνύματα. Ένα διάσημο παράδειγμα padding oracle είναι το POODLE που εκμεταλλεύτηκε την ευπάθεια στο SSL 3.0.(Möller, Duong and Kotowicz, 2014).
- *Signature Oracle Attack:* Αφορά τις κρυπτογραφικές λειτουργίες υπογραφής και το πώς μπορεί κάποιος να εκμεταλλευτεί τη δυνατότητα υπογραφής δεδομένων για να μάθει πληροφορίες σχετικά με το ιδιωτικό κλειδί (Boneh and Boyen, 2008).
- *Oracle-Induced Side-Channel Attacks:* Σχετίζεται με τις επιθέσεις πλευρικού καναλιού, οι οποίες εκμεταλλεύονται διαφορές στην κατανάλωση πόρων του συστήματος για να αντλήσουν πληροφορίες για την κρυπτογραφική διαδικασία (Rajendran *et al.*, 2023).

Επίθεση σύγκρουσης (collision attack)

Μια επίθεση σύγκρουσης (collision attack) επικεντρώνεται ώστε να εντοπίσει δύο τιμές (εισόδου) που οδηγούν στον ίδιο κατακερματισμό (hash), χρησιμοποιώντας μια συγκεκριμένη συνάρτηση κατακερματισμού (hash function). Οφείλεται σε αδυναμίες στη σχεδίαση ή υλοποίηση μιας συνάρτησης κατακερματισμού, ιδιαίτερα όταν καθίσταται υπολογιστικά εύκολη η διερεύνηση ύπαρξης των δύο τιμών εισόδου που οδηγούν στον ίδιο κατακερματισμό. Ως αποτέλεσμα της επίθεσης αυτής, ο επιτιθέμενος μπορεί να χρησιμοποιεί ψεύτικα δεδομένα στη θέση των νόμιμων όταν έχουν τον ίδιο κατακερματισμό χωρίς αυτό να γίνει αντιληπτό. Αυτό μπορεί να οδηγήσει σε επικίνδυνες καταστάσεις στην επικύρωση της ακεραιότητας ή αυθεντικότητας των δεδομένων, όπως στην περίπτωση των ψηφιακών υπογραφών και την αυθεντικοποίηση μηνυμάτων. (Preneel, 2011)

Επίθεση σφυρί (Rowhammer attack)

Η επίθεση σφυρί εκμεταλλεύεται την συμπαγή αρχιτεκτονική της σύγχρονης δυναμικής μνήμης τυχαίας προσπέλασης (Dynamic Random Access Memory - DRAM). Η συνεχής ανάγνωση μιας σειράς μνήμης μπορεί να προκαλέσει διαρροή ηλεκτρικού φορτίου της στα κοντινά κελιά μνήμης και να οδηγήσει στην μεταβολή του περιεχομένου των κελιών μνήμης. Αυτή η επίθεση απαιτεί μόνο λογισμικό για να εκτελεστεί, ώστε ένας επιτιθέμενος να μπορέσει να χειραγωγήσει τα δεδομένα. Οι συνέπειες μιας επιτυχούς επίθεσης σφυρί μπορεί να είναι σοβαρές, όπως η κλιμάκωση προνομίων (privilege escalation), καθιστώντας την μια σημαντική απειλή για τα συστήματα που βασίζονται σε μνήμες DRAM. (Farhadi *et al.*, 2020)

Επίθεση μέσω ηλεκτρομαγνητικών εκπομπών

Η επίθεση μέσω ηλεκτρομαγνητικών εκπομπών αποτελεί μια εξειδικευμένη μορφή κυβερνοεπίθεσης που στοχεύει άμεσα στην φυσική μνήμη μιας συσκευής. Για να πραγματοποιηθεί αυτή η επίθεση πρέπει ο επιτιθέμενος πρέπει να βρίσκεται με φυσική παρουσία στον χώρο όπου τοποθετούνται οι συσκευές, έτσι ώστε να διαπεράσει τα μέτρα φυσικής ασφάλειας και να αποκτήσει

πρόσβαση σε ευαίσθητα δεδομένα. Ακόμα και χωρίς προηγμένο εξοπλισμό, ένας επιτιθέμενος μπορεί να προκαλέσει τυχαίες αλλοιώσεις στα δεδομένα της μνήμης μέσω ηλεκτρομαγνητικών παρεμβολών. (Farhadi *et al.*, 2020)

Duplicate faking attack

Το duplicate faking attack αναφέρεται σε μια επίθεση κατά την οποία ένας κακόβουλος χρήστης προσπαθεί να πείσει το σύστημα (ή τον cloud server) ότι είναι ο ιδιοκτήτης δεδομένων που στην πραγματικότητα δεν κατέχει. Αυτή η επίθεση γίνεται μέσω της αποστολής ενός ψευδούς αποδεικτικού στοιχείου (όπως ένα tag) που δείχνει ότι το δεδομένο είναι ήδη αποθηκευμένο στον διακομιστή ώστε ο επιτιθέμενος να μπορέσει να το ανακτήσει ή να το χρησιμοποιήσει χωρίς να το έχει πραγματικά μεταφορτώσει. Η επίθεση αυτή μπορεί να προκαλέσει τη δημιουργία διπλότυπων δεδομένων και να παρακάμψει μηχανισμούς ασφάλειας που βασίζονται στην ιδιοκτησία των δεδομένων, καθώς ο χρήστης προσπαθεί είτε να αποκτήσει δεδομένα που δεν του ανήκουν είτε να αποθηκεύσει διπλότυπα δεδομένα σε ένα σύστημα. Ένα γνωστό παράδειγμά της παραπάνω επίθεσης είναι η επίθεση re-join. (Jiang, Jiang and Wang, 2017)

Differential attack

Αυτή η επίθεση συγκρίνει τις μεταβολές στην είσοδο με τις αντίστοιχες μεταβολές στην κρυπτογραφημένη έξοδο για να ανακαλύψει το επιθυμητό κλειδί ή το αρχικό μήνυμα (plaintext). Συνήθως χρησιμοποιείται σε κρυπτογραφικά συστήματα που παρουσιάζουν προβλέψιμες αλλαγές στην έξοδο όταν τροποποιούνται μικρές παράμετροι της εισόδου. Με αυτόν τον τρόπο, οι επιτιθέμενοι μπορούν να μειώσουν τον αριθμό των πιθανών κρυπτογραφικών κλειδιών, να αποκαλύψουν το σωστό, "σπάζοντας" την κρυπτογράφηση. Η differential attack μπορεί να χαρακτηριστεί ως ένας υπο-τύπος της επίθεσης oracle, καθώς ο επιτιθέμενος αξιοποιεί τις διαφοροποιήσεις στις εξόδους του συστήματος, προκαλούμενες από τις τροποποιήσεις στην είσοδο, για να αποκαλύψει το κλειδί ή το αρχικό μήνυμα, εκμεταλλευόμενος έτσι την πληροφορία που παρέχουν οι παρατηρήσεις του συστήματος. (Banday, 2019)

Network Data Remanence

Οι επιθέσεις Network Data Remanence (NDR) βασίζονται στην εκμετάλλευση των υπολειμμάτων δεδομένων που παραμένουν σε διάφορα σημεία του δικτύου, όπως πακέτα που δεν έχουν διαγραφεί πλήρως ή έχουν μείνει προσωρινά σε συσκευές δικτύου. Αυτές οι επιθέσεις αποτελούν σοβαρή απειλή για την ασφάλεια των δικτύων, καθώς μπορούν να επιτρέψουν σε επιτιθέμενους να ανακτήσουν ευαίσθητες πληροφορίες από παλιά ή διαγραμμένα πακέτα δεδομένων. Οι επιτιθέμενοι μπορεί να εκμεταλλευτούν αδυναμίες στις συσκευές δικτύου, όπως δρομολογητές, διακόπτες (switches), και κάρτες δικτύου, που δεν καθαρίζουν σωστά τη μνήμη μετά τη χρήση. Τα υπολειμματικά πακέτα δικτύου, που υποτίθεται ότι έχουν απομακρυνθεί, μπορούν να ανακτηθούν με τη χρήση εξειδικευμένων τεχνικών και εργαλείων (Rashidi *et al.*, 2021)

4.3.6 Επιθέσεις κακόβουλου λογισμικού

Τα συστήματα του ομιχλώδους προγραμματισμού είναι ευάλωτα στην δραστηριότητα κακόβουλου λογισμικού, το οποίο εφόσον εκχυθεί, μπορεί να μολύνει όχι μονό έναν κόμβο αλλά όλο το σύστημα ενός ομιχλώδους περιβάλλοντος και να προκαλέσει σοβαρές ζημίες, όπως η απώλεια δεδομένων, η διακοπή της λειτουργίας υπηρεσιών, η παραβίαση ευαίσθητων προσωπικών δεδομένων, καθώς και το αυξημένο κόστος ανάκαμψης από επιθέσεις (Khan, Parkinson and Qin, 2017).

4.3.6.1 Είδη κακόβουλου λογισμικού στον ομιχλώδη προγραμματισμό

Λυτρισμικό (ransomware)

Το λυτρισμικό αποτελεί ένα τύπο κακόβουλου λογισμικού που έχει σχεδιαστεί για να κρυπτογραφεί τα δεδομένα ενός συστήματος. Μόλις τα δεδομένα κρυπτογραφηθούν, ο επιτιθέμενος ζητά λύτρα από το θύμα για την αποκρυπτογράφηση τους. Η επίθεση λυτρισμικού αποτελεί δυνητική απειλή για τους κόμβους ομίχλης, καθώς αυτοί περιέχουν συνήθως μεγάλο όγκο ευαίσθητων δεδομένων. Η μόλυνση των κόμβων ομίχλης μπορεί να οδηγήσει σε σοβαρές συνέπειες για την ασφάλεια και ειδικότερα για την διαθεσιμότητα και ακεραιότητα των δεδομένων. (Homayoun *et al.*, 2019)

Rootkits

Το κακόβουλο λογισμικό rootkit είναι ένα σύνολο προγραμμάτων που επιτρέπει σε κακόβουλους χρήστες να αποκτήσουν τον έλεγχο του δικτύου ή διάφορων διεργασιών ενός πληροφοριακού συστήματος στο επίπεδο του διαχειριστή. Το rootkit μπορεί να εκμεταλλευτεί τρωτά σημεία που υπάρχουν στο λειτουργικό σύστημα των IoT συσκευών (ή κόμβων ομίχλης) έτσι ώστε να αποκτήσει δικαιώματα διαχειριστή στο σύστημα και να εγκαταστήσει άλλα κακόβουλα προγράμματα, όπως προγράμματα λυτρισμικού (ransomware), δούρειους ίππους (trojans), bots, κ.α. Όλες οι επιθέσεις rootkits έχουν ένα κοινό χαρακτηριστικό: είναι ικανές να εντοπίζουν και να εξαπατούν συστήματα ανίχνευσης και τεχνικές ψηφιακής εγκληματολογίας. (Rawat, *et al.*, 2022)

Ιός (Virus)

Οι ιοί υπολογιστών είναι ένας τύπος κακόβουλου λογισμικού που εισάγει ένα αντίγραφο του εαυτού τους μέσα σε άλλα προγράμματα ή αρχεία ενεργού περιεχομένου, έτσι ώστε εν τέλει να εξαπλώνεται εντός της προσβεβλημένης συσκευής και ενδεχομένως από αυτήν σε μια άλλη. Οι ιοί υπολογιστών μπορούν να προκαλέσουν από ήπιες έως σοβαρές ζημίες σε ένα σύστημα, όπως είναι η καταστροφή πολύτιμών δεδομένων. Οι περισσότεροι ιοί συνδέονται άμεσα με εκτελέσιμα αρχεία (executable file), πράγμα που σημαίνει ότι ένας ιός μπορεί να βρίσκεται αδρανής σε μια συσκευή μέχρι έως ότου το πρόγραμμα φιλοξενίας του (host file) εκτελεστεί από έναν χρήστη του συστήματος. Κατά την εκτέλεση του κώδικα του προγράμματος φιλοξενίας ενεργοποιείται πρώτα ο κώδικας του ιού, ο οποίος περιλαμβάνει δύο βασικά μέρη: (α) ο κώδικας πυροδότησης και (β) κώδικας εκτέλεσης. Αρχικά, θα εκτελεστεί ο κώδικας πυροδότησης του ιού που θα τον φέρει σε αδράνεια μέχρι να συμβεί κάποιο γεγονός (π.χ. συγκεκριμένη ημερομηνία, παρουσία άλλου προγράμματος). Εφόσον συμβεί το γεγονός, ο κώδικας πυροδότησης θα εκτελέσει τον κώδικα εκτέλεσης, ο οποίος είναι υπεύθυνος για την μετάδοση του ιού και την εκτέλεση των κακόβουλων

δράσεων του. Οι ιοί εξαπλώνονται από μια συσκευή σε μία άλλη μόνο όταν το πρόγραμμα ή το έγγραφο στο οποίο είναι ενσωματωμένοι μεταφέρεται μέσω του δικτύου, ενός δίσκου, με τον διαμοιρασμό κοινών αρχείων ή μολυσμένων συνημμένων αρχείων ηλεκτρονικού μηνύματος. (Mohammed, Ibrahim and Abdulkareem, 2021)

Σκουλήκι (worm)

Το σκουλήκι είναι ένας τύπος κακόβουλου λογισμικού για δίκτυα υπολογιστών, το οποίο μοιάζει ως ένα βαθμό με τους ιούς, αφού μπορεί να αναπαράγει αντίγραφο του εαυτού του και να προκαλέσει τον ίδιο βαθμό ζημίας σε ένα σύστημα με αυτόν που μπορεί να προξενήσει ένας ιός. Τα σκουλήκια είναι αυτόνομες εφαρμογές και δεν χρειάζονται πρόγραμμα κεντρικού υπολογιστή ή ανθρώπινη βοήθεια για να διαδοθούν, σε αντίθεση με τους ιούς, που απαιτούν τη διάδοση ενός μολυσμένου αρχείου στον κεντρικό υπολογιστή. Ένα σκουλήκι μπορεί να εξαπλωθεί με διάφορους τρόπους: (α) εκμεταλλεύεται διάφορα κενά ασφάλειας, (β) με χειριστικές τεχνικές, όπως η κοινωνική μηχανική (social engineering), (γ) μπορεί να εντοπίσει διάφορες πήγες διευθύνσεων ώστε να προσπαθήσει να συνδεθεί σε αυτές, (δ) μπορεί να εντοπίσει αφαιρούμενες συσκευές για να αντιγραφεί σε αυτές και να εξαπλωθεί σε άλλα συστήματα μέσω αυτών κ.α. Ενδέχεται να εκτελεστεί όχι ένας αλλά πολλοί από αυτούς τους τρόπους ώστε να επιτευχθεί ένα ικανοποιητικό επίπεδο διάδοσης του σκουληκιού. Η διάδοση με αυτό τον τρόπο μπορεί να εξαπλώνεται εκθετικά. (Mohammed, Ibrahim and Abdulkareem, 2021)

Δούρειος ίππος στο υλικό (hardware trojan)

Ένας Δούρειος ίππος στο υλικό (hardware trojan) αναφέρεται σε μια κακόβουλη τροποποίηση του κυκλώματος ενός ολοκληρωμένου κυκλώματος (IC) κατά την διάρκεια της σχεδίασης ή της κατασκευής του, συχνά χωρίς την γνώση του αρχικού σχεδιαστή. Οι δούρειοι ίπποι είναι μικρές, κρυφές τροποποιήσεις του υλικού που ενσωματώνονται σε μεγαλύτερα συστήματα και παραμένουν σε κατάσταση αδράνειας μέχρι να ενεργοποιηθούν σε απρόβλεπτα χρονικά διαστήματα, προκαλώντας μη αναμενόμενες και κακόβουλες ενέργειες. Η εισαγωγή ενός δούρειου ίππου στο υλικό μπορεί να πραγματοποιηθεί τόσο πριν όσο και μετά την παραγωγή του ολοκληρωμένου κυκλώματος και εκτελείται από έναν επιτιθέμενο με σκοπό να επιτύχει την κρυφή και την αθέατη τροποποίηση του IC. Το συγκεκριμένο είδος δούρειου ίππου σχεδιάζεται με σκοπό να είναι αόρατο και επιβαρύνει ελάχιστα το σύστημα, καθιστώντας το εξαιρετικά δύσκολο στην ανίχνευση του. Η αρχιτεκτονική του δούρειου ίππου στο υλικό περιλαμβάνει δύο βασικά στοιχεία: τον ενεργοποιητή (trigger), ο οποίος καθορίζει ποτέ θα ενεργοποιηθεί ο δούρειος ίππος και το φορτίο (payload), το οποίο καθορίζει την κακόβουλη ενέργεια που θα εκτελεστεί όταν ενεργοποιηθεί. Όταν ενεργοποιηθεί ο δούρειος ίππος στο υλικό μπορεί να προκαλέσει σοβαρές συνέπειες, όπως η απώλειας περιούσιας ενός οργανισμού και σε σοβαρότερες περιπτώσεις απώλεια ανθρώπινων ζωών. (GeeksforGeeks, 2022)

Κατασκοπευτικό λογισμικό (spyware)

Το κατασκοπευτικό λογισμικό είναι ένα κακόβουλο λογισμικό που εγκαθίσταται σε έναν υπολογιστή χωρίς να το γνωρίζει ο χρήστης και συλλέγει δεδομένα από την συσκευή του χρήστη.

Στη συνέχεια, το κατασκοπευτικό λογισμικό στέλνει αυτά τα δεδομένα σε τρίτους, όπως είναι οι διαφημιστές ή σε κακόβουλους παράγοντες, χωρίς την συναίνεση του χρήστη με σκοπό το κέρδος. Οι πληροφορίες που συλλέγει το κατασκοπευτικό λογισμικό, ανάλογα με τις δυνατότητες του, μπορεί να περιλαμβάνουν τα δεδομένα από την περιήγηση ενός χρήστη στο διαδίκτυο, συζητήσεις μέσω email και chat, πληροφορίες συστήματος και δικτύωσης, τα στοιχεία προσωπικών καρτών, τους τραπεζικούς λογαριασμούς και τα διαπιστευτήρια σύνδεσης (τα δύο τελευταία εφόσον το λογισμικό αυτί έχει δυνατότητες keylogging ή μπορεί να «κλέβει» τα δεδομένα από αδύναμες συνδέσεις). Το κατασκοπευτικό λογισμικό είναι από τις πιο κοινές μεθόδους κυβερνοεπιθέσεων και μπορεί να είναι δύσκολο να εντοπιστεί, προκαλώντας ενδεχομένως σοβαρές επιπτώσεις τόσο στις συσκευές όσο και στα δίκτυα. Επιπλέον, μπορεί ενδεχομένως να επηρεάσει την απόδοση του υπολογιστή και να επιβραδύνει την λειτουργία του, ενώ παράλληλα εκθέτει τις επιχειρήσεις σε κινδύνους, όπως είναι οι παραβιάσεις των δεδομένων. (Fortinet, 2024)

Στην παρακάτω εικόνα φαίνεται η ιεραρχική κατηγοριοποίηση όλων των επιθέσεων της Ενότητας 4.3 της παρούσας διπλωματικής εργασία

Εικόνα 10 - Ιεραρχική κατάταξη των επιθέσεων του ομιχλώδους προγραμματισμού

4.4 Οι επιπτώσεις των επιθέσεων στον ομιχλώδη προγραμματισμό

Σε ένα περιβάλλον ομίχλης, οι υπολογιστικοί πόροι και οι υπηρεσίες βρίσκονται (επί τω πλείστο) κοντά στους χρήστες και τις συσκευές τους. Η ασφάλεια είναι πολύ σημαντική, καθώς οι επιθέσεις σε αυτά τα συστήματα μπορούν να προκαλέσουν σοβαρές επιπτώσεις. Αυτές οι επιπτώσεις δεν αφορούν μόνο την τεχνολογία και την υποδομή, αλλά επηρεάζουν την λειτουργία του συστήματος, την προστασία των δεδομένων και την απόδοση των υπηρεσιών. Σε αυτό το πλαίσιο, αντί να επικεντρωθούμε στις τεχνικές των επιθέσεων, θα εξετάσουμε τις επιπτώσεις που αυτές μπορεί να έχουν σε κάθε επιμέρους συστατικό ενός συστήματος ομίχλης, όπως το υλικό, το λογισμικό, το δίκτυο τις υπηρεσίες και τους χρήστες. Αυτή η ανάλυση θα μας επιτρέψει να κατανοήσουμε βαθύτερα τις επιπτώσεις των επιθέσεων και να αναγνωρίσουμε τις ευάλωτες περιοχές που μπορούν να επηρεάσουν κρίσιμες λειτουργίες και υπηρεσίες.

Ακολουθώντας την κατηγοριοποίηση των συστατικών μερών ενός συστήματος / περιβάλλοντος ομίχλης, μπορούμε να οργανώσουμε τις επιπτώσεις από κακόβουλες επιθέσεις ως εξής:

1. **Υλικό / υποδομή**
    - *Έλεγχος των κόμβων / συσκευών από κακόβουλους χρήστες*: Σε αυτή την απειλή κακόβουλοι χρήστες μπορούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο σύστημα και να αποκτήσουν τον έλεγχο των κόμβων ομίχλης του συστήματος θέτοντας σε κίνδυνο την ακεραιότητα και την εμπιστευτικότητα του συστήματος. (Roman, Lopez and Mambo, 2018)
    - *Ανεπαρκής υλική υποδομή:* Όταν το υλικό είναι ακατάλληλο ή υπολειτουργεί, μπορεί να οδηγήσει σε υπερφόρτωση των πόρων ή σε μη σωστή λειτουργία των εφαρμογών, επιβραδύνοντας τις διαδικασίες και μειώνοντας την απόδοση και τη διαθεσιμότητα.
    - *Διακοπή κόμβων (Node outage):* Η πλειονότητα των συσκευών σε ένα δίκτυο ενδέχεται να βγει εκτός λειτουργίας μετά από κάποια επίθεση, οδηγώντας σε απώλεια συνδεσιμότητας είτε μεταξύ των κόμβων που έχουν απομείνει, είτε των χρηστών, είτε με εξωτερικές συσκευές ή με άλλα δίκτυα (Puthal *et al.*, 2019).
    - *Καταστροφή κόμβων:* τα αδύναμα μέτρα ελέγχου φυσικής πρόσβασης μπορεί να επιτρέψουν σε έναν επιτιθέμενο να καταστρέψει πόρους ή κόμβους, όπως συσκευές δικτύωσης. Αυτό μπορεί να περιορίσει τη διαθεσιμότητα των πόρων του συστήματος και άρα και των εφαρμογών/υπηρεσιών που εκτελούνται σε αυτό (Κρητικός, 2023).
    - *Κλοπή κόμβων:* τα αδύναμα μέτρα φυσικής ασφάλειας μπορεί να οδηγήσουν και σε πραγματική κλοπή των κόμβων / συσκευών σε ένα ομιχλώδες περιβάλλον / σύστημα.
2. **Λογισμικό**
    - *Αδυναμία κλιμάκωσης*: Αν ο ενορχηστρωτής ή άλλα λογισμικά διαχείρισης πόρων υποστούν παραβίαση, αυτό μπορεί να επηρεάσει την δυνατότητα κλιμάκωσης του συστήματος.
    - *Τροποποίηση του κώδικα στο λογισμικό:* Η ακεραιότητα του κώδικα των υπηρεσιών / εφαρμογών απειλείται, με πιθανή τροποποίηση ή αλλοίωση του κώδικα, επηρεάζοντας την συνολική λειτουργικότητα και την ασφάλεια των εφαρμογών ή

των υπηρεσιών που παρέχονται από τα ομιχλώδη περιβάλλοντα. (Roman, Lopez and Mambo, 2018)

- *Μόλυνση λογισμικού:* Εφόσον μπορεί να επηρεαστεί η ακεραιότητα του κώδικα του λογισμικού, αυτό μπορεί να μολυνθεί με κακόβουλο κώδικα. Αυτό μπορεί να οδηγήσει σε διάφορες ανεπιθύμητες συνέπειες στο ομιχλώδες σύστημα.
- *Διακοπή εκτέλεσης:* Επιθέσεις, όπως υπερχείλισης στοίβας, μπορεί να οδηγήσουν στη διακοπή εκτέλεσης του λογισμικού. Όταν το λογισμικό αυτό είναι ένα λειτουργικό σύστημα ή ένας ενορχηστρωτής, αυτό σημαίνει πως οι κόμβοι μπορεί να μπουν εκτός λειτουργίας ή οι υπηρεσίες / εφαρμογής του ομιχλώδους προγραμματισμού θα παύσουν να λειτουργούν (Κρητικός, 2023).
- *Μείωση διαθεσιμότητας:* Η διαθεσιμότητα του λογισμικού μπορεί να επηρεαστεί αν οι πόροι του υποκείμενου κόμβου δεν είναι πλέον διαθέσιμοι ή αρκετά περιορισμένοι. Αυτό έχει ως συνέπεια την μείωση της διαθεσιμότητας των ομιχλωδών υπηρεσιών & εφαρμογών.
- *Απώλεια / κλοπή κώδικα:* Ο κώδικας ενδέχεται να κλαπεί, π.χ. με την μεταφορά του σε ένα αποθετήριο που ελέγχεται από τον επιτιθέμενο. Επιπλέον, μπορεί απλώς να διαγραφεί, οδηγώντας στην απώλειά του.

3. Δεδομένα / Πληροφορίες / Ιδιωτικότητα

- *Κακόβουλα δεδομένα (Malicious Data):* Όταν ένας κακόβουλος κόμβος ενσωματώνεται στο σύστημα μπορεί να εκμεταλλευτεί διαφορές ευπάθειες του συστήματος ή να βοηθήσει στην εξάπλωση κακόβουλων δεδομένων σε άλλες συνδεδεμένες συσκευές στο δίκτυο. Αυτό έχει ως αποτέλεσμα την συνολική μόλυνση του δικτύου, υποβαθμίζοντας την ασφάλεια, την ακεραιότητα και την λειτουργικότητα του. (Puthal *et al.*, 2019)
- *Αποκάλυψη δεδομένων (Data Disclosure):* Οι επιτιθέμενοι χρησιμοποιούν τεχνικές ανάκτησης / αποκάλυψης δεδομένων για να εξάγουν πληροφορίες από κόμβους, κάτι που μπορεί να οδηγήσει σε κίνδυνο παραβίασης της ιδιωτικότητας (Puthal *et al.*, 2019).
- *Απώλεια δεδομένων (Data Loss):* Η απώλεια δεδομένων μπορεί να οφείλεται σε φυσικές καταστροφές, σε ανθρώπινα λάθη ή σε κακόβουλες ενέργειες, με αποτέλεσμα την απώλεια ανεκτίμητων πληροφοριών, η οποία μπορεί να επιφέρει σημαντικές επιπτώσεις στην ομαλή λειτουργία των συστημάτων και να θέσει σε κίνδυνο την συνέχιση των παρεχόμενων υπηρεσιών. (Archana Lisbon and Kavitha, 2017)
- *Παραποίηση δεδομένων (Data Tampering):* Εφόσον επιτραπεί, π.χ. λόγω σχετικής επίθεσης, η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, αυτά μπορεί να τροποποιηθούν, οδηγώντας σε παραβίαση της ακεραιότητάς τους. Τα δεδομένα σε αυτή την περίπτωση μπορεί να είναι πλέον άκυρα (invalid) και άρα μη χρήσιμα ή μη ταυτοποιήσιμα, οδηγώντας σε αδυναμία εντοπισμού τους στο σύστημα από τον ιδιοκτήτη τους. Οπότε, ουσιαστικά, στην τελευταία περίπτωση, μπορεί να έχουμε και *απώλεια ιδιοκτησίας* των δεδομένων (Κρητικός, 2023).

- *Κλείδωμα δεδομένων (Data Lock-in):* Το κλείδωμα των δεδομένων περιορίζει την πρόσβαση σε σημαντικά δεδομένα, καθιστώντας τα προσωρινά ή μόνιμα απρόσιτα (π.χ. λόγω έκχυσης λυτρισμικού) για τους εξουσιοδοτημένους χρήστες, επηρεάζοντας την ομαλή ροή των επιχειρησιακών διαδικασιών του περιβάλλοντος ομίχλη (Karimli, 2023).
- *Διαφυγή δεδομένων (Data Remanence)*: Η διαφυγή δεδομένων, λόγω της ανεπαρκούς διαχείρισης των δεδομένων ή της ατελής διαγραφής τους, απειλεί την ακεραιότητα και την εμπιστευτικότητα των ευαίσθητων πληροφοριών των χρηστών, καθώς τα δεδομένα μπορεί να διαρρεύσουν σε μη εξουσιοδοτημένους χρήστες (Archana Lisbon and Kavitha, 2017).

4. Υπηρεσίες / Εφαρμογές

- *Μείωση διαθεσιμότητας:* Η αδυναμία πρόσβασης σε υπηρεσίες και εφαρμογές μπορεί να προκαλέσει σοβαρές επιπτώσεις σε συστήματα που απαιτούν υψηλή διαθεσιμότητα και αδιάλειπτη λειτουργία, οδηγώντας σε απώλειες για τους οργανισμούς και σε μείωση της ικανοποίησης των χρηστών.
- *Μείωση απόδοσης:* Η μειωμένη διαθεσιμότητα πόρων, η επιθέσεις άρνησης υπηρεσίας και η μη εξουσιοδοτημένη τροποποίηση του κώδικα μπορεί να οδηγήσει σε σημαντική μείωση της απόδοσης των σχετικών υπηρεσιών/εφαρμογών και σε ενδεχόμενη οικονομική ζημία, ιδιαίτερα λόγω ύπαρξης συμφωνιών (π.χ. SLA) με πελάτες που προβλέπουν χρηματικές ποινές (penalties) στην περίπτωση παραβίασης εγγυήσεων απόδοσης / διαθεσιμότητας υπηρεσίας (Κρητικός, 2023).
- *Αναξιοπιστία υπηρεσιών:* Η επίθεση σε ένα σύστημα μπορεί να μειώσει την αξιοπιστία της υπηρεσίας, κάνοντας την ασταθή ή ακατάλληλη προς χρήση και λειτουργίας.
- *Διακοπή υπηρεσίας / εφαρμογών:* Η πλήρης διακοπή μιας κρίσιμης υπηρεσίας / εφαρμογής μπορεί να έχει σοβαρές συνέπιες, όπως η αδυναμία εξυπηρέτησης των χρηστών.

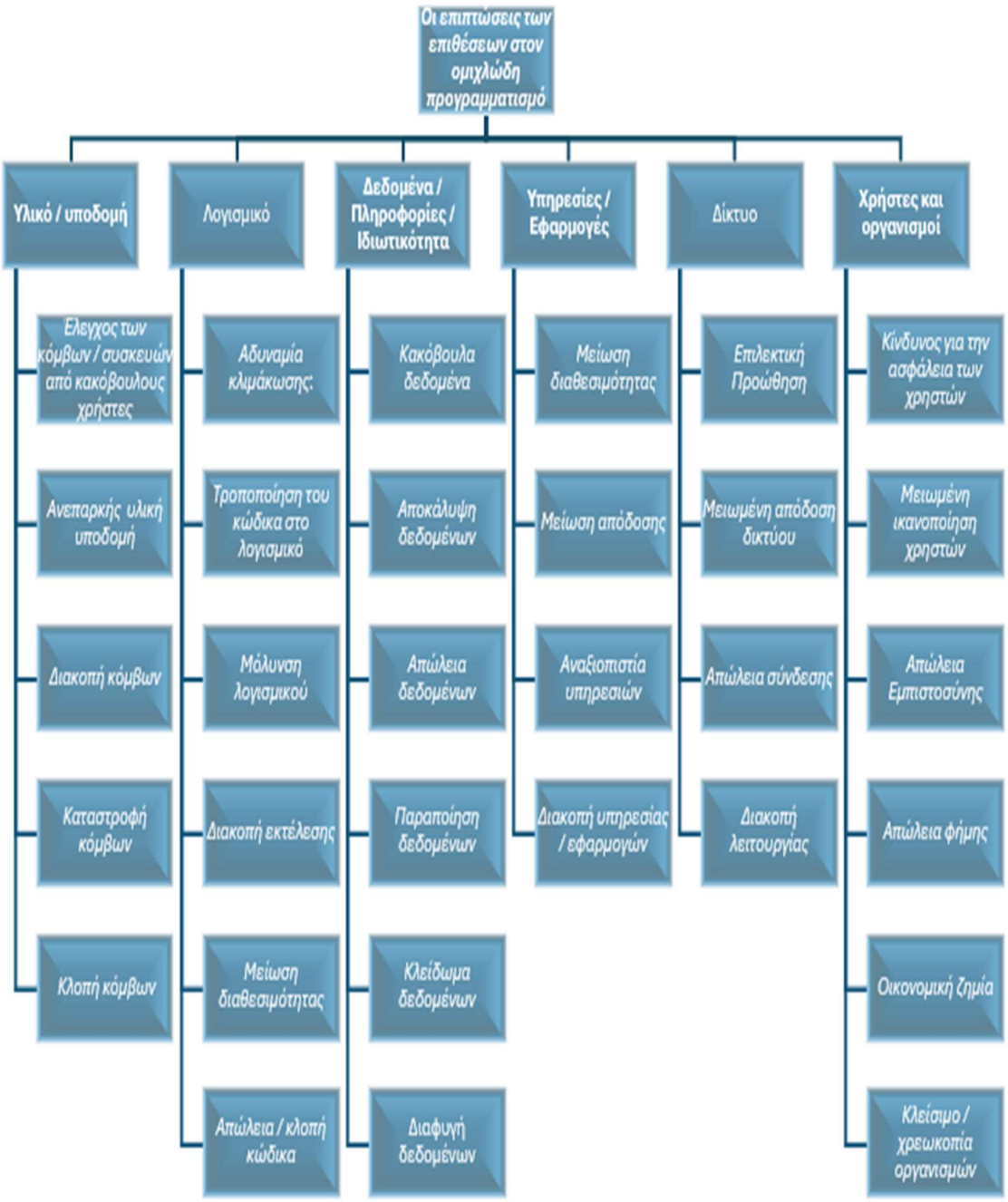
5. Δίκτυο

- *Επιλεκτική Προώθηση (Selective Forwarding):* Κάποια πακέτα δεδομένων μπλοκάρονται και δεν προωθούνται επιλεκτικά από κακόβουλους κόμβους. Οι κύριοι δύο τύποι επιθέσεων επιλεκτικής προώθησης είναι η αποπομπή πακέτων δεδομένων και η τυχαία παράλειψη της δρομολόγησης των πακέτων δεδομένων από τον μολυσμένο κόμβο (Puthal *et al.*, 2019). Αυτό μπορεί να οδηγήσει σε απώλεια των δεδομένων και μειωμένη απόδοση του δικτύου.
- *Μειωμένη απόδοση δικτύου:* Η επιβράδυνση του δικτύου ή μη σταθερότητα και διαταραχή του δικτύου μπορεί να επηρεάσει αρνητικά την ταχύτητα και την απόκριση των υπηρεσιών σε πραγματικό χρόνο του ομιχλώδους προγραμματισμού.
- *Απώλεια σύνδεσης:* Η διακοπή της επικοινωνίας και της ροής δεδομένων μπορεί να απομονώσει τα συστήματα ή να αποτρέψει την επικοινωνία μεταξύ των συσκευών. Στην πρώτη περίπτωση, ουσιαστικά έχουμε *τμηματοποίηση δικτύου* (network segmentation).

- *Διακοπή λειτουργίας:* Σε ορισμένες περιπτώσεις, η διατάραξη της λειτουργίας του δικτύου μπορεί να είναι σε τέτοιο βαθμό ώστε ουσιαστικά να πραγματοποιηθεί προσωρινή ή και μόνιμη διακοπή της λειτουργίας του.

6. Χρήστες και οργανισμοί

- *Κίνδυνος για την (φυσική ή ψηφιακή) ασφάλεια των χρηστών:* Οι εσφαλμένες πληροφορίες ή τα παραπλανητικά δεδομένα μπορεί να οδηγήσουν σε επικίνδυνες καταστάσεις για τους χρήστες, όπως για παράδειγμα οι λανθασμένες οδικές ειδοποιήσεις σε συστήματα ομιχλώδους οχηματικού υπολογισμού (fog vehicular computing) που θα μπορούσαν να προκαλέσουν ατυχήματα. ή οι εκχύσεις επιπλέον δόσεων ινσουλίνης σε ασθενείς σε ομιχλώδη συστήματα αντλίας ινσουλίνης / υγείας (fog-based healthcare systems), οδηγώντας σε ανεπιθύμητες επιπτώσεις στην υγεία των ασθενών.
- *Μειωμένη ικανοποίηση χρηστών:* Η κακή απόδοση υπηρεσιών/εφαρμογών, η υποβαθμισμένη διαθεσιμότητα και η υψηλή αναξιοπιστία μπορεί να οδηγήσουν σε σημαντική μείωση του βαθμού ικανοποίησης των χρηστών (user satisfaction).
- *Απώλεια Εμπιστοσύνης:* Οι επιθέσεις που διακυβεύουν την ιδιωτικότητα ή την ασφάλεια των χρηστών μπορεί να οδηγήσουν σε απώλεια της εμπιστοσύνης των πελατών.
- *Απώλεια φήμης:* Ένα περιστατικό ασφάλειας μπορεί να οδηγήσει σε πλήγμα στη φήμη του οργανισμού, κάτι που ενδέχεται να έχει μακροπρόθεσμες συνέπειες στην αγορά ή την μετοχική αξία.
- *Οικονομική ζημία:* Οι οργανισμοί μπορεί να υποστούν σοβαρές οικονομικές απώλειες από την διακοπή των υπηρεσιών, την μείωση της διαθεσιμότητας ή απόδοσής τους ή από τις αποζημιώσεις για την αποκατάσταση της φήμη τους.
- *Κλείσιμο / χρεωκοπία οργανισμών:* Σε ορισμένες περιπτώσεις, οι οικονομικές και ηθικές επιπτώσεις μπορεί να είναι τόσο κρίσιμες που μπορεί να οδηγήσουν σε χρεωκοπία ή κλείσιμο του οργανισμού.



Εικόνα 11 - Οι επιπτώσεις των επιθέσεων στον ομιχλώδη προγραμματισμό

4.5 Πραγματικές επιθέσεις στον ομιχλώδη προγραμματισμό

Η πανταχού παρούσα και η συνεχώς αυξανόμενη δημοτικότητα του Διαδικτύου των Πράγματων (IoT) και η ευρεία εξάπλωση των IoT συσκευών, έχουν καταστίσει τις IoT συσκευές ως μια ισχυρή ενισχυτική πλατφόρμα για κυβερνοεπιθέσεις, ειδικότερα λόγω της μεγάλής επιφανείας τρωτοτήτων και επιθέσεων που δημιουργείται σε ομιχλώδη / IoT περιβάλλοντα. Έτσι λοιπόν, αυτή η ενισχυτική πλατφόρμα βοηθάει τις κυβερνοεπιθέσεις που στοχεύουν σε IoT συσκευές και δυνητικά τους κόμβους ομίχλης να προκαλέσουν μεγαλύτερη ζημιά και να επηρεάσουν όσο των δυνατών περισσότερες συσκευές της πλατφόρμας ταυτόχρονα, αντί να στόχευαν μόνο σε ένα μεμονωμένο αριθμό συσκευών κάθε φορά (Kolias *et al.*, 2017). Πρακτικά, αυτό σημαίνει ότι αν μια IoT συσκευή / κόμβος ομίχλης έχει μολυνθεί από κακόβουλο λογισμικό μπορεί να χρησιμοποιηθεί ως ο αδύναμος κρίκος, έτσι ώστε να μολύνει τις άλλες «υγιείς» IoT συσκευές / κόμβους ομίχλης του δικτύου, καθώς και να βοηθήσει στην εφαρμογή και εξάπλωση μιας επίθεσης, όπως είναι η DDoS (Gulatas *et al.*, 2023).

Η έκθεση της εταιρείας Soniwall, αναφέρει ότι έχουν ανιχνευτεί 57 εκατομμύρια IoT συσκευές που είχαν μολυνθεί με κακόβουλο λογισμικό στο πρώτο εξάμηνο του 2022, γεγονός που υποδηλώνει αύξηση κατά 77% σε σύγκριση με το πρώτο εξάμηνο του προηγούμενου έτους. Επομένως, η παραπάνω έρευνα καταδεικνύει την αυξανομένη επικινδυνότητα που αντιμετωπίζουν οι IoT συσκευές από κακόβουλες επιθέσεις, καθώς και την επιτακτική ανάγκη για προστασία από τέτοιου είδους επιθέσεις. Πρέπει να σημειωθεί πως αν και IoT συσκευές όπου έχουν διαπιστωθεί είναι συχνότερα στόχος λόγω των τρωτοτήτων τους, όπου έχουν διαπιστωθεί ακόμη επιθέσεις τύπου zero-day, επιδεικνύοντας το υψηλό βαθμό στόχευσης σε αυτές. Επιπλέον, εκτός από τις διάφορες τρωτότητες που επιδεικνύουν, οι IoT συσκευές δεν διαθέτουν είτε καθόλου ή ελλιπείς / περιορισμένους τους μηχανισμούς άμυνας, γεγονός που τις καθιστά πιο ευάλωτες σε επιθέσεις σε σχέση με τους πιο ισχυρούς υπολογιστικά κόμβους ομίχλης, οι οποίοι μπορεί να εφαρμόζουν καλύτερους μηχανισμούς άμυνας, όταν οι επιτιθέμενοι καταλάβουν τον έλεγχο των IoT συσκευών, αυτές μπορούν να χρησιμοποιηθούν για την διενέργεια επιθέσεων, όπως οι επιθέσεις DDoS, τόσο στους κόμβους ομίχλης όσο και στις υπηρεσίες και τις εφαρμογές που φιλοξενούνται στους κόμβους αυτούς. (Gulatas *et al.*, 2023)

4.5.1 Θεωρητική ανάλυση επιθέσεων

4.5.1.1 Θεωρητική ανάλυση της επίθεσης DDoS

Οι κόμβοι ομίχλης είναι διασκορπισμένοι σε διάφορες τοποθεσίες σε ένα ομιχλώδης περιβάλλον ενώ κάθε κόμβος ομίχλης εξυπηρετεί κάθε φορά ένα μοναδικό σύνολο συσκευών. Επίσης, οι δυνατότητες των κόμβων ομίχλης διαφέρουν μεταξύ τους ως προς την ισχύ επεξεργασίας, το μέγεθος μνήμης και το εύρος ζώνης. Αυτή η διαφοροποίηση στους κόμβους ομίχλης προκαλεί διαφορές ευπάθειες τις οποίες μπορούν να εκμεταλλευτούν οι επιτιθέμενοι, όπως είναι οι επιθέσεις

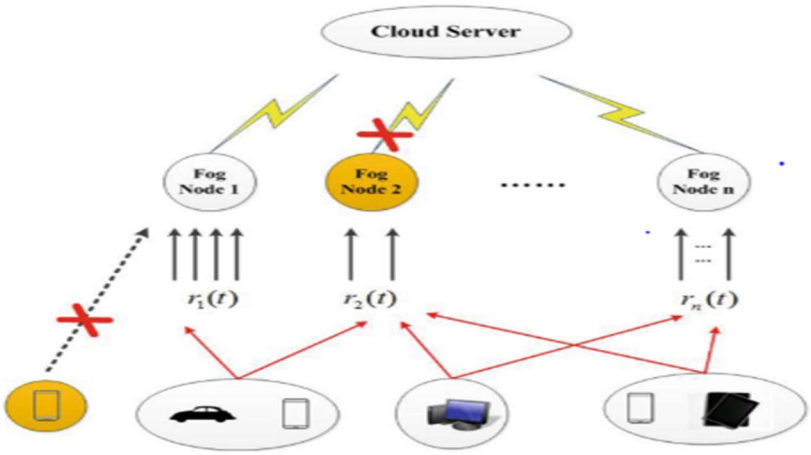
DDoS. Ο επιτιθέμενος θα ξεκινήσει μια κατανεμημένη επίθεση DDoS σε μια συγκεκριμένη χρονική στιγμή t, ενώ διαφορετικοί κόμβοι I (δηλαδή μηχανήματα και συσκευές υπό τον έλεγχο του επιτιθέμενου, όπως IoT συσκευές) θα ενεργοποιηθούν σταδιακά σε διαφορετικές χρονικές στιγμές $r_i(t)$ για να ενισχύσουν την επίθεση. Η επίθεση DDoS στους κόμβους ομίχλης έχει σημαντικές συνέπειες, όπως περιγράφονται παρακάτω και όπως απεικονίζονται στην παρακάτω εικόνα. (An *et al.*, 2018)

Τα βήματα μιας τέτοιας επίθεσης είναι τα ακόλουθα (An *et al.*, 2018):

- Ο επιτιθέμενος μπλοκάρει τον τρόπο με τον οποίο οι νόμιμοι χρήστες προσπαθούν να συνδεθούν σε έναν κόμβο ομίχλης είτε καταλαμβάνοντας είτε παρεμβάλλοντας την θύρα του δικτύου του κόμβου ομίχλης. Αυτό μπορεί να γίνει μέσω επιθέσεων, όπως η επίθεση MiTM, με την κατάληψη θυρών και με την εκμετάλλευση των ευπαθειών που υπάρχουν στα πρωτόκολλα επικοινωνίας.
- Ο επιτιθέμενος στέλνει έναν τεράστιο αριθμό παράνομων αιτημάτων σε έναν κόμβο ομίχλης, καταλαμβάνοντάς ουσιαστικά την θύρα του δικτύου. Καθώς ο κόμβος δεν μπορεί να διαχειριστεί τον υπερβολικό αριθμό αιτημάτων, αυτό έχει ως αποτέλεσμα να υπερφορτώνεται, αδυνατώντας να μπορεί να λειτουργήσει κανονικά και οδηγώντας έτσι στην διακοπή λειτουργίας του συστήματος.

Ένας επιτιθέμενος που παραβιάζει συσκευές ή τους κόμβους ομίχλης μπορεί να τους χρησιμοποιεί είτε μεμονωμένα είτε σε συνδυασμό με άλλες IoT συσκευές και άλλους κόμβους ομίχλης για την επιτυχή διενέργεια μιας DDoS επίθεσης. Αυτή η παραβίαση είναι ένα προπαρασκευαστικό βήμα, το οποίο πραγματοποιείται μέσω άλλων επιθέσεων με στόχο την κατάληψη του ελέγχου των συσκευών, ώστε να χρησιμοποιηθούν σε μεταγενέστερο στάδιο για επιθέσεις μεγάλης κλίμακας. (An *et al.*, 2018).

Στόχος του επιτιθέμενου είναι να κατευθύνει τον τεράστιο όγκο δεδομένων προς έναν στόχο, προκαλώντας συμφόρηση στο δίκτυο και καθιστώντας το μη προσβάσιμο. Όταν ένας κόμβος ομίχλης είναι υπερφορτωμένος με παράνομα αιτήματα δεν είναι σε θέση να εξυπηρετήσει τους αρχικούς νόμιμους χρήστες, οι οποίοι δεν μπορούν να αποκτήσουν πρόσβαση σε υπηρεσίες που χρειάζονται. Ο επιτιθέμενος μπορεί να αποτρέψει σε έναν κόμβο ομίχλης να επικοινωνεί με αλλά επίπεδα του συστήματος του ομιχλώδους προγραμματισμού, όπως το τερματικό επίπεδο καθώς και το επίπεδο του νέφους. Επίσης, η επίθεση DDoS μπορεί να στοχεύει σε άλλους κόμβους ομίχλης, με σκοπό να παραλύσει κρίσιμες υπηρεσίες ή εφαρμογές σε τοπικό επίπεδο. Ακόμα, οι κόμβοι ομίχλης μπορούν να εκτοξεύσουν μια επίθεσή DDoS σε έναν ιστότοπο ή σε μια υπηρεσία νέφους, προκαλώντας διακοπή ή αδυναμία πρόσβασης σε κεντρικούς διακομιστές ή πλατφόρμες (π.χ. σε διαδικτυακές υπηρεσίες, κοινωνικά δίκτυα κ.α.). Ο συνδυασμένος έλεγχος πολλών κόμβων (δηλαδή IoT συσκευών και κόμβων ομίχλης) καθιστά την επίθεση DDoS πιο δύσκολη στην ανίχνευση της και την αντιμετώπιση της, ενώ ταυτόχρονα αυξάνει την ισχύ της. Επομένως, μια επίθεση DDoS μπορεί να οδηγήσει σε σημαντική μείωση της απόδοσης και της διαθεσιμότητας των υπηρεσιών που παρέχονται από τους κόμβους ομίχλης, δημιουργώντας σοβαρά προβλήματα στην λειτουργικότητα του δικτύου / περιβάλλοντος του ομιχλώδους προγραμματισμού (An *et al.*, 2018).



Εικόνα 12 - Οι επιπτώσεις της επίθεσης DDoS στον ομιχλώδη προγραμματισμό, Πηγή: (An et al., 2018).

4.5.2 Επιθέσεις

4.5.2.1 Mirai Botnet

Το Mirai Botnet είναι από τα πιο γνωστά και επικίνδυνα IoT botnets που έχουν επηρεάσει τον κυβερνοχώρο τα τελευταία χρόνια (Gulatas *et al.*, 2023). Το Mirai Botnet ανήκει στην οικογένεια κακόβουλου λογισμικού τύπου σκουληκιού (worm) και εκμεταλλεύεται τις ευπάθειες των IoT συσκευών για να τις μετατρέψει σε απομακρυσμένα ελεγχόμενα bots ικανά να μπορούν να εξαπολύσουν επιθέσεις DDoS με σκοπό να κάνουν διαφορές υπηρεσίες του διαδικτύου μη προσβάσιμες (Radware, 2024), (Antonakakis *et al.*, 2017).

Τον Σεπτέμβριο του 2016, η ιστοσελίδα του συμβούλου ασφάλειας Brian Krebs δέχτηκε επίθεση με ρυθμό κίνησης δεδομένων 620 Gbps, δηλαδή έναν αρκετά μεγαλύτερης τάξης μεγέθους ρυθμό σε σύγκριση με το συνηθισμένο ρυθμό που απαιτείται έτσι ώστε να τεθούν εκτός λειτουργίας αρκετοί ιστότοποι. Την ιδία περίοδο, σημειώθηκε ακόμη μια μεγάλη επίθεση DDoS στην OVH, η οποία χρησιμοποιούσε το Mirai κακόβουλο λογισμικό και έφτασε σε ρυθμούς κίνησης δεδομένων τα 1.1 Tbps. (Antonakakis *et al.*, 2017)

4.5.2.2 Η επίθεση DDoS στον πάροχο υπηρεσιών διαδικτύου Dyn

Το 2016, η επίθεση DDoS που πραγματοποιήθηκε στο Dyn, έναν πάροχο υπηρεσιών διαδικτύου (ISP), αποτέλεσε ένα κρίσιμο σημείο στην ιστορία της ασφάλειας του κυβερνοχώρου. Η επίθεση αυτή ξεκίνησε από μια στρατιά μικρών, παραβιασμένων IoT συσκευών, όπως εκτυπωτές, web κάμερες, βρεφικές συσκευές παρακολούθησης κ.α., οι οποίες θεωρούνταν αρχικά ακίνδυνες. Ωστόσο, οι συσκευές αυτές οι συσκευές παρουσίαζαν συγκεκριμένες τρωτότητες, όπως αδύναμους ή προκαθορισμένους κωδικούς και μη ενημερωμένο λογισμικό, που τις καθιστούσαν

εκμεταλλεύσιμες από κακόβουλους χρήστες. Στη συνέχεια αποδείχθηκε ότι αυτές οι παραβιασμένες IoT συσκευές μπορούν να μετατραπούν σε όπλα επίθεσης κακόβουλου λογισμικού. (Junejo, 2019)

Για την πραγματοποίηση της μεγαλύτερης επίθεσης DDoS στην ιστορία χρησιμοποιήθηκε το botnet «Mirai», γνωστή και ως επίθεση DDoS Mirai, η οποία επηρέασε τους μεγαλύτερους οργανισμούς και υπηρεσίες. Οι παραβιασμένες IoT συσκευές δημιουργήσαν ένα τεράστιο botnet, το οποίο αφού πρώτα βομβάρδισε τους διακομιστές της Dyn, κατάφερε να οδηγήσει στην κατάρρευση ολόκληρης της υποδομής του δικτύου. Κατά την διάρκεια αυτής της επίθεσης, διάφορες ιστοσελίδες κοινωνικών μέσων, όπως το Twitter και το Facebook, καθώς και άλλες ιστοσελίδες ή υπηρεσίες, όπως PayPal, Amazon και Netflix, ήταν εκτός λειτουργίας ή μη προσβάσιμες για παρά πολλές ώρες. Επειδή τα συστήματα του ομιχλώδους προγραμματισμού συνδέονται στενά με τις IoT συσκευές, είναι ευάλωτα σε τέτοιου είδους επιθέσεις και άρα πρέπει να εφαρμοστούν μέτρα για την αποτροπή τους. (Junejo, 2019)

4.5.2.3 IoT Reaper

Το 2017 η Checkpoint, μια ισραηλινή εταιρεία ασφάλειας εντόπισε ένα καινούργιο botnet με την ονομασία IoT Reaper ή IoTroop. Το IoT Reaper είναι μια εξελιγμένη μορφή του Mirai και μπορεί να εκμεταλλευτεί 9 γνωστές τρωτότητες, δηλαδή περισσότερες ευπάθειες σε σχέση με το Mirai. Το botnet Reaper μέχρι στιγμής έχει μολύνει πάνω από 2 εκατομμύρια συσκευές (Zahra and Chishti, 2020). Για παράδειγμα, το IoT Reaper χρησιμοποιήθηκε το 2018 για την εκτέλεση μιας DDoS επίθεσης με την χρήση ενός botnet σε χρηματοπιστωτικές υπηρεσίες στην Ολλανδία (Dwyer *et al.*, 2019). Εξαιτίας της κατανεμημένης φύσης του ομιχλώδους προγραμματισμού, η επεξεργασία των δεδομένων διαμοιράζεται σε περισσότερες από μία συσκευές, γεγονός που αυξάνει σημαντικά την πιθανότητα να πραγματοποιηθούν περισσότερες επιθέσεις. Το Reaper, ως IoT botnet, εκμεταλλεύεται ακριβώς αυτή την αύξηση της επιφάνειας επίθεσης, σαρώνοντας και μολύνοντας ευάλωτες συσκευές σε ευρεία κλίμακα. (Zahra and Chishti, 2020)

4.5.2.4 Mozi botnet

Το Mozi IoT κακόβουλο λογισμικό (malware) εμφανίστηκε στο διαδίκτυο στα τέλη του 2019 και έχει καταφέρει να μολύνει πάνω από 1.5 εκατομμύρια IoT συσκευές, δημιουργώντας έτσι ένα εκτεταμένο δίκτυο υπολογιστών (botnet) ικανό να εκτελεί επιθέσεις (DDoS) μεγάλης κλίμακας. Αυτός ο ιός ξεχώρισε για την εξαιρετικά υψηλή δραστηριότητα του, καθώς παρήγαγε περισσότερη κίνηση επιθέσεων το 2020 συγκριτικά με οποιαδήποτε άλλο κακόβουλο IoT λογισμικό. (Sahota and Vlajic, 2021)

Αν και το Mozi botnet βασίζεται σε προηγούμενες οικογένειες ιών, όπως Mirai, Gargyt και IoT Reaper, παρουσιάζει μια σημαντική καινοτομία: την υιοθέτηση της αρχιτεκτονικής δικτύωσης τύπου peer-to-peer (P2P) (Sahota and Vlajic, 2021). Σε αντίθεση, με τις προηγούμενες απειλές (Mirai και Gargyt), το Mozi botnet επιτρέπει στις μολυσμένες συσκευές να επικοινωνούν απευθείας μεταξύ τους, δημιουργώντας ένα πιο ανθεκτικό και ευέλικτο δίκτυο από botnets. Η αποκεντρωμένη

φύση του Mozi botnet καθιστά εξαιρετικά δύσκολή την εξουδετέρωση του, καθώς η απουσία ενός ενιαίου σημείου ελέγχου απαιτεί μια πιο πολύπλοκη και ολοκληρωμένη στρατηγική αντιμετώπισης. Η επιτυχία του Mozi botnet αποδεικνύεται από την ταχεία εξάπλωση του, καθώς κατάφερε να μολύνει πάνω από 15.000 συσκευές μόνο σε διάστημα τεσσάρων μηνών (Ioulianou, 2021). Ένα γνωστό περιστατικό με το Mozi botnet συνέβη στα τέλη του 2019, όταν ανακαλύφθηκε από τους ερευνητές της 360 Netlab, που εντόπισαν ότι το Mozi στόχευε σε δρομολογητές (routers), οι οποίοι είχαν κατασκευαστεί από την Netgear, την Huawei και την D-Link, εκμεταλλευόμενο αδύναμους κωδικούς πρόσβασης Telnet και ευπάθειες σε αυτές τις συσκευές. Παρότι το Mozi καταγράφηκε για πρώτη φόρα το 2019 με την μόλυνση των δρομολογητών, συνέχισε τη λειτουργία του μέχρι τον Νοέμβριο του 2020, όποτε και αναχαιτίστηκε (Paganini, 2020).

5 Αντίμετρα

Ο ομιχλώδης προγραμματισμός ως μια πολλά υποσχόμενη λύση για την επεξεργασία των δεδομένων κοντά στην πηγή από την οποία παράγονται προσφέρει πολλά οφέλη, όπως την κατανεμημένη επεξεργασία δεδομένων σε διαφορές τοποθεσίες, την κινητικότητα και η ετερογένεια των πόρων. Όπως το υπολογιστικό νέφος έτσι και ο ομιχλώδης προγραμματισμός θεωρείται πλέον μια επαναστατική μέθοδος και δυναμική τεχνολογία στον τομέα της πληροφορικής επιτρέποντας την κοινή χρήση των πόρων, όπως η αποθήκευση στο διαδίκτυο και η παροχή εφαρμογών και λογισμικού ως υπηρεσίες κοντά στην άκρη του δικτύου (Ahmadi *et al.*, 2021), (Manzoor *et al.*, 2019). Μικρές και μεγάλες εταιρείες, όπως Amazon, Google, Facebook, Twitter και Linked In έχουν αρχίσει να μεταβαίνουν σε υποδομές που υποστηρίζουν τον ομιχλώδη προγραμματισμό (Manzoor *et al.*, 2019).

Ωστόσο, τα ιδιαίτερα χαρακτηριστικά του ομιχλώδους προγραμματισμού δημιουργούν καινούργιες προκλήσεις στον τομέα της ασφάλειας και της ιδιωτικότητας. Ειδικότερα, οι υπάρχουσες λύσεις για την ασφάλεια του υπολογιστικού νέφους που έχουν αναπτυχθεί μέχρι στιγμής, συχνά αποτυγχάνουν να καλύψουν πλήρως τις ανάγκες των περιβαλλόντων ομίχλης, λόγω της αυξανόμενης πολυπλοκότητας σε συνδυασμό με τις διαφοροποιημένες απαιτήσεις που προκαλεί η κινητικότητα και η ετερογένεια των συσκευών του ομιχλώδους προγραμματισμού. Επομένως, αναδεικνύεται η επιτακτική ανάγκη για την ανάπτυξη νέων και εξειδικευμένων αντιμέτρων ικανών να ανταποκριθούν αποτελεσματικά στις ιδιάζουσες προκλήσεις των συστημάτων ασφάλειας του ομιχλώδους προγραμματισμού.

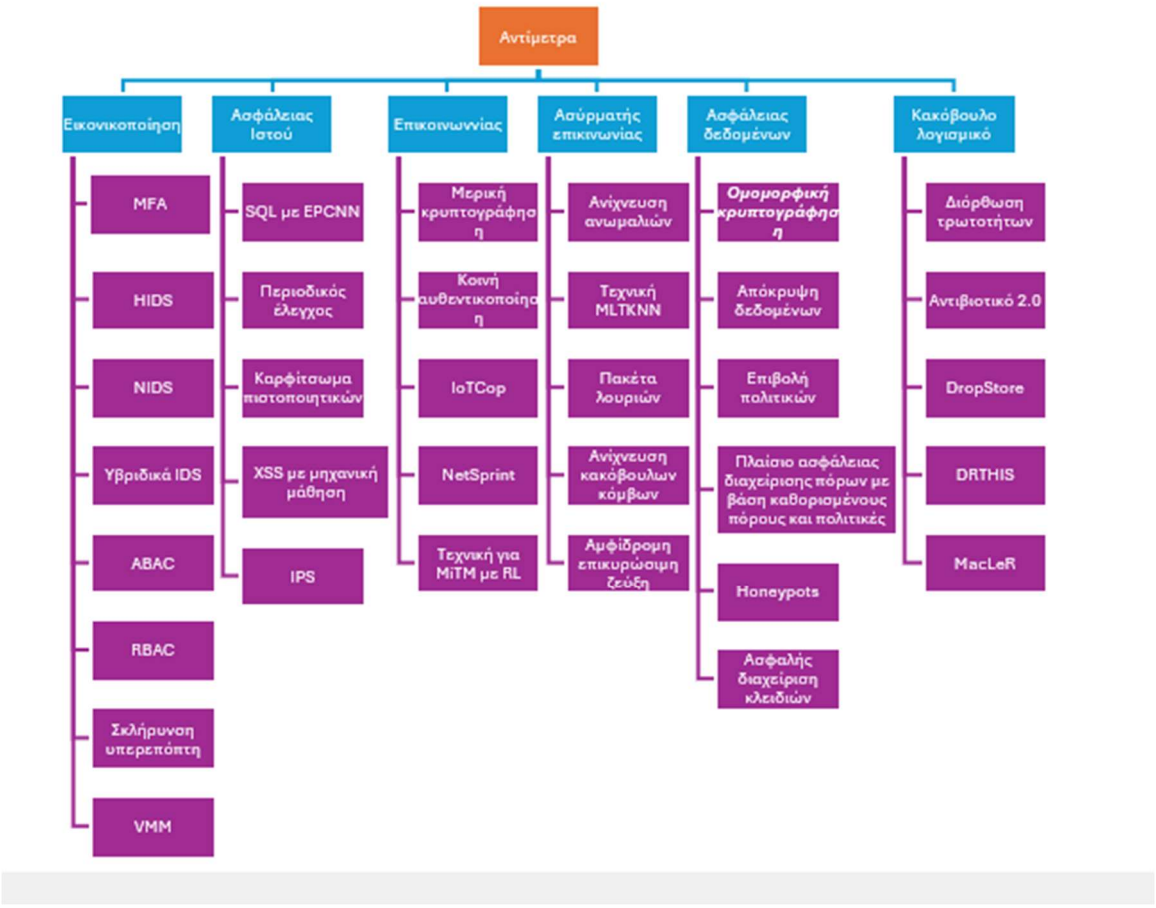
5.1 Ιεραρχική κατηγοριοποίηση των αντιμέτρων

Η παρούσα κατηγοριοποίηση των αντιμέτρων στον ομιχλώδη προγραμματισμό βασίζεται στην κατηγοριοποίηση των επιθέσεων που πραγματοποιήθηκε στην ενότητας 4.3 της παρούσας διπλωματικής εργασίας. Η σύνδεση αυτή επιτρέπει μια πιο στοχευμένη και αποτελεσματική προσέγγιση στην αντιμετώπιση των επιθέσεων προσφέροντας λύσεις που αντιμετωπίζουν τις συγκεκριμένες επιθέσεις που αναλύθηκαν προηγουμένως. Η κατηγοριοποίηση των αντιμέτρων (Εικόνα 13) διευκολύνει την επιλογή των κατάλληλων μέτρων προστασίας, με βάση τα χαρακτηριστικά και το μέγεθος της εκάστοτε επιθέσεις. Αυτή η κατηγοριοποίηση παρουσιάζεται συνοπτικά παρακάτω:

- **Αντίμετρα για τις επιθέσεις εικονικοποίησης**
  Τα αντίμετρα αυτά επικεντρώνονται στην προστασία των εικονικών μηχανών και του υπερεπόπτη από κακόβουλες ενέργειες που εκμεταλλεύονται την τεχνολογία

εικονικοποίησης. Περιλαμβάνονται αντίμετρα όπως η αυθεντικοποίηση πολλαπλών παραγόντων, τα συστήματα ανίχνευσης εισβολών, ο εκλεπτυσμένος έλεγχος πρόσβασης κ.α.

- **Αντίμετρα για τις επιθέσεις ασφάλειας ιστού**
  Τα αντίμετρα αυτά στοχεύουν στην προστασία των εφαρμογών ιστού από επιθέσεις, όπως οι εκχύσεις SQL και οι XSS, χρησιμοποιώντας τεχνολογίες ανίχνευσης κακόβουλων ενεργειών μέσω αλγορίθμων μηχανικής μάθησης (π.χ. το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στο EPCNN), καθώς και συστήματα πρόληψης για την ενίσχυση της ασφάλειας.
- **Αντίμετρα για τις επιθέσεις επικοινωνίας εντός ή εκτός του οργανισμού / επιχείρησης**
  Τα αντίμετρα αυτά προστατεύουν τα δεδομένα κατά την μεταφορά τους, τόσο εντός όσο και εκτός του οργανισμού / επιχείρησης μέσω της κρυπτογράφησης και των τεχνικών αυθεντικοποίησης. Αυτές οι τεχνολογίες αποτρέπουν τις επιθέσεις τύπου Man-in-the-Middle (επιθέσεις ενδιάμεσου) και άλλες επικοινωνιακές απειλές που μπορεί να θέσουν σε κίνδυνο την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των δεδομένων κατά την μεταφορά τους.
- **Αντίμετρα για τις επιθέσεις ασύρματης επικοινωνίας**
  Αυτά τα αντίμετρα αποσκοπούν στην ανίχνευση και την αποτροπή των επιθέσεων που πλήττουν τα ασύρματα δίκτυα, όπως επιθέσεις από κακόβουλους κόμβους και ανωμαλίες στην ασύρματη επικοινωνία, ενισχύοντας την ασφάλεια του δικτύου.
- **Αντίμετρα για τις επιθέσεις ασφάλειας των δεδομένων**
  Τα αντίμετρα αυτά εστιάζουν στην προστασία των δεδομένων που αποθηκεύονται και μεταφέρονται στα ομιχλώδη περιβάλλοντα. Περιλαμβάνουν τεχνικές κρυπτογράφησης, την ασφαλή διαχείριση κλειδιών και άλλες μεθόδους για την προστασία της εμπιστευτικότητας και της ακεραιότητας των δεδομένων.
- **Αντίμετρα για τις επιθέσεις κακόβουλου λογισμικού**
  Τα αντίμετρα αυτά στοχεύουν στην αποτροπή της εξάπλωσης κακόβουλου λογισμικού μέσω της διορθώσεις των τρωτοτήτων του συστήματος, των προηγμένων λύσεων ανίχνευσης κακόβουλου λογισμικού και της τακτικής εφαρμογής αντιγράφων ασφαλείας, διασφαλίζοντας την ακεραιότητα του συστήματος.



Εικόνα 13 - Ιεραρχική κατηγοριοποίηση των αντιμέτρων στον ομιχλώδη προγραμματισμό

5.2 Κριτήρια σύγκρισης για την αξιολόγηση των αντιμέτρων

Τα κριτήρια σύγκρισης που χρησιμοποιήθηκαν για την αξιολόγηση των αντιμέτρων που εφαρμόζονται για την αντιμετώπιση διάφορων ζητημάτων στον ομιχλώδη προγραμματισμό βασίζονται στις βασικές ανάγκες και τα χαρακτηριστικά των συστημάτων αυτών. Η παρούσα διπλωματική εργασία εισάγει κάποια κατάλληλα κριτήρια σύγκρισης για την σύγκριση των αντιμέτρων ανά κατηγορία επιθέσεων του ομιχλώδους προγραμματισμού, αλλά και για μια καθολική σύγκριση όλων των αντιμέτρων. Τα κριτήρια αυτά προέρχονται από την εμπειρία και οπτική γωνία του συγγραφέως της διπλωματικής και δεν αντλούνται από την βιβλιογραφία. Σκοπός των συγκρίσεων που θα γίνει στις επόμενες ενότητες του τρέχοντος κεφαλαίου είναι να αναδειχθούν οι πραγματικές ανάγκες και οι προκλήσεις που αντιμετωπίζουν οι χρήστες σε διάφορα σενάρια εφαρμογής του ομιχλώδους προγραμματισμού, επιδιώκοντας μια πιο ρεαλιστική αξιολόγηση της απόδοσης και της αποτελεσματικότητας των αντιμέτρων. Τα κριτήρια σύγκρισης είναι τα εξής:

1. Κατανάλωση πόρων
2. Κλιμακωσιμότητα
3. Ασφάλεια δεδομένων
4. Ευκολία χρήσης

5. Εκπαίδευση χρηστών
6. Αντίκτυπος στον χρήστη
7. Εφαρμοσιμότητα
8. Βαθμός κάλυψης
9. Επεκτασιμότητα

Για να πραγματοποιηθεί η ποσοτικοποίηση και η σύγκριση των διάφορων κριτήριων, υιοθετήθηκε μια πενταβάθμια κλίμακα αξιολόγησης, όπου η τιμή 1 αντιστοιχεί στην χαμηλότερη επίδοση και η τιμή 5 στην υψηλότερη επίδοση. Η ανάλυση για το κάθε κριτήριο εξηγεί πως αποδίδονται οι συγκεκριμένες τιμές με βάση τις συνθήκες που επικρατούν κατά την εφαρμογής του αντιμέτρου για το εκατοστέ αντίμετρο.

Παρακάτω αναλύονται τα κριτήρια που επιλέχθηκαν:

Κατανάλωση Πόρων: Αξιολογείται η ποσοτικοποίηση των απαιτήσεων για υπολογιστικούς πόρους (π.χ. CPU, μνήμη) που προϋποθέτει η εκτέλεση του αντιμέτρου, καθώς και η συνολική απόδοση του συστήματος. Όταν ένα αντίμετρο παίρνει την τιμή 1 στην κατανάλωση των πόρων σημαίνει ότι απαιτεί υπερβολικά υψηλή κατανάλωση, μειώνοντας δραστικά την απόδοση του συστήματος, ειδικά σε σενάρια με περιορισμένους πόρους. Η τιμή 2 στην κατανάλωση των πόρων ενός αντίμετρου υποδηλώνει ότι το αντίμετρο απαιτεί αρκετούς πόρους και μπορεί να προκαλέσει αισθητή μείωση της συνολικής απόδοσης, αν και μπορεί να είναι κατάλληλο για περιβάλλοντα με περισσότερη διαθεσιμότητα πόρων. Όταν ένα αντίμετρο πάρει την τιμή 3 στην κατανάλωση των πόρων αυτό σημαίνει ότι αν και είναι εξαιρετικά απαιτητικό, μπορεί να επηρεάσει την απόδοση του συστήματος σε ορισμένες περιπτώσεις. Η τιμή 4 στην κατανάλωση των πόρων ενός αντίμετρου υποδηλώνει ότι το αντίμετρο έχει χαμηλές απαιτήσεις σε πόρους, επηρεάζοντας ελάχιστα την απόδοση και καθιστώντας το κατάλληλο για συστήματα με περιορισμούς. Τέλος, η τιμή 5 στην κατανάλωση των πόρων σημαίνει ότι το αντίμετρο έχει ελάχιστες ή μηδαμινές απαιτήσεις και δεν επηρεάζει την απόδοση, καθιστώντας το ιδανικό για κάθε περιβάλλον.

Κλιμακωσιμότητα: Εξετάζεται η ικανότητα ενός αντιμέτρου να προσαρμόζεται σε υπό συνθήκες αυξημένου φόρτου εργασίας χωρίς να υπάρχει σημαντική μείωση της απόδοσης του συστήματος, δηλαδή μπορεί να διαχειρίζεται με αποτελεσματικότητα την αύξηση του αριθμού των χρηστών ή των διαδικασιών του συστήματος με επιτυχία. Εφόσον ένα αντίμετρο πάρει την τιμή 1 στην κλιμακωσιμότητα σημαίνει ότι το αντίμετρο δεν κλιμακώνεται και επηρεάζει αρνητικά την απόδοση του δικτύου με την αύξηση του φόρτου εργασίας. Η τιμή 2 στην κλιμακωσιμότητα σημαίνει ότι ένα αντίμετρο χαρακτηρίζεται από περιορισμένη κλιμακωσιμότητα και απαιτούνται σημαντικές προσαρμογές σε αυτό για να διατηρηθεί η απόδοση. Όταν το αντίμετρο λαμβάνει την τιμή 3, αυτό υποδεικνύει ότι μπορεί να κλιμακωθεί, αλλά απαιτούνται κάποιες προσαρμογές για να λειτουργεί ικανοποιητικά σε μεγάλα φορτία. Η τιμή 4, υποδηλώνει ότι ένα αντίμετρο κλιμακώνεται με επιτυχία, δηλαδή μπορεί να υποστηρίξει ένα μεγάλο αριθμό χρηστών ή δεδομένων με ελάχιστη επίπτωση στην απόδοση του συστήματος. Τέλος, η τιμή 5 στην κλιμακωσιμότητα φανερώνει την ικανότητα του αντιμέτρου να προσαρμόζεται εύκολα στην οποιαδήποτε αύξηση του φόρτου, χωρίς να απαιτούνται αλλαγές ή να μειώνεται η απόδοση του συστήματος.

Ασφάλεια δεδομένων: Αξιολογείται ο βαθμός στον οποίο το αντίμετρο προστατεύει πλήρως τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις ακεραιότητας και άλλες απειλές ασφάλειας. Όταν ένα αντίμετρο πάρει την τιμή 1 στην ασφάλεια των δεδομένων σημαίνει ότι το αντίμετρο προσφέρει καθόλου ή ελάχιστη προστασία, καθιστώντας το ευάλωτο σε απλές επιθέσεις και κατάλληλο μόνο για περιβάλλοντα χαμηλού ρίσκου, καθώς ενδέχεται να αντιμετωπίζει κάποιες απλές επιθέσεις, αλλά δεν παρέχει επαρκή προστασία για πιο σύνθετες απειλές. Η τιμή 2 στην ασφάλεια των δεδομένων υποδηλώνει ότι ένα αντίμετρο μπορεί να προσφέρει βασική προστασία, ωστόσο παραμένει ευάλωτο σε πιο εξειδικευμένες απειλές, καθιστώντας το κατάλληλο για περιβάλλοντα με απειλές περιορισμένης πολυπλοκότητας. Όταν το αντίμετρο πάρει την τιμή 3 στην ασφάλεια των δεδομένων, προσφέρει αυξημένη προστασία από συνήθεις και μέτριας πολυπλοκότητας απειλές, διαθέτοντας καλύτερη ανθεκτικότητα σε πιο εξελιγμένες επιθέσεις σε σχέση με την τιμή 2, αλλά μπορεί να μην είναι επαρκές για στοχευμένες ή υψηλής πολυπλοκότητας επιθέσεις. Η τιμή 4 στην ασφάλεια των δεδομένων σημαίνει ότι το αντίμετρο παρέχει υψηλό επίπεδο προστασίας αντιμετωπίζοντας τις περισσότερες απειλές και καθιστώντας το κατάλληλο για περιβάλλοντα με σημαντικές απαιτήσεις ασφάλειας. Τέλος, η τιμή 5 στην ασφάλεια των δεδομένων σημαίνει ότι το αντίμετρο προσφέρει υψηλό επίπεδο ασφάλειας, εξασφαλίζοντας την πλήρη προστασίας από κάθε τύπο απειλής, γεγονός που το καθιστά ιδανικό για περιβάλλοντα που διαχειρίζονται ευαίσθητα ή κρίσιμα δεδομένα.

***Ευκολία Χρήσης*:** Αξιολογείται η ευχρηστία του αντιμέτρου από την πλευρά του χρήστη. Όταν το αντίμετρο πάρει την τιμή 1 στην ευκολία χρήσης σημαίνει ότι το αντίμετρο χαρακτηρίζεται ως πολύπλοκο και δύσχρηστο, απαιτώντας σημαντική προσπάθεια για την καθημερινή χρήση. Η τιμή 2 στην ευκολία χρήσης υποδηλώνεται ότι το αντίμετρο απαιτεί σημαντική εξοικείωση και είναι δύσκολο να χρησιμοποιηθεί σε καθημερινές εργασίες. Όταν το αντίμετρο πάρει την τιμή 3 στην ευκολία χρήσης σημαίνει ότι ο χρήστης απαιτείται να έχει κάποια εξοικείωση με το αντίμετρο, αλλά δεν είναι ιδιαίτερα περίπλοκο. Η τιμή 4 στην ευκολία χρήσης υποδηλώνει ότι το αντίμετρο είναι σχετικά εύκολο στην χρήση με απλές και κατανοητές λειτουργίες που διευκολύνουν την καθημερινή διαχείριση ενός συστήματος. Τέλος, η τιμή 5 στην ευκολία χρήσης σημαίνει ότι ένα αντίμετρο είναι απόλυτα φιλικό προς έναν χρήστη, αφού είναι απλό στην χρήση του και ο χρήστης δεν απαιτείται ιδιαίτερη προσπάθεια για να το κατανοήσει και να το χειριστεί αποτελεσματικά.

***Εκπαίδευση χρηστών**:* Αξιολογείται ο βαθμός εκπαίδευσης που απαιτείται για την χρήση του αντιμέτρου, καθώς και το βάθος και η συχνότητα εκπαίδευσης. Ένα αντίμετρο που λαμβάνει την τιμή 1 απαιτεί εκτενή και επαναλαμβανόμενη εκπαίδευση λόγω της πολυπλοκότητας του. Με την τιμή 2 υποδηλώνεται ότι το αντίμετρο χρειάζεται σημαντική αλλά περιοδική εκπαίδευση, εστιάζοντας σε συγκεκριμένες δεξιότητες που απαιτούνται για τη σωστή χρήση του, χωρίς να απαιτείται συνεχής ή εκτενής κατάρτιση. Όταν το αντίμετρο πάρει την τιμή 3 στην εκπαίδευση χρηστών, αυτό σημαίνει ότι για το αντίμετρο απαιτείται μέτρια εκπαίδευση για να κατανοηθεί πλήρως και να μπορέσει να χρησιμοποιηθεί σωστά. Η βαθμολογία 4 στην εκπαίδευση χρηστών σημαίνει ότι για το αντίμετρο απαιτείται περιορισμένη και σύντομη εκπαίδευση με τους χρήστες να εξοικειώνονται γρήγορα με αυτό. Τέλος, η τιμή 5 δείχνει ότι το αντίμετρο απαιτεί ελάχιστη ή καθόλου εκπαίδευση, καθώς είναι απλό και δεν απαιτείται κάποια εξειδικευμένη γνώση για την σωστή την χρήση του.

Αντίκτυπος στον χρήστη: Αξιολογείται ο βαθμός στον όποιο το αντίμετρο επηρεάζει την εμπειρία του χρήστη. Το ιδανικότερο είναι ότι ένα αντίμετρο πρέπει να ενσωματώνεται στη ροή των

εργασιών του συστήματος που εφαρμόζεται χωρίς να επηρεάζει αρνητικά την αποδοτικότητα των χρηστών. Όταν ένα αντίμετρο παίρνει την τιμή 1 σημαίνει ότι έχει έντονα αρνητικό αντίκτυπο στον χρήστη, καθώς επηρεάζει την εμπειρία του χρήστη με τρόπο που μειώνει την αποδοτικότητά του. Η τιμή 2 υποδηλώνει ότι ο αντίκτυπος παραμένει αρνητικός για το αντίμετρο, οι δυσκολίες που συναντούν οι χρήστες είναι λιγότερο σοβαρές σε σχέση με την τιμή 1, επιτρέποντας τη λειτουργία με κάποια μείωση στην αποδοτικότητα. Όταν το αντίμετρο πάρει την τιμή 3, αυτό σημαίνει ότι το αντίμετρο μπορεί να προσφέρει ορισμένα οφέλη, αλλά επίσης προκαλεί κάποιες ελαφριές ενοχλήσεις στον χρήστη, οι οποίες δεν επηρεάζουν σημαντικά την αποδοτικότητά του. Η τιμή 4 στον αντίκτυπο χρήστη υποδηλώνει ότι αυτός είναι θετικός, καθώς η εφαρμογή του αντιμέτρου βελτιώνει την εμπειρία του χρήστη και ενισχύει την αποδοτικότητά του. Τέλος, ένα αντίμετρο που λαμβάνει τιμή 5 σημαίνει ότι είναι εξαιρετικά ωφέλιμο για τους χρήστες, προσφέροντας σημαντική βελτίωση στην εμπειρία και την αποδοτικότητά τους.

Εφαρμοσιμότητα: Αξιολογείται η ευκολία ενσωμάτωσης του αντιμέτρου σε διάφορα περιβάλλοντα και συστήματα, καθώς και οι ανάγκες που προκύπτουν από αυτή την εφαρμογή (ανάγκες σε ενοποίηση, σε επιπλέον πόρους προς δέσμευση και χρήση, κ.α.). Όταν το αντίμετρο πάρει τιμή 1 στην εφαρμοσιμότητα σημαίνει ότι το αντίμετρο είναι δύσκολο να ενσωματωθεί και απαιτεί σημαντικές προσαρμογές τόσο στο ίδιο το σύστημα όσο και στις διαδικασίες που ακολουθούν οι χρήστες. Αν το αντίμετρο πάρει τιμή 2 στην εφαρμοσιμότητα, αυτό σημαίνει ότι το αντίμετρο παρουσιάζει μέτριες δυσκολίες κατά την εφαρμογή του, απαιτώντας κάποιες προσαρμογές, κυρίως σε συγκεκριμένες διαδικασίες ή τμήματα του συστήματος, χωρίς να χρειάζεται ευρεία αναδιάρθρωση ή σημαντική τροποποίηση των διαδικασιών των χρηστών. Στην περίπτωση που το αντίμετρο βαθμολογείται με 3 στην εφαρμοσιμότητα, αυτό σημαίνει ότι αντίμετρο μπορεί σχετικά εύκολα να ενσωματωθεί, αλλά απαιτείται περιορισμένος αριθμός προσαρμογών και αλλαγές για να είναι λειτουργικό σε διαφορετικά συστήματα, χωρίς όμως να επηρεάζει δραστικά τις διαδικασίες ή τις υποδομές. Αν το αντίμετρο πάρει τιμή 4 στην εφαρμοσιμότητα, αυτό σημαίνει ότι το αντίμετρο ενσωματώνεται σχετικά γρήγορα και πολύ εύκολα σε ένα περιβάλλον με ελάχιστες αλλαγές και χωρίς να απαιτούνται επιπλέον πόροι ή σημαντικές τροποποιήσεις στις διαδικασίες. Τέλος, όταν το αντίμετρο βαθμολογείται με 5 στην εφαρμοσιμότητα, αυτό σημαίνει ότι μπορεί να ενσωματωθεί άμεσα και πλήρως σε οποιοδήποτε περιβάλλον ή σύστημα, χωρίς να απαιτείται καμία προσαρμογή σε οποιοδήποτε υπάρχον περιβάλλον ή σύστημα, καθιστώντας το εξαιρετικά ευέλικτο.

Βαθμός κάλυψης: Αξιολογείται το εύρος των περιβαλλόντων και των σεναρίων στα οποία μπορεί να προσαρμοστεί και να εφαρμοστεί το αντίμετρο. Όταν το αντίμετρο πάρει την τιμή 1 στον βαθμό κάλυψης αυτό σημαίνει ότι το αντίμετρο μπορεί να προσαρμοστεί μόνο σε ελάχιστα περιβάλλοντα και σενάρια, περιορίζοντας την ευρύτερη χρησιμότητα του. Αν το αντίμετρο πάρει τιμή 2 στον βαθμό κάλυψης, αυτό υποδηλώνει ότι το αντίμετρο μπορεί να προσαρμοστεί μόνο σε περιορισμένο αριθμό περιβαλλόντων, ενώ η προσαρμογή του σε διαφορετικά σενάρια παρουσιάζει σημαντικές δυσκολίες. Στην περίπτωση που το αντίμετρο βαθμολογείται με 3 στον βαθμό κάλυψης, αυτό σημαίνει ότι το αντίμετρο μπορεί να προσαρμοστεί σε αρκετά περιβάλλοντα, αλλά εξακολουθεί να έχει συγκεκριμένους περιορισμούς. Αν το αντίμετρο πάρει την τιμή 4 στον βαθμό κάλυψης, αυτό δείχνει ότι το αντίμετρο είναι ευέλικτο και μπορεί να προσαρμοστεί σε πολλά περιβάλλοντα και σενάρια με σχετική ευκολία. Τέλος, όταν το αντίμετρο βαθμολογείται με 5 στον βαθμό κάλυψης,

αυτό σημαίνει ότι προσαρμόζεται εύκολα σε ένα ευρύ φάσμα περιβαλλόντων και σεναρίων χωρίς να υπάρχουν περιορισμοί.

Επεκτασιμότητα: Αξιολογείται η δυνατότητα του αντιμέτρου να αναβαθμίζεται και να επεκτείνεται καθ' όλη την διάρκεια ζωής του συστήματος. Όταν ένα αντίμετρο πάρει την τιμή 1 στην επεκτασιμότητα, αυτό σημαίνει ότι δεν μπορεί να επεκταθεί και δεν προσαρμόζεται σε νέες ανάγκες ή τεχνολογίες, καθιστώντας το ακατάλληλο για μελλοντική χρήση. Αν το αντίμετρο πάρει τιμή 2 στην επεκτασιμότητα, αυτό υποδηλώνει ότι το αντίμετρο παρουσιάζει περιορισμένη επεκτασιμότητα και απαιτεί σημαντικές προσαρμογές για να αναβαθμιστεί και να ανταποκριθεί σε νέες απαιτήσεις. Αν το αντίμετρο λάβει τιμή 3 στην επεκτασιμότητα, αυτό σημαίνει ότι δεν περιορίζεται η επεκτασιμότητα του αντιμέτρου, αλλά η διαδικασία επέκτασης είναι χρονοβόρα και απαιτεί επιπλέον πόρους. Αν το αντίμετρο πάρει την τιμή 4 στην επεκτασιμότητα δείχνει ότι το αντίμετρο είναι εύκολα επεκτάσιμο, καθώς και μπορεί να προσαρμοστεί σε νέες τεχνολογικές ή απαιτήσεις με λίγες αλλαγές. Τέλος, όταν το αντίμετρο βαθμολογείται με 5 στην επεκτασιμότητα, αυτό σημαίνει ότι το αντίμετρο προσαρμόζεται εύκολα και γρήγορα στις νέες ανάγκες και τεχνολογίες με ελάχιστες αλλαγές να απαιτούνται, διασφαλίζοντας την μελλοντική βιωσιμότητα του.

5.3 Αντίμετρα ομιχλώδους προγραμματισμού

5.3.1 Εισαγωγή

Η παρούσα ενότητα εξετάζει αναλυτικά τα αντίμετρα που μπορούν να εφαρμοστούν για την προστασία των συστημάτων ομιχλώδους προγραμματισμού ενάντια των διαφορετικών κατηγοριών επιθέσεων. Κάθε κατηγορία επιθέσεων αναλύεται σε ξεχωριστή υποενότητα, όπου παρουσιάζονται τα αντίστοιχα αντίμετρα που αποσκοπούν στην πρόληψη ή την μετρίαση των κίνδυνών που προκαλούνται από αυτές.

Η δομή της ενότητας διαρθρώνεται ως εξής:

- **Υποενότητες 5.3.1 – 5.3.7:** Αρχικά, παρουσιάζονται τα αντίμετρα που σχετίζονται με την κατηγορία των επιθέσεων της υποενότητας. Το κάθε αντίμετρο αναλύεται σε επιμέρους υποτμήματά του, όπου εξετάζονται διεξοδικά τα τεχνικά χαρακτηριστικά του, οι προϋποθέσεις εφαρμογής του, καθώς και τα πλεονεκτήματα και τα μειονεκτήματα του. Στο τέλος, κάθε υποενότητας πραγματοποιείται μια συγκριτική αξιολόγηση των αντιμέτρων που παρουσιαστήκαν για την αντίστοιχη κατηγορία επιθέσεων.
- **Υποενότητα 5.3.8:** Στην υποενότητα αυτή παρέχεται μια συνολική αποτίμηση όλων των αντιμέτρων που εξετάστηκαν στις προηγούμενες υποενότητες 5.3.1 έως 5.3.7. Εξετάζεται η αποδοτικότητα τους συνολικά ανεξαρτήτως σε ποια κατηγορία ανήκουν, ενώ παράλληλα αξιολογούνται οι δυνατότητες τους να αντιμετωπίζουν πολλαπλές επιθέσεις σε περιβάλλοντα ομίχλης. Στόχος είναι να αναδείχνουν τα πιο ισχυρά και αποδοτικά αντίμετρα που μπορούν να εφαρμοστούν διαχρονικά και σε ευρεία κλίμακα.

5.3.2 Αντίμετρα για τις επιθέσεις εικονικοποίησης

5.3.2.1 Αυθεντικοποίηση πολλαπλών παραγόντων (Multi-factor Authentication)

Η αυθεντικοποίηση πολλαπλών παραγόντων είναι ένας μηχανισμός ασφάλειας που ενισχύει σημαντικά την προστασία των δικτυακών πόρων έναντι των απειλών (Manzoor *et al.*, 2019). Ενώ η παραδοσιακή αυθεντικοποίηση βασίζεται σε έναν μόνο παράγοντα για την αυθεντικοποίηση του χρήστη, όπως ο κωδικός πρόσβασης, στην αυθεντικοποίηση πολλαπλών παραγόντων απαιτούνται δύο ή περισσότεροι παράγοντες για την επαλήθευση της ταυτότητας του χρήστη (Loffi *et al.*, 2020). Στόχος του μηχανισμού ασφάλειας αυθεντικοποίησης πολλαπλών παραγόντων είναι να δυσκολέψουν την προσπάθεια ενός εισβολέα να εκμεταλλευτεί τυχόν τρωτότητες κατά την διαδικασία της σύνδεσης ενός χρήστη έτσι ώστε να εισβάλει σε προσωπικά ή εταιρικά δίκτυα, προκαλώντας την καταστροφή ολόκληρων υπολογιστικών συστημάτων ή ακόμα χειροτέρα την κλοπή διαφόρων εμπιστευτικών πληροφοριών που αφορούν τους χρήστες του συστήματος (Strom, 2019).

Παρόλο που στις μέρες μας η αυθεντικοποίηση των χρηστών γίνεται κυρίως μέσω διαδικασιών, όπως η διαδικασία μόνο μίας εισόδου (single sign-in process - SSO), όπου οι χρήστες συνδέονται μία φορά για να έχουν πρόσβαση σε πολλαπλές υπηρεσίες, ή μέσω της διαδικασίας της απλής αυθεντικοποίησης, δηλαδή με τη χρήση διαπιστευτηρίων για κάθε μεμονωμένη υπηρεσία, δεν εξασφαλίζεται η επαρκούμενη ασφάλεια του συστήματος. Έχουν προταθεί διαφορές τεχνικές που μπορούν να χρησιμοποιηθούν για την αύξηση των παραγόντων στην αυθεντικοποίηση, όπως είναι οι κωδικοί μιας χρήσης (One Time Password (OTP)), ο κώδικας ταχείας απόκρισης (quick response (QR) code), τα γραφικά μοτίβα (graphic pattern), καθώς και άλλες τεχνικές που βασίζονται στην βιομετρική επαλήθευση (biometric verification). Στην τεχνική των κωδικών μιας χρήσης δημιουργείται ένας μοναδικός κωδικός για κάθε σύνδεση, ο οποίος λήγει μετά από ένα σύντομο χρονικό διάστημα. Στους κώδικες ταχείας απόκρισης επιτρέπεται η επαλήθευση μέσω σκαναρίσματος ενός μοναδικού κωδικού με τη χρήση της κάμερας από μια κινητή συσκευή. Στην τεχνική με τα γραφικά μοτίβα ο χρήστης μπορεί να σχεδιάσει ένα συγκεκριμένο σχέδιο πάνω στην οθόνη αφής, συνήθως με την σύνδεση κουκίδων σε προκαθορισμένη σειρά. Τέλος, οι τεχνικές βιομετρικές επαλήθευσης βασίζονται σε μοναδικά φυσικά χαρακτηριστικά του χρήστη, όπως είναι η αναγνώριση των δακτυλικών αποτυπωμάτων, η αναγνώριση προσώπου, η σάρωση της ίριδας του ματιού κ.α. (Manzoor *et al.*, 2019)

Με τον σχεδιασμό του μηχανισμού αυθεντικοποίησης πολλαπλών παραγόντων μπορεί να επιτευχθεί ευχρηστία, ανθεκτικότητα και ισχυρή ασφάλεια. Οι μηχανισμοί αυτοί πρέπει να έχουν σχεδιαστεί ώστε να επιτυγχάνουν υψηλό επίπεδο ασφάλειας, προκειμένου να προστατεύουν τα δεδομένα και τους πόρους του ομιχλώδους περιβάλλοντος και να είναι ανθεκτικοί σε επιθέσεις, όπως η κλοπή των στοιχείων ταυτοποίησης του χρήστη. Παράλληλα, κατά την διαδικασία του σχεδιασμού τους πρέπει να λαμβάνουν υπόψη τους χρήστες του συστήματος, δημιουργώντας φιλικά συστήματα ασφάλειας που δεν δημιουργούν εμπόδια στην καθημερινή εργασία των χρηστών. Για παράδειγμα, οι μέθοδοι αυθεντικοποίησης πολλαπλών παραγόντων που στηρίζεται σε βιομετρικούς παράγοντες προτιμώνται από τους χρήστες για την απλότητα της χρήσης τους,

αφού δεν χρειάζεται να απομνημονεύουν πολύπλοκους κωδικούς ή να διαχειριστούν πολύπλοκες διαδικασίες. (Manzoor *et al.*, 2019)

Η αυθεντικοποίηση πολλαπλών παραγόντων ενισχύει την διαδικασία της αυθεντικοποίησης των χρηστών, δυσχεραίνοντας την πρόσβαση σε μη εξουσιοδοτημένους χρήστες και αποτρέποντας απειλές, όπως είναι οι κακόβουλες επιθέσεις μέσω των οποίων εκμεταλλεύονται αδυναμίες σε σημεία πρόσβασης και της ανατροπής των λειτουργίας συσκευών (Manzoor *et al.*, 2019). Η αυθεντικοποίηση πολλαπλών παραγόντων σε συνδυασμό με την υποδομή δημόσιου κλειδιού (PKI) μπορεί να επιλύει αποτελεσματικά διάφορα θέματα ασφάλειας που υπάρχουν σε διαφορετικά επίπεδα της αρχιτεκτονικής του ομιχλώδους προγραμματισμού (Yi, Li and Li, 2015). Για παράδειγμα, το πιστοποιητικό PKI μπορεί να λειτουργήσει ως ηλεκτρονική ταυτότητα του κατόχου του κλειδιού σε άλλους συμμετέχοντες, ενισχύοντας την ασφάλεια του περιβάλλοντος του ομιχλώδους περιβάλλοντος και την εμπιστευτικότητα των δεδομένων (Yi, Li and Li, 2015), (Chen, Raj and Wolman, 2014). Επιπλέον, η αυθεντικοποίηση πολλαπλών παραγόντων μαζί με ένα αξιόπιστο περιβάλλον εκτέλεσης (TEE) προσφέρουν πολλά οφέλη σε ένα περιβάλλον ομίχλης, όπως η απομόνωση και η ασφαλής επεξεργασία δεδομένων αυθεντικοποίησης (Yi, Li and Li, 2015), (Valadares *et al.*, 2021).

Από την άλλη πλευρά, η αυθεντικοποίηση πολλαπλών παραγόντων παρουσιάζει διάφορες προκλήσεις. Μια από τις σημαντικότερες προκλήσεις είναι η ετερογένεια των κινητών συσκευών και των ασύρματων δικτύων, η οποία δημιουργεί προβλήματα, όπως η διαφορετικότητα στις δυνατότητες και τις απαιτήσεις ασφάλειας των συσκευών, οι ασυμβατότητες στα πρωτόκολλα και οι περιορισμένοι πόροι. Τα παραπάνω προβλήματα που προκαλεί η ετερογένεια δημιουργούν την ανάγκη για την σχεδίαση ευέλικτων συστημάτων αυθεντικοποίησης πολλαπλών παραγόντων. Αυτά τα συστήματα θα πρέπει να μπορούν να επιλέγουν αυτομάτως το καταλληλότερο επίπεδο ασφάλειας λαμβάνοντας υπόψη τους διαθέσιμους πόρους και την ευαισθησία των δεδομένων, προκειμένου να αντιμετωπιστούν συναφείς προκλήσεις ασφάλειας. Επίσης, η επαλήθευση κατά τη διάρκεια της διαδικασίας παράδοσης (handover) αποτελεί μια μεγάλη πρόκληση στα ασύρματα δίκτυα, καθώς η επιλογή του κατάλληλου πρωτοκόλλου επηρεάζεται από την αρχιτεκτονική και το υλικό, ενώ η ομαλή μετάβαση σε δίκτυα υψηλής κινητικότητας απαιτεί μείωση του χρόνου επαλήθευσης. Επιπλέον, η διατήρηση της ιδιωτικότητας των χρηστών στον ομιχλώδη προγραμματισμό αποτελεί μια πρόκληση για την εφαρμογή της αυθεντικοποίησης πολλαπλών παραγόντων, αλλά είναι και ένα δύσκολο έργο, καθώς απαιτεί την διαχείριση των ευαίσθητων προσωπικών δεδομένων, ενώ ταυτόχρονα πρέπει να διασφαλίζεται ότι η MFA δεν παραβιάζει την ιδιωτικότητα των χρηστών και δεν επηρεάζει αρνητικά την εμπειρία τους. Επιπρόσθετα, η χρήση των βιομετρικών μεθόδων αυθεντικοποίησης αυξάνει την χρηστικότητα αλλά και την πολυπλοκότητα της υλοποίησης. Τέλος, δεν πρέπει να αυθεντικοποιούνται μόνο οι χρήστες, αλλά και οι διαδικασίες ή οι συσκευές / κόμβοι ομίχλης. Αυτό σημαίνει ότι οι μέθοδοι αυθεντικοποίησης πρέπει να σχεδιάζονται και για μη ανθρώπινους παράγοντες και να διαφοροποιούνται ανάλογα με το αν πρόκειται για αυθεντικοποίηση χρήστη ή διαδικασίας / συσκευής, χρησιμοποιώντας διαφορετικούς παράγοντες σε κάθε περίπτωση. (Manzoor *et al.*, 2019)

5.3.2.2 Συστήματα ανίχνευσης εισβολών (Intrusion Detection System)

Με την διασυνδεσιμότητα (interconnection) στον ομιχλώδη προγραμματισμό δημιουργείται ένα δίκτυο όπου οι κόμβοι ομίχλης συνεργάζονται για την αποτελεσματική εκτέλεση υπηρεσιών και εφαρμογών που βρίσκονται κοντά στην άκρη του δικτύου, βελτιώνοντας την καθυστέρηση και τον φόρτο του δικτύου, αλλά παράλληλα επιτρέποντας την γρήγορη ανταπόκριση στις απαιτήσεις των εφαρμογών και των χρηστών (Hassan and Rashad, 2023). Η επέκταση του Διαδικτύου οδήγησε στη δημιουργία ενός κόσμου διασυνδεδεμένων συστημάτων. Αυτή η επέκταση έχει κάνει πιο συχνές τις κακόβουλες επιθέσεις σε δίκτυα υπολογιστών. Συνηθώς αυτές οι επιθέσεις ξεκινούν από έναν επιτιθέμενο (offensive actor), ο όποιος χρησιμοποιεί αισθητήρες (sensors) με σκοπό να εντοπίσει τυχόν ευπάθειες σε κάποιον κεντρικό υπολογιστή (host), έτσι ώστε να προχωρήσει σε παραβιάσεις (breaches) του δικτύου στόχου. Επομένως, κρίνεται απαραίτητη η υιοθέτηση ολοένα και πιο σύγχρονων μεθόδων αντιμετώπισης, όπως είναι τα συστήματα ανίχνευσης εισβολών που βασίζονται σε εξελιγμένες τεχνικές, όπως η μηχανική μάθηση (Chang *et al.*, 2022).

Τρεις κρίσιμες απαιτήσεις είναι απαραίτητες για τον επιτυχή σχεδιασμό και την υλοποίηση συστημάτων ανίχνευσης εισβολών στον ομιχλώδη προγραμματισμό: η διαχείριση της κατανομής των διαθέσιμων πόρων και του υπολογιστικών φορτιού στους κόμβους ομίχλης, η οποία σχετίζεται στενά με την διαχείριση των περιορισμένων πόρων, η κλιμακωσιμότητα (η δυνατότητα του συστήματος να διαχειρίζεται αποτελεσματικά την αύξηση του όγκου δεδομένων και των δικτυακών κόμβων) και η σχεδίαση ισχυρών αλγορίθμων με μεγάλη ακρίβεια στα αποτελέσματα ανίχνευσης εισβολών (Diro, Mahmood and Chilamkurti, 2021).

Υπάρχουν δύο κύριες κατηγορίες συστημάτων ανίχνευσης εισβολών: τα host-based (Host-based IDS - HIDS) και τα network-based (Network-based IDS - NIDS). Το HIDS μπορεί να λειτουργεί προστατευτικά για ένα τελικό σημείο (endpoint) μέσω συγκεκριμένων λειτουργιών. Ειδικότερα, ένα HIDS μπορεί να παρακολουθεί την δραστηριότητα του συστήματος, όπως είναι η εκκίνηση των εφαρμογών, η πρόσβαση σε αρχεία και οι συνδέσεις χρηστών, τις αλλαγές που συμβαίνουν στο σύστημα με την πάροδο του χρόνου, καθώς και τις διαφορές τροποποιήσεις σε αρχεία. Με αυτόν τον τρόπο, το HIDS μπορεί να εντοπίσει ύποπτες κινήσεις που μπορεί να υπάρχουν σε ένα κόμβο / τελικό σημείο του ομιχλώδους προγραμματισμού, οι οποίες τελικά μπορεί να υποδηλώνουν κάποιο είδος κακόβουλης δραστηριότητας. Το NIDS λειτουργεί παρακολουθώντας την κίνηση του δικτύου και αποτελείται από ένα εργαλείο ανίχνευσης πακέτων (packet sniffer), το οποίο συλλέγει και ταξινομεί πακέτα δεδομένων από το δίκτυο ή αναλύει την κίνηση ενός ασύρματου δικτύου. Στην συνέχεια, το NIDS αξιολογεί αυτή την κίνηση του δικτύου για τυχόν ενδείξεις κακόβουλης δραστηριότητας, οι οποίες μπορεί να υποδηλώνουν κοινούς τύπους επιθέσεων, όπως είναι μία DDoS επίθεση. Θα πρέπει να σημειώσουμε πως είναι δυνατή η δημιουργία υβριδικών λύσεων που συνδυάζουν τα πλεονεκτήματα και των δύο αυτών τεχνολογιών (HIDS & NIDS) για την δημιουργία μιας πιο αποδοτικότερης και αποτελεσματικότερης λύσης. (Chang *et al.*, 2022)

Ένα HIDS παρέχει μια πιο λεπτομερή παρακολούθηση και ανάλυση των επιθέσεων σε επίπεδο μεμονωμένων συστημάτων, όπως οι υπολογιστές, επιτρέποντας την ανίχνευση εσωτερικών απειλών και ανωμαλιών σε πραγματικό χρόνο. Ένα NIDS εξειδικεύεται στην ανίχνευση επιθέσεων

σε επίπεδο δικτύου, ανιχνεύοντας εξωτερικές επιθέσεις χωρίς να επιβαρύνουν τα συστήματα που παρακολουθούν. Το υβριδικό σύστημα, δηλαδή ο συνδυασμός του HIDS και του NIDS συνδυάζει τα πλεονεκτήματα των δύο αυτών τεχνολογιών, δηλαδή προσφέρει μεγαλύτερη ακρίβεια στην ανίχνευση των επιθέσεων και καλύτερη αναγνώριση των μη κανονικών συμπεριφορών σε σύγκριση με το κάθε σύστημα μεμονωμένα. Επιπλέον, η υβριδική αυτή προσέγγιση βοηθά στην αντιμετώπιση ορισμένων από τα μειονεκτήματα που έχουν τα συστήματα HIDS και NIDS, όπως η περιορισμένη ορατότητα που μπορεί να έχει κάθε σύστημα από μόνο του, καθώς και την μείωση του κινδύνου των ψευδών θετικών αποτελεσμάτων ανίχνευσης επιθέσεων. (Chang *et al.*, 2022)

Οι παραδοσιακές λύσεις συστημάτων ανίχνευσης εισβολών δεν μπορούν να εφαρμοστούν στο Διαδίκτυο των Πραγμάτων και στον ομιχλώδη προγραμματισμό. Επομένως, κρίνεται απαραίτητο ο σχεδιασμός ελαφρύτερων συστημάτων ανίχνευσης εισβολών για την αντιμετώπιση των προκλήσεων ασφάλειας σε IoT περιβάλλοντα, τα οποία περιλαμβάνουν διαφορετικούς τύπους συσκευών αλλά πάντοτε με περιορισμένους πόρους. (Diro, Mahmood and Chilamkurti, 2021).

Τα συστήματα ανίχνευσης εισβολών στον ομιχλώδη προγραμματισμό προσφέρουν σημαντικά πλεονεκτήματα στην ασφάλεια των δικτύων και των δεδομένων. Ένα από τα κύρια πλεονεκτήματα των IDS συστημάτων είναι ότι τοποθετούνται κοντά στην πηγή της δικτυακής κίνησης, επιτρέπουν την άμεση παρακολούθηση και την ανάλυση της κίνησης, μειώνοντας τον χρόνο απόκρισης στην ανίχνευση των επιθέσεων. Αυτό είναι ιδιαιτέρα χρήσιμο για IoT περιβάλλοντα, στα οποία παράγονται τεράστιες ποσότητες δεδομένων σε πραγματικό χρόνο, καθώς οι απειλές μπορούν να εντοπίζονται και αντιμετωπίζονται πιο γρήγορα. (Zwayed *et al.*, 2021)

Η ενσωμάτωση της μηχανικής μάθησης στα ελαφριά IDS συστήματα επιτρέπει την αναγνώριση προτύπων συμπεριφοράς και την ανίχνευση ευπαθειών σε ένα σύστημα ομιχλώδους προγραμματισμού με χαμηλό υπολογιστικό κόστος, ενώ η ανάλυση δεδομένων σε συνδυασμό με διάφορους αλγορίθμους μηχανικής μάθησης βελτιώνει το ποσοστό ανίχνευσης των επιθέσεων (Khater *et al.*, 2021). Επιπλέον, η ενσωμάτωση του blockchain σε συστήματα ανίχνευσης εισβολών επιτρέπει την ασφαλή και αξιόπιστη ανταλλαγή δεδομένων μεταξύ των κόμβων ομίχλης, την προστασία των μοντέλων εκπαίδευσης IDS, καθώς και την αύξηση της ανθεκτικότητας των συστημάτων ομιχλώδους προγραμματισμού έναντι διάφορων επιθέσεων. Ωστόσο, πρέπει να ληφθεί υπόψη ότι το blockchain μπορεί να είναι υπολογιστικά απαιτητικό και η εφαρμογή του ενδέχεται να μην είναι κατάλληλη για συσκευές με περιορισμένους πόρους, όπως πολλές IoT συσκευές. (Diro, Mahmood and Chilamkurti, 2021).

Τα IDS συστήματα βασίζονται συχνά σε αλγορίθμους που απαιτούν πολλούς υπολογιστικούς πόρους για να λειτουργήσουν αποτελεσματικά. Οι κόμβοι ομίχλης, όμως είναι συχνά συσκευές με περιορισμένες δυνατότητες, όπως η περιορισμένη ισχύ επεξεργασίας, η μικρή μνήμη και ο αποθηκευτικός χώρος. Αυτό κάνει δύσκολη την απευθείας εφαρμογή εξεζητημένων ή πολύπλοκων IDS συστημάτων στους κόμβους ομίχλης, καθώς μπορεί να επιβραδύνουν σημαντικά την λειτουργία τους. Επομένως, μια από τις προκλήσεις που προκύπτουν είναι η ανάγκη για την δημιουργία αποτελεσματικών IDS συστημάτων για περιβάλλοντα ομίχλης. Η υλοποίηση των IDS

συστημάτων σε περιβάλλοντα ομίχλης προϋποθέτει την αντιμετώπιση διαφορετικών προκλήσεων, όπως η απαιτούμενη χαμηλή καθυστέρηση για την ανταλλαγή δεδομένων και η γεωγραφική κατανομή των IoT συσκευών. Επιπλέον, ο όγκος των δεδομένων προς επεξεργασία είναι πολύ μεγάλος και αυτό αποτελεί μια πρόκληση, γεγονός που καθιστά απαραίτητη την κατανεμημένη αρχιτεκτονική των συστημάτων IDS, τα οποία θα πρέπει να εγκαθίστανται και να λειτουργούν στους κόμβους ομίχλης. (Selim and Sadek, 2021)

5.3.2.3 Εκλεπτυσμένος Έλεγχος Πρόσβασης

Ο έλεγχος πρόσβασης βασισμένος σε ρόλους (Role-based Access control - RBAC) αποτελεί έναν ισχυρό μηχανισμό ασφάλειας για τον έλεγχο της διαχείρισης και εφαρμογής των δικαιωμάτων πρόσβασης ενός χρήστη σε ένα σύστημα, καθώς και την προστασία των πόρων, των δεδομένων και πληροφοριών ενός συστήματος (Kayes *et al.*, 2020). Το RBAC χαρακτηρίζεται ως ένας θεμελιώδης μηχανισμός ελέγχου πρόσβασης, επειδή παρέχει έναν δομημένο και αποτελεσματικό έλεγχο πρόσβασης μέσω τον συσχετίσεων χρήστη-ρόλου και ρόλου-δικαιώματος. Η βασική φιλοσοφία πίσω από το μοντέλο RBAC είναι ότι οι αρμοδιότητες ενός χρήστη είναι πιο σημαντικές από το ποιος είναι ο χρήστης. Έτσι σε ένα μοντέλο RBAC, οι χρήστες μπορούν να αποκτήσουν πρόσβαση σε αντικείμενα του συστήματος χρησιμοποιώντας τους ρόλους τους, οι οποίοι εκχωρούνται με βάση της λειτουργίας των εργασιών που τους έχουν ανατεθεί. Επομένως, κάθε χρήστης αντιστοιχίζεται σε έναν ή περισσοτέρους ρόλους, όπου κάθε ρόλος έχει ένα συγκεκριμένο σύνολο δικαιωμάτων πρόσβασης, τα οποία καθορίζουν ποιες ενέργειες μπορεί να εκτελέσει ένας χρήστης σε δεδομένα, υπηρεσίες ή εφαρμογές (Zhang *et al.*, 2018). Παρακάτω αναλύονται περιληπτικά τα βασικά στοιχεία που περιλαμβάνονται σε ένα μοντέλο RBAC (Kayes *et al.*, 2020):

- *Χρήστης (user):* Ο χρήστης σε ένα μοντέλο RBAC μπορεί είναι είτε ένα φυσικό πρόσωπο είτε μια ψηφιακή οντότητα, όπως ένας πράκτορας (λογισμικού), που υποβάλει αιτήσεις πρόσβασης στο σύστημα, οι οποίες πρέπει να ελεγχθούν. Στο πλαίσιο του RBAC μπορούν να δημιουργηθούν και ρητές ομάδες χρηστών που αντιστοιχίζονται σε συγκεκριμένους ρόλους. Αυτό σημαίνει ότι μια ομάδα χρηστών μπορεί να αντιστοιχηθεί απευθείας σε έναν ρόλο, ώστε όλα τα μέλη της ομάδας να έχουν τα ίδια δικαιώματα και αρμοδιότητες, απλοποιώντας την διαχείριση πρόσβασης σε μεγάλους οργανισμούς.
- *Ρόλος (Role):* Οι ρόλοι αντιπροσωπεύουν ομάδες χρηστών με κοινές αρμοδιότητες και δικαιώματα πρόσβασης σε έναν οργανισμό (π,χ. στον τομέα της υγειονομικής περίθαλψης). Για παράδειγμα, ένας ρόλος στον τομέα της υγειονομικής είναι ο «νοσηλευτής», ο οποίος περιλαμβάνει αρμοδιότητες, όπως η φροντίδα των ασθενών, η παρακολούθηση ζωτικών σημείων και η χορήγηση φαρμάκων, ενώ τα δικαιώματα πρόσβασης περιορίζονται σε ιατρικούς φακέλους, αποκλείοντας διοικητικά, οικονομικά δεδομένα και ιατρικές αποφάσεις.
- *Άδειες* (*Permission*): Οι άδειες επιτρέπουν στους χρήστες να εκτελούν συγκεκριμένες λειτουργίες σε προστατευμένους πόρους, όπως είναι η ανάγνωση ιατρικών αρχείων.

Το περιβάλλον ενός RBAC μπορεί να περιλαμβάνει διάφορες συνθήκες, όπως η φυσική τοποθεσία, το δίκτυο και οι διαπροσωπικές σχέσεις που αναπτύσσονται μεταξύ των χρηστών και του κατόχου των δεδομένων (Kayes *et al.*, 2020). Αυτές οι συνθήκες είναι ιδιαίτερα σημαντικές σε δυναμικά περιβάλλοντα, όπως τα περιβάλλοντα ομίχλης, όπου απαιτείται εκλεπτυσμένος έλεγχος πρόσβασης. Στο πλαίσιο αυτό, εισάγονται δύο νέα βασικά χαρακτηριστικά που ενισχύουν την δυναμικότητα και προσαρμοστικότητα ενός εκλεπτυσμένο έλεγχο πρόσβασης μοντέλου RBAC:

- *Πολιτική αντιστοίχισης ρόλων χρήστη με επίγνωση του περιβάλλοντος (Context-aware user-role assignment policy):* Αναφέρεται στην αντιστοίχιση ενός χρήστη με περισσότερους από έναν ρόλους, η οποία ενεργοποιείται βάσει ενός συνόλου μεταβαλλόμενων συνθήκων του περιβάλλοντος που επικρατούν την δεδομένη χρονική στιγμή. Αυτό επιτρέπει στο σύστημα να προσαρμόζεται στις συνθήκες του περιβάλλοντος, όπως τα ομιχλώδη περιβάλλοντα, όπου οι συνθήκες αλλάζουν συνεχώς. (Kayes *et al.*, 2020)
- *Πολιτική ανάθεσης δικαιωμάτων ρόλων με επίγνωση περιβάλλοντος (context-aware role-permission assignment policy):* Αναφέρεται στην πολιτική της ανάθεσης δικαιωμάτων-ρόλων, όπου η αντιστοίχιση μεταξύ ρόλων και δικαιωμάτων λαμβάνει υπόψη περιβαλλοντικές συνθήκες. Ένας ρόλος μπορεί να έχει διαφορετικά δικαιώματα ανάλογα με τις τρέχουσες συνθήκες του περιβάλλοντος, όπως για παράδειγμα η τοποθεσία, ο χρόνος ή η συσκευή πρόσβασης. Αυτή η αντιστοίχιση έχει πρώτα περάσει από αξιολόγηση για να διασφαλιστεί η ασφάλεια, η ακεραιότητα και η αποτελεσματική διαχείριση των πόρων του συστήματος. (Kayes *et al.*, 2020)

Ένα μοντέλο RBAC είναι πιο ευέλικτο σε σύγκριση με τα παραδοσιακά μοντέλα ελέγχου πρόσβασης (δηλαδή το Διακριτικό Μοντέλο Ελέγχου Πρόσβασης (Discretionary Access Control - DAC) και το Υποχρεωτικό Μοντέλο Ελέγχου Πρόσβασης (Mandatory Access Control - MAC) (Zhang *et al.*, 2018). Το DAC επιτρέπει στον ιδιοκτήτη ενός πόρου να ορίζει ποιος έχει πρόσβαση, κάτι που μπορεί να οδηγήσει σε κενά ασφάλειας, καθώς οι χρήστες μπορούν να μεταβιβάζουν τα δικαιώματα τους σε άλλους χρήστες. Αντίθετα, το MAC βασίζεται σε αυστηρές κεντρικές πολιτικές για την καθορισμένη πρόσβαση, χωρίς να επιτρέπεται στους χρήστες να αλλάξουν ή να τροποποιήσουν τα δικαιώματα που τους έχουν δοθεί , κάνοντας το λιγότερο ευέλικτο και δύσκολο στην διαχείριση (Manor, 2024). Επίσης, το RBAC είναι πιο ισχυρό και γενικευμένο από το MAC και το DAC, επειδή χορηγεί δικαιώματα πρόσβασης μέσω της ανάθεσης ρόλων (Ali *et al.*, 2020). Επομένως, ένα μοντέλο RBAC είναι καταλληλότερο για ομιχλώδη περιβάλλοντα, αφού επιτρέπει την ευκολότερη διαχείριση των δικαιωμάτων πρόσβασης με βάση τους ρόλους, ανεξάρτητα από τις στατικές ταυτότητες των χρηστών, καθιστώντας το ιδανικό για δυναμικά περιβάλλοντα, όπως ένα ομιχλώδες περιβάλλον με συχνές αλλαγές στους χρήστες, τα δικαιώματα χρηστών και στους πόρους (Zhang *et al.*, 2018), (Ali *et al.*, 2020). Για παράδειγμα, η ενσωμάτωση του μοντέλο RBAC στο πλαίσιο υγειονομικής περίθαλψης Fog-Asssisted Blockchain-IoMT αποτελεί μια καινοτόμα αρχιτεκτονική για την ασφαλή, γρήγορη και κλιμακωτή διαχείριση των δεδομένων υγείας στην υγειονομική περίθαλψη 4.0 (Mallick *et al.*, 2024).

Από την άλλη πλευρά, ένα μοντέλο RBAC μπορεί να παρουσιάζει πολλά μειονεκτήματα σε ένα ομιχλώδες περιβάλλον. Πρώτα από όλα, το βασικό RBAC αναπτύχθηκε για την κατανομή των

αδειών σε χρήστες με στατικό τρόπο, οπότε ένα μειονέκτημα του είναι ότι ο ομιχλώδης προγραμματισμός απαιτεί δυναμική κατανομή αδειών που να μπορούν να προσαρμόζονται σε πραγματικό χρόνο. Επίσης, δεν λαμβάνει υπόψη τις περιβαλλοντικές συνθήκες (π.χ. τοποθεσία, χρόνος, περιορισμοί συσκευής) και την δυναμική/τυχαία συμπεριφορά των χρηστών, γεγονός που αποτελεί σοβαρό μειονέκτημα, καθώς αυτές οι συνθήκες είναι κρίσιμες για την ασφάλεια και την αποδοτικότητα στον ομιχλώδη προγραμματισμό. Ωστόσο, σε ένα δυναμικό RBAC, αυτό το πρόβλημα μπορεί να λυθεί, αν και ενδέχεται να προκύψουν άλλες προκλήσεις, όπως η αυξημένη πολυπλοκότητα στην υλοποίηση και την διαμόρφωσή. Επομένως, ένα RBAC δυσκολεύεται να διαχειριστεί σύνθετες ροές εργασίας, όπου απαιτείται δυναμικός διαχωρισμός καθηκόντων, ο οποίος είναι κρίσιμος για την πρόληψη καταστάσεων, όπου οι χρήστες με πρόσβαση στα δεδομένα ή σε συστήματα δύναται να τα αξιοποιήσουν προς όφελος τους, με τρόπο που βλάπτει την οργάνωση ή άλλα άτομα. Ακόμα, οι ανακλήσεις πρόσβασης (access revocations) είναι επώδυνες, επιρρεπείς σε λάθη και χρονοβόρες. Αυτό μπορεί να δημιουργήσει καθυστερήσεις και κενά ασφάλειας στην διαχείριση του ελέγχου πρόσβασης, η οποία είναι κρίσιμη για τον ομιχλώδη προγραμματισμό. (Patwary *et al.*, 2020)

Μια σημαντική έννοια για ένα μοντέλο RBAC είναι η χονδρική κατανομή δικαιωμάτων (coarse-grained), όπου οι ρόλοι περιλαμβάνουν ευρύτερα σύνολα δικαιωμάτων και αδειών. Πιο συγκεκριμένα, ένας ρόλος με γενικές διευρυμένες αρμοδιότητες μπορεί να περαιώσει παραπάνω λειτουργίες (από το κανονικό με βάση τις υπευθυνότητές του) με κίνδυνο να προκαλέσει σοβαρές επιπτώσεις στα συστήματα του ομιχλώδους προγραμματισμού. Για παράδειγμα, στον ρόλο του «Διαχειριστή», μπορεί να του αποδοθεί μια πρόσθετη άδεια, όπως «να προβάλλει τις εγγραφές των υπαλλήλων» επεκτείνοντας έτσι τις αρμοδιότητες του. Αυτό σημαίνει ότι κάθε χρήστης που του ανατίθεται ο ρόλος του Διαχειριστή έχει την άδεια να βλέπει όλα τα αρχεία των υπάλληλών του οργανισμού. Η απονομή αυτής της συγκεκριμένης νέας αρμοδιότητας στις ήδη υπάρχουσες μπορεί να γίνεται αυτόματα και να οδηγήσει τον διευρυμένο ρόλο να αναλάβει υπερβολικά παρά πολλές αρμοδιότητες, αυξάνοντας τον κίνδυνο για μη εξουσιοδοτημένη πρόσβαση στους πόρους και τα δεδομένα του ομιχλώδους προγραμματισμού. (Patwary *et al.*, 2020)

Ο Έλεγχος Πρόσβασης βάσει Χαρακτηριστικών (Attribute-Based Access Control - ABAC) είναι ένα μοντέλο ελέγχου πρόσβασης που βασίζεται σε χαρακτηριστικά (attributes), αντί για ρόλους και άδειες. Τα χαρακτηριστικά μπορεί να αφορούν τον χρήστη (π.χ. ρόλους, τοποθεσία, ώρα), το αντικείμενο που ζητά πρόσβαση ή ακόμα και περιβαλλοντικούς παράγοντες (Coyne and Weil, 2013). Το ABAC ξεχωρίζει, διότι ελέγχει την πρόσβαση σε αντικείμενα αξιολογώντας κανόνες που βασίζονται στα χαρακτηριστικά των οντοτήτων (υποκείμενο και αντικείμενο) και του περιβάλλοντος που σχετίζεται με το αίτημα. Τα χαρακτηριστικά μπορούν να θεωρηθούν ως ιδιότητες οποιουδήποτε πράγματος που μπορεί να οριστεί και στο οποίο μπορεί να ανατεθεί μια τιμή. Στην πιο βασική μορφή το ABAC βασίζεται στην αξιολόγηση, των χαρακτηριστικών του υποκείμενου, των χαρακτηριστικών του αντικειμένου και ενός τυπικού κανόνα σχέσης ή ελέγχου πρόσβασης που ορίζει τις επιτρεπόμενες ενέργειες για συνδυασμούς χαρακτηριστικών υποκειμένων – αντικειμένων. Όλες οι λύσεις ABAC περιλαμβάνουν αυτές τις βασικές ικανότητες αξιολόγησης

χαρακτηριστικών και επιβολής κανόνων ή σχέσεων μεταξύ αυτών των χαρακτηριστικών. Τα συστήματα ABAC υπάγουν τόσο τα μοντέλα DAC όσο και τα MAC. (Hu *et al.*, 2013)

Τα πλεονεκτήματα του ABAC περιλαμβάνουν την ευελιξία του να ενσωματώνει δυναμικά μεταβαλλόμενα χαρακτηριστικά, όπως η ώρα και η τοποθεσία, καθιστώντας το κατάλληλο για κατανεμημένα συστήματα, όπως είναι ο ομιχλώδης προγραμματισμός. Επίσης, επιτρέπει την απλούστερη διαχείριση των δικαιωμάτων χωρίς την λεπτομερή ανάγκη για σχεδιασμό ρόλων , όπως απαιτεί το RBAC. Ακόμη, θεωρείται πως είναι πιο εκφραστικό μοντέλο πρόσβασης από τα υπόλοιπά, κάνοντάς το ιδανική περίπτωση σε περιβάλλοντα ομιχλώδους προγραμματισμού, καλύπτοντας όλα τα δυνατά σενάρια ελέγχου πρόσβασης. (Coyne and Weil, 2013)

Ένα μειονέκτημα του ABAC είναι η πολυπλοκότητα στην διαχείριση του μεγάλου αριθμού των χαρακτηριστικών και η δυσκολία ελέγχου, καθώς δεν είναι εύκολο να παρακολουθεί ποιοι χρήστες έχουν πρόσβαση σε συγκεκριμένες άδειες χωρίς την εξαντλητική ανάλυση των χαρακτηριστικών. Επιπλέον, το ABAC ενδέχεται να επιβαρύνει την απόδοση του συστήματος, καθώς απαιτεί αυξημένο υπολογιστικό φορτίο για την ανάλυση των χαρακτηριστικών κατά την διάρκεια της διαδικασίας ελέγχου πρόσβασης. (Coyne and Weil, 2013)

5.3.2.4 Σκλήρυνση υπερεπόπτη (Hypervisor Hardening)

Η σκλήρυνση του υπερεπόπτη αποτελεί έναν κρίσιμο παράγοντα για την συνολική ασφάλεια του συστήματος του ομιχλώδους προγραμματισμού. Αυτό δεν περιορίζεται μόνο στην εγκατάσταση των τελευταίων επιδιορθώσεων ασφάλειας (patches) στον υπερεπόπτη, αλλά περιλαμβάνει σημαντικά μέτρα που αποσκοπούν στην μείωση της επιφανείας επίθεσης και στην ενίσχυση της ασφάλειας (Roman, Lopez and Mambo, 2018).

Ειδικότερα, υπάρχουν κι άλλες ενέργειες προς σκλήρυνση του υπερεπόπτη που επιφέρουν πολλά πλεονεκτήματα. Πρώτον, η ελαχιστοποίηση του μεγέθους του κώδικα στον υπερεπόπτη, μπορεί να μειώσει την επιφάνεια επίθεσης του υπερεπόπτη στον ομιχλώδη προγραμματισμό, καθώς μειώνει τον αριθμό των πιθανών (τρωτών) σημείων εισόδου που μπορεί να εκμεταλλευτούν οι κακόβουλοι παράγοντες για να διεισδύσουν, να βλάψουν ή να ελέγξουν το σύστημα (Pék, Buttyán and Bencsáth, 2013).

Μια άλλη μέθοδος σκλήρυνσης αφορά την προστασία των υπερεποπτών μέσω φιλτραρίσματος ύποπτων αιτημάτων προς τον υπεροπόπτη μειώνοντας έτσι την επίθεση επιφάνειας και λειτουργώντας σαν τείχος προστασίας για τα εικονικά μηχανήματα του συστήματος του ομιχλώδους προγραμματισμού, ενισχύοντας με αυτό τον τρόπο την ασφάλεια των περιβαλλόντων ομίχλης. Αυτό μπορεί να γίνει με την προσθήκη ενός firewall ή IDS πάνω από τον υπερεπόπτη (Ishiguro and Kono, 2018). Ακόμη, μια σημαντική μέθοδος σκλήρυνσης είναι η δημιουργία ασφαλών και απομονωμένων περιβαλλόντων στον ομιχλώδη προγραμματισμό μέσω διαφόρων τεχνικών, όπως το NoHype για την μείωση ή την εξάλειψη της επίθεσης επιφάνειας. Το NoHype

στοχεύει στην μείωση της εξάρτησης από τον υπερεπόπτη, εξαλείφοντας πιθανά σημεία επίθεσης (Pék, Buttyán and Bencsáth, 2013). Επιπλέον, ο κατάλληλος έλεγχος πρόσβασης και η απενεργοποίηση μη απαραίτητων χαρακτηριστικών στον υπερεπόπτη αποτελούν σημαντικά βήματα σκλήρυνσης του, καθώς μειώνουν τα τρωτά σημεία του συστήματος και περιορίζουν πιθανές επιθέσεις.

Από την άλλη πλευρά, παρά την πρόοδο που έχει σημειωθεί στην ανάπτυξη των προϊόντων υπερεποπτών, αυτά συχνά παρουσιάζουν αυξημένη πολυπλοκότητα, ενώ παράλληλα οδηγούν σε αυξημένη επιφάνεια επίθεσης. Αν και υπάρχουν ήδη ακαδημαϊκές προτάσεις και εξειδικευμένες λύσεις, όπως η μέθοδος των ελαφριών υπερεποπτών (lightweight hypervisors), που προσπαθούν να αντιμετωπίσουν τα παραπάνω ζητήματα, η διαχείριση πολλαπλών εικονικών μηχανών σε περιβάλλοντα ομίχλης παραμένει δύσκολη, καθώς αυτές οι εικονικές μηχανές απαιτούν σημαντικούς υπολογιστικούς πόρους και είναι βαριές. Αυτό δεν σημαίνει μόνο ότι η απόδοση και η ενέργεια των κόμβων ομίχλης μειώνεται, αλλά ότι αυξάνεται η επιφάνεια επιθέσεις στους κόμβους ομίχλης. Επομένως, είναι προτιμότερο να εξετάζονται και άλλες τεχνολογίες εικονικοποίησης, όπως είναι τα δοχεία που αντιπροσωπεύουν ελαφρύτερες λύσεις και εκθέτουν το σύστημα σε λιγότερες ευπάθειες, βελτιώνοντας την απόδοση και την ασφάλεια του συστήματος. Επιπλέον, οι εικονικές μηχανές θα πρέπει να είναι σκληρυμένες, προκειμένου να μειωθεί η έκθεση σε ευπάθειες. Ακόμα, καμία τεχνική σκλήρυνσης από μόνη της δεν μπορεί να εξαλείψει όλες τις ευπάθειες σε ένα σύστημα ομιχλώδης προγραμματισμού. Για παράδειγμα, το FWinst[5], μειώνει τον κίνδυνο έκθεσης σε κενά ασφάλειας στον εξομοιωτή[6] (emulator), άλλα δεν εξαλείφει όλες τις απειλές, όπως είναι η αποκάλυψη των δεδομένων, διαφυγή δεδομένων κ.α. Οπότε, δεν είναι δυνατόν να καλυφθούν όλες οι απειλές. Άρα, είναι απαραίτητο να εφαρμοστούν επιπρόσθετα μέτρα ασφάλειας για την εξασφάλιση της συνολικής προστασίας του συστήματος. (Ishiguro and Kono, 2018)

5.3.2.5 Επόπτης Εικονικής Μηχανής (Virtual Machine Monitor)

Η ασφάλεια των εικονικών μηχανών είναι άρρηκτα συνδεδεμένη με την ασφάλεια ολοκλήρου του ομιχλώδους προγραμματισμού. Ο επόπτης εικονικής μηχανής (Virtual Machine Monitor, VMM) είναι μέρος / συστατικό του υπερεπόπτη που παρέχει μηχανισμούς ασφάλειας για εικονικές μηχανές και βρίσκεται μεταξύ του υποκείμενου λειτουργικού συστήματος του οικοδεσπότη (host operating system) και των επισκεπτών εικονικής μηχανής (guest virtual machine). Ο VMM περιλαμβάνει τον

[5] Το FWinst είναι εργαλείο ασφάλειας που επικεντρώνεται στην μείωση των κίνδυνων από την εξομοίωση εντολών (instruction emulation) σε περιβάλλοντα υπερεπόπτων, εφαρμόζοντας διαφορετικά σύνολα εντολών ανάλογα με το περιβάλλον (context) στο οποίο εκτελούνται (Ishiguro and Kono, 2018).

[6] Ένας εξομοιωτής μπορεί να είναι είτε υλικό είτε λογισμικό, ο οποίος επιτρέπει σε λογισμικό που σχεδιάστηκε για ένα περιβάλλον να εκτελείται σε διαφορετικό περιβάλλον, μιμούμενος τη λειτουργία του αρχικού συστήματος. Στο πλαίσιο της εικονικοποίησης, ο εξομοιωτής χρησιμοποιείται για την αναπαραγωγή της λειτουργίας του υλικού, επιτρέποντας σε εικονικές μηχανές να τρέχουν λογισμικό που είναι γραμμένο για διαφορετικό υλικό (Pure Storage, 2024).

ανιχνευτή (detector) και έναν καταγραφέα προειδοποιήσεων (warning recorder). Ο ανιχνευτής είναι ικανός να εντοπίζει κάθε απρόβλεπτο γεγονότος, καθώς και ασυνήθιστες ή ύποπτες δραστηριότητες, ενώ ο καταγραφέας διατηρεί ένα αρχείο ως ιστορικό, στο οποίο καταγράφεται κάθε (κακόβουλη) δραστηριότητα για μελλοντική χρήση. Ο διαχωρισμός του VMM ως ξεχωριστού στοιχείου είναι απαραίτητος, καθώς αναλαμβάνει εξειδικευμένες λειτουργίες ασφάλειας που επηρεάζουν άμεσα την ασφάλεια των εικονικών μηχανών, τις οποίες δεν καλύπτει ο υπερεπόπτης. (Abbasi and Shah, 2017)

Η υιοθέτηση των VMM προσφέρει σημαντικά οφέλη για την ενίσχυση της ασφάλειας του ομιχλώδους προγραμματισμού, μειώνοντας τον κίνδυνο των κυβερνοεπιθέσεων και προστατεύοντας τα δεδομένα και τους πόρους των χρηστών. Πρώτα από όλα, ο VMM επιφέρει ένα επιπλέον επίπεδο προστασίας σε συνεργασία με άλλα αντιδραστικά συστήματα ασφάλειας, όπως τα IDS και τα IPS, που ανιχνεύουν κακόβουλες δραστηριότητες. Με αυτό τον τρόπο, αυτό το επιπλέον επίπεδο προστασίας που παρέχει ο VMM, το οποίο περιλαμβάνει μηχανισμούς όπως η απομόνωση των εικονικών μηχανών, η παρακολούθηση της συμπεριφοράς των εικονικών μηχανών και η ανίχνευση κακόβουλων δραστηριοτήτων, βοηθά στην απομόνωση και του λειτουργικού συστήματος του οικοδεσπότη, περιορίζοντας την εξάπλωση κακόβουλου λογισμικού μεταξύ του λειτουργικού συστήματος του οικοδεσπότη και των εικονικών μηχανών ή το αντίστροφο. (Volokyta, Kokhanevych and Ivanov, 2012)

Ο περιορισμός της εξάπλωσης κακόβουλου λογισμικού επιτυγχάνεται μέσω της χρήσης μηχανισμών ελέγχων πρόσβασης, οι οποίοι ενσωματώνονται στον υπερεπόπτη και αποτρέπουν την άμεση αλληλεπίδραση μεταξύ των εικονικών μηχανών και του οικοδεσπότη. Επιπλέον, μέσω της διαχείρισης πόρων, ο VMM διασφαλίζει την απομόνωση των λειτουργιών των εικονικών μηχανών, έτσι ώστε σε περίπτωση που κακόβουλο λογισμικό μολύνει μία από τις εικονικές μηχανές, να περιορίζεται η εξάπλωση του και να μειώνεται η πιθανότητα μετάδοσης στον οικοδεσπότη ή στις άλλες εικονικές μηχανές. Επίσης, ο επόπτης εικονικής μηχανής μέσω της παρακολούθησης της συμπεριφοράς των εικονικών μηχανών και της ανάλυσης των δεδομένων του, εξασφαλίζει τον έγκυρο εντοπισμό των επιθέσεων σε πρώιμο στάδιο. Για την αποτελεσματική πρόληψη των επιθέσεων, ο VMM συνεργάζεται με εσωτερικά συστατικά του υπερεπόπτη, όπως το hypervisor security modules, τα οποία παρέχουν μηχανισμούς προστασίας κατά των επιθέσεων στο επίπεδο του υπερεπόπτη, καθώς και το hypervisor introspection, το οποίο επιτρέπει την ανάλυση της δραστηριότητας των εικονικών μηχανών για την ανίχνευση ύποπτων ή κακόβουλων ενεργειών. Επίσης, ο VMM συνεργάζεται με εξωτερικά συστήματα ασφάλειας, όπως τα IDS, τα συστήματα παρακολούθησης ακεραιότητας (integrity monitoring systems) κ.α. (Volokyta, Kokhanevych and Ivanov, 2012)

Από την άλλη πλευρά, ο μηχανισμός ασφάλειας VMM σε συνεργασία με το IDS μπορεί κάποιες φορές να χαρακτηρίσει λανθασμένα μια δραστηριότητα ως κακόβουλη δραστηριότητα, ενώ δεν είναι, καθώς το IDS είναι υπεύθυνο για την ανίχνευση και την κατηγοριοποίηση των δραστηριοτήτων. Το παραπάνω μειονέκτημα μπορεί να οδηγήσει σε λανθασμένες ενέργειες, όπως ο αποκλεισμός χρηστών ή στην διακοπή υπηρεσιών στα συστήματα του ομιχλώδους

προγραμματισμού. Επιπλέον, η συνεχής παρακολούθηση των εικονικών μηχανών και η ανάλυση των δεδομένων από τον VMM, απαιτούν τεράστια υπολογιστική ισχύ και αποθηκευτικό χώρο. Αυτό μπορεί να οδηγήσει σε αυξημένη κατανάλωση πόρων του συστήματος, επηρεάζοντας την απόδοση άλλων ομιχλωδών εφαρμογών ή υπηρεσιών. (Volokyta, Kokhanevych and Ivanov, 2012)

5.3.2.6 Σύγκριση αντιμέτρων για την αντιμετώπιση των ζητημάτων εικονικοποίησης στον ομιχλώδη προγραμματισμό

Τα κριτήρια σύγκρισης που παρουσιάζονται στην ενότητα 5.2 της παρούσας διπλωματικής εργασίας εφαρμόστηκαν για την αξιολόγηση των αντιμέτρων που αφορούν την αντιμετώπιση των ζητημάτων εικονικοποίησης, όπως αυτά περιγράφονται στις ενότητες 5.3.2.6-5.3.2.5 της διπλωματικής εργασίας. Παρακάτω πρώτα δικαιολογούνται τα αποτελέσματά της αξιολόγησης των αντιμέτρων με βάση τα κριτήρια αυτά και έπειτα παρουσιάζονται τα αποτελέσματα αυτά στον Πίνακας 3.

Κατανάλωση Πόρων

- Η MFA χαρακτηρίζεται από μέτρια κατανάλωση πόρων (η τιμή κυμαίνεται μεταξύ του 2 και του 3 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων»), γιατί δεν απαιτούνται πολλοί πόροι, αλλά η απαίτηση σε πόρους σε ορισμένες περιπτώσεις μπορεί να αυξηθεί. Αυτή η διακύμανση εξαρτάται από τους αλγόριθμους που χρησιμοποιούνται (π.χ. βιομετρική επαλήθευση) και την υποδομή που εφαρμόζονται στην κάθε περίσταση του προβλήματος που αυτά καλούνται να εφαρμοστούν.
- Το HIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων», δηλαδή χαρακτηρίζεται από μεσαία κατανάλωση πόρων, αφού μπορεί να απαιτεί σημαντικούς υπολογιστικούς πόρους έτσι ώστε να παρακολουθεί και να αναλύει τα αρχεία και τις δραστηριότητες σε επίπεδο συστήματος.
- Ένα NIDS έχει μέτρια κατανάλωση πόρων στο σύστημα (αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων»), καθώς η παρακολούθηση μεγάλου όγκου δεδομένων μπορεί να επιβαρύνει τους διαδικτυακούς πόρους του περιβάλλοντος ομίχλης
- Τα υβριδικά IDS αξιολογούνται με τιμή 2 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων», επειδή τα υβριδικά συστήματα είναι ο συνδυασμός των συστημάτων HIDS και NIDS, γεγονός που σημαίνει ότι καταναλώνουν παρά πολλούς πόρους, καθώς χρειάζεται να παρακολουθούν και να αναλύουν τόσο το δίκτυο όσο και τις μεμονωμένες συσκευές ταυτόχρονα.
- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων», γιατί το RBAC είναι πιο αποδοτικό στην διαχείριση των πόρων του, ιδιαίτερα όταν οι ρόλοι και οι άδειες είναι στατικές και προκαθορισμένες.
- Το ABAC αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων», γιατί το ABAC μπορεί να χρειάζεται να καταναλώσει παρά πολλούς πόρους σε σύγκριση με το RBAC για την ανάλυση και την διαχείριση των χαρακτηριστικών τους, αλλά και των χαρακτηριστικών των υποκειμένων και του περιβάλλοντος, ιδιαίτερα σε περιβάλλοντα με μεγάλο όγκο δεδομένων.

- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων», καθώς η ανάγκη υιοθέτησης επιπλέον μέτρων ασφάλειας για την αντιμετώπιση ευπαθειών, όπως η επιφάνεια επίθεσης αυξάνουν την πολυπλοκότητα του συστήματος και επομένως και την κατανάλωση των πόρων.
- Το VMM αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Κατανάλωση Πόρων», αφού δεν απαιτεί υψηλή υπολογιστική ισχύ και αποθηκευτικό χώρο για την συνεχή παρακολούθηση και την ανάλυση των εικονικών μηχανών ως συστατικό μέρος του υπερεπόπτη.

Κλιμακωσιμότητα

- Η τιμή αξιολόγησης της MFA κυμαίνεται με από 2 έως 4 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», διότι υποστηρίζει άνετα έναν μεγάλο αριθμό χρηστών, αλλά ορισμένοι παράγοντες αυθεντικοποίησης, όπως οι βιομετρικοί μπορεί να επηρεάσουν αρνητικά την κλιμακωσιμότητα.
- Το HIDS αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», δηλαδή έχει περιορισμένη κλιμακωσιμότητα, αφού το HIDS είναι σχεδιασμένο για μεμονωμένα συστήματα και όχι για ολόκληρα δίκτυα που σημαίνει ότι δεν μπορεί να κλιμακωθεί ευκολά.
- Το NIDS έχει μέτρια κλιμακωσιμότητα (αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα»), διότι αν και τα NIDS έχουν σχεδιαστεί για την παρακολούθηση του δικτύου σε μεγάλα δίκτυα, όπως αυτά των περιβαλλόντων ομίχλης, μπορεί να υπάρχουν περιορισμοί στην κλιμάκωσή τους, λόγω της αυξημένης κίνησης μεταξύ των κόμβων που μπορεί να προκαλέσει επιπλέον καθυστερήσεις.
- Τα υβριδικά IDS αξιολογούνται με τιμή 4 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», καθώς η αρχιτεκτονική τους επιτρέπει την απορρόφηση των επιθέσεων πρώτα σε δικτυακό επίπεδο και στην συνέχεια σε επίπεδο ξενιστών (host), βελτιώνοντας την απόδοση και επιτρέποντας και επιτρέποντας την κατανομή του φόρτου σε πολλαπλά επίπεδα, κάνοντας το σύστημα πιο ανθεκτικό και διαχειριστικό όταν αυξάνεται ο όγκος των δεδομένων.
- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», καθώς μπορεί να κλιμακωθεί και να διαχειριστεί τον μεγάλο αριθμό των χρηστών και των δικαιωμάτων μέσω ρόλων. Όμως, η διαχείριση του μεγάλου αριθμού αντικειμένων για τα οποία πρέπει να ελεγχθεί η πρόσβαση προσθέτει πολυπλοκότητα. Αυτό μπορεί να επηρεάσει την κλιμακωσιμότητα του συστήματος και να την καθιστά λιγότερο αποτελεσματική σε μεγάλα περιβάλλοντα.
- Το ABAC αξιολογείται με τιμή 5 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», καθώς το ABAC μπορεί να επεκταθεί εύκολα, αφού η διαχείριση των χαρακτηριστικών γίνεται με βάση δυναμικών παραμέτρων και δεν περιορίζεται από προκαθορισμένες δομές.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», διότι ο υπερεπόπτης εκτελείται σε μηχάνημα με περιορισμένες δυνατότητες (υπολογιστικές).
- Ο VMM αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Κλιμακωσιμότητα», γιατί ο VMM ως μέρος του υπερεπόπτη εκτελείται σε μηχανήματα με περιορισμένες υπολογιστικές δυνατότητες.

Ασφάλεια δεδομένων

- Η MFA αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», αλλά δεν είναι απολυτά αδιαπέραστη σε καινούργιες απειλές
- Το HIDS αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», διότι μπορεί να παρακολουθεί εις βάθος τις δραστηριότητες σε ένα σύστημα και να ανιχνεύει εσωτερικές απειλές.
- Το NIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», διότι αν και μπορεί να ανιχνεύει απειλές στο δίκτυο είναι πιο δύσκολο η πλήρης κάλυψης της ασφάλειας σε όλα τα επίπεδα του δικτύου, λόγω της αποκεντρωμένης φύσης του ομιχλώδους προγραμματισμού και της διαφορετικότητας των συσκευών.
- Τα υβριδικά συστήματα IDS αξιολογούνται με τιμή 4 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», διότι αν και τα υβριδικά συστήματα IDS προσφέρουν υψηλό επίπεδο προστασίας παρακολουθώντας τόσο την δραστηριότητα του συστήματος όσο και την κίνηση του δικτύου, πάντα θα υπάρχει η πιθανότητα κάποιας απειλής που δεν θα ανιχνεύεται.
- Το RBAC αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», διότι αν και παρέχει έναν οργανωμένο έλεγχο πρόσβασης μέσω ρόλων, η απονομή υπερβολικών δικαιωμάτων σε γενικούς ρόλους μπορεί να δημιουργήσει πιθανούς κινδύνους ασφάλειας.
- Το ABAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», παρόλο που ο έλεγχος πρόσβασης στο ABAC βασίζεται σε ένα συνδυασμό πολλών παραμέτρων, όπως η τοποθεσία και ο χρόνος, προσφέροντας πιο αυστηρούς περιορισμούς στην πρόσβαση των χρηστών σε δυναμικά περιβάλλοντα δεν μπορεί να προστατεύσει από κάθε πιθανή απειλή. Επιπλέον, υπάρχει ο κίνδυνος της μη σωστής μοντελοποίησης των κανόνων πρόσβασης.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων». Αυτό σημαίνει ότι μπορεί να προσφέρει σχετικά πολύ καλή προστασία από επιθέσεις, αφού μειώνει την επιφάνεια επίθεσης, αλλά μπορεί να είναι επιρρεπής σε επιθέσεις, όπως οι πλευρικές επιθέσεις.
- Το VMM αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ασφάλεια δεδομένων», παρόλο που προσφέρει προστασία μέσω της απομόνωσης του λειτουργικού συστήματος του οικοδεσπότη και των εικονικών μηχανών, η προστασία του εξαρτάται από την συνεργασία με άλλα συστήματα ασφάλειας.

Ευκολία χρήσης

- Η MFA αξιολογείται με τιμή 3-4 στο κριτήριο σύγκρισης «Ευκολία χρήσης», καθώς εξαρτάται από τον συγκεκριμένο μηχανισμό MFA και τους παράγοντες αυθεντικοποίησης που εφαρμόζεται κάθε φόρα. Ενώ η MFA είναι πιο περιπλοκή σε σχέση με τους απλούς κωδικούς πρόσβασης, αλλά οι σύγχρονοι μηχανισμοί, όπως οι βιομετρικοί παράγοντες παρόλο που προσφέρουν μεγαλύτερη ασφάλεια μπορεί να οδηγήσουν σε περισσότερη πολυπλοκότητα στον χρήστη.
- Το HIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ευκολία χρήσης». Αν θεωρήσουμε ότι ο χρήστης είναι ο διαχειριστής του συστήματος, τότε ένα HIDS απαιτεί

καλή γνώση του συστήματος και των αρχείων που παρακολουθούνται, γεγονός που καθιστά την διαμόρφωση και την ρύθμιση του δύσκολη, ειδικά για διαχειριστές χωρίς εξειδικευμένες γνώσεις. Αν ο χρήστης είναι απλός, τότε δεν ασχολείται άμεσα με την εγκατάσταση και την διαμόρφωση του αντιμέτρου.

- Το NIDS αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Ευκολία χρήσης», διότι η παρακολούθηση και ανάλυση της κατανεμημένης κίνησης του δικτύου πραγματοποιείται αυτόματα από το αντίμετρο, αλλά η σωστή ρύθμιση του αντιμέτρου απαιτεί πιο εξειδικευμένη γνώση και εμπειρία από έναν διαχειριστή, γεγονός που καθιστά την χρήση του πιο απαιτητική σε σχέση με τα αλλά συστήματα ασφάλειας, όπως το HIDS.
- Τα υβριδικά συστήματα IDS αξιολογούνται με τιμή 1 στο κριτήριο σύγκρισης «Ευκολία χρήσης», διότι τα υβριδικά συστήματα είναι πιο πολύπλοκα στην διαχείριση από τα απλά HIDS και NIDS, λόγω της ανάγκης για συντονισμό μεταξύ αυτών των δύο συστημάτων.
- Το ABAC αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ευκολία χρήσης», διότι η διαχείριση των χαρακτηριστικών του μπορεί να είναι αρκετά περιπλοκή και να απαιτείται πιο εξειδικευμένη γνώση για την σωστή εφαρμογή του.
- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Ευκολία χρήσης», διότι παρέχει μια δομημένη διαχείριση πρόσβασης μέσω ρόλων, κάνοντας την πρόσβαση στο σύστημα και τα δεδομένα πιο κατανοητή για τους χρήστες. Ωστόσο, υπάρχει κάποια πολυπλοκότητα στη διαχείριση και την διαμόρφωση του συστήματος, γεγονός που καθιστά την χρήση του λίγο απαιτητική σε σχέση με άλλα συστήματα.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Ευκολία χρήσης», καθώς η πολυπλοκότητα του υπερεπόπτη σε συνδυασμό με τα προσθετά μετρά ασφάλειας, καθιστούν το αντίμετρο αυτό πιο δύσκολο και λιγότερο φιλικό προς τους χρήστες.
- Το VMM αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Ευκολία χρήσης», καθώς οι αυτόματες λειτουργίες ανίχνευσης του VMM το κάνουν πιο εύκολο στην χρήση για τους διαχειριστές του VMM. Ωστόσο, η ενοποίηση του με άλλα συστατικά του υπερεπόπτη και με εξωτερικούς μηχανισμούς, όπως το IDS, αυξάνει την πολυπλοκότητα της διαχείρισης και της διαμόρφωσης του αντιμέτρου.

Εκπαίδευση χρηστών

- Η MFA αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», αφού οι διαχειριστές όσο και οι απλοί χρήστες χρειάζονται κάποια εκπαίδευση για να κατανοήσουν την σημασία της MFA και πως να την χρησιμοποιήσουν σωστά.
- Το HIDS αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», αφού οι διαχειριστές ενημερώνονται κυρίως από το HIDS σε περίπτωση κάποιου συμβάντος, αλλά σε περίπτωση διερεύνησης, μπορεί να απαιτηθεί ο έλεγχος των δεδομένων που έχει συλλέξει το σύστημα.
- Το NIDS αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», διότι οι διαχειριστές των NIDS απαιτούν να έχουν εξειδικευμένες γνώσεις γύρω από τα δίκτυα για την σωστή ρύθμιση τους. Παράλληλα, απαιτείται μακροχρόνια εκπαίδευση για την πλήρη αξιοποίηση των δυνατότητων του εργαλείου και την σωστή χρήση του.

- Τα υβριδικά συστήματα IDS αξιολογούνται με τιμή 1 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», διότι η πολυπλοκότητα διαχείρισης και ρύθμισης αυξάνει, απαιτώντας την εκπαίδευση των διαχειριστών των HIDS και NIDS.
- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», διότι απαιτείται εκπαίδευση για την σωστή διαχείριση και την σωστή εφαρμογή του μοντέλου RBAC, ιδιαίτερα για τους διαχειριστές του RBAC. Το μοντέλο αυτό ρυθμίζεται και εφαρμόζεται από τους διαχειριστές, οι οποίοι εισάγουν τα δεδομένα και καθορίζουν τα δικαιώματα πρόσβασης.
- Το ABAC αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», διότι οι χρήστες και οι διαχειριστές του ABAC πρέπει να κατανοήσουν πρώτα πως λειτουργούν τα χαρακτηριστικά και οι δυναμικές παράμετροι του ABAC, που σημαίνει ότι απαιτείται επιπλέον εκπαίδευση ως προς αυτές τις δύο πλευρές. Η εκπαίδευση αυτή είναι πιο απαιτητική σε σχέση με το RBAC, λόγω της μεγαλύτερης πολυπλοκότητας του ABAC.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με την τιμή 2 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», διότι η αυξημένη πολυπλοκότητα που συνεπάγεται η σκλήρυνση του υπερεπόπτη, καθώς και η βαθιά κατανόηση των τεχνικών και των στρατηγικών που χρησιμοποιούνται για την προστασία του συστήματος απαιτεί εξειδικευμένη και εκτεταμένη εκπαίδευση των διαχειριστών.
- Το VMM αξιολογείται με την τιμή 3 στο κριτήριο σύγκρισης «Εκπαίδευση Χρηστών», διότι απαιτείται εκπαίδευση για τη σωστή χρήση του, την ενοποίηση του με συστατικά του υπερεπόπτη και εξωτερικά αντίμετρα, καθώς και για την σωστή ρύθμιση του VMM και των εξωτερικών αντιμέτρων. Η εκπαίδευση αυτή είναι απαραίτητη για να εξασφαλιστεί η ακρίβεια ανίχνευσης και αποφευχθούν οι λανθασμένες ανιχνεύσεις επιθέσεων.

Αντίκτυπος στον χρήστη

- Η MFA αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στο χρήστη», διότι η MFA μπορεί να αυξήσει τον χρόνο σύνδεσης καθώς προσθέτει ένα επιπλέον βήμα στην διαδικασία της σύνδεσης.
- Το HIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στο χρήστη», δηλαδή έχει μέτριο αντίκτυπο, διότι ένα HIDS επιβαρύνει ελαφρώς την απόδοση του συστήματος, Ιδιαίτερα σε συστήματα με περιορισμένους πόρους μπορεί να οδηγήσει σε μικρές καθυστερήσεις στις εφαρμογές ή να προκαλέσει λανθασμένα θετικά, τα οποία ενδέχεται να επηρεάσουν σημαντικά την εμπειρία του χρήστη.
- Το NIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στον χρήστη», αφού δεν επηρεάζει άμεσα το σύστημα που παρακολουθεί, σε περιπτώσεις όπου μπλοκάρονται πακέτα, ενδέχεται να παρουσιαστούν προβλήματα σε δικτυακές εφαρμογές, όπως η επαναποστολή πακέτων ή απώλεια πακέτων.
- Τα υβριδικά συστήματα IDS αξιολογούνται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στο χρήστη», διότι τα υβριδικά συστήματα IDS παρέχουν ισχυρότερη προστασία και γρήγορη ανίχνευση απειλών, αλλά η απόδοση τους εξαρτάται από την διαχείριση των πόρων, κάτι που αν δεν γίνει αποτελεσματικά μπορεί να επηρεάσει αρνητικά την εμπειρία χρήσης.

- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Αντίκτυπος στο χρήστη», διότι αν η ρύθμιση των ρόλων γίνει σωστά, ο αντίκτυπος είναι θετικός, παρέχοντας στους χρήστες την κατάλληλη πρόσβαση χωρίς περιορισμούς ή υπερβολική εξουσιοδότηση.
- Το ABAC αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στο χρήστη», καθώς η πολυπλοκότητα του αντιμέτρου και το αυξημένο επίβαρο απόδοσης σε σχέση με το RBAC ενδέχεται να επηρεάσουν αρνητικά την απόδοση του συστήματος, προκαλώντας αντίκτυπο στην εμπειρία του χρήστη.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στο «χρήστη», διότι η πολυπλοκότητα του συστήματος που προκαλεί η σκλήρυνση του υπερεπόπτη, καθώς και η πιθανή μείωση της απόδοσης του συστήματος μπορεί να επηρεάσουν αρνητικά την εμπειρία του χρήστη.
- Το VMM αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Αντίκτυπος στο χρήστη», διότι τα ψευδή αποτελέσματα επιθέσεων του VMM μπορεί να οδηγήσουν στον αποκλεισμό των χρηστών ή στην διακοπή των υπηρεσιών του συστήματος.

Εφαρμοσιμότητα

- Η MFA αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», παρόλο που μπορεί να εφαρμοστεί σε διάφορα συστήματα, ενδέχεται να απαιτήσει προσαρμογές ανάλογα με την υφιστάμενη υποδομή. Για παράδειγμα, η χρήση βιομετρικών συστημάτων μπορεί να επηρεάσει αρνητικά την εφαρμοσιμότητα σε ομιχλώδη περιβάλλοντα, ενώ ορισμένα συστήματα, όπως οι IoT συσκευές, μπορεί να απαιτούν κατάλληλο αποθηκευτικό χώρο και αξιόπιστους βιομετρικούς αισθητήρες.
- Ένα HIDS αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», διότι η εφαρμογή του HIDS σε κόμβους ομίχλης είναι περιορισμένη λόγω της ετερογένειας των κόμβων και των περιορισμένων πόρων τους.
- Το NIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», διότι τα NIDS έχουν σχεδιαστεί για να εφαρμόζονται σε διαδικτυακά περιβάλλοντα με μεγάλα δίκτυα και μπορεί να ανταποκριθεί σε διάφορα είδη δικτύων, προσφέροντας καλή εφαρμοσιμότητα. Ωστόσο, η εφαρμογή του μπορεί να περιοριστεί σε περιβάλλοντα ομίχλης, λόγω των σημαντικών πόρων που απαιτεί, οι οποίοι μπορεί να μην είναι διαθέσιμοι.
- Τα υβριδικά συστήματα IDS αξιολογούνται με τιμή 2 στο κριτήριο σύγκρισης «Εφαρμοσιμοτήτα», διότι προσφέρουν μια ευρεία κάλυψη τόσο σε επίπεδο δικτύου όσο και σε επίπεδο συστήματος, καθιστώντας τα κατάλληλα για εφαρμογές σε ποικίλα περιβάλλοντα.
- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», διότι το RBAC μπορεί να εφαρμοστεί σε πολλούς οργανισμούς και περιβάλλοντα.
- Το ABAC αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», διότι αν και μπορεί να προσαρμοστεί ευκολά σε μεταβαλλόμενες συνθήκες σε πραγματικό χρόνο, απαιτεί πολλούς πόρους και δεν έχει πάντα καλή απόδοση. Επιπλέον, μπορεί να μην είναι εφικτό να λαμβάνονται όλες οι απαραίτητες παράμετροι από το περιβάλλον, ενώ η εφαρμογή καταλλήλου μοντέλου εμπιστοσύνης είναι ιδιαίτερα δύσκολη σε ομιχλώδη περιβάλλοντα.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 2-3 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», διότι η ενσωμάτωση του υπερεπόπτη σε ομιχλώδη περιβάλλοντα

μπορεί να παρουσιάσει δυσκολίες εξαιτίας όχι μόνο της πολυπλοκότητας της σκλήρυνσης, άλλα και της αυξημένης χρήσης των πόρων. Εάν προστεθούν και οι απαιτούμενοι μηχανισμοί ή λειτουργίες ασφάλειας, η εφαρμογή γίνεται ακόμα πιο απαιτητική.

- Το VMM αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Εφαρμοσιμότητα», διότι αν και μπορεί να εφαρμοστεί σε περιβάλλοντα ομίχλης και να συνδυαστεί με άλλους μηχανισμούς ασφάλειας, η εφαρμοσιμότητα του επηρεάζεται από την εφαρμοσιμότητα του υπερεπόπτη, του οποίου αποτελεί μέρος. Επιπλέον, το VMM απαιτεί σημαντικούς πόρους, γεγονός που περιορίζει την αποτελεσματική του χρήση, ιδιαιτέρα σε περιβάλλοντα με περιορισμένους πόρους.

Βαθμός κάλυψης

- Η MFA αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Βαθμός κάλυψης», διότι η MFA μπορεί να εφαρμοστεί σε ευρύ φάσμα εφαρμογών και σεναρίων.
- Ένα HIDS έχει μέτριο βαθμό κάλυψης (αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Βαθμός Κάλυψης»), διότι επικεντρώνεται σε μεμονωμένα συστήματα και μπορεί να καλύψει πολλά σενάρια.
- Το NIDS έχει καλή κάλυψη (αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Βαθμός κάλυψης) αφού μπορεί να εντοπίσει εξωτερικές επιθέσεις σε επίπεδο δικτύου, αλλά αυτό εξαρτάται από το είδος ανίχνευσης που χρησιμοποιείται. Αν εφαρμόζεται rule/ signature-based ανίχνευση, καλύπτονται μόνο γνώστες απειλές και όχι παραλλαγές ή νέες απειλές. Επίσης, οι αυξημένες απαιτήσεις σε πόρους περιορίζουν την εφαρμογή του σε ορισμένα περιβάλλοντα, όπως αυτά με περιορισμένους πόρους.
- Τα υβριδικά συστήματα IDS αξιολογούνται με τιμή 4 στο κριτήριο σύγκρισης «Βαθμός κάλυψης, καθώς μπορούν να ανιχνεύσουν τόσο εσωτερικές απειλές όσο και εξωτερικές απειλές σε επίπεδο δικτύου και σε επίπεδο host. Αυτό τα καθιστά ιδιαίτερα ευέλικτα και ικανά να καλύψουν διάφορα περιβάλλοντα και σενάρια.
- Το RBAC αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Βαθμός κάλυψης», διότι αν και παρέχει μια ευρεία κάλυψη δικαιωμάτων δεν καλύπτει τις ανάγκες των πιο δυναμικών ή των πιο κατανεμημένων συστημάτων.
- Το ABAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Βαθμός κάλυψης», διότι προσφέρει εξαιρετική κάλυψη όλων των συνθηκών που μπορεί να επηρεάσουν την πρόσβαση, αλλά η ανάγκη για συνεχείς προσαρμογές στις πολιτικές και στα χαρακτηριστικά μπορεί να αυξήσει την πολυπλοκότητα του συστήματος.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Βαθμός κάλυψης», διότι η πολυπλοκότητα και η ποικιλομορφία των ομιχλωδών περιβαλλόντων δυσκολεύουν την αποτελεσματική κάλυψη όλων των σημείων ασφάλειας, εκτός και αν γίνουν σημαντικές τροποποιήσεις σε αυτά τα περιβάλλοντα. Επιπλέον, καθώς πρόκειται για ένα host-based μέτρο, η σκλήρυνση του υπερεπόπτη μπορεί να είναι ακόμα πιο απαιτητική και βαρύτερη.
- Το VMM αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Βαθμός κάλυψης», διότι περιορίζεται από συγκεκριμένα μηχανήματα.

Επεκτασιμότητα

- Η MFA αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Επεκτασιμότητα», καθώς η MFA είναι μια τεχνολογία που εξελίσσεται συνεχώς και μπορεί να προσαρμοστεί με μικρές αλλαγές για να υποστηρίξει νέους μηχανισμούς αυθεντικοποίησης ή να ενσωματωθεί σε νέες εφαρμογές.
- Ένα HIDS αξιολογείται με τιμή 2 στο κριτήριο σύγκρισης «Επεκτασιμότητα», διότι για να επεκταθεί και να βελτιωθεί απαιτούνται σημαντικές αλλαγές. Παρόλου που μπορεί να προσαρμοστεί σε κάποιο βαθμό, η επέκταση του δεν είναι απλή και απαιτεί σημαντική αναδιάρθρωση.
- Το NIDS αξιολογείται με τιμή 3 στο κριτήριο σύγκρισής «Επεκτασιμότητα», διότι ένα NIDS μπορεί να επεκταθεί για να υποστηρίξει καινούργια πρωτόκολλα και εφαρμογές, αλλά η επέκταση απαιτεί περισσότερες τροποποιήσεις και προσαρμογές, γεγονός που περιορίζει την ευκολία της διαδικασίας.
- Τα υβριδικά IDS συστήματα αξιολογούνται με 3 στο κριτήριο σύγκρισης «Επεκτασιμότητα», καθώς αυτά τα συστήματα απαιτούν σημαντική προσπάθεια για να υποστηρίξουν μεγαλύτερες ανάγκες, καθιστώντας την επέκταση τους λιγότερο απλή και άμεση.
- Το RBAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Επεκτασιμότητα», διότι έχει την ιδιότητα να επεκτείνεται σε μεγάλα συστήματα, αλλά σε περιβάλλοντα με συχνές αλλαγές στις ανάγκες πρόσβασης και στους πόρους, η διαχείριση των ρόλων μπορεί να απαιτεί επιπρόσθετους πόρους, καθώς απαιτεί συνεχή αναθεώρηση και επικαιροποίηση των ρόλων και των δικαιωμάτων πρόσβασης.
- Το ABAC αξιολογείται με τιμή 4 στο κριτήριο σύγκρισης «Επεκτασιμότητα», καθώς μπορεί να επεκταθεί σε νέες τεχνολογίες ή απαιτήσεις, αν και απαιτούνται κάποιες ελάχιστες αλλαγές για να υποστηρίξει αυτές τις επεκτάσεις.
- Η σκλήρυνση του υπερεπόπτη αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Επεκτασιμότητα», καθώς τεχνολογίες όπως το NoHype μπορούν να ενισχύσουν την ασφάλεια χωρίς να περιορίζουν σημαντικά την ικανότητα επέκτασης του συστήματος και η επέκταση μπορεί να πραγματοποιηθεί με την σωστή αναδιάρθρωση του συστήματος.
- Το VMM αξιολογείται με τιμή 3 στο κριτήριο σύγκρισης «Επεκτασιμότητα», καθώς το VMM πρέπει να συνδυαστεί με άλλες λειτουργίες ή εργαλεία ασφάλειας και η επεκτασιμότητα της συνολικής λύσης θα είναι περιορισμένη.

Πίνακας 3 - Πίνακας σύγκρισης των αντιμέτρων για την αντιμετώπιση των επιθέσεων εικονικοποίησης στον ομιχλώδη προγραμματισμό

Αντί-μετρα	**Κατανά-λωση Πόρων**	**Κλιμα-κωσιμό-τητα**	**Ασφά-λεια δεδομέ-νων**	**Ευκο-λία χρή-σης**	**Εκπαί-δευση χρησ-τών**	**Αντίκ-τυπος στον χρήστη**	**Εφαρ-μοσιμό-τητα**	**Βαθ-μός κάλυ-ψης**	**Επεκ-τασιμό-τητα**
MFA	2-3	2-4	4	3-4	3	3	3	4	4
HIDS	3	2	4	3	2	3	2	3	2

NIDS	3	3	3	2	2	3	3	3	3
Υβριδικά IDS	2	4	4	1	1	3	2	4	3
RBAC	4	4	3	4	4	4	4	3	4
ABAC	2	4	4	3	3	3	2	4	4
Σκλήρυν-ση Υπερεπό-πτη	2	2	3	2	2	3	2-3	2	3
VMM	4	2	3	3	3	3	3	2	3

Με βάση τον παραπάνω πίνακα έχουμε μπορούμε να προχωρήσουμε σε ανάλυση των καλύτερων και των χειρότερων αντιμέτρων για κάθε κριτήριο:

Ανάλυση καλύτερου και χειρότερου αντιμέτρου ανά κριτήριο: Θα εντοπίσουμε ποιο/-α αντίμετρο/-α έχει την καλύτερη και την χειρότερη απόδοση σε κάθε κριτήριο αξιολόγησης:

1. Κατανάλωση πόρων:
    a. Καλύτερο: RBAC, VMM (4)
    b. Χειρότερο: υβριδικό IDS, ABAC, σκλήρυνση υπερεπόπτη (2)
2. Κλιμακωσιμότητα:
    a. Καλύτερο: υβριδικό IDS, ABAC, RBAC (4)
    b. Χειρότερο: HIDS, VMM, σκλήρυνση υπερεποπτή (2)
3. Ασφάλεια δεδομένων:
    a. Καλύτερο: ABAC, MFA, HIDS, υβριδικό IDS, VMM (4)
    b. Χειρότερο: σκλήρυνση υπερεπόπτη, NIDS, RBAC (3)
4. Ευκολία χρήσης:
    a. Καλύτερο: RBAC (4)
    b. Χειρότερο: υβριδικό IDS (1)
5. Εκπαίδευση χρηστών:
    a. Καλύτερο: RBAC (4)
    b. Χειρότερο: υβριδικό IDS (1)
6. Αντίκτυπος στον χρήστη:
    a. Καλύτερο: ABAC (4)
    b. Χειρότερο: Όλα τα αντίμετρα έχουν την ίδια βαθμολογία 3 (εκτός του ABAC), χωρίς ιδιαίτερη διαφοροποίηση.
7. Εφαρμοσιμότητα:
    a. Καλύτερο: RBAC (4)
    b. Χειρότερο: HIDS, υβριδικό IDS, ABAC (2)
8. Βαθμός κάλυψης:
    a. Καλύτερο: MFA, υβριδικό IDS, ABAC (4)
    b. Χειρότερο:VMM, σκλήρυνση υπερεποπτή (2)
9. Επεκτασιμότητα:
    a. Καλύτερο: MFA, ABAC, RBAC (4)

b. Χειρότερο: HIDS (2)

Καλύτερο και χειρότερο αντίμετρο συνολικά (στην κατηγόρια): Για να βρούμε το καλύτερο και το χειρότερο αντίμετρο, μπορούμε να κάνουμε έναν γρήγορο υπολογισμό, μετρώντας τον συνολικό αριθμό βαθμών για το κάθε αντίμετρό για όλα τα κριτήρια σύγκρισης: MFA: 28-32 (ανάλογα με τις μεταβλητές τιμές), HIDS: 24, NIDS: 25, υβριδικά IDS: 24, ABAC: 31, RBAC: 34, σκλήρυνση υπερεποπτή: 22, VMM: 27. Επομένως, το RBAC με συνολική βαθμολογία 32 είναι το καλύτερο αντίμετρο συνολικά, ενώ τα χειρότερα αντίμετρα είναι το HIDS και η σκλήρυνση υπερεποπτή με βαθμολογία 21-22.

Αντίμετρο με καλύτερη και χειρότερη απόδοση: Για την καλύτερη και χειρότερη απόδοση, πρέπει να εξετάσουμε την απόδοση των αντιμέτρων σε κάθε κριτήριο και να καταλήξουμε στο καλύτερο και το χειρότερο αντίμετρο βασιζόμενοι στο ποσοστό των υψηλών ή των χειρότερων βαθμολογίων τους που έχουν λάβει στα κριτήρια. Θεωρούμε την τιμή 1 με 2 χαμηλές τιμές και 4 με 5 υψηλές τιμές. Τα αντίμετρα που έχουν εύρος τιμών στον παρακάνω πίνακα δεν συμπεριλαμβάνονται στο παρακάτω υπολογισμό.

Ποσοστά υψηλών και χαμηλών βαθμολογιών:

- MFA:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές:0 /9 = 0 %
- HIDS:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 4/9 = 44,4 %
- NIDS:
  - Υψηλές: 0/9 = 0 %
  - Χαμηλές: 2/9 = 22,2 %

- Υβριδικά IDS:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 4/9 = 44,4%
- ABAC
  - Υψηλές: 5/9 = 55,6 %
  - Χαμηλές: 2/9 = 22,2 %
- RBAC:
  - Υψηλές: 7/9 = 77,7 %
  - Χαμηλές: 1/9 = 11,1 %
- Σκλήρυνση υπερεπόπτη:
  - Υψηλές: 0/9 = 0 %
  - Χαμηλές: 5/9 = 55.6 %
- VMM:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 2/9 = 22.2 %

Το αντίμετρο με την καλύτερη απόδοση βάσει του ποσοστού των υψηλών βαθμολογίων είναι το RBAC 77,7% . Το αντίμετρο με την χειρότερη απόδοση βάσει του μεγαλύτερού ποσοστού χαμηλών βαθμολογίων είναι η σκλήρυνση υπερεπόπτη με ποσοστό 55,6 %.

Η συγκεκριμένη μεθοδολογία σύγκρισης που ακολουθείτε στην ενότητα 5.3.2.6 εφαρμόζεται και στις άλλες κατηγορίες αντιμέτρων (ενότητες 5.3.3.6, 5.3.4.6, 5.3.5.6, 5.3.6.6, 5.3.7.6) για την ανάδειξη του καλύτερου και χειρότερου αντιμέτρου.

5.3.3 Αντίμετρα για τις επιθέσεις της ασφάλειας ιστού

Για την αντιμετώπιση των ζητημάτων της ασφάλειας ιστού στον ομιχλώδη προγραμματισμό μπορούν να εφαρμοστούν διάφορα αντίμετρα, όπως είναι το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο σε CNN ελαστικής συγκέντρωσης πόρων (SQL injection detection based on Elastic-Pooling CNN), το συστήματα αποτροπής εισβολών (Intrusion Prevention System, IPS), οι περιοδικοί έλεγχοι (periodic auditing), το καρφίτσωμα πιστοποιητικών (certificate pinning) και η ανίχνευση των επιθέσεων XSS (Khan, Parkinson and Qin, 2017).

5.3.3.1 Σύστημα ανίχνευσης εκχύσεων SQL βασισμένο σε CNN στην ελαστικής συγκέντρωσης πόρων (SQL injection detection based on Elastic-Pooling CNN)

Οι Xie et al. (2019) προτείναν μια εργασία, η οποία παρουσιάζει ένα καινούργιο σύστημα για την έγκυρη ανίχνευση των επιθέσεων εκχύσεων SQL. Το νέο αυτό σύστημα βασίζεται στην εξειδικευμένη αρχιτεκτονική νευρωσικών δικτύων ελαστικής συγκέντρωσης πόρων EPCNN (Elastic Pooling Convolution Neural Network), ικανή να ανιχνεύει με ακρίβεια επιθέσεις έκχυσης SQL (Xie *et al.*, 2019), (Ometov *et al.*, 2022). Το EPCNN είναι μια παραλλαγή του CNN (Convolutional Neural Network), ειδικά σχεδιασμένο για την διαχείριση εισόδων μεταβλητού μήκους, όπως είναι οι συμβολοσειρές ερωτημάτων SQL. Το στρώμα ελαστικής συγκέντρωσης (elastic pooling layer) αποτελεί την βασική καινοτομία του EPCNN, καθώς αντικαθιστά το στρώμα μεγίστης συγκέντρωσης (max pooling layer) του παραδοσιακού CNN και εξασφαλίζει ότι στην έξοδο του στρώματος της ελαστικής συγκέντρωσης παράγεται ένας πίνακας με σταθερό αριθμό στηλών, αλλά με μεταβλητό αριθμό γραμμών. Στην ουσία, το στρώμα ελαστικής συγκέντρωσης επιτρέπει την αποτελεσματική επεξεργασία δεδομένων μεταβλητού μήκους και βελτιώνει την απόδοση του μοντέλου ανίχνευσης επιθέσεων έκχυσης SQL που βασίζεται στο EPCNN που παράγεται (Xie *et al.*, 2019).

Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στο EPCNN δεν αναζητά απλά συγκεκριμένες λέξεις ή φράσεις στις συμβολοσειρές των ερωτημάτων SQL για την εύρεση απειλών, όπως συμβαίνει στα παραδοσιακά συστήματα ανίχνευσης απειλών. Αντιθέτως, το στρώμα ελαστικής προσέγγισης του EPCNN, αξιοποιώντας την δυνατότητα ανίχνευσης πολύπλοκων μοτίβων (irregular matching characteristics) μαθαίνει να αναγνωρίζει σύνθετα μοτίβα, τα οποία διαφέρουν από επίθεση σε επίθεση, δηλαδή μπορεί να εντοπίζει άγνωστες μορφές νέων επιθέσεων που δεν

ήταν προγραμματισμένες να γίνουν. Επίσης, λόγω της χρήσης ακανόνιστων χαρακτηριστικών αυξάνεται η ανθεκτικότητα του συστήματος ανίχνευσης εκχύσεων SQL βασισμένο στο EPCNN απέναντι σε επιθέσεις, καθιστώντας το πιο δυσχερέστερο για τους επιτιθέμενους να αναπτύξουν στοχευμένες επιθέσεις που να παρακάμπτουν τους μηχανισμούς ανίχνευσης. (Xie *et al.*, 2019)

Από την άλλη πλευρά, η εκπαίδευση και η λειτουργία νευρωνικού δικτύου EPCNN απαιτεί σημαντική υπολογιστική ισχύ (πραγματοποιείται σε ισχυρούς διακομιστές ή στο υπολογιστικό νέφος), την οποία μπορεί να μην διαθέτουν όλοι οι διακομιστές του ομιχλώδους προγραμματισμού. Η μεταφορά του εκπαιδευμένου μοντέλου EPCNN και η εκτέλεση του σε μια συσκευή με περιορισμένους πόρους του ομιχλώδους περιβάλλοντος μπορεί να είναι προβληματική λόγου του μεγέθους του μοντέλου. Αυτό μπορεί να οδηγήσει σε σημαντική καθυστέρηση, ενώ η απώλεια ακρίβειας μπορεί να οφείλεται στην ανάγκη συμπίεσης του μοντέλου EPCNN ή σε άλλες προσαρμογές για να λειτουργήσει σε περιορισμένα συστήματα, γεγονός που μπορεί να μειώσει την απόδοση του μοντέλου EPCNN. Ακόμα, το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στο EPCNN χρειάζεται έναν μεγάλο όγκο δεδομένων εκπαίδευσης για να αποφευχθεί η υπερ-προσαρμογή (overfitting) και άρα να βελτιωθεί η ανθεκτικότητα του. Η τελευταία διαδικασία είναι αρκετά χρονοβόρα. (Xie *et al.*, 2019)

5.3.3.2 Περιοδικοί έλεγχοι (Periodic Auditing)

Ο περιοδικός έλεγχος είναι μια διαδικασία εντός του μηχανισμού ελέγχου (mechanism auditing) για μοντέλα ελέγχου πρόσβασης (access control) που πραγματοποιείται σε καθορισμένα χρονικά διαστήματα. Στόχος του περιοδικού ελέγχου είναι να διασφαλίσει ότι τα δεδομένα και οι πολιτικές πρόσβασης παραμένουν έγκυρες και επίκαιρες. Σε ομιχλώδη περιβάλλοντα, όπου υποστηρίζεται η κλιμακωσιμότητα, ο περιοδικός έλεγχος συμβάλλει στην ανθεκτικότητα του μοντέλου ελέγχου πρόσβασης. Ο συνεχής και λεπτομερής περιοδικός έλεγχος σε τακτική βάση είναι απαραίτητος για την διατήρηση της εμπιστευτικότητας και της ακεραιότητας των δεδομένων και των εφαρμογών των συστημάτων του ομιχλώδους προγραμματισμού. Επιπλέον, οι έξυπνοι μηχανισμοί ελέγχου έχουν τη δυνατότητα να εντοπίζουν αυτόματα παραβιάσεις πολιτικής. Κατά την ανίχνευση των παραβιάσεων, οι έξυπνοι μηχανισμοί ελέγχου προσαρμόζουν τις πολιτικές πρόσβασης, ώστε να αποτραπούν μελλοντικές παραβιάσεις, ενώ ταυτόχρονα διασφαλίζουν την ακριβή και επικαιροποιημένη καταγραφή των χαρακτηριστικών των χρηστών για την ασφαλή και ομαλή λειτουργία του συστήματος. (Aleisa, Abuhussein and Sheldon, 2020)

Ωστόσο, οι περιοδικοί έλεγχοι στον ομιχλώδη προγραμματισμό μπορεί να μην είναι επαρκής για την έγκαιρη ανίχνευση απειλών ή παραβιάσεων ασφάλειας που συμβαίνουν μεταξύ των προγραμματισμών ελέγχων, εξαιτίας της κατανομής των κόμβων ομίχλης και της αποθήκευσης των δεδομένων σε διαφορετικά σημεία, γεγονός που καθιστά δύσκολή την παρακολούθηση των απειλών σε πραγματικό χρόνο. Επιπλέον, η συχνή ανάγκη για περιοδικούς ελέγχους και οι συνεχείς ενημερώσεις των δικαιωμάτων πρόσβασης προσθέτουν ακόμα περισσότερο υπολογιστικό φόρτο, γεγονός που ενδέχεται να επιδεινώσει την συνολική απόδοση του συστήματος του ομιχλώδους

προγραμματισμού, εάν δεν υπάρξει σωστή διαχείριση των πόρων. (Aleisa, Abuhussein and Sheldon, 2020)

5.3.3.3 Σύστημα Πρόληψης Εισβολών (Intrusion Prevention System - IPS)

Το σύστημα πρόληψης εισβολών (IPS) είναι ένα εργαλείο που χρησιμοποιείται στα δίκτυα για την ανίχνευση και την αποτροπή κακόβουλων δραστηριοτήτων που προσπαθούν να αποκτήσουν πρόσβαση στο δίκτυο. Η βασική λειτουργία του IPS περιλαμβάνει την ανίχνευση επιθέσεων, την καταγραφή τους, καθώς και την άμεση απομάκρυνση ή αποτροπή κακόβουλου λογισμικού από τα σημεία εισόδου στο δίκτυο. Όσον αναφορά τις ειδικά σχεδιασμένες επιθέσεις, όπως εκείνες που εκμεταλλεύονται άγνωστες ευπάθειες, το IPS μπορεί να μπλοκάρει την πρόσβαση ή να διακόψει την σύνδεση, αποτρέποντας την εκτέλεση αυτών των επιθέσεων. (Selim and Sadeκ, 2021).

Η εφαρμογή των συστημάτων πρόληψης εισβολών σε περιβάλλοντα ομίχλης, ειδικότερα στο πλαίσιο των IoT δικτύων έχουν να προσφέρουν πολλά πλεονεκτήματα. Πρώτα από όλα, το IPS έχει την δυνατότητα να εντοπίζει και να αποτρέπει επιθέσεις σε πραγματικό χρόνο. Συνήθως το IPS τοποθετείται πίσω από ένα τείχος προστασίας (firewall) προσφέροντας με αυτό τον τρόπο μια επιπλέον γραμμή άμυνας έναντι των κακόβουλων δραστηριοτήτων. Επίσης, το IPS χρησιμοποιεί την μέθοδο ανίχνευσης βασισμένη σε υπογραφές (signature-based identification) για να εντοπίζει γνώστες επιθέσεις μέσω μοτίβων που έχουν καταγραφεί σε βάσεις δεδομένων έτσι ώστε να προστατεύσει τις τοπικές συσκευές και τα τοπικά δίκτυα, προσφέροντας έναν επιπλέον μηχανισμό κοντά στην πηγή των δεδομένων. Ακόμα, το IPS προστατεύει το δίκτυο όσο σε αυτό εφαρμόζονται ενημερώσεις. Τέλος, το IPS δεν περιορίζεται μόνο στην ανίχνευση επιθέσεων, αλλά επεμβαίνει ενεργά για να μετριάσει τα τρέχοντα συμβάντα επιθέσεων και να προλάβει την εμφάνιση μελλοντικών επιθέσεων. Με αυτό τον τρόπο ενισχύεται η συνολική ασφάλεια του δικτύου προσφέροντας διαρκή προστασία στο σύστημα σε βάθος χρόνου. (Prajapati *et al.*, 2021)

Από την άλλη πλευρά, η αποτελεσματικότητα του IPS εξαρτάται από τη διαθεσιμότητα μεγάλου όγκου δεδομένων, που σημαίνει ότι μπορεί να δυσκολευτεί να εντοπίσει και να σταματήσει επιθέσεις όταν τα δεδομένα είναι περιορισμένα ή ανεπαρκή. Επίσης, η χρήση των μεθόδων βασισμένων σε υπογραφές οδηγεί σε ψευδή αρνητικά αποτελέσματα, δηλαδή να αναγνωρίσει κανονικές δραστηριότητες ως επιθέσεις, καθώς το IPS εντοπίζει μόνο γνώστες και καταγεγραμμένες επιθέσεις. Ένα ακόμα σημαντικό μειονέκτημα του IPS είναι ο υψηλός φόρτος που ενδέχεται να προκαλέσει στο σύστημα, ο οποίος σε ορισμένες περιπτώσεις μπορεί να οδηγήσει σε καθυστερήσεις ή να επηρεάσει την απόδοση του δικτύου ιδιαίτερα όταν το σύστημα επεξεργάζεται μεγάλο όγκο δεδομένων. Επιπρόσθετα, το IPS δεν είναι επαρκές στην αποτροπή νέων ή εξελιγμένων επιθέσεων που δεν έχουν καταγραφεί στο σύστημα περιορίζοντας την δυνατότητα του να ανταποκρίνεται σε καινοτόμες απειλές. Τέλος, η συνεχής παρακολούθηση και η ανανέωση του IPS με τις τελευταίες υπογραφές και αλγορίθμους είναι απαραίτητη για την διατήρηση της αποτελεσματικότητας του, καθώς η απουσία αυτών των διαδικασιών ανανέωσης ενδέχεται να εκθέσει το σύστημα σε νέους κίνδυνους. (Prajapati *et al.*, 2021)

5.3.3.4 Ασφαλής Επαλήθευση μέσω Πιστοποιητικού

Το καρφίτσωμα πιστοποιητικών (certificate pinning) είναι ένα μέτρο ασφάλειας που εφαρμόζεται στις κινητές εφαρμογές και σε εφαρμογές ιστού, με σκοπό να εξασφαλίσει ότι η εφαρμογή επικοινωνεί μόνο με τον νόμιμο και όχι με ένα κακόβουλο διακομιστή που παριστάνει τον νόμιμο. Αυτή η τεχνική χρησιμοποιείται για την επαλήθευση της ταυτότητας ενός διακομιστή μέσω της σύγκρισης του ψηφιακού του πιστοποιητικού με ένα προκαθορισμένο σύνολο εμπιστευτικών πιστοποιητικών (Zimperium, 2024).

Το καρφίτσωμα πιστοποιητικών προσφέρει σημαντικά πλεονεκτήματα στην ενίσχυση της ασφάλειας των επικοινωνιών. Πρώτα από όλα, ενισχύει την εμπιστοσύνη στα πιστοποιητικά του διακομιστή, προσφέροντας μια εναλλακτική μέθοδο επαλήθευσης που ελαχιστοποιεί τον κίνδυνο από πλαστά πιστοποιητικά που ενδέχεται να έχουν εκδοθεί ως αποτέλεσμα σχετικών επιθέσεων. Επίσης, το καρφίτσωμα πιστοποιητικών συμβάλλει στην μειώσει των κινδύνων που σχετίζονται με την λανθασμένη διαχείριση / λειτουργία των Αρχών Πιστοποίησης (Certificate Authorities - CAs), ενισχύοντας την ασφάλεια των συνδέσεων μέσω της περιορισμένης εξάρτησης από τις Αρχές Πιστοποίησης και της ενισχυμένης επαλήθευσης των πιστοποιητικών. Ωστόσο, για την προστασία από την έκδοση μη αυθεντικών πιστοποιητικών απαιτείται επιπλέον μηχανισμός, όπως το DANE, το οποίο καλύπτει και το DNS CAA (Díaz-Sánchez *et al.*, 2018). Ειδικότερα, ο μηχανισμός DNS CAA (Certification Authority Authorization) αναφέρεται ως μια μέθοδος που επιτρέπει στους ιδιοκτήτες τομέων (domain) να περιορίσουν ποια CAs μπορούν να εκδώσουν πιστοποιητικά για το τομέα τους, παρέχοντας καλύτερο έλεγχο. Προφανώς, σε αυτή την περίπτωση, το καρφίτσωμα πιστοποιητικών θα πρέπει να συνδυαστεί με αυτή την λύση. Τέλος, η Διαφάνεια Πιστοποιητικών (Certificate Transparency), που βασίζεται σε ένα μηχανισμό της IETF (RFC 6962) προσφέρει μια παγκόσμια πλατφόρμα για την καταγραφή και την παρακολούθηση των πιστοποιητικών. Συνδυάζοντας το Καρφίτσωμα Πιστοποιητικών, την Διαφάνεια Πιστοποιητικών και το DANE, ενισχύεται η ασφάλεια μέσω παρακολούθησης και την επαλήθευσης των πιστοποιητικών από οποιονδήποτε και οπουδήποτε, ενώ η διαφάνεια επιτυγχάνεται με τη χρήση δημοσίων καταλόγων (logs) που είναι προσβάσιμοι διεθνώς (Diaz-Sanchez et al., 2019).

Ο μηχανισμός καρφιτσώματος πιστοποιητικών στο πλαίσιο του ομιχλώδους προγραμματισμού ενέχει σημαντικές προκλήσεις, οι οποίες πρέπει να λαμβάνονται υπόψιν κατά την εφαρμογή του και χρήζουν ιδιαίτερης προσοχής. Παρόλο που έχουν προταθεί διάφορα πρωτόκολλα για την διαχείριση της εμπιστοσύνης, παραμένει ο κίνδυνος παραβίασης μιας αρχής πιστοποίησης (CA), γεγονός που επιτρέπει την έκδοση κακόβουλων πιστοποιητικών από μία CA που βρίσκεται στην λίστα εμπιστοσύνης του συστήματος. Επίσης, οι κίνδυνοι που απορρέουν από την εισαγωγή Ενδιάμεσων Αρχών Πιστοποίησης (Intermediate CAs) συνδέονται με την πιθανή κακή χρήση αυτόν των αρχών από τους πάροχους δικτύου, γεγονός που ενδέχεται να εκθέσει την κίνηση του δικτύου σε μη ασφαλή σημεία. Για παράδειγμα, η χρήση των Ενδιάμεσων Αρχών Πιστοποίησης αν και αποσκοπεί στην επιτάχυνση της κυκλοφορίας SSL/TLS, δύναται να υπονομεύσει την ασφάλεια της επικοινωνίας, καθιστώντας το σύστημα ευάλωτο σε επιθέσεις που παρακάμπτουν την ασφάλεια από άκρο σε άκρο, ενώ υπάρχει και η πιθανότητα μη ασφαλούς αποκάλυψης της κρυπτογραφημένης κίνησης (Diaz-Sanchez et al., 2019). Επιπλέον, το καρφίτσωμα πιστοποιητικών

μπορεί να προκαλέσει προβλήματα εάν δεν υπάρχει σωστή ενημέρωση και τακτική συντήρηση, καθώς αν ένα πιστοποιητικό λήξει ή αλλάξει χωρίς την ενημέρωση του καρφιτσωμένου (pinning) πιστοποιητικού μπορεί να διακοπεί η επικοινωνία της εφαρμογής. Τέλος, το καρφίτσωμα πιστοποιητικού απαιτεί σταθερότητα και προκαθορισμένη γνώση του διακομιστή, αλλά σε IoT περιβάλλοντα, όπου οι υπηρεσίες και τα πιστοποιητικά αλλάζουν συχνά, η διαδικασία αυτή γίνεται πιο δύσκολη, καθώς οποιαδήποτε αλλαγή στο πιστοποιητικό απαιτεί ενημέρωση του καρφιτσωμένου πιστοποιητικού, αλλιώς μπορεί να οδηγήσει σε σφάλματα επικοινωνίας ή αποτυχία επαλήθευσης (Díaz-Sánchez *et al.*, 2018).

5.3.3.5 Ανίχνευση επιθέσεων XSS με αλγορίθμους μηχανικής μάθησης

Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση (Machine-Learning XSS detection) αφορά τη χρήση τεχνικών μηχανικής μάθησης για τον εντοπισμό επιθέσεων XSS. Οι αλγόριθμοι μηχανικής μάθησης αναλύουν χαρακτηριστικά του κώδικα Javascript (σε ιστοσελίδες εφαρμογών ιστού) ή χαρακτηριστικά της δικτυακής κίνησης (π.χ. οι διευθύνσεις URLs, τα HTML tags κ.α.), προκειμένου να αναγνωρίσουν μοτίβα που υποδεικνύουν κακόβουλες επιθέσεις. Αυτή η τεχνική επιτρέπει την αυτόματη ανίχνευση των επιθέσεων και βοηθά στη βελτίωση της ασφάλειας των εφαρμογών ιστού. (Kaur, Garg and Bathla, 2023)

Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση στον ομιχλώδη προγραμματισμό προσφέρει σημαντικά πλεονεκτήματα. Πρώτα από όλα, η αποτελεσματικότητα των αλγόριθμων μηχανικής μάθησης, όπως ο Random Forest, έχει αποδειχθεί εξαιρετικά υψηλή σε σύγκριση με τις παραδοσιακές μεθόδους ανίχνευσης XSS επιθέσεων. Η ακρίβεια ανίχνευσης των επιθέσεων XSS των αλγόριθμών μηχανικής μάθησης φτάνει τις περισσότερες φορές στο 98%, καθιστώντας τους ιδιαίτερα αξιόπιστους σε πραγματικές συνθήκες. Επίσης, οι αλγόριθμοι μηχανικής μάθησης που εφαρμόζονται για την ανίχνευση επιθέσεων XSS διαθέτουν την ικανότητα της αυτόματης ανίχνευσης επιθέσεων XSS, καθώς μετά την αρχική τους εκπαίδευση μπορούν να εντοπίζουν και να ταξινομούν άμεσα τον κώδικα ως κακόβουλο ή ασφαλή χωρίς να απαιτείται χειροκίνητη παρέμβαση. Ακόμη, οι αλγόριθμοι μηχανικής μάθησης που εφαρμόζονται για την ανίχνευση επιθέσεων XSS μπορούν να ανιχνεύσουν νέες και απρόβλεπτες μορφές επιθέσεων μέσω της ανάλυσης των χαρακτηριστικών που σχετίζονται με κακόβουλες ενέργειες, ενισχύοντας με αυτό τον τρόπο την προστασία των συστημάτων του ομιχλώδους προγραμματισμού έναντι των εξελισσόμενων απειλών. (Banerjee *et al.*, 2020)

Ωστόσο, η ανίχνευση επιθέσεων XSS με μηχανική μάθηση στον ομιχλώδη προγραμματισμό παρουσιάζει ορισμένα μειονεκτήματα. Πρώτα από όλα, η εκπαίδευση των αλγορίθμων μηχανικής μάθησης για την ανίχνευση επιθέσεων XSS απαιτεί μεγάλο όγκο δεδομένων, το οποίο οδηγεί σε ανάγκη χρήσης αυξημένου όγκου πόρων δεν είναι πάντοτε διαθέσιμοι σε περιβάλλοντα ομίχλης, ενώ ενδέχεται να επιβαρύνει και την συνολική απόδοση του συστήματος. Επίσης, οι αλγόριθμοι μηχανικής μάθησης παρά την υψηλή απόδοση τους στην ακρίβεια ανίχνευσης επιθέσεων XSS εξακολουθούν να παράγουν ψευδώς θετικά αποτελέσματα, όπου νόμιμες ιστοσελίδες ενδέχεται να χαρακτηριστούν λανθασμένα ως κακόβουλες. Τέλος, η εκτέλεση των αλγορίθμων μηχανικής μάθησης σε κόμβους ομίχλης για την ανίχνευση επιθέσεων XSS επιβαρύνουν την συνολική

απόδοση του συστήματος του ομιχλώδους προγραμματισμού, διότι οι κόμβοι ομίχλης έχουν περιορισμένους πόρους. (Banerjee *et al.*, 2020)

5.3.3.6 Σύγκριση αντιμέτρων που εφαρμόζονται για την αντιμετώπιση των ζητημάτων ασφάλειας ιστού στον ομιχλώδη προγραμματισμό

Τα κριτήρια σύγκρισης που παρουσιάζονται στην ενότητα 5.2 της παρούσας διπλωματικής εργασίας εφαρμόστηκαν για την αξιολόγηση των αντιμέτρων που αφορούν την αντιμετώπιση των ζητημάτων ασφάλειας ιστού στον ομιχλώδη προγραμματισμό, όπως αυτά περιγράφονται στις ενότητες 5.3.3.1-5.3.3.5 της διπλωματικής εργασίας. Η δικαιολόγηση της αξιολόγησης αυτής παρέχεται, ενώ αποδίδεται και ο Πίνακας 4, ο οποίος παρουσιάζει συνοπτικά τα αποτελέσματα αυτής της αξιολόγησης.

Κατανάλωση Πόρων

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN λαμβάνει την τιμή από 1 έως 3 στο τρέχων κριτήριο σύγκριση. Η εκπαίδευση του μοντέλου απαιτεί υψηλή ισχύ και πόρους μνήμης, εξαιτίας των πολύπλοκων αλγορίθμων μηχανικής μάθησης CNN, με την τιμή να κυμαίνεται μεταξύ 1 και 2 ανάλογα με τις απαιτήσεις. Η τιμή αυξάνεται στο 3 κατά την εφαρμογή του παραγόμενου μοντέλου, καθώς το μέγεθος του μπορεί να απαιτεί αυξημένη υπολογιστική ισχύ για την φόρτωση και την επεξεργασία των δεδομένων σε πραγματικό χρόνο. Η απόδοση του συστήματος επηρεάζεται κυρίως σε περιπτώσεις όπου η επεξεργασία πρέπει να γίνει σε πραγματικό χρόνο ή όταν η υποδομή του συστήματος δεν επαρκεί για την υποστηρίξει του μοντέλου.
- Οι περιοδικοί έλεγχοι αξιολογούνται με τιμή 3 στο παρών κριτήριο σύγκρισης. Παρότι οι περιοδικοί έλεγχοι απαιτούν χρήση CPU και μνήμης, η κατανάλωση αυτών των πόρων παραμένει εντός αποδεκτών ορίων επιφέροντας μια μέτρια επιβάρυνση στο σύστημα και επιτρέποντας την συνέχιση των υπόλοιπων λειτουργιών του συστήματος.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με τιμή 2, διότι χαρακτηρίζονται από υψηλή κατανάλωση πόρων, εφόσον απαιτούν συνεχή παρακολούθηση και ανάλυση της δικτυακής κίνησης σε πραγματικό χρόνο για την αποτελεσματική ανίχνευση και την αποτροπή των κυβερνοεπιθέσεων.
- Το καρφίτσωμα πιστοποιητικών έχει υψηλή βαθμολογία, δηλαδή αξιολογείται με 4 στο τρέχων κριτήριο σύγκρισης, καθώς χρειάζεται χαμηλές απαιτήσεις σε πόρους, καθιστώντας το κατάλληλο αντίμετρο για εφαρμογές με περιορισμένη υπολογιστική ισχύ, όπως τις IoT συσκευές. Παρόλο που έχει χαμηλές απαιτήσεις, η χρήση πιστοποιητικών εν γένει μπορεί να οδηγήσει σε κατανάλωση πόρων για την επαλήθευση τους.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 3, διότι απαιτεί σημαντικούς πόρους για την εκπαίδευση του μοντέλου, λόγω της ανάλυσης μεγάλων συνόλων δεδομένων και της εφαρμογής πολύπλοκων αλγορίθμων μηχανικής μάθησης. Όμως, η εκπαίδευση του μοντέλου δεν απαιτείται να επαναλαμβάνεται συχνά, καθώς το παραγόμενο μοντέλο είναι σε θέση να αναγνωρίζει και νέες επιθέσεις. Επίσης, η εφαρμογή

του μοντέλου σε νέα δεδομένα απαιτεί μέτρια κατανάλωση πόρων και εξαρτάται από τον αλγόριθμό μηχανικής μάθησης που χρησιμοποιείται.

Κλιμακωσιμότητα

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN αξιολογείται 2 στο κριτήριο σύγκρισης «κλιμακωσιμότητα», διότι αν και η χρήση μοντέλων μηχανικής μάθησης είναι κλιμακώσιμη, η διαθεσιμότητα των πόρων είναι περιορισμένη εφόσον το μοντέλο εκτελείται σε έναν κόμβο ομίχλης.
- Ο περιοδικός έλεγχος παίρνει την 3 στο κριτήριο σύγκρισης «κλιμακωσιμότητα». υποδηλώνοντας ότι η αυτοματοποίηση των περιοδικών ελέγχων διευκολύνει την κλιμάκωση τους σε μεγάλο βαθμό καθιστώντας εφικτή την επεξεργασία δεδομένων και την ύπαρξη σύνθετων συστημάτων. Όμως, η πραγματική κλιμακωσιμότητα του περιοδικού ελέγχου εξαρτάται από την σωστή διαχείριση του φόρτου εργασίας και των δεδομένων. Οι περιοδικοί έλεγχοι, αν η συχνότητα τους είναι αραιή, ενδέχεται να μην προκαλέσουν σοβαρά προβλήματα, ακόμα και σε περιπτώσεις με αυξημένου φόρτου εργασίας
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με τιμή 2, διότι το IPS αν και έχει την ικανότητα να προσαρμόζονται στις αυξανόμενες απαιτήσεις το δικτύου, η διαθεσιμότητα των πόρων περιορίζει την αποδοτικότητα του αντιμέτρου όταν εκτελείται σε έναν κόμβο ομίχλης.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 5, διότι παρά τις δυσκολίες στη διαχείριση των πιστοποιητικών σε μεγάλα δίκτυα είναι αρκετά κλιμακώσιμο λόγω της ιεραρχίας του όλου συστήματος και της κατανομής, αλλά και της ελαφρότητάς του.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 2, διότι επηρεάζεται αρνητικά η απόδοση του αντιμέτρου από την περιορισμένη διαθεσιμότητα των πόρων στους κόμβους ομίχλης.

Ασφάλεια Δεδομένων

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN αξιολογείται με 4 στο κριτήριο «ασφάλεια δεδομένων», διότι το σύστημα βασίζεται στην ανίχνευση πολύπλοκων μοτίβων, καθιστώντας το ανθεκτικό απέναντι σε επιθέσεις που δεν έχουν προβλεφθεί, κάτι που ενισχύει την ασφάλεια των δεδομένων. Ωστόσο, υπάρχει ο κίνδυνος της μειωμένης αποτελεσματικότητας στην ανίχνευση επιθέσεων SQL σε περιβάλλοντα με χαμηλούς πόρους, εξαιτίας των υψηλών απαιτήσεων σε υπολογιστικούς πόρων που απαιτεί ο CNN.
- Ο περιοδικός έλεγχος αξιολογείται με τιμή 3 σε αυτό το κριτήριο αξιολόγησης. Ο περιοδικός έλεγχος βοηθά στην διατήρηση της ασφάλειας των δεδομένων με το να διασφαλίζει ότι οι πολιτικές παραμένουν έγκυρες και ενημερωμένες. Ωστόσο, ο περιοδικός έλεγχος δεν αντιμετωπίζει άμεσα παραβιάσεις πολιτικών και σε συνδυασμό με τον έλεγχο πρόσβασης δεν παρέχει άμεση προστασία σε περίπτωση επιθέσεων. Μπορεί, ωστόσο, να περιορίσει τις επιπτώσεις μιας επίθεσης εφόσον αυτή ήταν επιτυχής.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με τιμή 4, επειδή χαρακτηρίζονται από την ικανότητα τους να ανιχνεύουν και να αποτρέπουν με υψηλή ακρίβεια ένα ευρύ φάσμα

απειλών, συμπεριλαμβανομένων γνωστών εκμεταλλεύσεων και ανωμαλιών που υποδηλώνουν μη εξουσιοδοτημένη πρόσβαση ή παραβίαση της ακεραιότητας των δεδομένων, καθώς και άγνωστων επιθέσεων. Ωστόσο, λόγω του γεγονότος ότι βασίζονται κυρίως σε υπογραφές (signature-based), η ακρίβεια τους μπορεί να μειωθεί για παραλλαγές επιθέσεων ή νέες επιθέσεις. Αν και η ενσωμάτωση της μηχανικής μάθησης και άλλων τεχνικών ανίχνευσης μπορεί να βελτιώσει την αποτελεσματικότητα τους, η προστασία τους δεν είναι πάντα πλήρης απέναντι σε άγνωστες απειλές.

- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 4, διότι προσφέρει υψηλή ασφάλεια δεδομένων, καθώς διασφαλίζει την επικοινωνία μόνο με αξιόπιστους διακομιστές, εφόσον χρησιμοποιείται βέβαια το κατάλληλο ασφαλές πρωτόκολλο επικοινωνίας. Ωστόσο, σε περιβάλλοντα ομίχλης τα ασφαλή πρωτόκολλα επικοινωνίας μπορεί να είναι απαιτητικά σε πόρους και η χρήση πιστοποιητικών να μην έχει νόημα εάν χρησιμοποιείται πρωτόκολλο χωρίς επαλήθευση των μερών επικοινωνίας. Επιπλέον, η μέθοδος αυτή καλύπτει μόνο την επαλήθευση του εξυπηρετητή και όχι του πελάτη, οπότε υπάρχει η περίπτωση να είναι επιτυχής οι επιθέσεις ενδιάμεσου, ακόμη και αν χρησιμοποιούνται πιστοποιητικά.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 4, διότι μπορεί να ανιχνεύει νέες μορφές επιθέσεων και να προστατεύει τα δεδομένα. Αν και τα ψευδώς θετικά αποτελέσματα μπορούν να επηρεάσουν την διαδικασία, το μέτρο αυτό καλύπτει αποτελεσματικά το συγκεκριμένο είδος επιθέσεων.

Ευκολία χρήσης

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN του αξιολογείται με 2 στο κριτήριο αξιολόγησης «Ευκολία χρήσης». Η εφαρμογή και η συντήρηση ενός νευρωνικού δικτύου, όπως το EPCNN, απαιτεί εξειδικευμένη γνώση για την εγκατάσταση και την συντήρηση του, ενώ η χρήση του από μη ειδικούς μπορεί να είναι δύσκολη χωρίς υποστήριξη.
- Ο περιοδικός έλεγχος αξιολογείται με 4 σε αυτό το κριτήριο σύγκρισης, διότι είναι μία αυτοματοποιημένη διαδικασία που δεν απαιτεί σημαντική αλληλεπίδραση με τον χρήστη. Αν και πρέπει να υπάρχει κάποια εξοικείωση με το συγκεκριμένο αντίμετρο, είναι σχετικά εύχρηστο για έναν χρήστη, αφού μπορεί να εγκατασταθεί και να χρησιμοποιηθεί με απλές διαδικασίες.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με τιμή 2, επειδή απαιτούν εξειδικευμένη γνώση για την εγκατάσταση, την παραμετροποίηση και την συνεχή παρακολούθηση, καθιστώντας τα δύσχρηστα για μη εξειδικευμένους χρήστες.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 3, διότι η εφαρμογή και η διαχείριση του καρφιτσώματος πιστοποιητικών δεν είναι πάντα εύκολη, καθώς απαιτεί γνώση για την σωστή ενημέρωση και την συντήρηση των πιστοποιητικών.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 2, διότι, ενώ η μηχανική μάθηση προσφέρει αυτοματισμό και ακρίβεια, η εφαρμογή της δεν είναι τόσο εύκολη. Απαιτεί εξειδικευμένες γνώσεις στη χρήση αλγορίθμων και μοντέλων μηχανικής μάθησης, καθώς και επαρκή εκπαίδευση των δεδομένων για να ανιχνεύει αποτελεσματικά τις επιθέσεις. Η εφαρμογή αυτών των τεχνικών μπορεί να είναι πιο περίπλοκη από τις

παραδοσιακές μεθόδους, ειδικά για χρήστες που δεν έχουν εμπειρία στον τομέα της μηχανικής μάθησης.

Εκπαίδευση χρηστών

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN του αξιολογείται με 2 στο κριτήριο αξιολόγησης «εκπαίδευση χρηστών», γιατί είναι αναγκαία η εκπαίδευση των χρηστών εξαιτίας της φύσης του EPCNN και της ανάγκης για την κατανόηση των ακανόνιστων χαρακτηριστικών του συστήματος. Η κατανόηση αυτών των ακανόνιστων χαρακτηριστικών μπορεί να απαιτεί σημαντική επένδυση, κάτι που επηρεάζει την αξιολόγηση, καθώς ενδέχεται να χρειάζεται μακροχρόνια και εκτενής εκπαίδευση για την αποτελεσματική χρήση του συστήματος.
- Ο περιοδικός έλεγχος αξιολογείται με 3 σε αυτό το κριτήριο σύγκρισης, διότι απαιτείται μέτρια εκπαίδευση των χρηστών για να κατανοήσουν την διαδικασία και τα αποτέλεσμα της, αλλά δεν είναι ιδιαίτερα περίπλοκη.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με τιμή 2, επειδή είναι σχετικά πολύπλοκα συστήματα και απαιτείται κατάλληλη εκπαίδευση για την χρήση και την διαχείριση τους, η οποία μπορεί να είναι χρονοβόρα και απαιτητική.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 3, διότι οι χρήστες και οι προγραμματιστές πρέπει να εκπαιδευτούν σχετικά με το πως να εφαρμόζουν και να συντηρούν το καρφίτσωμα πιστοποιητικών, ειδικά σε περιβάλλοντα με πολλές αλλαγές πιστοποιητικών. Ωστόσο, η εκπαίδευση που απαιτείται δεν είναι ιδιαιτέρα περιπλοκή, καθώς η διαχείριση και η χρήση των πιστοποιητικών δεν είναι ιδιαίτερα περίπλοκη, καθώς η χρήση και η διαχείριση των πιστοποιητικών δεν είναι τόσο πολύπλοκες διαδικασίες.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 3, διότι οι χρήστες θα χρειαστούν μέτρια εκπαίδευση για να κατανοήσουν πως λειτουργούν οι αλγόριθμοι μηχανικής μάθησης που εφαρμόζονται για την ανίχνευση των επιθέσεων και πως να τους χρησιμοποιήσουν σωστά.

Αντίκτυπος Χρήστη

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN αξιολογείται με 2 στο κριτήριο σύγκρισης «Αντίκτυπος Χρήστη», διότι παρά την αυξημένη ασφάλεια που προσφέρει, η λειτουργία του μπορεί να προκαλέσει μικρές καθυστερήσεις ενώ απαιτεί σημαντικούς υπολογιστικούς πόρους, ειδικά σε περιβάλλοντα με περιορισμένους πόρους, γεγονός που μπορεί να επηρεάσει αρνητικά την απόδοση των συστημάτων εφαρμογών και την εμπειρία του χρήστη.
- Ο περιοδικός έλεγχος αξιολογείται με 3 δεδομένου ότι οι περιοδικοί έλεγχοι που πραγματοποιούνται για την διασφάλιση της ακεραιότητας και της ασφάλειας δεδομένων, μπορεί να οδηγήσουν σε προσωρινές καθυστερήσεις και περιορισμούς στη χρήση του συστήματος. Αν και αυτές οι επιπτώσεις δεν είναι ιδιαίτερα σοβαρές, ενδέχεται να δημιουργήσουν ορισμένες ενοχλήσεις, όπως οι προσωρινές διακοπές στη λειτουργία του συστήματος, προκαλώντας κάποια αναστάτωση στους χρήστες που επιθυμούν ή απαιτούν μια αδιάλειπτη πρόσβαση στο σύστημα του ομιχλώδους προγραμματισμού.

- Τα συστήματα πρόληψης εισβολών αξιολογούνται με 2, διότι ενδέχεται να προκαλέσουν καθυστερήσεις στη δικτυακή κίνηση, εξαιτίας της συνεχούς παρακολούθησης και ανάλυσης, που απαιτείται για την ανίχνευση και την αποτροπή κακόβουλων δραστηριοτήτων. Ωστόσο, αν λειτουργούν με βάση τα πακέτα, οι καθυστερήσεις δεν αναμένονται να είναι σημαντικές. Παρά το γεγονός, ότι το IPS είναι απαραίτητο για την προστασία των δικτύων, ειδικά σε περιβάλλοντα IoT και περιβάλλοντα ομίχλης, η χρήση του μπορεί να οδηγήσει σε επιπρόσθετο υπολογιστικό φόρτο και καθυστερήσεις, οι οποίες μπορεί να επηρεάσουν την απόδοση του συστήματος και την αλληλεπίδραση των χρηστών με αυτό.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 3, λόγω του επιπλέον overhead που απαιτείται για τον έλεγχο των πιστοποιητικών και την αυθεντικοποίηση του εξυπηρετητή κατά την εγκαθίδρυση της σύνδεσης. Αν και το κόστος αυτό είναι προσωρινό, μετά την εγκαθίδρυση η αποστολή κρυπτογραφημένων δεδομένων αποτελεί σταθερό κόστος. Σε περιβάλλοντα ομίχλης, η χρήση κρυπτογράφησης συμμετρικού κλειδιού περιορίζει το κόστος σε λογικά επίπεδα σε σχέση με την ασύμμετρη κρυπτογράφηση.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 2, διότι αν και η αυτόματη ανίχνευση επιθέσεων XSS προσφέρει μεγαλύτερη ασφάλεια και προστασία στους χρήστες μειώνοντας την ανάγκη για χειροκίνητη παρέμβαση, υπάρχει κάποιο overhead από την εφαρμογή του αντιμέτρου, κυρίως λόγω της επεξεργαστικής ισχύος που απαιτείται για την ανάλυση των δεδομένων σε πραγματικό χρόνο.

Εφαρμοσιμότητα

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN αξιολογείται με 2 στο κριτήριο «Εφαρμοσιμότητα», διότι απαιτεί σημαντικούς υπολογιστικούς πόρους, όπως ισχυρούς επεξεργαστές και μνήμη, γεγονός που μπορεί να δημιουργήσει δυσκολίες στην εφαρμογή του συστήματος στα υπάρχοντα ομιχλώδη περιβάλλοντα με περιορισμένους πόρους. Συνεπώς, η ανάγκη για αναβάθμιση της υποδομής ή η ενσωμάτωση νέων πόρων ενδέχεται να καθιστά την εφαρμογή του συστήματος πιο δύσκολη και χρονοβόρα.
- Ο περιοδικός έλεγχος αξιολογείται με 3, διότι οι περιοδικοί έλεγχοι μπορούν να ενσωματωθούν στα υπάρχοντα περιβάλλοντα ομίχλης, αλλά απαιτούν επιπλέον πόρους, γεγονός που μπορεί να επιβαρύνει την απόδοση. Παρόλα αυτά, με την σωστή διαχείριση των πόρων, δεν απαιτούν αναβάθμιση της υποδομής ή την ενσωμάτωση νέων πόρων για την εφαρμογή του αντιμέτρου.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με 3, διότι μπορούν να ενσωματωθούν στα υπάρχοντα δίκτυα και συστήματα, ωστόσο η εφαρμογή τους απαιτεί πρόσθετους πόρους, όπως υπολογιστική ισχύ και αποθηκευτικό χώρο, καθώς και πιθανές προσαρμογές ή ενοποιήσεις με άλλες λύσεις ασφάλειας.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 2, διότι η εφαρμογή του σε υπάρχοντα ομιχλώδη περιβάλλοντα είναι δύσκολη λόγω των απαιτήσεων για συχνή ενημέρωση των πιστοποιητικών, κάτι που απαιτεί σημαντικούς πόρους και συνεχιζόμενη διαχείριση. Επίσης, υπάρχουν περιορισμένοι πόροι και η ενοποίηση με τις υπάρχουσες υποδομές μπορεί να αντιμετωπίζει προκλήσεις, όπως η ανάγκη για συμβατότητα με διάφορες τεχνολογίες και

η υποστήριξη διαφορετικών πρωτοκόλλων ασφάλειας, γεγονός που καθιστά την υλοποίηση του αντιμέτρου πιο περίπλοκη.

- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 3, διότι η μέθοδος μπορεί να εφαρμοστεί στα υπάρχοντα ομιχλώδη περιβάλλοντα, αν και απαιτεί σημαντικούς πόρους για την εκπαίδευση του μοντέλου και την ανάλυση των δεδομένων, γεγονός που ενδέχεται να απαιτήσει κάποιες προσαρμογές στις υπάρχουσες υποδομές και διαδικασίες.

Βαθμός κάλυψης

- Το σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN αξιολογείται με 3 στο κριτήριο σύγκρισης «Βαθμός κάλυψης», διότι αν και το σύστημα μπορεί να ανιχνεύει σύνθετα και άγνωστα μοτίβα επιθέσεων σε διάφορα σενάρια, οι υψηλές απαιτήσεις σε υπολογιστική ισχύ που χρειάζεται περιορίζουν την εφαρμογή του σε περιβάλλοντα με περιορισμένους πόρους.
- Ο περιοδικός έλεγχος αξιολογείται με 3, καθώς είναι μια διαδικασία που είναι αρκετά ευέλικτη και εφαρμόσιμη σε διάφορα περιβάλλοντα, όπως του ομιχλώδους προγραμματισμού. Ωστόσο, υπάρχουν περιπτώσεις όπου η εφαρμογή του μπορεί να συναντήσει δυσκολίες, όπως σε περιβάλλοντα με περιορισμένους υπολογιστικούς πόρους ή σε συστήματα με ιδιαίτερα απαιτητικές ανάγκες για παρακολούθηση επιθέσεων σε πραγματικό χρόνο. Αυτή η ευελιξία του περιοδικού ελέγχου δεν είναι απόλυτη, αλλά εξαρτάται από την αποτελεσματικότητα του περιοδικού ελέγχου, η οποία σε μεγάλο βαθμό επηρεάζεται από την σωστή διαχείριση των υπολογιστικών πόρων.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με 3, διότι καλύπτουν ένα ευρύ φάσμα περιβαλλόντων και σεναρίων, από IoT δίκτυα μέχρι και μεγάλες εταιρικές υποδομές, αλλά ενδέχεται να αντιμετωπίζουν περιορισμούς σε περιβάλλοντα με πολύ εξειδικευμένες ανάγκες.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 3, διότι η εφαρμογή του είναι περιορισμένη σε περιβάλλοντα όπου οι υπηρεσίες και τα πιστοποιητικά δεν αλλάζουν συχνά, πράγμα το δεν ισχύει για περιβάλλοντα ομίχλης ή σε περιβάλλοντα με συχνές ανανεώσεις πιστοποιητικών.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 3, διότι αν και μπορεί να εφαρμοστεί σε ένα ευρύ φάσμα περιβαλλόντων και σεναρίων, καλύπτοντας διαφορετικές περιπτώσεις επιθέσεων και προσαρμόζοντας τις διαδικασίες ανίχνευσης σε ποικιλία δικτυακών εφαρμογών και περιβαλλόντων ανάπτυξης, οι υψηλές απαιτήσεις σε υπολογιστική ισχύ που χρειάζεται περιορίζουν την εφαρμογή του σε περιβάλλοντα με περιορισμένους πόρους

Επεκτασιμότητα

- Στο σύστημα ανίχνευσης εκχύσεων SQL βασισμένο στην ελαστική συγκέντρωση πόρων CNN αξιολογείται με 2 στο κριτήριο σύγκρισης «Επεκτασιμότητα». Παρά την ικανότητα του CNN να εκπαιδεύεται με νέα δεδομένα και να προσαρμόζεται σε διαφορετικές περιπτώσεις, η υψηλή απαίτηση σε πόρους περιορίζει την επεκτασιμότητα του., ειδικά όσον αφορά την ενσωμάτωση νέων τεχνολογιών.

- Ο περιοδικός έλεγχος αξιολογείται με 3, διότι βασίζεται σε μοντέλα ελέγχου πρόσβασης που επιτρέπουν την επέκταση νέων τεχνολογιών και νέων χρηστών, αλλά η διαδικασία αυτή μπορεί να απαιτεί σημαντικό χρονικό διάστημα για να ολοκληρωθεί, καθώς συχνά απαιτεί προσαρμογές ή επεκτάσεις στα υπάρχοντα συστήματα.
- Τα συστήματα πρόληψης εισβολών αξιολογούνται με 4, διότι έχουν την δυνατότητα αναβάθμισης για την ενσωμάτωση νέων κανόνων ή υπογραφών και την αντιμετώπιση νέων απειλών, κάτι που διασφαλίζει την συνεχή αποτελεσματικότητα τους, ειδικά σε ομιχλώδη περιβάλλοντα.
- Το καρφίτσωμα πιστοποιητικών αξιολογείται με 4, διότι αν και η διαδικασία της ανανέωσης και της διαχείρισης των πιστοποιητικών μπορεί να περιορίσει την ευχέρεια για γρήγορη ενοποίηση νέων λειτουργιών, η επίδραση αυτή μπορεί να περιοριστεί αν υπάρχει κατάλληλο separation of concerns. Ωστόσο, σε περιβάλλοντα όπου απαιτούνται συχνές αλλαγές ή προσαρμογές στους διακομιστές, αυτή η διαδικασία μπορεί να προκαλέσει καθυστερήσεις.
- Η ανίχνευση των επιθέσεων XSS με μηχανική μάθηση αξιολογείται με 2, διότι προσφέρει την δυνατότητα προσαρμογής του μοντέλου να δέχεται νέα είδη δεδομένων , αλλά η ανάγκη για πρόσθετους πόρους και η προσαρμογή του συστήματος μπορεί να περιορίσει την ευκολία της επεκτασιμότητας σε πολύπλοκα ή περιορισμένα περιβάλλοντα.

Πίνακας 4 - Πίνακας σύγκρισης των αντιμέτρων για την αντιμετώπιση των επιθέσεων ασφάλειας ιστού στον ομιχλώδη προγραμματσιμό

Αντίμε-τρα	**Κα-ταναλω-ση Πό-ρων**	**Κλι-μακω-σιμό-τητα**	**Ασφά-λεια Δεδο-μενων**	**Ευκο-λία Χρή-σης**	**Εκπαί-δευση χρηστ-ών**	**Αντίκ-τυπος στον χρήστη**	**Εφα-ρμο-σιμό-τητα**	**Βαθ-μός κάλυ-ψης**	**Επεκ-τασι-μότη-τα**
Σύστημα ανίχνευ-σης εκχύσε-ων SQL βασισμέν-ο στο EPCNN	1-3	2	4	2	2	2	2	3	2
Περιοδικ-οί έλεγχοι	3	3	3	4	3	3	3	3	3
Συστήμα Πρόληψη-ς Εισβολών	2	2	4	2	2	2	3	3	4

Καρφίτσωμα πιστοποιητικών	4	5	4	3	3	3	2	3	4
Ανίχνευση επιθέσεων XXS με μηχανική μάθηση	2	2	4	2	3	2	3	3	2

Με βάση τον παραπάνω πίνακα έχουμε μπορούμε να προχωρήσουμε σε ανάλυση των καλύτερων και των χειρότερων αντιμέτρων για κάθε κριτήριο:

Ανάλυση καλύτερου και χειρότερου αντιμέτρου: Θα εντοπίσουμε ποιο/-α αντίμετρο/-α έχει την καλύτερη και την χειρότερη απόδοση σε κάθε κριτήριο αξιολόγησης:

- Κατανάλωση πόρων:
  - Καλύτερο: Καρφίτσωμα πιστοποιητικών (4)
  - Χειρότερο: IPS, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση (2)
- Κλιμακωσιμότητα:
  - Καλύτερο: Καρφίτσωμα πιστοποιητικών (5)
  - Χειρότερο: IPS, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση, σύστημα ανίχνευσης εκχύσεων SQL με EPCNN (2)
- Ασφάλεια δεδομένων:
  - Καλύτερο: Καρφίτσωμα πιστοποιητικών, IPS, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση IPS, σύστημα ανίχνευσης εκχύσεων SQL με EPCNN (4)
  - Χειρότερο: περιοδικός έλεγχος (3)
- Ευκολία χρήσης:
  - Καλύτερο: περιοδικός έλεγχος (4)
  - Χειρότερο: IPS, σύστημα ανίχνευσης εκχύσεων SQL με EPCNN, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση IPS (2)
- Εκπαίδευση χρηστών:
  - Καλύτερο: Καρφίτσωμα πιστοποιητικών, IPS, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση, περιοδικός έλεγχος (3)
  - Χειρότερο: IPS, σύστημα ανίχνευσης εκχύσεων SQL με EPCNN (2)
- Αντίκτυπος στον χρήστη:
  - Καλύτερο: Καρφίτσωμα πιστοποιητικών, IPS, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση, περιοδικός έλεγχος (3)
  - Χειρότερο: ανίχνευσης εκχύσεων SQL με EPCNN, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση IPS, IPS (2)
- Εφαρμοσιμότητα:
  - Καλύτερο: ανίχνευση των επιθέσεων XSS με μηχανική μάθηση, ανίχνευσης εκχύσεων SQL με EPCNN, περιοδικός έλεγχος (3)

- Χειρότερο: Καρφίτσωμα πιστοποιητικών, IPS (2)

❖ Βαθμός κάλυψης:
- Όλα τα αντίμετρα έχουν την ίδια βαθμολογία 3, χωρίς ιδιαίτερη διαφοροποίηση

❖ Επεκτασιμότητα:
- Καλύτερο: IPS, καρφίτσωμα πιστοποιητικών (4)
- Χειρότερο: ανίχνευση των επιθέσεων XSS με μηχανική μάθηση, σύστημα ανίχνευσης εκχύσεων SQL με EPCNN (2)

Καλύτερο και χειρότερο αντίμετρο συνολικά (στην κατηγόρια): σύστημα ανίχνευσης εκχύσεων SQL με EPCNN: 20-24 (ανάλογα με τις μεταβλητές τιμές), περιοδικός έλεγχος: 28. IPS: 24, καρφίτσωμα πιστοποιητικών: 31, ανίχνευση των επιθέσεων XSS με μηχανική μάθηση: 23. Επομένως, το καρφίτσωμα πιστοποιητικών με συνολική βαθμολογία 31 είναι το καλύτερο αντίμετρο συνολικά, ενώ τα χειρότερα αντίμετρα είναι το σύστημα ανίχνευσης εκχύσεων SQL με EPCNN με συνολική βαθμολόγια από 20-24.

Αντίμετρο με καλύτερη και χειρότερη απόδοση: Για την καλύτερη και χειρότερη απόδοση, πρέπει να εξετάσουμε την απόδοση των αντιμέτρων σε κάθε κριτήριο και να καταλήξουμε στο καλύτερο και το χειρότερο αντίμετρο βασιζόμενοι στο ποσοστό των υψηλών ή των χειρότερων βαθμολογίων τους που έχουν λάβει στα κριτήρια. Θεωρούμε την τιμή 1 με 2 χαμηλές τιμές και 4 με 5 υψηλές τιμές. Τα αντίμετρα που έχουν εύρος τιμών στον παρακάνω πίνακα δεν συμπεριλαμβάνονται στο παρακάτω υπολογισμό.

Ποσοστά υψηλών και χαμηλών βαθμολογιών:

- Σύστημα ανίχνευσης εκχύσεων SQL με EPCNN:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 6/9 = 66,7 %
- Περιοδικός έλεγχος:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 0/9 = 0 %
- IPS:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 5/9 = 55,6 %
- Καρφίτσωμα πιστοποιητικών:
  - Υψηλές: 4/9 = 44,4 %
  - Χαμηλές: 1/9 = 11,1 %
- Ανίχνευση των επιθέσεων XSS με μηχανική μάθηση:
  - Υψηλές: 3/9 = 11,1 %
  - Χαμηλές: 5/9 = 55,6 %

Το αντίμετρο με την καλύτερη απόδοση βάσει του ποσοστού των υψηλών βαθμολογίων είναι η καρφίτσωμα πιστοποιητικών με ποσοστό 44,4 %. Το αντίμετρο με την χειρότερη απόδοση βάσει του μεγαλύτερου ποσοστού χαμηλών βαθμολογίων είναι το σύστημα ανίχνευσης εκχύσεων SQL με EPCNN με ποσοστό 66,7 %.

5.3.4 Αντίμετρα για τις επιθέσεις ασφάλειας σχετικά με την επικοινωνία εντός ή εκτός του οργανισμού / επιχείρησης

Για την αντιμετώπιση των ζητημάτων ασφάλειας σχετικά με την επικοινωνία εντός ή εκτός του οργανισμού / επιχείρησης μπορούν να εφαρμοστούν διάφορα αντίμετρα, όπως η μερική κρυπτογράφηση (partial authentication), η κοινή αυθεντικοποίηση (mutual authentication), το IoTCop, το NetSprint και μια τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM (Khan, Parkinson and Qin, 2017).

5.3.4.1 Μερική κρυπτογράφηση

Η μερική κρυπτογράφηση ονομάζεται αλλιώς επιλεκτική κρυπτογράφηση (selective encryption). Αυτή η μέθοδος κρυπτογραφεί μόνο ένα μέρος των αρχικών δεδομένων, αφήνοντας τα υπόλοιπα δεδομένα αμετάβλητα (IGI GLOBAL, 2024).

Η επιλεκτική κρυπτογράφηση προσφέρει σημαντικά πλεονεκτήματα στην προστασία των δεδομένων, επιτρέποντας τη στοχευμένη και την αποτελεσματική εφαρμογή κρυπτογράφησης δεδομένων μόνο στα κρίσιμα ή ευαίσθητα μέρη των δεδομένων, γεγονός που ενισχύει την προστασία των δεδομένων στον ομιχλώδη προγραμματισμό. (Song, Choi and Kim, 2016)

Οι Song κ.α. (2016) ανέπτυξαν το SEACOD (Selective Encryption and Component-Oriented Deduplication) μια καινοτόμο λύση που στηρίζεται στην επιλεκτική κρυπτογράφηση. Χάρις την επιλεκτική κρυπτογραφία, η οποία επικεντρώνεται στα πιο σημαντικά ή πιο ευαίσθητα δεδομένα, το σύστημα SEACOD επιλέγει τις πιο κατάλληλες μεθόδους συμπίεσης και κρυπτογράφησης ανάλογα με τον τύπο των δεδομένων, για ολόκληρα μηνύματα, μειώνοντας το συνολικό κρυπτογραφικό κόστος (encryption overhead) στις κινητές συσκευές. Μειώνοντας τον όγκο των κρυπτογραφημένων δεδομένων που υποβάλλονται σε επεξεργασία μέσω της επιλεκτικής κρυπτογράφησης, η ενσωμάτωση του SEACOD στον ομιχλώδη προγραμματισμό μπορεί να βελτιώσει την απόδοση και να βοηθήσει στην εξοικονόμηση σημαντικών πόρων του ομιχλώδους προγραμματισμού, όπως ο χρόνος επεξεργασίας και η ισχύς, λόγω της ανάλογης σχέσης μεταξύ του όγκου των δεδομένων και του χρόνου επεξεργασίας. Επιπλέον, η επιλεκτική κρυπτογράφηση σε συνδυασμό με τις διαφορετικές πλατφόρμες, επιτρέπει την επιλογή του βέλτιστου αλγορίθμου για κάθε συγκεκριμένο σύνολο δεδομένων και συσκευής, εξασφαλίζοντας έτσι την ισορροπία μεταξύ ασφάλειας και αποδοτικότητας του συστήματος του ομιχλώδους προγραμματισμού. Για παράδειγμα, ο κρυπτογραφικός αλγόριθμος AES μπορεί να είναι πιο αποδοτικός σε πλατφόρμες με επεξεργαστές της Intel, λόγω τον εντολών AES-NI, ενώ ο κρυπτογραφικός αλγόριθμος Blowfish μπορεί να είναι η καλύτερη επιλογή σε συσκευές με επεξεργαστές ARM. Τέλος, η επιλεκτική κρυπτογράφηση αποτελεί μια αποτελεσματική στρατηγική για την ενίσχυση της ασφάλειας των δεδομένων κατά την μεταφορά τους μεταξύ των έξυπνων συσκευών, καθώς μειώνει τόσο την ποσότητα των δεδομένων που είναι εκτεθειμένα σε κινδύνους όσο και τον υπολογιστικό φόρτο που απαιτείται για την προστασία τους. (Song, Choi and Kim, 2016)

Η επιλεκτική κρυπτογράφηση παρουσιάζει αρκετά μειονεκτήματα που σχετίζονται με την εφαρμογή και την διαχείριση της παραπάνω τεχνικής κρυπτογράφησης. Πρώτα από όλα, η επιλεκτική κρυπτογράφηση απαιτεί πιο εξειδικευμένο λογισμικό για την ανάλυση και την κατάτμηση των δεδομένων σε τμήματα, αυξάνοντας το κόστος υλοποίησης και της συντήρησης. Επίσης, υπάρχει ο κίνδυνος να διακυβεύεται η ασφάλεια ολοκλήρου του συστήματος αν η επιλεκτική κρυπτογράφηση δεν επιλέξει τα σωστά δεδομένα. Σε αυτή την περίπτωση, ευαίσθητα δεδομένα μπορεί να μεταδοθούν μέσω μη ασφαλών πρωτοκόλλων σε μη κρυπτογραφημένη μορφή, αποκαλύπτοντας τα σε μη εξουσιοδοτημένα μέρη. Επιπλέον, η χρήση διαφορετικών αλγορίθμων κρυπτογράφησης σε διαφορετικά συσχετιζόμενα δεδομένα που στέλνονται σε διαφορετικές συσκευές μπορεί να δημιουργήσει προβλήματα συμβατότητας, ιδιαιτέρα όταν πρόκειται για την αποθήκευση και την ανάκτηση των δεδομένων από διαφορετικά συστήματα ή πλατφόρμες. Καθώς η επιλεκτική κρυπτογράφηση εφαρμόζει διαφορετικές μεθόδους κρυπτογράφησης σε διαφορετικά μέρη των δεδομένων, η παρακολούθηση, η διαχείριση και η συντήρηση του συστήματος κρυπτογράφησης μπορεί να καταστούν πιο δύσκολες και απαιτητικές. Τέλος, εφόσον δεν γίνεται κάποια περαιτέρω επεξεργασία των δεδομένων, ενδέχεται να μπορεί να γίνει αποκάλυψη των ευαίσθητών δεδομένων μέσω των συσχετίσεων τους με τα μη ευαίσθητα δεδομένα που δεν κρυπτογραφούνται και άρα είναι ορατά στους επιτιθέμενους. (Song, Choi and Kim, 2016)

5.3.4.2 Κοινή αυθεντικοποίηση

Οι Kalaria κ.α. (2021) ορίζουν την κοινή ή αμοιβαία αυθεντικοποίηση (mutual authentication) ως μια αμφίδρομη διαδικασία κατά την οποία τόσο ο πελάτης όσο και ο διακομιστής πρέπει να επαληθεύσει ο ένας την ταυτότητα του αλλού ώστε να δημιουργηθεί ένα ασφαλές κρυπτογραφημένο κανάλι επικοινωνίας μεταξύ των δύο μερών. Σκοπός της κοινής αυθεντικοποίησης είναι να διασφαλίσει τις επικοινωνίες μεταξύ του πελάτη και του διακομιστή, ώστε μόνο τα εξουσιοδοτημένα μέρη να έχουν πρόσβαση στα ευαίσθητα δεδομένα εντός του δικτύου. Το παραπάνω μπορεί να επιτευχθεί με την χρήση κλειδιών, τα οποία περιλαμβάνουν είτε δημόσια κλειδιά, είτε ιδιωτικά κλειδιά είτε κλειδιά συνεδρίας (session keys), καθώς και πιστοποιητικών που περιέχουν βασικές πληροφορίες για τον πελάτη / διακομιστή. Μάλιστα, προς αυτό τον σκοπό, πρωτόκολλα όπως είναι το Diffie-Hellam, μπορούν να εφαρμοστούν και σε ομιχλώδη περιβάλλοντα για την ασφαλή ανταλλαγή κλειδιών και την διασφάλιση της εμπιστευτικότητας των επικοινωνιών. (Kalaria et al., 2021)

Η κοινή αυθεντικοποίηση προσφέρει πολλά σημαντικά πλεονεκτήματα στην ασφάλεια των επικοινωνιών. Αρχικά, εξασφαλίζει ότι μόνο ο αποστολέας και ο παραλήπτης έχουν πρόσβαση σε ευαίσθητα δεδομένα εντός του δικτύου, καθιστώντας την επικοινωνία ασφαλή. Επίσης, η κοινή αυθεντικοποίηση εξασφαλίζει ότι τόσο ο πελάτης όσο και ο διακομιστής επαληθεύουν την ταυτότητα ο ένας του άλλου, προσφέροντας ένα πρόσθετο επίπεδο ασφάλειας (Kalaria et al., 2021). Σημαντικό είναι επίσης το γεγονός ότι αλγόριθμοι κρυπτογράφησης, όπως RSA και AES, όταν χρησιμοποιούνται σε συνδυασμό με μηχανισμούς, όπως το challenge-response και το nonce, συμβάλουν στην προστασία της ακεραιότητας των δεδομένων που μεταφέρονται μετά την

εγκαθίδρυση ενός κρυπτογραφημένου καναλιού. Αυτοί οι μηχανισμοί διασφαλίζουν με αυτόν τον τρόπο ότι αυτά τα δεδομένα δεν τροποποιούνται ή να αλλοιώνονται κατά την μεταφορά τους από τον αποστολέα στον παραλήπτη, καθώς είναι πλέον εύκολο να ανιχνευθούν οι μη εξουσιοδότημενες αλλαγές (Loffi *et al.*, 2019). Τέλος, η ελλειπτική καμπύλη κρυπτογραφίας (Elliptic Curve Cryptography-ECC), παρέχει την ίδια ασφάλεια με άλλες κρυπτογραφικές μεθόδους, αλλά με μικρότερο μέγεθος κλειδιών, καθιστώντας την ιδανική για IoT συσκευές, οι οποίες διαθέτουν περιορισμένη υπολογιστική ισχύ, και άρα και για ομιχλώδη περιβάλλοντα. (Kalaria et al., 2021)

Η κοινή αυθεντικοποίηση αντιμετωπίζει ορισμένες σημαντικές προκλήσεις που μπορούν να επηρεάσουν την αποτελεσματικότητα της. Αρχικά, η εξάρτηση από ένα αξιόπιστο τρίτο μέρος, όπως ένας διακομιστής σύννεφου (cloud server), για την διαχείριση των κλειδιών και την επαλήθευση των ταυτοτήτων, ενέχει τον κίνδυνο αυτό να αποτελέσει μοναδικό σημείο αποτυχίας. Σε περίπτωση που αυτός ο διακομιστής παραβιαστεί, η συνολική ασφάλεια του συστήματος κοινής αυθεντικοποίησης μπορεί να τεθεί σε κίνδυνο. Ωστόσο, αξίζει να σημειωθεί ότι η διαχείριση των κλειδιών και η επαλήθευση ταυτοτήτων μπορεί να γίνει και με άλλους τρόπους, χωρίς να απαιτείται η συμμετοχή ενός τρίτου μέρους. Αυτές οι διαδικασίες μπορούν να εκτελούνται τοπικά από τα μέρη, χρησιμοποιώντας τοπικές λύσεις ασφάλειας, μειώνοντας έτσι τον κίνδυνο εξάρτησης από εξωτερικούς διακομιστές. Επίσης, ενώ το σύστημα κοινής αυθεντικοποίησης χαρακτηρίζεται ως «ελαφρύ» και χαμηλής πολυπλοκότητας σε ορισμένες περιπτώσεις, η υλοποίηση του απαιτεί μια σημαντική υποδομή για την καταχώριση και την διαχείριση των κλειδιών και των ταυτοτήτων, γεγονός που μπορεί να αυξήσει την επιχειρησιακή πολυπλοκότητα, ειδικά όταν χρησιμοποιείται κρυπτογραφία δημόσιου κλειδιού. Τέλος, η αποτελεσματικότητα του συστήματος κοινής αυθεντικοποίησης εξαρτάται σε μεγάλο βαθμό από την ορθή διαχείριση των κλειδιών. Μια τυχόν διαρροή ή μια εσφαλμένη διαχείριση της ιδιωτικότητας των κλειδιών μπορεί να οδηγήσει σε ευπάθειες, υπονομεύοντας την ασφάλεια ολοκλήρου του συστήματος κοινής αυθεντικοποίησης. (Kalaria et al., 2021)

5.3.4.3 IoTCop

Το IoTCop είναι ένα σύστημα ασφάλειας που χρησιμοποιεί τεχνολογία τύπου blockchain για να επιβλέπει και να διασφαλίζει την ασφάλεια των IoT συσκευών σε δίκτυα με άδειες (permissioned networks). Το IoTCop βασίζεται σε πρωτόκολλα συναίνεσης, όπως είναι το Hyperledger, έτσι ώστε να εξασφαλίζεται η επιβολή κανόνων ασφάλειας, ενώ παρακολουθεί τα μηνύματα που ανταλλάσσονται μεταξύ των συσκευών για να διασφαλίσει ότι πληρούνται συγκεκριμένες πολιτικές ασφάλειας, όπως το ότι το κάθε μήνυμα πρέπει να έχει ένα μοναδικό αναγνωριστικό (unique ID). Εάν ανιχνευτεί ότι μια συσκευή δεν συμμορφώνεται με τις πολιτικές ασφάλειας, το IoTCop εμποδίζει την εξερχόμενη κίνηση από αυτή την συσκευή, προστατεύοντας το δίκτυο από την εξάπλωση της απειλής. (Khan and Namin, 2022)

Το IoTCop προσφέρει παρά πολλά πλεονεκτήματα στον ομιχλώδη προγραμματισμό. Αρχικά, το IoTCop αξιοποιώντας την τεχνολογία blockchain, προσφέρει ένα ισχυρό πλαίσιο ασφάλειας για τα IoT δίκτυα του ομιχλώδους προγραμματισμού. Το IoTCoP είναι ανθεκτικό σε παραβιάσεις που

αφορούν την ενημέρωση των πολιτικών ασφάλειας σε πραγματικό χρόνο, εκτός αν ένας εισβολέας καταφέρει να παραβιάσει την πλειοψηφία των κόμβων, κάτι που είναι τεχνικά δύσκολο, λόγω και της χρήσης του πρωτοκόλλου συναίνεσης. Επίσης, το IoTCoP προσφέρει διαφορετικές επιλογές ασφάλειας, από μηδενική ασφάλεια έως ελάχιστη (όπου απαιτούνται μόνο ψηφιακά υπογεγραμμένα μηνύματα), επιτρέποντας την προσαρμογή των πολιτικών ασφάλειας ανάλογα με τα ανάγκες τις δικτύου. Ακόμα, το IoTCop δεν εξαρτάται από μια κεντρική αρχή ελέγχου, γεγονός που αυξάνει την ανθεκτικότητα του σε κακόβουλες επιθέσεις που προσπαθούν να στοχεύσουν σε ένα κεντρικό σημείο ελέγχου. (Khan and Namin, 2022), (Seshadri *et al.*, 2020)

Ωστόσο, το IoTCop δεν υποστηρίζει την κρυπτογράφηση των μηνυμάτων, αφήνοντας τα δεδομένα ευάλωτα κατά την μετάδοση τους, κάτι που θα μπορούσε να οδηγήσει σε διαρροή ευαίσθητων δεδομένων. Καθώς το δίκτυο μεγαλώνει, η απόδοση του IoTCoP μπορεί να μειωθεί. Αυτό είναι ιδιαίτερα εμφανές σε μεγάλα IoT δίκτυα, όπου η κλιμάκωση μπορεί να οδηγήσει σε καθυστερήσεις και προβλήματα απόδοσης. Επιπλέον, σε περιπτώσεις όπου μια συσκευή δεν υποστηρίζει το IoTCoP απαιτείται η χρήση πρόσθετου υλικού (hardware modules) για την ενσωμάτωση του, αυξάνοντας το κόστος και την πολυπλοκότητα της εγκατάστασης. Το IoTCop δεν είναι ξεκάθαρα μια λύση τύπου blockchain, αλλά ενσωματώνει αρχές που σχετίζονται με την ασφάλεια και την αξιοπιστία που προσφέρει το blockchain. Δεν έχει την ίδια πολυπλοκότητα με ένα πλήρες blockchain, καθιστώντας το πιο κατάλληλο για περιβάλλοντα με περιορισμένους πόρους, όπως τα περιβάλλοντα ομίχλης. (Khan and Namin, 2022)

5.3.4.4 NetSprint

Το NetSprint ανιχνεύει επιθέσεις DDoS χρησιμοποιώντας μηχανική μάθηση με ημι-επίβλεψη (semi-supervised learning) και τεχνικές κλαδέματος (pruning) για την βελτίωση της απόδοσης και της ακρίβειας ως προς την ανίχνευση των επιθέσεων DDoS του συστήματος (Khan and Namin, 2022).

Τα συστατικά μέρη του NetSprint είναι τα εξής (Khan and Namin, 2022):

1. *Τοπική Μονάδα Εκπαίδευσης (Local training module*): Εκπαιδεύει το μοντέλο αναγνώρισης επιθέσεων DDoS χρησιμοποιώντας τοπικά δεδομένα, βελτιώνοντας την απόδοση χωρίς να απαιτείται η αποστολή όλων των δεδομένων στον κεντρικό διακομιστή.
2. *Κεντρική Μονάδα Ενοποίησης Μοντέλων (Global aggregation module):* Συνδυάζει τα τοπικά μοντέλα νευρωνικού δικτύου σε ένα κεντρικό νευρωτικό δίκτυο, το οποίο στη συνέχεια ενημερώνεται μέσω της τεχνικής του κλαδέματος (pruning), έτσι ώστε να μειωθεί το μέγεθος του, καθώς και το κόστος υπολογισμού και η μνήμη του.
3. *Μονάδα Ανάλυσης Πακέτων (Packet parse Module):* Αναγνωρίζει τον τύπο των δεδομένων (πακέτα ελέγχου ή κυκλοφορίας), επιτρέποντας την άμεση ανίχνευση επιθέσεων DDoS σε πραγματικό χρόνο.

Το NetSprint ενσωματώνει μια αξιόπιστη αρχιτεκτονική δικτύου που αναλύεται σε τρία επίπεδα (Khan and Namin, 2022):

1. *Επίπεδο Ευφυΐας:* Είναι υπεύθυνο για την ανίχνευση των επιθέσεων DDoS μέσω της εκπαίδευσης του μοντέλου.
2. *Επίπεδο Ταυτοποίησης:* Ελέγχει την αυθεντικότητα της διεύθυνσης προέλευσης.
3. *Επίπεδο Υποδομής:* Παρέχει αξιόπιστη αποθήκευση και υπολογιστική ισχύ, χρησιμοποιώντας τεχνολογίες όπως το blockchain για την ασφάλεια και την ακεραιότητα των δεδομένων.

Το NetSprint προσφέρει σημαντικά πλεονεκτήματα σε περιβάλλοντα ομίχλης, ιδίως όσον αναφορά την ανίχνευση των επιθέσεων DDoS. Χρησιμοποιώντας μηχανική μάθηση με ημι-επίβλεψη και τεχνικές κλαδέματος, το σύστημα μπορεί να ανιχνεύει επιθέσεις DDoS σε πραγματικό χρόνο με μεγάλη αποτελεσματικότητα ακόμα και σε περιπτώσεις με αυξημένη κίνηση στο δίκτυο. Επίσης, η τεχνική κλαδέματος μειώνει το μέγεθος του κεντρικού νευρωνικού δικτύου, βοηθώντας με αυτό τον τρόπο στην βελτιστοποίηση των περιορισμένων υπολογιστικών και αποθηκευτικών πόρων του δικτύου. Ακόμα, το NetSprint μπορεί να διαχειρίζεται το φόρτο εργασίας μεταξύ των τοπικών μονάδων και των κεντρικών μονάδων, επιτρέποντας στις συσκευές να εκπαιδεύουν τα μοντέλα τους τοπικά και να στέλνουν μόνο το αποτελέσματα στο κεντρικό σύστημα, χωρίς να χρειάζεται να στέλνουν πολλά δεδομένα στην κεντρική μονάδα. Τέλος, η εφαρμογή πολλαπλών επιπέδων στο NetSprint ενισχύει την ασφάλεια, διασφαλίζοντας την αυθεντικότητα των δεδομένων και την ακεραιότητα του δικτύου. (Khan and Namin, 2022)

Από την άλλη πλευρά, η εφαρμογή του NetSprint σε ένα περιβάλλον ομίχλης, μπορεί να αυξήσει το υπολογιστικό κόστος, καθώς η εκπαίδευση των νευρωνικών δικτυών απαιτεί σημαντική υπολογιστική ισχύ. Επίσης, η μηχανική μάθηση με ημι-επίβλεψη εξαρτάται από την ποιότητα των δεδομένων, κάτι που είναι δύσκολο να επιτευχθεί σε κατανεμημένα και ανομοιογενή περιβάλλοντα, όπως αυτά του ομιχλώδους προγραμματισμού. Τέλος, η πολυεπίπεδη αρχιτεκτονική του NetSprint μπορεί να δυσχεραίνει την ανάπτυξη και την συντήρηση του συστήματος, καθώς απαιτεί αποτελεσματικό συγχρονισμό μεταξύ των τοπικών μονάδων και των κεντρικών μονάδων. (Khan and Namin, 2022)

5.3.4.5 Τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση για την αποτροπή επιθέσεων MitM

Οι Elmansy, Metawally και Metwally (2023) πρότειναν μια τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM στον ομιχλώδη προγραμματισμό. Η πρόταση συνδυάζει το επίπεδο ομίχλης με την αρχιτεκτονική SDN (Software-Defined Network), ενώ παράλληλα ενσωματώνει τεχνικές όπως το MPTCP (Multi-Path Transmission Control Protocol), το MTD (Moving Target Defense) και την ενισχυμένη μηχανική μάθηση σε ένα ενιαίο πλαίσιο, το οποίο βελτιώνει την ασφάλεια του δικτύου, δυσχεραίνοντας την αναγνώριση και την ανακάλυψη του δικτύου από επιτιθέμενους. Η αξιολόγηση

αυτού του πλαισίου πραγματοποιήθηκε σε ένα περιβάλλον προσομοίωσης με όνομα Mininet, με την χρήση του πυρήνα MPTCP και τον ελεγκτή SDN Ryn. Τα πειραματικά αποτελέσματα έδειξαν ότι το προτεινόμενο πλαίσιο διατήρησε την ανθεκτικότητα του δικτύου και βελτίωσε την αξιοποίηση των πόρων του, χωρίς να προκαλεί σημαντική αύξηση στο φόρτου του δικτύου, όπως συνήθως συμβαίνει με το παραδοσιακό πρωτόκολλο ελέγχου μετάδοσης TCP (Transmission Control Protocol). (Elmansy, Metwally and Badran, 2023)

Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM στον ομιχλώδη προγραμματισμό προσφέρει πολλά πλεονεκτήματα. Αρχικά, η αβεβαιότητα στο δίκτυο αυξάνεται μέσω της τεχνικής MTD, η οποία αλλάζει συνεχώς τα κρίσιμα σημεία του δικτύου, όπως είναι οι διαδρομές και οι διευθύνσεις IP, καθιστώντας δύσκολο για τον επιτιθέμενο να εντοπίσει και να κατανοήσει την δομή του δικτύου. Επίσης, η ενσωμάτωση της ενισχυμένης μηχανικής μάθησης μέσω του RL-routing επιτρέπει την βελτιστοποίηση των διαδρομών με το RL agent να αναλύει συνεχώς τα δεδομένα και να επιλέγει τις πιο αποδοτικές διαδρομές, μειώνοντας με αυτό τον τρόπο την καθυστέρηση και αυξάνοντας την απόδοση του δικτύου. Παράλληλα, η χρήση πολλαπλών διαδρομών μέσω του MPTCP και η προσαρμογή αυτών μέσω του RL-routing ενισχύει την ανθεκτικότητα του δικτύου σε περιπτώσεις επιθέσεων MiTM ή δυσλειτουργιών. Τέλος, παρά τις επιπρόσθετες τεχνικές, η προτεινόμενη λύση ασφάλειας καταφέρνει να διατηρεί την χαμηλή καθυστέρηση, καθιστώντας την κατάλληλη και αποδοτική για εφαρμογές σε ομιχλώδη περιβάλλοντα. (Elmansy, Metwally and Badran, 2023)

Ωστόσο, η προτεινόμενη λύση ασφάλειας παρουσιάζει ορισμένα μειονεκτήματα. Πρώτα από όλα, η ενσωμάτωση των τεχνολογιών, όπως το SDN, το MTD και η ενισχυμένη μηχανική μάθηση αυξάνει σημαντικά την πολυπλοκότητα του συστήματος, απαιτώντας εξειδικευμένη γνώση για την υλοποίηση και την συντήρηση του. Επίσης, το MPTCP, αν και βελτιώνει την απόδοση, μπορεί να εισάγει καθυστερήσεις λόγω τον πολλαπλών υπο-διαδρομών, με πιθανή επιδείνωση όταν η αλλαγή γίνεται πιο συχνά μέσω του MTD. Επιπλέον, η ενισχυμένη μηχανική μάθηση απαιτεί καλά εκπαιδευμένα μοντέλα για να αποδώσει βέλτιστα, και αυτό μπορεί να απαιτήσει χρόνο και υψηλής ποιότητας δεδομένα. Τέλος, αν και το RL-routing έχει την ικανότητα να βρίσκει τις βέλτιστες διαδρομές, η συνεχής παρακολούθηση και η συντήρησή του είναι απαραίτητα για να εξασφαλιστεί η μακροχρόνια απόδοση και η ασφάλεια της προτεινόμενης λύσης ασφάλειας για την ανίχνευση των επιθέσεων MiTM. (Elmansy, Metwally and Badran, 2023)

5.3.4.6 Σύγκριση αντιμέτρων ασφάλειας σχετικά με την επικοινωνία εντός ή εκτός του οργανισμού / επιχείρησης

Τα κριτήρια σύγκρισης που παρουσιάζονται στην ενότητα 5.2 της παρούσας διπλωματικής εργασίας εφαρμόστηκαν για την αξιολόγηση των αντιμέτρων που αφορούν την αντιμετώπιση των ζητημάτων ασφάλειας σχετικά με την επικοινωνία εντός ή εκτός του οργανισμού επιχείρησης στον ομιχλώδη προγραμματισμό, όπως αυτά περιγράφονται στις ενότητες 5.3.4.1-5.3.4.5 της διπλωματικής εργασίας. Η δικαιολόγηση της αξιολόγησης αυτής παρατίθεται παρακάτω

συνοδευόμενη από τον Πίνακας 5 που παρουσιάζει συνοπτικά τα αποτελέσματα της. Κατόπιν, παρέχονται ορισμένα σημαντικά συμπεράσματα που προκύπτουν από τα αποτελέσματα αυτά.

Κατανάλωση Πόρων

- Η μερική κρυπτογράφηση αξιολογείται με 3, διότι αν και κρυπτογραφεί μόνο τα κρίσιμα δεδομένα, η κατανάλωση πόρων μπορεί να διαφέρει ανάλογα με το ποσοστό των ευαίσθητων δεδομένων και τον αλγορίθμων κρυπτογράφησης που χρησιμοποιείται. Σε περιπτώσεις όπου το ποσοστό των ευαίσθητων δεδομένων είναι υψηλό ή απαιτείται συχνή κρυπτογράφηση και αποκρυπτογράφησης, η κρυπτογράφηση μπορεί να θεωρηθεί πιο «βαριά» και να οδηγήσει σε μέτρια κατανάλωση πόρων.
- Η κοινή αυθεντικοποίηση αξιολογείται με 2, καθώς αν και η διαχείριση των κλειδιών δεν απαιτεί πολλούς πόρους, η διαδικασία επαλήθευσης των ταυτοτήτων μπορεί να χρειαστεί σημαντικούς πόρους. Η επαλήθευση αυτή γίνεται μονό μια φόρα για κάθε συνεδρία, αλλά το βάρος της αυθεντικοποίησης συνδυάζεται με την ανάγκη για κρυπτογράφηση των δεδομένων κατά την επικοινωνία, κάνοντας την διαδικασία της κοινής αυθεντικοποίησης με αρκετά βαρύτερη και απαιτητική σε πόρους.
- Το IoTCop αξιολογείται με 2, διότι εκτός από τους υπολογιστικούς πόρους που απαιτούνται για τη λειτουργία των πρωτοκόλλων συναίνεσης, απαιτούνται επίσης σημαντικοί πόροι αποθήκευσης για την αποθήκευση ολόκληρου του blockchain. Η απόδοση του συστήματος επηρεάζεται κυρίως σε συγκεκριμένες περιπτώσεις, όπως όταν πραγματοποιούνται πολλές συναλλαγές ή όταν η υποδομή του blockchain είναι ιδιαίτερα φορτωμένη.
- Το NetSprint αξιολογείται με 2, διότι το σύστημα απαιτεί υψηλή υπολογιστική ισχύ για την λειτουργία του, ειδικά λόγω της μηχανικής μάθησης και των νευρωνικών δικτύων, αλλά η χρήση τεχνικών κλαδέματος βοηθά στην μείωση του μεγέθους του τελικού παραγόμενου μοντέλου. Επίσης, η εκπαίδευση πραγματοποιείται συνεχώς και τοπικά και άρα η απόδοση του συστήματος NetSprint επηρεάζεται συνεχώς.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 3, διότι αν και η ενσωμάτωση πολλαπλών τεχνολογιών (SDN, MPTCP, MTD) μπορεί να αυξάνει τις απαιτήσεις σε πόρους, η απόδοση του δικτύου βελτιώνεται και η καθυστέρηση παραμένει γενικά μικρή.

Κλιμακωσιμότητα

- Η μερική κρυπτογράφηση αξιολογείται με 2 στο παρόν αντίμετρο. Σε περιπτώσεις όπου το μεγαλύτερο ποσοστό των δεδομένων είναι κρίσιμο και χρειάζεται κρυπτογράφηση, ο φόρτος εργασίας αυξάνεται και οι απαιτήσεις σε πόρους αυξάνονται σημαντικά προσεγγίζοντας την πλήρη κρυπτογράφηση. Επομένως, θα έχει αρνητική επίδραση στην απόδοση του συστήματος.
- Η κοινή αυθεντικοποίηση αξιολογείται με 3, διότι ο μεγάλος φόρτος αφορά μόνο την αρχή της εφαρμογής του αντιμέτρου για την εγκαθίδρυση του ασφαλούς καναλιού. Από εκεί και πέρα, η κρυπτογράφηση μπορεί να γίνεται πολύ γρήγορα, π.χ. με την χρήση συμμετρικού κλειδιού.

- Το IoTCop αξιολογείται με 2, διότι σε μεγάλα δίκτυα η απόδοση του μειώνεται και μπορεί να προκαλέσει καθυστερήσεις.
- Το NetSprint αξιολογείται με 4, διότι μπορεί να κλιμακωθεί και να διατηρήσει την απόδοση του, καθώς αυξάνεται ο φόρτος εργασίας μεταξύ των τοπικών και των κεντρικών μονάδων.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 4, διότι το σύστημα διατηρεί την καλή απόδοσή του παρά την αύξηση του φόρτου εργασίας, ειδικά όταν εφαρμόζεται το RL-routing. Όμως η πολυπλοκότητα του μπορεί να προκαλέσει περιορισμούς σε δίκτυα μεγαλύτερου μεγέθους, γεγονός που θα μπορούσε να επηρεάσει την επεκτασιμότητα σε ορισμένες περιπτώσεις, όπως ο μεγάλος αριθμός κόμβων, χωρίς όμως να μειώνει την συνολική απόδοση, λόγω της αποδοτικής διαχείρισης του φόρτου εργασίας στα περισσότερα σενάρια.

Ασφάλεια Δεδομένων

- Η μερική κρυπτογράφηση αξιολογείται με 4, διότι προσφέρει υψηλή ασφάλεια, αλλά η πολυπλοκότητα της διαχείρισης των κλειδιών και των δεδομένων ενδέχεται να δημιουργήσει ευπάθειες.
- Η κοινή αυθεντικοποίηση αξιολογείται με 4, διότι προσφέρει υψηλή ασφάλεια, αλλά η πολυπλοκότητα της διαχείρισης των κλειδιών, η κρυπτογράφηση των δεδομένων και η επαλήθευση ταυτοτήτων ενδέχεται να δημιουργήσει ευπάθειες.
- Το IoTCop αξιολογείται με 2, διότι εξασφαλίζει την ασφάλεια μέσω τον πρωτοκόλλων συναίνεσης, αλλά η απουσία κρυπτογράφησης μειώνει την προστασία των δεδομένων.
- Το NetSprint αξιολογείται με 4, διότι η εφαρμογή τεχνολογιών όπως το blockchain για την ασφάλεια των δεδομένων και την ακεραιότητα τους παρέχει πολύ ισχυρή προστασία, καθιστώντας το σύστημα εξαιρετικά ασφαλές. Επιπλέον, η αποτροπή DDoS επιθέσεων μπορεί να επιτρέψει την διατήρηση της σωστής λειτουργίας του συστήματος, με αποτέλεσμα η ακεραιότητα των δεδομένων να διατηρείται.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 4, διότι ο συνδυασμός του MTD και του RL-routing προσφέρουν υψηλό επίπεδο ασφάλειας, δυσχεραίνοντας την παρακολούθηση του δικτύου και την υλοποίηση επιθέσεων MiTM, αλλά δεν καλύπτει όλες τις πιθανές απειλές.

Ευκολία Χρήσης

- Η μερική κρυπτογράφηση αξιολογείται με 2, διότι μπορεί να είναι πιο σύνθετη στην εφαρμογή και την διαχείριση, ειδικά σε πολύπλοκα συστήματα.
- Η κοινή αυθεντικοποίηση αξιολογείται με 4, διότι αν και απαιτεί κάποιες εξειδικευμένες γνώσεις για την υλοποίηση και την διαχείριση των ταυτοτήτων και των κλειδιών, οι διαχειριστές συνήθως διαθέτουν ήδη αυτές τις γνώσεις. Επιπλέον, υπάρχουν εργαλεία για την αυτοματοποίηση της διαδικασίας και έτοιμα πρωτόκολλα που υποστηρίζουν την κοινή αυθεντικοποίηση, εφόσον ρυθμιστούν σωστά.

- Το IoTCop αξιολογείται με 2, διότι η χρήση απαιτεί σημαντική εξοικείωση με το blockchain και τα πρωτοκόλλα συναίνεσης, γεγονός που καθιστά την διαδικασία υλοποίησης και διαχείρισης τους αρκετά δύσκολη για τους χρήστες χωρίς εξειδικευμένες γνώσεις. Η πολυπλοκότητα του μπορεί να αποτελέσει σοβαρό εμπόδιο στην ευκολία χρήσης, καθιστώντας το λιγότερο προσιτό για οργανισμούς που δεν διαθέτουν εμπειρία σε αυτές τις τεχνολογίες.
- Το NetSprint αξιολογείται με 2, διότι αν και ο συντονισμός μεταξύ των τοπικών και κεντρικών μονάδων γίνεται αυτόματα, απαιτείται σωστή αρχική ρύθμιση από τον διαχειριστή. Ο διαχειριστής πρέπει να έχει γνώσεις για την παραμετροποίηση του συστήματος και τον έλεγχο των διαδικασιών, κάτι που το καθιστά δύσκολο στη χρήση για μη εξειδικευμένους χρήστες.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 2, διότι εκτός από την πολυπλοκότητα του συστήματος, απαιτείται επίσης εξοικείωση με διαφορετικές τεχνολογίες που δεν είναι ευρέως γνωστές, καθιστώντας την εγκατάσταση και την διαχείριση του δύσκολη για μη ειδικούς.

Εκπαίδευση χρηστών

- Η μερική κρυπτογράφηση αξιολογείται με 2, διότι απαιτεί υψηλό επίπεδο εκπαίδευσης των χρηστών, ειδικότερα του προσωπικού ασφάλειας για την απόκτηση των αναγκαίων γνώσεων ώστε να γίνει σωστή χρήση του αντιμέτρου αυτού. Η χρήση του απαιτεί κάποια εξειδίκευση, ενώ είναι σημαντικό να υπάρχουν καλές ικανότητες διαχωρισμού των δεδομένων ανάλογα με την ευαισθησία τους. Η εκπαίδευση για την μερική κρυπτογράφηση μπορεί να απαιτεί εξειδίκευση, αλλά συνήθως δεν είναι μακροχρόνια, εάν οι χρήστες είναι ήδη εξοικειωμένοι με τις βασικές αρχές ασφάλειας δεδομένων.
- Η κοινή αυθεντικοποίηση αξιολογείται με 4, διότι αν και απαιτεί εκπαίδευση για την σωστή διαχείριση των κλειδιών και την χρήση των πιστοποιητικών, οι γνώσεις αυτές είναι εύκολο να αποκτηθούν ή να εξουσιοδοτηθούν μέσω εργαλείων / υπηρεσιών, καθιστώντας την διαδικασία λιγότερο επιβαρυντική για τους χρήστες.
- Το IoTCop αξιολογείται με 3, διότι οι χρήστες χρειάζονται κάποιες βασικές γνώσεις blockchain, αλλά η εκπαίδευση είναι εφικτή σε σύντομο χρόνιο διάστημα και δεν είναι μακροχρόνια.
- Το NetSprint αξιολογείται με 2, διότι η εκπαίδευση των χρηστών είναι απαραίτητη για την καλή λειτουργία του NetSprint. Επιπλέον, οι χρήστες πρέπει να μάθουν πως να διαχειρίζονται την πολυπλοκότητα του συστήματος και να κατανοήσουν την λειτουργία του, κάτι που μπορεί να απαιτεί χρόνο.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 2, διότι απαιτεί εξειδικευμένη γνώση και εκπαίδευση για την υλοποίηση και την συντήρηση του συστήματος.

Αντίκτυπος Χρήστη

- Η μερική κρυπτογράφηση αξιολογείται με 3, διότι προκαλούνται καθυστερήσεις στην αποστολή των δεδομένων. Οι καθυστερήσεις εξαρτώνται από το είδος της κρυπτογράφησης που χρησιμοποιείται που χρησιμοποιείται, ενώ μπορεί να μειωθούν αν χρησιμοποιείται συμπίεση. Οι τελικοί χρήστες εφαρμογών και υπηρεσιών επηρεάζονται αρνητικά από το overhead της αυθεντικοποίησης και της διαχείρισης των πιστοποιητικών, καθώς απαιτούν γρήγορη αποστολή και λήψη δεδομένων σε πραγματικό χρόνο, όπως στην περίπτωση του online gaming, όπου η καθυστέρηση μπορεί να είναι πιο αισθητή.
- Η κοινή αυθεντικοποίηση αξιολογείται με 3, διότι μπορεί να προκαλέσει καθυστερήσεις ή επιπλέον βήματα για τους χρήστες, κυρίως λόγω των πρόσθετων διαδικασιών ταυτοποίησης. Ωστόσο, τα δεδομένα προστατεύονται αποτελεσματικά, ενώ η επικοινωνία πραγματοποιείται αυτόματα μέσω λογισμικού (clients και server), χωρίς να απαιτούνται επιπλέον βήματα από τους χρήστες.
- Το IoTCop αξιολογείται με 4, διότι η έλλειψη κεντρικής αρχής ενισχύει την αξιοπιστία του συστήματος και η απόδοση του βελτιώνεται σε μεγάλα δίκτυα, επηρεάζοντας θετικά την εμπειρία του χρήστη.
- Το NetSprint αξιολογείται με 4, διότι ο χρήστης δεν θα παρατηρήσει σημαντικές αλλαγές στην λειτουργία του συστήματος, καθώς το NetSprint διαχειρίζεται τις επιθέσεις DDoS χωρίς άμεση παρέμβαση. Επίσης, η μείωση της απόδοσης είναι ανεπαίσθητη και δεν επηρεάζει αρνητικά την εμπειρία του χρήστη.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 3, διότι οι πολλαπλές υποδιαδρομές του MPTCP εισάγουν κάποιες καθυστερήσεις στο σύστημα, οι οποίες μπορεί να έχουν αρνητικό αντίκτυπο στον χρήστη.

Εφαρμοσιμότητα

- Η μερική κρυπτογράφηση αξιολογείται με 3, διότι αν και μπορεί να εφαρμοστεί στα περιβάλλοντα ομίχλης, ενδέχεται να αντιμετωπίζει κάποιες δυσκολίες, όπως η ανάγκη για ενοποίηση με τις υφιστάμενες υποδομές, η δέσμευση επιπλέον πόρων και το κόστος για την σωστή εφαρμογή της.
- Η κοινή αυθεντικοποίηση αξιολογείται με 4, διότι ελαφριές κρυπτογραφικές μέθοδοι, όπως η ECC, απαιτούν λιγότερους πόρους και μπορεί να εφαρμοστεί σε περιβάλλοντα με περιορισμένους πόρους, όπως τα περιβάλλοντα ομίχλης.
- Το IoTCop αξιολογείται με 2, διότι η τεχνολογία blockchain και τα πρωτόκολλα συναίνεσης καθιστούν δύσκολη την εφαρμογή σε περιβάλλοντα ομίχλης με περιορισμένους πόρους, κάτι που μπορεί να περιορίσει την αποδοτικότητα του συστήματος σε τέτοια περιβάλλοντα.
- Το NetSprint αξιολογείται με 3, διότι η εφαρμογή του απαιτεί προσαρμογές και επιπλέον πόρους για να ενσωματωθεί στα υπάρχοντα περιβάλλοντα ομίχλης.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 3, διότι μπορεί να εφαρμοστεί στα υπάρχοντα περιβάλλοντα ομίχλης, καθώς συνδυάζει τεχνολογίες όπως το SDN και το MPTCP, όπου είναι συμβατές με την κατανεμημένη φύση του ομιχλώδους προγραμματισμού, ωστόσο απαιτεί προσαρμογές και πρόσθετους πόρους για την πλήρη ενσωμάτωση τους και λειτουργία τους.

Βαθμός κάλυψης

- Η μερική κρυπτογράφηση αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε πολλές περιπτώσεις, αλλά δεν είναι κατάλληλη για όλες τις εφαρμογές, ιδιαίτερα αν τα δεδομένα είναι όλα κρίσιμα, καθώς απαιτούνται περισσότεροι πόροι για να εξασφαλιστεί η πλήρης προστασία τους.
- Η κοινή αυθεντικοποίηση αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε ποικίλα περιβάλλοντα, όπως IoT περιβάλλοντα, περιβάλλοντα νέφους και περιβάλλοντα ομίχλης.
- Το IoTCop αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε πολλά περιβάλλοντα και σενάρια, καθώς και υπάρχουν σημαντικοί περιορισμοί στους αποθηκευτικούς πόρους.
- Το NetSprint αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε ένα ευρύ φάσμα περιβαλλόντων και σεναρίων, καθώς η αρχιτεκτονική του είναι ευέλικτη και μπορεί να ενσωματωθεί σε διάφορες τεχνολογίες.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM αξιολογείται με 3, διότι μπορεί να προσαρμοστεί σε πολλαπλά σενάρια και περιβάλλοντα. Ωστόσο, η απόδοση της μπορεί να επηρεαστεί από την πολυπλοκότητα του δικτύου, γεγονός που ενδέχεται να αποτελέσει έναν σημαντικό περιορισμό.

Επεκτασιμότητα

- Η μερική κρυπτογράφηση αξιολογείται με 4, διότι το σύστημα κρυπτογράφησης και οι μέθοδοι επιλογής δεδομένων είναι σχεδιασμένα για να υποστηρίζουν νέες απαιτήσεις και συσκευές.
- Η κοινή αυθεντικοποίηση αξιολογείται με 4, διότι μπορεί να επεκταθεί με την χρήση διαφορετικών αλγόριθμών κρυπτογράφησης, χωρίς να αποτελεί σημαντικό ζήτημα η διαχείριση των κλειδιών σε αυτό το πλαίσιο.
- IoTCop αξιολογείται με 3, διότι μπορεί να ενσωματώσει νέες λειτουργίες, αλλά η διαδικασία επέκτασης είναι χρονοβόρα, χωρίς όμως να υπάρχουν περιορισμοί στην επεκτασιμότητα του.
- Το NetSprint αξιολογείται με 4, διότι η επέκταση του είναι δυνατή και επιτρέπει την προσθήκη νέων λειτουργιών, όπως η ανίχνευση νέων ειδών επιθέσεων, με ελάχιστες τροποποίησης στις παραμέτρους ρύθμισης ή την ενσωμάτωση νέων κανόνων ανίχνευσης χωρίς την ανάγκη για σημαντικές αλλαγές στον βασικό σχεδιασμό ή την δομή του συστήματος.
- Η τεχνική ασφάλειας, η οποία βασίζεται στην ενισχυμένη μηχανική μάθηση (reinforcement learning) για την αποτροπή επιθέσεων ενδιάμεσου MiTM, αξιολογείται με 3, διότι αν και η ενσωμάτωση νέων τεχνολογιών είναι δυνατή μπορεί να αυξήσει την πολυπλοκότητα και τις απαιτήσεις για τη συντήρηση του συστήματος.

Πίνακας 5 - Πίνακας σύγκρισης αντιμέτρων ασφάλειας σχετικά με την επικοινωνίας εντός ή εκτός του οργανισμού / επιχείρησης

Αντίμετρα	**Κατανάλωση Πόρων**	**Κλιμακώσιμοτητα**	**Ασφάλεια δεδομένων**	**Ευκολία χρήσης**	**Εκπαίδευση χρηστών**	**Αντικτυπος στον χρήστη**	**Εφαρμοσιμότητα**	**Βαθμός κάλυψης**	**Επεκτασιμότητα**
Μερική κρυπτογράφηση	3	2	4	3	2	2	3	3	4
Κοινή αυθεντι-κοποίη-ση	2	3	4	4	4	2	4	4	4
IoTCop	2	2	2	2	3	4	2	3	3
NetSpri-nt	2	4	4	2	2	4	3	4	4
Τεχνική ασφαλεί-ας βασισμέ-νη στην ενισχυμέ-νη μηχανι-κή μάθηση κατά των MiTM	3	4	4	2	2	3	3	3	3

Με βάση τον παραπάνω πίνακα έχουμε μπορούμε να προχωρήσουμε σε ανάλυση των καλύτερων και των χειρότερων αντιμέτρων για κάθε κριτήριο:

Ανάλυση καλύτερου και χειρότερου αντιμέτρου: Θα εντοπίσουμε ποιο/-α αντίμετρο/-α έχει την καλύτερη και την χειρότερη τιμή σε κάθε κριτήριο αξιολόγησης:

- Κατανάλωση πόρων:
  - Καλύτερο: μερική κρυπτογράφηση, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM (3)
  - Χειρότερο: Κοινή αυθεντικοποίηση, NetSprint, IoTCop (2)
- Κλιμακωσιμότητα:

- Καλύτερο: τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM, NetSprint (4)
- Χειρότερο: IoTCop, μερική κρυπτογράφηση (2)

❖ Ασφάλεια δεδομένων:
- Καλύτερο: μερική κρυπτογράφηση, κοινή αυθεντικοποίηση, NetSprint, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM (4)
- Χειρότερο: IoTCop (2)

❖ Ευκολία χρήσης:
- Καλύτερο: κοινή αυθεντικοποίηση (4)
- Χειρότερο: μερική κρυπτογράφηση, IoTCop, NetSprint, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM (2)

❖ Εκπαίδευση χρηστών:
- Καλύτερο: κοινή αυθεντικοποίηση (4)
- Χειρότερο: μερική κρυπτογράφηση, NetSprint, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM (2)

❖ Αντίκτυπος στον χρήστη:
- Καλύτερο: IoTCop, NetSprint (4)
- Χειρότερο: μερική κρυπτογράφηση, κοινή αυθεντικοποίηση (2)

❖ Εφαρμοσιμότητα:
- Καλύτερο: Κοινή αυθεντικοποίηση (4)
- Χειρότερο: IoTCop (2)

❖ Βαθμός κάλυψης:
- Καλύτερο: NetSprint, κοινή αυθεντικοποίηση (4)
- Χειρότερο: IoTCop, μερική κρυπτογράφηση, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM (3)

❖ Επεκτασιμότητα:
- Καλύτερο: μερική κρυπτογράφηση, κοινή αυθεντικοποίηση, NetSprint (4)
- Χειρότερο: IoTCop, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM (3)

Καλύτερο και χειρότερο αντίμετρο συνολικά (στην κατηγορία): μερική κρυπτογράφηση: 26, κοινή αυθεντικοποίηση: 31, IoTCop: 23, NetSprint: 29, τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM: 26. Επομένως, η κοινή αυθεντικοποίηση με συνολική βαθμολογία 31 είναι το καλύτερο αντίμετρο συνολικά, ενώ το χειρότερο αντίμετρο συνολικά είναι το IoTCop με συνολική βαθμολογία 23.

Αντίμετρο με καλύτερη και χειρότερη απόδοση: Για την καλύτερη και χειρότερη απόδοση, πρέπει να εξετάσουμε την απόδοση των αντιμέτρων σε κάθε κριτήριο και να καταλήξουμε στο καλύτερο και το χειρότερο αντίμετρο βασιζόμενοι στο ποσοστό των υψηλών ή των χειρότερων βαθμολογίων τους που έχουν λάβει στα κριτήρια. Θεωρούμε την τιμή 1 με 2 χαμηλές τιμές και 4 με 5 υψηλές τιμές.

Ποσοστά υψηλών και χαμηλών βαθμολογιών:

- Μερική κρυπτογράφηση:
  - Υψηλές: 3/9 = 33,3 %

- Χαμηλές: 3/9 = 33,3 %
- Κοινή αυθεντικοποίηση:
  - Υψηλές: 6/9 = 66,7 %
  - Χαμηλές: 2/9 = 22,2 %
- IoTCop:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 5/9 = 55,6%
- NetSprint:
  - Υψηλές: 5/9 = 55,6 %
  - Χαμηλές: 3/9 = 33,3 %
- Τεχνική ασφάλειας βασισμένη στην ενισχυμένη μηχανική μάθηση κατά των MiTM:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 2/9 = 22,2 %

Το αντίμετρο με την καλύτερη απόδοση βάσει του ποσοστού των υψηλών βαθμολογίων είναι η κοινή αυθεντιποίηση με ποσοστό 66,7 %. Το αντίμετρο με την χειρότερη απόδοση βάσει του μεγαλύτερού ποσοστού χαμηλών βαθμολογίων είναι το IoTCop με ποσοστό 55,6 %.

5.3.5 Αντίμετρα για τις επιθέσεις που αφορούν την ασύρματη επικοινωνία

Για την αντιμετώπιση των επιθέσεων που αφορούν την ασύρματη επικοινωνία υπάρχουν αρκετά αντίμετρα που μπορούν για να εφαρμοστούν ώστε να βελτιωθεί η ασφάλεια και η προστασία των δικτύων. Ορισμένα από αυτά είναι η μέθοδος για την παρακολούθηση ευαίσθητων παραμέτρων ενός δικτύου και την ανίχνευση των ανωμαλιών (monitoring sensitive networks parameters detecting the anomalies), η τεχνική MLTKNN για την ανίχνευση επιθέσεων κατάταξης, τα πακέτα λουριών, η ανίχνευση κακόβουλων κόμβων και η αμφίδρομη επικύρωση ζεύξης (Khan, Parkinson and Qin, 2017).

5.3.5.1 Μέθοδος για την παρακολούθηση ευαίσθητων παραμέτρων ενός δικτύου και την ανίχνευση ανωμαλιών

Οι Le κα. (2013) προτείνουν μια μέθοδο για την παρακολούθηση ευαίσθητων παραμέτρων ενός δικτύου και την ανίχνευση των ανωμαλιών (monitoring sensitive networks parameters & detecting the anomalies), η οποία βοηθάει στην ενίσχυση της ασφάλειας έναντι των επιθέσεων κατάταξης στον ομιχλώδη προγραμματισμό (Le *et al.*, 2013). Η παραπάνω στρατηγική διαθέτει πολλά πλεονεκτήματα και μειονεκτήματα, τα οποία επηρεάζουν τον ομιχλώδη προγραμματισμό και αναφέρονται παρακάτω.

Η προαναφερόμενη μέθοδος βοηθάει στην συνεχόμενη παρακολούθηση ευαίσθητων παραμέτρων του δικτύου, όπως είναι η μέση καθυστέρηση από άκρο σε άκρο όλων των παραδομένων πακέτων και το ποσοστό παράδοσης, δηλαδή το ποσοστό όλων των απεσταλμένων πακέτων που παραλαμβάνονται με επιτυχία στον τελικό προορισμό τους, για την παραγωγή ενδείξεων που

μπορεί να χρησιμοποιηθούν για την πρώιμη ανίχνευση και την μείωση των επιθέσεων κατάταξης πριν επηρεάσουν σοβαρά όλο το υπόλοιπο δίκτυο. Επίσης, η ταυτοποίηση συγκεκριμένων περιοχών ή κόμβων με ανώμαλες παραμέτρους επιτυγχάνεται μέσω της παρακολούθησης συγκεκριμένων μετρικών στο επίπεδο των κόμβων, οι οποίες στην συνέχεια σχετίζονται με ανωμαλίες που έχουν εντοπιστεί. Αυτή η προσέγγιση επιτρέπει την εφαρμογή πιο στοχευμένων μέτρων ασφάλειας, τα οποία προσαρμόζονται δυναμικά στις επιθέσεις κατάταξης, βελτιώνοντας την ανθεκτικότητα του δικτύου και μειώνοντας την επίδραση αυτών των επιθέσεων, κάτι που μπορεί να είναι πιο αποτελεσματικό σε σχέση με την γενική εφαρμογή μέτρων σε ολόκληρο το δίκτυο. (Le *et al.*, 2013)

Ωστόσο, η συνεχής παρακολούθηση των δικτυών και η ανίχνευση ανωμαλιών σε ένα περιβάλλον ομίχλης όπου εφαρμόζεται η παραπάνω μέθοδος απαιτεί σημαντικούς πόρους, όπως επεξεργαστική ισχύ, μνήμη και εύρος ζώνης, που μπορεί να επηρεάσουν την απόδοση του δικτύου του ομιχλώδους προγραμματισμού. Επίσης, η μέθοδος αυτή μπορεί να δημιουργεί ψευδώς θετικά αποτελέσματα (αναγνωρίζοντας την κανονική συμπεριφορά ως ανώμαλη) ή ψευδώς αρνητικά (αποτυγχάνοντας να ανιχνεύσει πραγματικές επιθέσεις κατάταξης), κάτι που μπορεί να οδηγήσει είτε σε περιττό φόρτο εργασίας είτε σε αδιάγνωστες παραβιάσεις ασφάλειας. Επιπλέον, αν εφαρμοστεί κάποιο μέτρο, μπορεί να επηρεαστεί η απόδοση των εφαρμογών, εφόσον ένας κόμβος αποκλείεται με βάση τα αποτελέσματα αυτής της ανίχνευσης. Πιο συγκεκριμένα, οι Le κ.α. (2013) περιγράφουν στην εργασία τους για το πως ορισμένοι τύποι επιθέσεων κατάταξης σε δίκτυα RPL, μπορούν να επηρεάσουν την απόδοση του δικτύου με απρόβλεπτο τρόπο, δημιουργώντας αναποτελεσματικότητα στην ανίχνευση πραγματικών επιθέσεων κατάταξης ή διαταραχών στην σταθερότητα του δικτύου. Τέλος, η υλοποίηση και η συντήρηση ενός τέτοιου συστήματος σχετικά με την παρακολούθηση των δικτύων και την ανίχνευση των ανωμαλιών μπορεί να είναι περίπλοκη, καθώς μπορεί να απαιτεί προηγμένους αλγορίθμους για την ανάλυση των δεδομένων και τον εντοπισμό ύποπτων μοτίβων, αλλά και εξειδικευμένες ρυθμίσεις για να είναι αποτελεσματική. (Le *et al.*, 2013)

5.3.5.2 Τεχνική μηχανικής μάθησης βασισμένη στον αλγόριθμο Κ-Πλησιέστερων Γειτόνων (MLTKNN) για την ανίχνευση επιθέσεων κατάταξης

Οι Neerugatti κ.α. (2019) προτείνουν μια τεχνική τύπου MLTKNN, η οποία στηρίζεται σε μια προσέγγιση μηχανικής μάθησης που βασίζεται στον αλγόριθμο των K - πλησιέστερων γειτόνων (KNN) για την ανίχνευση επιθέσεων κατάταξης που συμβαίνουν στο RPL πρωτόκολλο. Στην προτεινόμενη τεχνική υπολογίζεται η απόσταση μεταξύ των κόμβων σε ένα IoT δίκτυο και η απόσταση αυτή συγκρίνεται με μια τιμή κατάταξης, η οποία έχει υπολογιστεί βάσει των χαρακτηριστικών ή της απόδοσης των κόμβων, όπως ορίζονται από προκαθορισμένες μετρήσεις ή παραμέτρους του δικτύου. Εάν παρατηρηθεί ασυμφωνία μεταξύ της υπολογισμένης απόστασης, όπως καθορίζεται από τον αλγόριθμο KNN και της αναφερόμενης τιμής κατάταξης που έχει προκύψει μέσω της εκπαίδευσης του μοντέλου μηχανικής μάθησης, η τεχνική MLTKNN καθορίζει ότι πρόκειται για κακόβουλο κόμβο και βοηθά στην απομάκρυνσή του από το δίκτυο. Η τεχνική MLTKNN περιλαμβάνει ορισμένα πλεονεκτήματα και μειονεκτήματα, τα οποία αναλύονται παρακάτω. (Neerugatti and Mohan Reddy, 2019)

Η τεχνική MLTKNN αποδεικνύεται εξαιρετικά αποτελεσματική στην αναγνώριση των επιθέσεων κατάταξης (rank attacks). Η υψηλή ακρίβεια της τεχνικής υποστηρίζεται από τα υψηλά ποσοστά των αληθώς θετικών αποτελεσμάτων, τα οποία υποδηλώνουν την δυνατότητα της να εντοπίζει με ακρίβεια τις απειλές και να συμβάλλει στην ενίσχυση της ασφάλειας του δικτύου του ομιχλώδους προγραμματισμού. Επίσης, η εφαρμογή της παραπάνω τεχνικής σε ομιχλώδη περιβάλλοντα είναι ιδιαίτερα επωφελής, διότι οδηγεί στην σημαντική μείωση της καθυστέρησης της μεταφοράς των δεδομένων και στην αύξηση του ποσοστού επιτυχούς παράδοσης πακέτων, πράγμα που είναι απαραίτητο σε ομιχλώδη περιβάλλοντα όπου οι πόροι είναι περιορισμένοι και απαιτείται αποτελεσματική διαχείριση τους. Επιπλέον, η ενσωμάτωση του KNN στην τεχνική MLTKNN επιτρέπει στο σύστημα του ομιχλώδους προγραμματισμού να προσαρμόζεται δυναμικά, καθώς το μοντέλο μηχανικής μάθησης αναπροσαρμόζει τις παραμέτρους του βάσει των νέων δεδομένων που συλλέγονται από το δίκτυο. Αυτό ενισχύει την συνεχιζόμενη βελτίωση της ακρίβειας ανίχνευσης του συστήματος στην αναγνώριση των επιθέσεων κατάταξης, καθώς το μοντέλο εξελίσσεται και προσαρμόζεσαι στις μεταβαλλόμενες συνθήκες του δικτύου. (Neerugatti and Mohan Reddy, 2019)

Παρά τα πλεονεκτήματα της τεχνικής MLTKNN, αυτή η τεχνική παρουσιάζει και ορισμένα μειονεκτήματα. Πρώτον, η τεχνική MLTKNN εστιάζει κυρίως στην ανίχνευση των επιθέσεων κατάταξης που προέρχονται από κακόβουλους κόμβους εντός του IoT δικτύου, χωρίς να παρέχει επαρκή προστασία από εξωτερικές επιθέσεις, οι οποίες μπορούν να επηρεάσουν αρνητικά την ασφάλεια όλου του δικτύου ενός περιβάλλοντος ομίχλης. Επιπλέον, η ενσωμάτωση της μεθόδου μηχανικής μάθησης KNN στην τεχνική MLTKNN, απαιτεί αυξημένους υπολογιστικούς πόρους για IoT περιβάλλοντα και για περιβάλλοντα ομίχλης, τα οποία χαρακτηρίζονται από περιορισμένες δυνατότητες επεξεργασίας και ενέργειας. Τέλος, η τεχνική MLTKNN, αν και αποδίδει ικανοποιητικά σε μικρά δίκτυα, όπως εκείνα που περιλαμβάνουν 30 κόμβους, ενδέχεται να προκύψουν προκλήσεις κατά την εφαρμογή της σε μεγαλύτερα δίκτυα, όπου η πολυπλοκότητα και οι απαιτήσεις επεξεργασίας αυξάνονται σημαντικά. (Neerugatti and Mohan Reddy, 2019)

5.3.5.3 Πακέτα λουριών

Το πακέτα λουριών (Packet Leashes) είναι μια μέθοδος ασφάλειας για την αποτροπή επιθέσεων σκουληκότρυπας (wormhole) στον ομιχλώδη προγραμματισμό. Η βασική της ιδέα στηρίζεται στο να περιορίζεται με κάποιο τρόπο (είτε χρονικό είτε γεωγραφικό) το κάθε πακέτο δεδομένων ως προς το ταξίδι του στο δίκτυο για να αποτραπούν οι κακόβουλες επιθέσεις ή οι ανεπιθύμητες δραστηριότητες. Τα πακέτα λουριών χωρίζονται σε δύο κατηγορίες: το γεωγραφικό λουρί (geographical leash) και τον χρονικό λουρί (temporal leash). Στο γεωγραφικό λουρί, το δίκτυο αποστέλλει την τοποθεσία και τον χρόνο μετάδοσης πριν στείλει το πακέτο δεδομένων. Όταν ο παραλήπτης λαμβάνει ένα πακέτο δεδομένων υπολογίζει τον χρόνο που πηρέ το πακέτο δεδομένων να φτάσει από τον αποστολέα στον παραλήπτη. Αυτός ο χρόνος λέγεται χρόνος διαδρομής. Στη συνέχεια, ο παραλήπτης συγκρίνει αυτόν τον υπολογισμό με τις πληροφορίες που έστειλε ο αποστολέας (τοποθεσίες και χρόνος αποστολής). Ο υπολογισμός αυτός βοηθά να εξακριβωθεί αν το πακέτο ήρθε από την σωστή τοποθεσία και μέσα σε λογικό χρόνο. Αν ο χρόνος διαδρομής ή η τοποθεσία δεν ταιριάζουν υπάρχει πιθανότητα να έχει γίνει προσπάθεια αλλοίωσης του πακέτου ή

επίθεσης. Ο χρόνος μετάβασης και επιστροφής (Round Trip Time - RTT) και ο χρόνος πτήσης (time of flight) είναι μερικές μέθοδοι (υλοποίησης ορίων στο χρόνο διαδρομής) που χρησιμοποιούνται στον γεωγραφικό περιορισμό για την ανίχνευση επιθέσεων. (Bhushan *et al.*, 2023)

Το χρονικό λουρί (temporal leash), όπως και το γεωγραφικό λουρί, απαιτεί τον συγχρονισμό των ρολογιών όλων των κόμβων του δικτύου, καθώς και τα δύο βασίζονται σε χρονικές παραμέτρους. Ορίζεται ένας χρόνος λήξης για το πακέτο (expiry timestamp). Ο παραλήπτης ελέγχει την ώρα κατά την οποία λαμβάνει το πακέτο και την συγκρίνει με την ώρα που στάλθηκε. Μια επίθεση ανιχνεύεται εάν ο χρόνος αυτός υπερβαίνει το ανώτερο όριο μετάδοσης. Ένας άλλος τρόπος ανίχνευσης της επίθεσης είναι η προσθήκη της χρονοσφαγίδας αποστολής και μέγιστου επιτρεπτού χρόνου παράδοσης. Οπότε, ο κάθε κόμβος προσθέτει αυτά τα δύο πράγματα και τα συγκρίνει με την τρέχουσα ώρα. Αν το πακέτο έχει λήξει (τρέχουσα ώρα μεγαλύτερη από το άθροισμα), τότε αποπέμπεται. (Zahra, Bostanci, and Soyturk, 2024)

Τα πακέτα λουριών προσφέρουν σημαντικά πλεονεκτήματα στην ανίχνευση και την αποτροπή επιθέσεων σκουληκότρυπας, όπου οι κακόβουλοι κόμβοι επιχειρούν να δημιουργήσουν παραπλανητικές διαδρομές στο δίκτυο. Όταν ένας κόμβος προσπαθεί να επικοινωνήσει με έναν άλλο κόμβο που είναι πολύ μακριά ή σε μια περιοχή εκτός των φυσιολογικών περιορισμών, όπως το εύρος ζώνης ή οι δυνατότητές του πρωτόκολλου δρομολόγησης, αυτό μπορεί να υποδεικνύει κακόβουλη δραστηριότητα, όπως οι επιθέσεις σκουληκότρυπας. Εντοπίζοντας και μπλοκάροντας τέτοιες κακόβουλες επιθέσεις σκουληκότρυπας, το δίκτυο ενισχύει την ασφάλεια του και αποτρέπει τέτοιου είδους επιθέσεις ή διαρροές δεδομένων. Επίσης, η προσθήκη μιας επιπλέον στρώσης ασφάλειας μέσω της χρονοσήμανσης (timestamp) ή των γεωγραφικών δεδομένων επιτρέπει τον ακριβέστερο υπολογισμό της απόστασης μεταξύ των κόμβων, περιορίζοντας τις πιθανότητες επιτυχίας των επιθέσεων. Ακόμα, η παραπάνω μέθοδος ασφάλειας μπορεί να εφαρμοστεί σε δίκτυα μικρής κλίμακας, όπου οι αποστάσεις μεταξύ των κόμβων είναι πιο εύκολα διαχειρίσιμες και ο έλεγχος της ακεραιότητας των πακέτων είναι πιο άμεσος. (Patil and Gaikwad, 2015), (Hu, Perrig and Johnson, 2003)

Ωστόσο, υπάρχουν σημαντικά μειονεκτήματα που περιορίζουν την εφαρμογή των πακέτων λουριών. Πρώτον, το υψηλό κόστος υλοποίησης είναι ένα σοβαρό εμπόδιο, καθώς η απόκτηση και η διαχείριση ακριβών πληροφοριών, όπως τα γεωγραφικά δεδομένα ή οι χρονοσημάνσεις, απαιτούν συγχρονισμό των ρολογιών των κόμβων, γεγονός που καταναλώνει σημαντικούς υπολογιστικούς πόρους από κάθε κόμβο. Αυτό καθιστά την παραπάνω μέθοδο ασφάλειας δύσκολα εφαρμόσιμη σε μεγάλα δίκτυα ή σε περιβάλλοντα με σύνθετες δομές. Επίσης, τα πακέτα λουριών εξαρτώνται από την ακριβή γνώση της τοποθεσίας των κόμβων ομίχλης και του χρόνου αποστολής των πακέτων δεδομένων στο δίκτυο. Σε περιβάλλοντα με δυναμική τοπολογία, όπως στον ομιχλώδη προγραμματισμό, όπου η δομή του δικτύου αλλάζει συχνά, η συγκεκριμένη μέθοδος ασφάλειας μπορεί να μην είναι και τόσο αποτελεσματική. Οι συνεχείς μεταβολές στην θέση των κόμβων δυσκολεύουν την αξιόπιστη παρακολούθηση της πορείας των πακέτων δεδομένων μέσα στο δίκτυο. (Patil and Gaikwad, 2015)

5.3.5.4 Ανίχνευση κακόβουλων κόμβων

Η ανίχνευση κακόβουλων κόμβων (rogue node detection) αναφέρεται στην διαδικασία εντοπισμού και της αναγνώρισης κακόβουλων κόμβων σε περιβάλλοντα, όπως τα IoT περιβάλλοντα ή τα περιβάλλοντα ομίχλης. Οι Patwary κ.α. (2019) προτείνουν μία μέθοδο για την ανίχνευση κακόβουλων κόμβων που στηρίζεται σε ένα στατικό μοντέλο, το HMM (Hidden Markov Model). Η μέθοδος αυτή λαμβάνει υπόψη συγκεκριμένα δεδομένα για την συμπεριφορά των κόμβων, όπως τις πιθανότητες μετάβασης μεταξύ των καταστάσεων και εκπαιδεύει το μοντέλο με βάση αυτά τα δεδομένα, ώστε να εντοπίζει ασυνήθιστες η κακόβουλες ενέργειες. Με αυτή την μέθοδο το σύστημα μπορεί να εντοπίζει άμεσα την παρουσία κακόβουλων κόμβων μέσω ανωμαλιών που παρουσιάζονται στους κόμβους ομίχλης, όπως η ακατάλληλη χρήση πόρων ή ασυνήθιστων συμπεριφορών των κόμβων. (Patwary, Hossain and Sami, 2019)

Η ανίχνευση κακόβουλων κόμβων μέσω του HMM έχει να προσφέρει πολλά πλεονεκτήματα στον ομιχλώδη προγραμματισμό. Αρχικά, ενισχύει την ασφάλεια του δικτύου και την προστασία των δεδομένων, διασφαλίζοντας ότι μόνο οι έγκυροι κόμβοι επεξεργάζονται και μεταδίδουν δεδομένα, αποτρέποντας την κλοπή η την παραποίηση των δεδομένων. Επίσης, η μέθοδος HMM επιτρέπει την άμεση και την ακριβή ανίχνευση κακόβουλων κόμβων με χαμηλή υπολογιστική κατανάλωση, κάτι που καθιστά την τεχνική αποδοτική και κατάλληλη για δυναμικά περιβάλλοντα ομίχλης. Τέλος, η μέθοδος έχει δοκιμαστεί σε προσομοιώσεις σε Matlab, κάτι που ενδεχομένως επιβεβαιώνει την αποτελεσματικότητα της μεθόδου σε πραγματικά περιβάλλοντα ομίχλης. Ωστόσο, δεν είναι σαφές στην εάν η απόδοση της παραμένει εξίσου καλή σε περιβάλλοντα με μεγάλο αριθμό κόμβων, καθώς η μελέτη των Patwary κ.α. (2019) δεν παρέχει συγκεκριμένες πληροφορίες για την αξιολόγησης της σε τέτοιες συνθήκες. (Patwary, Hossain and Sami, 2019)

Παρά την αποτελεσματικότητα που παρουσιάζει η παραπάνω μέθοδος στο σενάριο εφαρμογής που περιγράφουν οι Patwary κ.α. (2019), η διαδικασία ανίχνευσης κακόβουλων κόμβων σε μεγαλύτερα δίκτυα απαιτεί σημαντικούς υπολογιστικούς πόρους. Επίσης, υπάρχει η πιθανότητα να εντοπιστούν κόμβοι ως κακόβουλοι χωρίς να είναι, αυξάνοντας με αυτό τον τρόπο την κατανάλωση των πόρων του συστήματος. Αυτό μπορεί να οδηγήσει στον αδικαιολόγητο αποκλεισμό αυτών των κόμβων από μελλοντική επικοινωνία, κάτι που θα μπορούσε να επηρεάσει τη συνολική λειτουργία του δικτύου. Ακόμα η απόδοση του HMM εξαρτάται από την ποιότητα εκπαίδευσης των δεδομένων, τα οποία πρέπει είναι σωστά και να περιγράφουν την σωστή κατάστασή του δικτύου. Συνεπώς, αν υπάρξουν λάθη στην διαδικασία της εκπαίδευσης του μοντέλου, αυτή θα επηρεάσει και την απόδοση του συστήματος. Τέλος, η συνεχής ανάλυση μεγάλων δεδομένων σε πραγματικό μπορεί να επηρεάσει την ταχύτητα ανίχνευσης και απόκρισης του αντιμέτρου. (Patwary, Hossain and Sami, 2019)

5.3.5.5 Αμφίδρομη επικύρωση ζεύξη

Η αμφίδρομη επικύρωση ζεύξη είναι η διαδικασία κατά την οποία οι κόμβοι ενός δικτύου συνεργάζονται μεταξύ τους σε ένα δίκτυο για να επικυρώσουν την ακεραιότητα και την νομιμότητα

της επικοινωνίας μεταξύ τους, διασφαλίζοντας με αυτό τον τρόπο ότι οι κόμβοι δεν έχουν παραβιαστεί ή δεν είναι κακόβουλοι (Κρητικός, 2023). Η παραπάνω διαδικασία είναι κρίσιμη για τα ασύρματα δίκτυα, όπως τα κινητά ασύρματα δίκτυα αισθητήρων (Mobile Wireless Sensor Networks - MWSNs) για την αποτροπή επιθέσεων, όπως η επιλεκτική προώθηση (selective forwarding attack) όπου οι κακόβουλοι κόμβοι επιλέγουν να προωθούν ή να απορρίπτουν επιλεκτικά πακέτα δεδομένων, επηρεάζοντας την ροή της επικοινωνίας. Στο πλαίσιο της αμφίδρομης επικύρωσης ζεύξης, οι watchdog κόμβοι λειτουργούν ως παρατηρητές που εντοπίζουν αν οι κόμβοι συμπεριφέρονται σωστά. Η χρήση αυτών των κόμβων βοήθα στην ενίσχυση της διαδικασίας επικύρωσης, διασφαλίζοντας ότι και οι δύο πλευρές της ζεύξης λειτουργούν σωστά και σύμφωνα με τους προκαθορισμένους κανόνες. Οι watchdog κόμβοι παρακολουθούν την επικοινωνία και μπορούν να επισημάνουν κακόβουλους κόμβους που δεν προωθούν σωστά τα πακέτα, παρακολουθώντας την αναμενόμενη ροή των δεδομένων και ανιχνεύοντας αποκλίσεις από αυτήν, όπως καθυστερήσεις, απώλειες πακέτων ή αλλαγές στη διαδρομή, ενισχύοντας έτσι την ασφάλεια του δικτύου. (Yaseen *et al.*, 2016).

Η αμφίδρομη επικύρωση ζεύξη στον ομιχλώδη προγραμματισμό προσφέρει πολλά πλεονεκτήματα. Βασικό πλεονέκτημα είναι η ασφάλεια στις επικοινωνίες, καθώς επιτρέπει στους κόμβους να επαληθεύουν την αξιοπιστία της σύνδεσης τους. Με αυτό τον τρόπο μειώνονται οι επιθέσεις που στοχεύουν στην υποκλοπή ή την αλλοίωση των δεδομένων. Επίσης, βοηθά στην αναγνώριση των επιθέσεων, όπως η επιλεκτική προώθηση, επιτρέποντας στους κόμβους να ανιχνεύουν κακόβουλες συμπεριφορές και να αντιδρούν κατάλληλα. Ακόμα, η διαδικασία είναι αυτόνομη και αποδοτική, καθώς δεν απαιτεί κεντρική υποδομή και αυξάνει την συνολική αξιοπιστία του δικτύου. (Yaseen *et al.*, 2016)

Ωστόσο, η εφαρμογή της αμφίδρομη επικύρωση ζεύξης παρουσιάζει στον ομιχλώδη προγραμματισμό ορισμένα μειονεκτήματα. Αρχικά, υπάρχει αυξημένη καθυστέρηση λόγω της επιπλέον ανταλλαγής μηνυμάτων μεταξύ των κόμβων, η οποία μπορεί να επηρεάσει αρνητικά τις εφαρμογές πραγματικού χρόνου όπου η ταχύτητα απόκρισης είναι σημαντική. Επίσης, η συνεχής επικύρωση προσθέτει φόρτο στο δίκτυο, γεγονός που ενδέχεται να μειώσει την συνολική αποδοτικότητα του συστήματος του ομιχλώδους προγραμματισμού, ενώ παράλληλα αυξάνει τις απαιτήσεις σε υπολογιστικούς πόρους. Ακόμα, η διαχείριση των κινητών κόμβων καθίσταται πιο δύσκολη, καθώς απαιτεί συχνή ανανέωση των επικυρώσεων, κάτι που επιβαρύνει το δίκτυο. Παρά την ενίσχυση της ασφάλειας, η αμφίδρομη επικύρωση ζεύξης δεν είναι αδιάβλητη, καθώς υπάρχει ο κίνδυνος των κακόβουλων κόμβων να παρακάμψουν την διαδικασία ή να μιμηθούν την διαδικασία επικύρωσης, δημιουργώντας έτσι κενά ασφάλειας. (Yaseen *et al.*, 2016)

5.3.5.6 Σύγκριση αντιμέτρων για τις επιθέσεις που αφορούν τις ασύρματες επικοινωνίες στον ομιχλώδη προγραμματισμό

Η επιλογή του κατάλληλου αντιμέτρου για την ασφάλεια των ασύρματων δικτύων αποτελεί κρίσιμη απόφαση, καθώς επηρεάζει άμεσα την προστασία των δεδομένων και των συστημάτων μιας επιχείρησης. Παρακάτω ακολουθεί μια συγκριτική ανάλυση των αντίμετρων για τις επιθέσεις που

αφορούν τις ασύρματες επικοινωνίες με βάση τα κριτήρια που αναλύθηκαν στην ενότητα 5.2. Παρακάτω ακολουθεί ο πίνακας σύγκρισης των αντιμέτρων για την ασφάλεια των ασύρματων δικτύων που αναλύθηκαν στις ενότητες 5.3.5.1-5.3.5.5 της παρούσας διπλωματικής εργασίας, καθώς και η ανάλυση των αποτελεσμάτων του πίνακα αυτού.

Ανάλυση τιμών των Κριτηρίων Αξιολόγησης

Κατανάλωση Πόρων

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 2, διότι απαιτείται σημαντική υπολογιστική ισχύ και κατανάλωση πόρων για την συλλογή, την αποθήκευση και την ανάλυση δεδομένων, ιδιαίτερα σε μεγάλα δίκτυα, καθώς και για την ανίχνευση ανωμαλιών. Αυτό μπορεί να επηρεάσει την απόδοση του δικτύου αρνητικά, καθώς η φόρτωση των πόρων του συστήματος μπορεί να μειώσει την ταχύτητα και την απόδοση της επικοινωνίας, καθιστώντας τη χρήση αυτής μεθόδου λιγότερο αποδοτική σε περιβάλλοντα ομίχλης, όπου οι πόροι είναι κατανεμημένοι και η καθυστέρηση πρέπει να είναι ελάχιστη.
- Η τεχνική MLTKNN αξιολογείται με 2, διότι απαιτεί πολλούς πόρους για την εκπαίδευση των μοντέλων, ενώ το παραγόμενο μοντέλο απαιτεί λιγότερους πόρους για την εφαρμογή. Η εφαρμογή του παραγόμενου μοντέλου μπορεί να επηρεάσει την απόδοση του δικτύου, καθώς η διαδικασία εφαρμογής του μπορεί να προκαλέσει καθυστερήσεις ή υπερφόρτωση των πόρων σε περιβάλλοντα με περιορισμένους πόρους.
- Τα πακέτα λουριών αξιολογούνται με 2, διότι απαιτούν πόρους για τον υπολογισμό αποστάσεων και την επαλήθευση χρονικών σφραγίδων, κάτι που μπορεί να επηρεάσει την απόδοση του δικτύου σε περιβάλλοντα ομίχλης, προκαλώντας καθυστερήσεις ή υπερφόρτωση στους κατανεμημένους πόρους και μειώνοντας την αποδοτικότητα της επικοινωνίας μεταξύ των συσκευών.
- Η μέθοδος ανίχνευσης κόμβων με HMM αξιολογείται με 3, διότι φαίνεται να έχει χαμηλή κατανάλωση πόρων σε μικρά δίκτυα, αλλά σε μεγαλύτερα περιβάλλοντα απαιτεί σημαντικούς υπολογιστικούς πόρους, γεγονός που μπορεί να επηρεάσει την απόδοση του δικτύου, προκαλώντας καθυστερήσεις ή υπερφόρτωση στους πόρους του συστήματος.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 2, διότι απαιτεί υπολογιστικούς πόρους και δημιουργεί επιπλέον φόρτο στο δίκτυο, λόγω της ανταλλαγής μηνυμάτων και της συνεχούς επικύρωσης, κάτι που μπορεί να επηρεάσει την απόδοση του δικτύου, ιδιαίτερα σε μεγάλα δίκτυα, όπου η φόρτωση των πόρων μπορεί να προκαλέσει καθυστερήσεις ή μειωμένη αποδοτικότητα.

Κλιμακωσιμότητα

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 3, διότι μπορεί να κλιμακωθεί αλλά η απόδοση της μπορεί να μειωθεί καθώς αυξάνονται οι κόμβοι, οπότε απαιτούνται προσαρμογές για να διατηρηθεί η αποτελεσματικότητα της.

- Η τεχνική MLTKNN αξιολογείται με 3, διότι η αποδοτικότητα του αλγορίθμου μηχανικής μάθησης KNN μπορεί να επηρεαστεί από την αύξηση του μεγέθους του δικτύου και του όγκου των δεδομένων.
- Τα πακέτα λουριών αξιολογούνται με 1, διότι δυσκολεύονται να παρακολουθήσουν την συνεχώς μεταβαλλόμενη τοπολογία του δικτύου.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 3, διότι όταν ο φόρτος εργασίας αυξάνεται σε μεγαλύτερα δίκτυα, η απόδοση της μεθόδου μειώνεται, ωστόσο αυτή η μείωση μπορεί να ελεγχθεί, ώστε η μέθοδος να συνεχίσει να λειτουργεί αποτελεσματικά παρά την ανάγκη για συνεχόμενη ανάλυση μεγάλων όγκων δεδομένων.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 3, διότι μπορεί να υποστηρίξει τον αυξημένο φόρτο εργασίας, όμως η διαδικασία της επικύρωσης προσθέτει καθυστερήσεις, που μπορεί να επηρεάσουν τα ήδη επιβαρυμένα δίκτυα.

Ασφάλεια δεδομένων

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 2, διότι εστιάζει σε ένα μόνο είδος επίθεσης και μπορεί να επηρεαστεί από ορισμένες παραλλαγές αυτής της επίθεσης, ενώ παραμένει ο κίνδυνος των ψευδώς θετικών αποτελεσμάτων.
- Η τεχνική MLTKNN αξιολογείται με 3, διότι η τεχνική εντοπίζει με ακρίβεια τις επιθέσεις κατάταξης και βοηθά στην ενίσχυση της ασφάλειας του δικτύου. Ωστόσο, δεν παρέχει επαρκή προστασία από εξωτερικές επιθέσεις, γεγονός που μειώνει την πλήρη κάλυψη της ασφάλειας του δικτύου.
- Τα πακέτα λουριών αξιολογούνται με 3, διότι είναι πολύ αποτελεσματικά στην ανίχνευση και την αποτροπή των επιθέσεων σκουληκότρυπας μέσω των γεωγραφικών και των χρονικών περιορισμών. Ωστόσο, η προστασία περιορίζεται σε αυτό το είδος επίθεσης.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 5, διότι ενισχύει την ασφάλεια του δικτύου μέσω της ακριβής ανίχνευσης των κακόβουλων κόμβων, αποτρέποντας διάφορες κακόβουλες ενέργειες, όπως είναι η κλοπή των δεδομένων.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 4, διότι ενισχύει την ασφάλεια των δεδομένων μέσω της επαλήθευσης, αλλά δεν είναι αδιάβλητη και υπάρχει ο κίνδυνος κακόβουλοι κόμβοι να βρουν τρόπο να παρακάμψουν την διαδικασία της επαλήθευσης.

Ευκολία Χρήσης

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 3, διότι οι παράμετροι για την ανίχνευση ανωμαλιών, όπως η καθυστέρηση end-to-end, το ποσοστό παράδοσης και τα μηνύματα DIO, είναι σε μεγάλο βαθμό προκαθορισμένες και αναγνωρισμένες ως κρίσιμες, μειώνοντας τον φόρτο εργασίας για την επιλογή τους. Αν και η διαδικασία υπολογισμού των ορίων δεν είναι πλήρως τεκμηριωμένη, η παρακολούθηση των παραμέτρων παρέχει επαρκή στοιχεία για την ανίχνευση ανωμαλιών.
- Η τεχνική MLTKNN αξιολογείται με 3, διότι απαιτεί εξειδικευμένες γνώσεις μηχανικής μάθησης για την προετοιμασία των δεδομένων και την ερμηνεία των αποτελεσμάτων.

- Τα πακέτα λουριών αξιολογούνται με 3, διότι είναι σχετικά απλά στην υλοποίηση τους, αλλά απαιτείται προσεκτική διαμόρφωση των παραμέτρων έτσι ώστε να επιτευχθεί η επιθυμητή ισορροπία μεταξύ της ασφάλειας και της απόδοσης, καθώς και κατάλληλος χρονικός συγχρονισμός (των κόμβων του ασύρματου δικτύου) που είναι σχετικά απλός, γεγονός που μειώνει την συνολική πολυπλοκότητα.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 2, διότι απαιτεί τεχνικές γνώσεις για την εφαρμογή της μεθόδου, η διαδικασία της ανίχνευσης είναι απαιτητική και η ερμηνεία των αποτελεσμάτων δεν είναι πάντα άμεση ή εύκολη, ειδικά εφόσον πρόκειται για εφαρμογή μιας συγκεκριμένης μεθόδου HMM. Επίσης, η ποιότητα των δεδομένων πρέπει να εξασφαλιστεί για να είναι σωστή, γεγονός που απαιτεί εξειδίκευση στην επεξεργασία τους πριν αυτά χρησιμοποιηθούν για την εκπαίδευση του μοντέλου.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 4, διότι αν και η διαδικασία είναι αυτοματοποιημένη, η διαχείριση των κινητών κόμβων καθίσταται δύσκολη λόγω της ανάγκης για συχνή ανανέωση των επικυρώσεων. Αυτό προσθέτει μια επιπλέον πολυπλοκότητα στη διαδικασία.

Εκπαίδευση χρηστών

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 2, διότι είναι απαραίτητη η εκπαίδευση των χρηστών για την κατανόηση των μεθόδων ασφάλειας, η οποία μπορεί να είναι μακροχρόνια και συνεχής, προκειμένου να επιτευχθεί η σωστή παρακολούθηση και η ανάλυση των επιθέσεων.
- Η τεχνική MLTKNN αξιολογείται με 2, διότι οι χρήστες πρέπει να εκπαιδευτούν στη σωστή εφαρμογή των αλγορίθμων μηχανικής μάθησης, αλλά και στο να μπορούν να ερμηνεύουν τα αποτελέσματα σωστά. Η εκπαίδευση αυτή απαιτεί να είναι μακροχρόνια και συνεχής για να εξασφαλιστεί η σωστή κατανόηση και η εφαρμογή της μεθόδου.
- Τα πακέτα λουριών αξιολογούνται με 3, διότι χρειάζεται βασική εκπαίδευση για την κατανόηση του τρόπου συγχρονισμού των ρολογιών που εφαρμόζονται στα δεδομένα, αλλά δεν είναι τόσο δύσκολη η κατανόηση του τρόπου αυτού, εφόσον υπάρχει μια βασική τεχνική κατάρτιση.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 2, διότι οι χρήστες πρέπει να εκπαιδευτούν στις βασικές αρχές του HMM όσο και στην σωστή εφαρμογή του μοντέλου, καθώς και στην επεξεργασία των δεδομένων, προκειμένου να κατανοήσουν το μοντέλο HMM και να ερμηνεύσουν σωστά τα αποτελέσματα που αυτό επιφέρει.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 3, διότι οι χρήστες απαιτείται να έχουν έναν μέτριο βαθμό γνώσεων και κάποια εξοικείωση με τις διαδικασίες επαλήθευσης και την λειτουργία των watchdog κόμβων, χωρίς αυτή να είναι υπερβολικά απαιτητική.

Αντίκτυπος στον χρήστη

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 3, καθώς οι χρήστες ενδέχεται να συναντήσουν κάποιες καθυστερήσεις, εξαιτίας των απαιτήσεων σε επεξεργαστική ισχύ και εύρους ζώνης, χωρίς να μειώνεται δραστικά η εμπειρία τους.

- Η τεχνική MLTKNN αξιολογείται με 4, διότι βελτιώνει την απόδοση του δικτύου, μειώνοντας τις καθυστερήσεις στην παράδοση των δεδομένων και βελτιώνοντας την εμπειρία του χρήστη. Ωστόσο, είναι σημαντικό να σημειώσουμε ότι ενδέχεται να υπάρχει κάποιο είδος ενόχλησης για τον διαχειριστή ή τον προγραμματιστή, λόγω της πιθανής πολυπλοκότητας της μεθόδου, κάτι που μπορεί να μειώσει κάπως την απόλυτα θετική επίδραση της τεχνικής. Οι ενοχλήσεις αυτές μπορεί να περιλαμβάνουν αυξημένη ανάγκη για παραμετροποίηση, δυσκολίες στην ενσωμάτωση στο υπάρχον σύστημα, καθυστερήσεις στην επεξεργασία ή απόδοση του συστήματος λόγω αυξημένων υπολογιστικών απαιτήσεων, καθώς και επιπλέον κόστος συντήρησης και αντιμετώπισης προβλημάτων. Παρ' όλα αυτά, η πολυπλοκότητα αυτή δεν φαίνεται να επηρεάζει τον τελικό χρήστη
- Τα πακέτα λουριών αξιολογούνται με 3, διότι η προσθήκη γεωγραφικών και χρονικών ελέγχων εξαρτώνται από το μέγεθος των πακέτων, το αν κρυπτογραφείται το περιεχόμενο τους και αν τα επιπλέον δεδομένα συμπιέζονται. Όμως, όλα αυτά μπορεί να έχουν αρνητικό αντίκτυπο στον διαχειριστή του συστήματος, καθώς προσθέτουν επιπλέον φόρτο εργασίας. Η ανάγκη για παραμετροποίηση των ελέγχων και για τη διαχείριση της κρυπτογράφησης και της συμπίεσης μπορεί να αυξήσει την πολυπλοκότητα και να απαιτεί περισσότερους πόρους, με αποτέλεσμα να επιβαρύνεται ο διαχειριστής. Παράλληλα, αυτά τα επιπλέον μέτρα ενδέχεται να επηρεάσουν την αποδοτικότητα του συστήματος και να οδηγήσουν σε καθυστερήσεις, μειώνοντας την απόδοση του δικτύου.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 3, διότι η ανίχνευση κακόβουλων κόμβων μπορεί να προκαλέσει καθυστερήσεις στην απόκριση του συστήματος σε περιβάλλοντα με υψηλό φόρτο εργασίας, επηρεάζοντας την συνολική εμπειρία του χρήστη.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 3, διότι η καθυστέρηση που προκύπτει μπορεί να επηρεάσει την απόκριση σε εφαρμογές πραγματικού χρόνου, δημιουργώντας έτσι αρνητικό αντίκτυπο στον χρήστη.

Εφαρμοσιμότητα

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 3, διότι η εφαρμογή της στα υπάρχοντα περιβάλλοντα ομίχλης μπορεί να παρουσιάσει μέτριες δυσκολίες λόγω των επιπρόσθετων πόρων που απαιτεί. Αυτές οι δυσκολίες επηρεάζουν την απόδοση της μεθόδου, αλλά δεν είναι υπερβολικά απαιτητικές.
- Η τεχνική MLTKNN αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε υπάρχοντα περιβάλλοντα ομίχλης, αλλά ενδέχεται να απαιτεί πρόσθετους πόρους ή προσαρμογές για να λειτουργήσει βέλτιστα στα υπάρχοντα περιβάλλοντα.
- Τα πακέτα λουριών αξιολογούνται με 2, διότι η εφαρμογή τους στα υπάρχοντα περιβάλλοντα ομίχλης είναι δύσκολή λόγω των απαιτήσεων σε συγχρονισμό και των γεωγραφικών δεδομένων, ειδικά σε δυναμικές τοπολογίες που αλλάζουν συνεχώς.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 3, διότι η εφαρμογή στα υπάρχοντα ομιχλώδη μπορεί να αντιμετωπίσει μέτριες δυσκολίες, καθώς μπορεί να χρειάζεται επιπρόσθετους πόρους και υποδομή. Αυτές οι δυσκολίες επηρεάζουν την απόδοση της μεθόδου, αλλά δεν είναι υπερβολικά απαιτητικές.

- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 3, διότι η ενσωμάτωση της είναι εφικτή σε περιβάλλοντα ομίχλης, αλλά απαιτεί επιπλέον πόρους και διαχείριση, γεγονός που μπορεί να δυσκολέψει την εφαρμογή σε κάποια συστήματα.

Βαθμός κάλυψης

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 4, διότι μπορεί να προσαρμοστεί σε πολλά περιβάλλοντα και σενάρια παρέχοντας αποτελεσματική ανίχνευση επιθέσεων, ανεξάρτητα από την διαμόρφωση του δικτύου ή τις συνθήκες περιβάλλοντος.
- Η τεχνική MLTKNN αξιολογείται με 4, διότι εφαρμόζεται κυρίως σε IoT, ασύρματα δίκτυα και ομιχλώδη περιβάλλοντα.
- Τα πακέτα λουριών αξιολογούνται με 2, διότι αυτό το αντίμετρο μπορεί να εφαρμοστεί σε συγκεκριμένα σενάρια και δίκτυα, αλλά δεν είναι κατάλληλο για όλα τα περιβάλλοντα, ειδικά σε μεγάλα και δυναμικά δίκτυα με πολλές μεταβολές.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 3, διότι είναι αποτελεσματική σε συγκεκριμένα σενάρια, αλλά μπορεί να μην είναι τόσο αποτελεσματική σε περιβάλλοντα με δυναμικές ή πολύ μεγάλες τοπολογίες, όπου οι ανάγκες σε υπολογιστικούς πόρους είναι αυξημένες.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε αρκετά περιβάλλοντα ομίχλης, αλλά ίσως το αντίμετρο αυτό δεν είναι ιδανικό για όλα τα είδη δικτύων ή εφαρμογών, καθώς σε δίκτυα με περιορισμένους πόρους ή απαιτήσεις σε πραγματικό χρόνο, η πολυπλοκότητα της επικύρωσης μπορεί να προκαλέσει καθυστερήσεις ή να απαιτήσει υπερβολικούς πόρους.

Επεκτασιμότητα

- Η μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών αξιολογείται με 3, διότι υπάρχει η δυνατότητα ενοποίησης νέων λειτουργιών, όπως η μετρικές για παρακολούθηση αλλά η πολυπλοκότητα της υλοποίησης της μεθόδου μπορεί να κάνει την επέκταση της χρονοβόρα.
- Η τεχνική MLTKNN αξιολογείται με 3, διότι αν και έχει την δυνατότητα επέκτασης ως προς νέα δεδομένα που λαμβάνονται υπόψη για την ταξινόμηση, η επέκτασή της περιορίζεται σε μεγαλύτερα δίκτυα, εξαιτίας της πολύπλοκης φύσης της.
- Τα πακέτα λουριών αξιολογούνται με 4, διότι η προσθήκη νέων λειτουργιών είναι εφικτή και δεν απαιτείται σημαντική αναδιάρθρωση του υπάρχοντος συστήματος.
- Η μέθοδος ανίχνευσης κακόβουλων κόμβων με HMM αξιολογείται με 4, διότι επιτρέπει την προσθήκη νέων λειτουργιών και χαρακτηριστικών χωρίς να χρειάζεται σημαντική αναδιάρθρωση στα υπάρχοντα περιβάλλοντα.
- Η αμφίδρομη επικύρωση ζεύξης αξιολογείται με 3, διότι υπάρχει η δυνατότητα επέκτασης με νέες λειτουργίες, άλλα η συνεχής επικύρωση μπορεί να περιορίσει την επέκταση σε πιο πολύπλοκα σενάρια.

Πίνακας 6 - Πίνακας σύγκρισης των αντιμέτρων για την ασφάλεια των ασύρματων δικτύων

Αντίμετρα	**Κατανάλωση Πόρων**	**Κλιμακωσιμότητα**	**Ασφάλεια δεδομένων**	**Ευκολία Χρήσης**	**Εκπαίδευση χρηστών**	**Αντίκτυπος στον χρήστη**	**Εφαρμοσιμότητα**	**Βαθμός κάλυψης**	**Επεκτασιμότητα**
Παρακολούθηση Ευαίσθητων παραμέτρων ενός δικτύων για την Ανίχνευση ανωμαλιών	2	3	2	3	2	3	3	4	3
Τεχνική MLTKNN	2	3	3	3	2	4	3	4	3
Πακέτα λουριών	2	1	3	3	3	3	2	2	4
Ανίχνευση κακόβουλων κόμβων με HMM	3	3	5	2	3	3	3	3	4
Αμφίδρομη επικύρωση ζεύξη	2	3	4	4	3	3	3	4	3

Σε πολλές περιπτώσεις, η υιοθέτηση ενός συνδυασμού αντιμέτρων μπορεί να προσφέρει ένα πιο ολοκληρωμένο επίπεδο ασφάλειας, εκμεταλλεύοντας τα πλεονεκτήματα κάθε μεμονωμένης λύσης και μειώνοντας τους κινδύνους που υπάρχουν σε κάθε μία λύση ξεχωριστά. Η μέθοδος της παρακολούθησης ευαίσθητων δικτύων για ανίχνευση ανωμαλιών και η τεχνική MLTKNN θεωρούνται ανταγωνιστικά αντίμετρα, καθώς επιδιώκουν παρομοίους στόχους (την ανίχνευση

ανωμαλιών), το καθένα από αυτά εστιάζει σε διαφορετικές μεθόδους ανίχνευσης. Όμως η μέθοδος της παρακολούθησης ευαίσθητων δικτύων για ανίχνευση ανωμαλιών ή η τεχνική MLTKNN σε συνδυασμό με τα πακέτα λουριών θεωρούνται συμπληρωματικά, καθώς τα πακέτα λουριών περιορίζουν την πρόσβαση και ενισχύουν την ασφάλεια, προσθέτοντας ένα επιπλέον επίπεδο προστασίας πέρα από την ανίχνευση απειλών.

Με βάση τον παραπάνω πίνακα έχουμε μπορούμε να προχωρήσουμε σε ανάλυση των καλύτερων και των χειρότερων αντιμέτρων για κάθε κριτήριο:

Ανάλυση καλύτερου και χειρότερου αντιμέτρου ανά κριτήριο: Θα εντοπίσουμε ποιο/-α αντίμετρο/-α έχει την καλύτερη και την χειρότερη απόδοση σε κάθε κριτήριο αξιολόγησης:

- Κατανάλωση πόρων:
  - Καλύτερο: HMM (3)
  - Χειρότερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, τεχνική MLTKNN, πακέτα λουριών, αμφίδρομη επικύρωση ζεύξης (2)
- Κλιμακωσιμότητα:
  - Καλύτερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, τεχνική MLTKNN, HMM, αμφίδρομη επικύρωση ζεύξης (3)
  - Χειρότερο: πακέτα λουριών (2)
- Ασφάλεια δεδομένων:
  - Καλύτερο: HMM (4)
  - Χειρότερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών (2)
- Ευκολία χρήσης:
  - Καλύτερο: αμφίδρομη επικύρωση ζεύξης (4)
  - Χειρότερο: HMM (2)
- Εκπαίδευση χρηστών:
  - Καλύτερο: αμφίδρομη επικύρωση ζεύξης, πακέτα λουριών (3)
  - Χειρότερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, τεχνική MLTKNN, HMM (2)
- Αντίκτυπος στον χρήστη:
  - Καλύτερο: τεχνική MLTKNN (4)
  - Χειρότερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, HMM, πακέτα λουριών ,αμφίδρομη επικύρωση ζεύξης (3)
- Εφαρμοσιμότητα:
  - Καλύτερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, τεχνική MLTKNN, HMM, αμφίδρομη επικύρωση ζεύξης (3)
  - Χειρότερο: πακέτα λουριών (2)
- Βαθμός κάλυψης:
  - Καλύτερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, τεχνική MLTKNN, αμφίδρομη επικύρωση ζεύξης (4)
  - Χειρότερο: πακέτα λουριών (2)

- Επεκτασιμότητα:
  - Καλύτερο: πακέτα λουριών, HMM (4)
  - Χειρότερο: Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών, τεχνική MLTKNN, αμφίδρομη επικύρωση ζεύξης (3)

Καλύτερο και χειρότερο αντίμετρο συνολικά (στην κατηγόρια): Μέθοδος παρακολούθησης ευαίσθητων παραμέτρων ενός δικτύου για την ανίχνευση ανωμαλιών: 25, τεχνική MLTKNN: 27, πακέτα λουριών: 23, ανίχνευση κακόβουλων κόμβων HMM: 28, αμφίδρομη επικύρωση ζεύξης: 29. Επομένως, η αμφίδρομη επικύρωση ζεύξης με συνολική βαθμολογία 29 είναι το καλύτερο αντίμετρο συνολικά, ενώ το χειρότερο αντίμετρο συνολικά είναι τα πακέτα λουριών με συνολική βαθμολογία 23.

Αντίμετρο με καλύτερη και χειρότερη απόδοση: Για την καλύτερη και χειρότερη απόδοση, πρέπει να εξετάσουμε την απόδοση των αντιμέτρων σε κάθε κριτήριο και να καταλήξουμε στο καλύτερο και το χειρότερο αντίμετρο βασιζόμενοι στο ποσοστό των υψηλών ή των χειρότερων βαθμολογίων τους που έχουν λάβει στα κριτήρια.

Ποσοστά υψηλών και χαμηλών βαθμολογιών:

- Παρακολούθηση Ευαίσθητων παραμέτρων ενός δικτύου για την Ανίχνευση ανωμαλιών:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 3/9 = 33,3 %
- Τεχνική MLTKNN:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 2/9 = 22,2 %
- Πακέτα λουριών:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 4/9 = 44,4 %
- Ανίχνευση κακόβουλων κόμβων HMM:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 1/9 = 11,1 %
- Αμφίδρομη επικύρωση ζεύξη:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 1/9 = 11,1 %

Το αντίμετρο με την καλύτερη απόδοση βάσει του ποσοστού των υψηλών βαθμολογίων είναι η ανίχνευση επικυρώσιμη ζεύξη με ποσοστό 33,3 %. Το αντίμετρο με την χειρότερη απόδοση βάσει του μεγαλύτερού ποσοστού χαμηλών βαθμολογίων είναι τα πακέτα λουριών με ποσοστό 44,4 %.

5.3.6 Αντίμετρα για την αντιμετώπιση των επιθέσεων ασφάλειας των δεδομένων στον ομιχλώδη προγραμματισμό

Η αυξημένη κατανάλωση των δεδομένων και η ανάγκη για μεγαλύτερες ταχύτητες του δικτύου έχουν οδηγήσει στην ανάπτυξη νέων τεχνολογιών, όπως είναι ο ομιχλώδης προγραμματισμός. Αν και ο ομιχλώδης προγραμματισμός επεκτείνει τις δυνατότητες του υπολογιστικού νέφους στα περιφερειακά δίκτυα που βρίσκονται στην «άκρη» του δικτύου, έχουν δημιουργηθεί νέα ζητήματα ασφάλειας σχετικά με την ιδιωτικότητα τοποθεσίας, χρήσης ή ταυτότητας και των προσωπικών δεδομένων, απαιτώντας έτσι πιο προηγμένες και ασφαλείς μεθόδους για την προστασία των δεδομένων τοποθεσίας / ταυτότητας (Naik *et al.*, 2019). Με την δημιουργία του ομιχλώδους προγραμματισμού γεννήθηκαν καινούργιες προκλήσεις στον τομέα της ασφάλειας των δεδομένων. Για αυτό τον λόγο έχουν αναπτυχθεί διαφορές στρατηγικές και τεχνικές για την αντιμετώπιση των ζητημάτων ασφάλειας των δεδομένων, όπως είναι η επιβολή πολιτικών (policy enforcement), η ομομορφική κρυπτογράφηση (encryption), η απόκρυψη δεδομένων (data obfuscation), τα honeypots και η ασφαλής διαχείριση κλειδιών (Secure Key Management) (Khan, Parkinson and Qin, 2017). Μερικές από αυτές θα αναλυθούν στις παρακάτω υποενότητες.

5.3.6.1 Ομομορφική κρυπτογράφηση

Η ομομορφική κρυπτογράφηση (homomorphic encryption) αποτελεί μια προηγμένη κρυπτογραφική τεχνική που επιτρέπει την εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα. Με τον τρόπο αυτό, η αίτηση επεξεργασίας δεδομένων περιλαμβάνει κρυπτογραφημένα δεδομένα που παραμένουν αθέατα στους ενδιάμεσους φορείς (servers), οι οποίοι λειτουργούν αποκλειστικά ως πάροχοι υπηρεσιών (επεξεργασία δεδομένων) και όχι ως χρήστες ή αποδέκτες των δεδομένων (Murugesan *et al.*, 2021). Επομένως, αυτός ο τύπος κρυπτογράφησης επιτρέπει την ασφαλή επεξεργασία και των δεδομένων σε εξωτερικές υπηρεσίες, διασφαλίζοντας την ιδιωτικότητα των δεδομένων (Κρητικός, 2023).

Η ομομορφική κρυπτογράφηση προσφέρει μια σειρά από σημαντικά πλεονεκτήματα στον τομέα της ασφάλειας των δεδομένων, ιδιαίτερα σε περιβάλλοντα ομίχλης. Επιτρέπει την εκτέλεση υπολογισμών απευθείας σε κρυπτογραφικά δεδομένα χωρίς να απαιτείται η αποκρυπτογράφησή τους, προσφέροντας αυξημένη ταχύτητα επεξεργασίας και μειωμένο συνολικό χρόνο απόκρισης, καθώς τα δεδομένα παραμένουν σε κρυπτογραφημένη μορφή κατά την διάρκεια και μετά την επεξεργασία, εξαλείφοντας την ανάγκη για αποκρυπτογράφηση και επανακρυπτογράφηση, όπως συμβαίνει στις παραδοσιακές προσεγγίσεις (Sendhil and Amuthan, 2020). Παράλληλα, η ομομορφική κρυπτογράφηση, σε συνδυασμό με τον αλγόριθμο της ελλειπτικής καμπύλης (ECC) για συμπληρωματικούς σκοπούς, όπως είναι η ασφαλής ανταλλαγή κλειδιών, ενισχύει την ασφάλεια των δεδομένων, μειώνει τον κίνδυνο των παραβιάσεων και προσφέρει αντοχή σε επιθέσεις τύπου επιλεγμένου απλού κειμένου (chosen-plaintext), όπου ένας επιτιθέμενος προσπαθεί να παραβιάσει το σύστημα με την εισαγωγή συγκεκριμένων δεδομένων και την παρατήρηση του αποτελέσματος. Επιπλέον, η ομομορφική κρυπτογράφηση σε συνδυασμό με τον ECC είναι ταχύτερη στην κρυπτογράφηση σε σύγκριση με τις παραδοσιακές μεθόδους κρυπτογράφησης, όπως την RSA, προσφέροντας με αυτό τον τρόπο υψηλή απόδοση σε περιβάλλοντα με συσκευές με περιορισμένους πόρους, όπως οι IoT συσκευές στα ομιχλώδη περιβάλλοντα, όπου η ταχύτητα είναι ένας κρίσιμος παράγοντας σε τέτοιες περιπτώσεις. Τέλος, η ομομορφική κρυπτογράφηση σε

συνδυασμό με τον ECC επιτρέπει την χρήση μικρότερων κλειδιών για το ίδιο επίπεδο ασφάλειας σε σχέση με άλλους αλγόριθμους, όπως την RSA. Αυτό μειώνει τις ανάγκες σε αποθήκευση και υπολογιστική ισχύ, καθιστώντας την ομομορφική κρυπτογράφηση πιο ελκυστική για συσκευές με περιορισμένους πόρους (Murugesan *et al.*, 2021).

Παρά το γεγονός ότι η πλήρως ομομορφική κρυπτογράφηση προσφέρει υψηλό επίπεδο ασφάλειας επιτρέποντας υπολογισμούς σε κρυπτογραφημένα δεδομένα, αντιμετωπίζει σημαντικές προκλήσεις στην υλοποίηση της. Παρά την υψηλή απόδοση που προσφέρει η εφαρμογή του ECC στην ομομορφική κρυπτογράφηση, ο χρόνος κρυπτογράφησης και αποκρυπτογράφησης είναι μεγαλύτερος για αυξημένα επίπεδα ασφάλειας (π.χ. 256 bits), όπως φαίνεται και από τα πειραματικά αποτελέσματα της έρευνας των Mutugesan κ.α. (2021). Αυτή η αύξηση του χρόνου μπορεί να αποτελέσει εμπόδιο σε εφαρμογές όπου η ταχύτητα είναι κρίσιμη. Ωστόσο, για ομιχλώδη περιβάλλοντα, η χρήση των 128 bits θεωρείται η ιδανικότερη τιμή που πρέπει να έχει ο ECC επιτυγχάνοντας εξισορρόπηση της ασφάλειας με την αποδοτικότητα. Επιπλέον, η ομομορφική κρυπτογράφηση απαιτεί σημαντική υπολογιστική ισχύ, ακόμη και παρά την μείωση του μεγέθους των κλειδιών που επιτυγχάνεται μέσω της ECC, ειδικά σε εφαρμογές που απαιτούν πραγματικό χρόνο επεξεργασίας, κάτι που μπορεί να μην είναι εφικτό σε όλα τα IoT περιβάλλοντα, ειδικά όταν πρόκειται για συσκευές με περιορισμένους πόρους. Τέλος, η ομομορφική κρυπτογράφηση μπορεί να υποστηρίξει μόνο συγκεκριμένα είδη επεξεργασίας των κρυπτογραφημένων δεδομένων και όχι όλα. Αυτό περιορίζει σημαντικά την εφαρμογή της. (Murugesan *et al.*, 2021)

5.3.6.2 Απόκρυψη δεδομένων

Η απόκρυψη δεδομένων (data obfuscation) είναι η διαδικασία αντικατάστασης ευαίσθητων πληροφοριών με δεδομένα που διαθέτουν ρεαλιστική μορφή, αλλά είναι πρακτικά μη αξιοποιήσιμα από μη εξουσιοδοτημένους χρήστες. Ο πρωταρχικός στόχος της απόκρυψης δεδομένων είναι η διασφάλιση της εμπιστευτικότητας των πραγματικών δεδομένων, διατηρώντας παράλληλα την λειτουργικότητα τους για περιπτώσεις, όπως είναι η ανάπτυξη και η δοκιμή λογισμικού (Imperva, 2024).

Υπάρχουν τρεις κύριες τεχνικές απόκρυψης δεδομένων (Imperva, 2024):

- **Κάλυψη δεδομένων (Data Masking):** Πρόκειται για μια διαδικασία δημιουργίας τροποποιημένων εκδόσεων των δεδομένων που διατηρούν την ίδια δομή άλλα περιέχουν διαφοροποιημένες τιμές. Ο τύπος των δεδομένων παραμένει αμετάβλητος, ενώ οι πληροφορίες αντικαθίστανται ή τροποποιούνται. Η τεχνική αυτή περιλαμβάνει ενέργειες, όπως η αλλαγή των αριθμών ή των γραμμάτων, η αντικατάσταση λέξεων ή η αναδιάταξη τμημάτων δεδομένων μεταξύ διαφορετικών εγγράφων, με στόχο την διατήρηση της ρεαλιστικής μορφής των δεδομένων χωρίς να αποκαλύπτονται οι πραγματικές πληροφορίες.
- **Κρυπτογράφηση δεδομένων (Data Encryption):** Η κρυπτογράφηση βασίζεται στην χρήση κρυπτογραφικών μεθόδων, όπως τα συμμετρικά κλειδιά ή δημόσια / ιδιωτικά κλειδιά, για την κωδικοποίηση των δεδομένων. Τα κρυπτογραφημένα δεδομένα είναι εντελώς μη αναγνωρίσιμα χωρίς την κατάλληλη διαδικασία αποκρυπτογράφησης. Αν και προσφέρουν

υψηλό επίπεδο ασφάλειας, τα κρυπτογραφημένα δεδομένα δεν μπορούν να υποβληθούν σε επεξεργασία ή ανάλυση όσο παραμένουν κρυπτογραφημένα.

- **Tokenization:** Είναι η διαδικασία κατά την οποία αντικαθίστανται ευαίσθητα δεδομένα με αδιάφορες ή χωρίς νόημα τιμές (tokens), αλλά παρέχεται η δυνατότητα εξουσιοδοτημένης αντιστοίχισης αυτών των tokens με τα αρχικά δεδομένα. Αυτή η τεχνική είναι ιδιαίτερα χρήσιμη για περιβάλλοντα παραγωγής, όπως η διεκπεραίωση οικονομικών συναλλαγών, καθώς επιτρέπει την διαχείριση ευαίσθητων πληροφοριών, όπως ο αριθμός πιστωτικών καρτών, χωρίς να απαιτείται η μετάδοση των πραγματικών δεδομένων.

Στην ανάλυση που ακολουθεί θα εστιάσουμε κυρίως στις τεχνικές κάλυψης δεδομένων και tokenization με την λογική πως η κρυπτογράφηση αποτελεί ξεχωριστό αντίμετρο.

Η απόκρυψη προσφέρει σημαντικά πλεονεκτήματα στον ομιχλώδη προγραμματισμό, συμπεριλαμβανομένου της προστασία της ιδιωτικότητας και της χαμηλής κατανάλωση ενεργείας, ενώ η μείωσης της καθυστέρησης εξαρτάται από τον τρόπο υλοποίησης, καθώς η χρήση κρυπτογράφησης μπορεί να αύξησει την καθυστέρηση. Πιο συγκεκριμένα η απόκρυψη επιτυγχάνει χαμηλότερη υπολογιστική πολυπλοκότητα σε σύγκριση με την κρυπτογράφηση, γεγονός που μειώνει τον χρόνο επεξεργασίας των αιτημάτων, κάτι που είναι κρίσιμο για τον ομιχλώδη προγραμματισμό, όπου η ταχύτητα είναι σημαντική. Επίσης, η μικρότερη υπολογιστική πολυπλοκότητα της απόκρυψης σε σύγκριση με την κρυπτογράφηση οδηγεί σε χαμηλότερη κατανάλωση ενέργειας, βελτιώνοντας την αποδοτικότητα του συστήματος του ομιχλώδους προγραμματισμού. Επιπλέον, τα δεδομένα που έχουν υποστεί απόκρυψη δεν μπορούν να αναστραφούν, διασφαλίζοντας την εμπιστευτικότητα των χρηστών (Naik *et al.*, 2019). Ακόμα, η απόκρυψη των δεδομένων στον ομιχλώδη προγραμματισμό ενισχύει την ασφάλεια και την προστασία της ιδιωτικότητας, καθιστώντας πιο δύσκολη την κατανόηση των ευαίσθητων δεδομένων (ειδικά στο tokenization) από μη εξουσιοδοτημένα άτομα και προστατεύοντας με αυτόν τον τρόπο τα δεδομένα αυτά, αποτρέποντας την παραποίηση ή την κακή χρήση των δεδομένων. Αν και τροποποίηση των δεδομένων μπορεί να είναι εφικτή, είναι συχνά ανιχνεύσιμη μέσω μεθόδων αυθεντικοποίησης ή υπογραφής μηνυμάτων, γεγονός που περιορίζει την κακόβουλη επέμβαση, εκτός εάν ο στόχος είναι η παρεμπόδιση της επικοινωνίας. Επιπροσθέτως, η απόκρυψη των δεδομένων περιορίζει τις δυνατότητες των επιτιθέμενων να εκμεταλλευτούν αδυναμίες του συστήματος, μειώνοντας τον κίνδυνο εξωτερικών επιθέσεων. Τέλος, συμβάλλει στην εφαρμογή και την διασφάλιση των αυστηρών πολιτικών ασφάλειας για την διαχείριση και την προστασία των δεδομένων του περιβάλλοντος ομίχλης (Chandramohan, 2019).

Ωστόσο, η εφαρμογή της απόκρυψης των δεδομένων στον ομιχλώδη προγραμματισμό παρουσιάζει ορισμένα μειονεκτήματα. Αρχικά, ο σχεδιασμός και η διαχείριση της απόκρυψης των δεδομένων απαιτούν ιδιαίτερη προσοχή, καθώς η ανεπαρκής προετοιμασία μπορεί να οδηγήσει στην εφαρμογή ακατάλληλων μεθόδων απόκρυψης δεδομένων, οι οποίες μπορεί να παραβιάσουν τους κανονισμούς συμμόρφωσης ή της ασφάλειας των δεδομένων. Επίσης, η απόκρυψη των δεδομένων προσθέτει επιπλέον πολυπλοκότητα στα συστήματα του ομιχλώδους προγραμματισμού, αυξάνοντας τις ανάγκες για εξειδικευμένο προσωπικό και εργαλεία, γεγονός που μπορεί να αυξήσει το κόστος

υλοποίησης. Παρόλο που η απόκρυψη των δεδομένων στοχεύει στην διατήρηση της λειτουργικότητας των δεδομένων, υπάρχει κίνδυνος τα τροποποιημένα δεδομένα να μην εξυπηρετούν τον επιδιωκόμενο σκοπό, επηρεάζοντας την αξιοπιστία των αποφάσεων που βασίζονται στα δεδομένα. Για παράδειγμα, σε εφαρμογές μηχανικής μάθησης, τα δεδομένα που έχουν αποκρυφθεί ή τροποποιηθεί μπορεί να μην είναι πλέον ακριβή ή αντιπροσωπευτικά, με αποτέλεσμα να επηρεάζεται η αξιοπιστία των προβλέψεων ή αποφάσεων που βασίζονται σε αυτά, όπως η αναγνώριση μοτίβων ή λήψη επιχειρησιακών αποφάσεων. Τέλος, η απόκρυψη δεδομένων δεν είναι κατάλληλη για όλα τα είδη των δεδομένων και των καταστάσεων, καθώς απαιτείται συνεχή προσαρμογή των μεθόδων ανάλογα με τις μεταβαλλόμενες ανάγκες του οργανισμού. (Bowman, 2024)

5.3.6.3 Πολιτικές

5.3.6.3.1 Επιβολή πολιτικών

Η κύρια ιδέα της επιβολής πολιτικών (policy enforcements) μπορεί να περιγράφει ως εξής: (α) συσχέτιση των δεδομένων που πρέπει να προστατευθούν με ένα σύνολο πολιτικών απορρήτου που καθορίζουν τους κανόνες χρήσης για αυτά τα δεδομένα, (β) για κάθε αίτημα χρήσης των δεδομένων, η αξιολόγηση των ισχυουσών πολιτικών για τα ζητούμενα δεδομένα και ο προσδιορισμός αν και με ποιον τρόπο μπορούν να χρησιμοποιηθούν αυτά τα δεδομένα και (γ) η χρήση ενός μηχανισμού επιβολής πολιτικής για την εφαρμογή των αποτελεσμάτων της αξιολόγησης πολιτικής. (Al-Hasnawi, Carr and Gupta, 2019)

Οι AI-Hasnawi κα. (2018) παρουσίασαν το PEFM (Μονάδα Επιβολής Πολιτικών Ασφάλειας σε Περιβάλλοντα Ομίχλης - Policy Enforcement Fog Module), ένα καινοτόμο σύστημα ασφάλειας σχεδιασμένο να εξασφαλίζει την αυστηρή τήρηση των πολιτικών απορρήτου για τα ευαίσθητα δεδομένα που παράγονται από IoT συσκευές σε ολόκληρο τον κύκλο ζωής τους. Το PEFM επιτυγχάνει αυτό το στόχο μέσω της υποχρεωτικής επιβολής των πολιτικών απορρήτου σε κάθε σημείο πρόσβασης στα δεδομένα. Το κλειδί της αποτελεσματικότητας του βρίσκεται στην τοποθέτηση του στην υποδομή του ομιχλώδους προγραμματισμού, επιτρέποντας έτσι την άμεση και την αποδοτική επεξεργασία των δεδομένων κοντά στην πηγή τους. Για την διασφάλιση της ασφάλειας των δεδομένων κατά την μεταφορά τους σε απομακρυσμένες τοποθεσίες, το σύστημα PEFM χρησιμοποιεί το Active Data Bundle (ADB). Το ADB αποτελεί μια αυτόνομη λογική οντότητα, ικανή να εκτελείται σε οποιοδήποτε κόμβο φιλοξενίας (host) και να εφαρμόζει αυτόματα πολιτικές προστασίας δεδομένων (π.χ. που αφορούν την εφαρμογή κρυπτογράφησης στα δεδομένα πριν την αποστολή τους). Με τον τρόπο αυτό, εξασφαλίζεται ότι τα ευαίσθητα δεδομένα παραμένουν προστατευμένα καθ’ όλη την διάρκεια του κύκλου ζωής τους, ανεξαρτήτως του σημείου πρόσβασης τους. (Al-Hasnawi, Mohammed and Al-Gburi, 2018)

Η εφαρμογή του συστήματος PEFM σε IoT περιβάλλοντα του ομιχλώδους προγραμματισμού δύναται να προσφέρει πολλά πλεονεκτήματα. Ένα σημαντικό πλεονέκτημα του PEFM είναι η ασφάλεια και η ιδιωτικότητα των δεδομένων. Με το PEFM, η επεξεργασία των δεδομένων πραγματοποιείται κοντά στις πηγές των δεδομένων με ασφάλεια, επιτρέποντας την τοπική

εφαρμογή πολιτικών ασφάλειας που αφορούν την ιδιωτικότητα. Αυτό εξασφαλίζει τόσο την ασφαλή επεξεργασία όσο και την μεταφορά των δεδομένων προς τον κοντινότερο κόμβο ομίχλης πριν αυτά κατευθυνθούν προς το υπολογιστικό νέφος ή τον ομιχλώδη προγραμματισμό για περαιτέρω επεξεργασία. Αυτό προσφέρει προσαρμοστικότητα, επιτρέποντας στους ιδιοκτήτες των δεδομένων να καθορίσουν και να επιβάλλουν εξατομικευμένες πολιτικές ιδιωτικότητας ανάλογα με τις ανάγκες τους. Παράλληλα, η τοπική επεξεργασία και η προστασία των δεδομένων μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης ή διαρροής, αφού το PEFM παρέχει καλύτερη διαχείριση των ρίσκων που σχετίζονται με την επεξεργασία των ευαίσθητων δεδομένων και την μετάδοση τους από διάφορες κατανεμημένες συσκευές από το επίπεδο συσκευών στο επίπεδο ομίχλης ή του νέφους του ομιχλώδους προγραμματισμού. Επιπλέον, το PEFM προσφέρει επεκτασιμότητα και ευελιξία, με την κατανεμημένη αρχιτεκτονική του να κλιμακώνεται εύκολα, έτσι ώστε να υποστηρίξει τον μεγάλο αριθμό των IoT συσκευών και των IoT εφαρμογών. Η ενσωμάτωση του PEFM σε διάφορες υποδομές και IoT πλατφόρμες είναι σχετικά απλή, καθιστώντας το εύκολο να ενσωματωθεί στα υπάρχοντα IoT συστήματα. Ένα άλλο σημαντικό πλεονέκτημα του PEFM είναι η χαμηλή καθυστέρηση και η βελτιωμένη απόδοση, αφού γίνεται ένα αρχικό φιλτράρισμα των δεδομένων είτε στις IoT συσκευές είτε στους κόμβους ομίχλης χωρίς να είναι απαραίτητη η αποστολή των δεδομένων στο επίπεδο του νέφους. Αυτό καθιστά το PEFM ιδανικό για την ασφάλεια διάφορων εφαρμογών, όπως των έξυπνών σπιτιών και των συστημάτων υγειονομικής περίθαλψης. (Al-Hasnawi and Lilien, 2017) (Al-Hasnawi, Carr and Gupta, 2019) (Al-Hasnawi, Mohammed and Al-Gburi, 2018)

Ωστόσο, η υλοποίηση του συστήματος PEFM σε περιβάλλοντα ομίχλης μπορεί να είναι περίπλοκη, λόγω του κατανεμημένου χαρακτήρα του επιπέδου ομίχλης, καθώς και της ποικιλίας των συσκευών και των πρωτοκόλλων που εμπλέκονται. Επίσης, η εγκατάσταση και η συντήρηση του PEFM προσθέτουν επιπλέον επίπεδα πολυπλοκότητας σε ένα IoT δίκτυο, καθιστώντας την υλοποίηση και την διαχείριση του πιο σύνθετη. Εφόσον το PEFM εφαρμόζεται σε επίπεδο IoT συσκευής, πριν τα δεδομένα μεταφερθούν στο επίπεδο ομίχλης ή του νέφους, ενδέχεται να προκύψουν προβλήματα λόγω των περιορισμένων υπολογιστικών πόρων των συσκευών αυτών, που ενδέχεται να δυσκολέψουν την εγκατάσταση της λύσης. Επομένως, χρειάζεται εξειδικευμένη γνώση για την σωστή ρύθμιση και την διαχείριση των πολιτικών ασφάλειας. Επιπλέον, η πρόσθετη επεξεργασία που απαιτείται από το PEFM στους κόμβους ομίχλης μπορεί να επιβαρύνει τους ήδη περιορισμένους υπολογιστικούς πόρους και τον μικρό σε μέγεθος αποθηκευτικό χώρο των κόμβων ομίχλης, καθώς η ασφάλεια και η προστασία της ιδιωτικότητητας απαιτούν αυξημένη τοπική επεξεργασία δεδομένων, γεγονός που μπορεί να μειώσει την συνολική απόδοση του συστήματος PEFM, καθώς και την απόδοση του συστήματος του ομιχλώδους προγραμματισμού. Επιπροσθέτως, οι κόμβοι ομίχλης είναι πιο ευάλωτοι σε φυσικές ή δικτυακές επιθέσεις σε σύγκριση με τα κέντρα δεδομένων του επιπέδου του νέφους, ενώ η διανομή των δεδομένων και των πολιτικών σε πολλαπλά σημεία μπορεί να αυξήσει την επιφάνεια επίθεσης. Τέλος, η εγκατάσταση του PEFM απαιτεί επιπλέον επενδύσεις τόσο σε υλικό όσο και σε λογισμικό, ενώ απαιτείται συνεχής παρακολούθηση και ενημέρωση για να διασφαλιστεί η αποτελεσματικότητα και η ασφάλεια του συστήματος PEFM. (Al-Hasnawi and Lilien, 2017) (Al-Hasnawi, Carr and Gupta, 2019) (Al-Hasnawi, Mohammed and Al-Gburi, 2018)

5.3.6.3.2 Σύστημα ασφάλειας «Διαχείριση πόρων με βάση καθορισμένους κανόνες και πολιτικές»

Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους κανόνες και πολιτικές (policy-driven secure management of resources) προσφέρει μια δομημένη προσέγγιση που χρησιμοποιεί προκαθορισμένους κανόνες και πολιτικές για την διαχείριση, την αλληλεπίδραση και την κατανομή των πόρων μέσα σε ένα κατανεμημένο σύστημα, όπως είναι ο ομιχλώδης προγραμματισμός. Η κύρια διαφοροποίηση με το προηγούμενο αντίμετρο της ενότητας 5.3.6.3.1 είναι ότι εδώ οι κανόνες και οι πολιτικές είναι κοινοί και προκαθορισμένοι, ενώ στο προηγούμενο αντίμετρο είναι ειδικοί για τα δεδομένα που επεξεργάζονται, γεγονός που καθιστά αυτή την προσέγγιση πιο γενική και κατάλληλη για τη διαχείριση των πόρων σε κατανεμημένα περιβάλλοντα. Οι πολιτικές και οι κανόνες στη διαχείριση πόρων επηρεάζουν την ασφάλεια των δεδομένων καθορίζοντας τον έλεγχο πρόσβασης, την πιστοποίηση των χρηστών, την κρυπτογράφηση και την εφαρμογή στρατηγικών ασφάλειας, διασφαλίζοντας την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, υποκλοπές ή κακόβουλες επιθέσεις. Πιο συγκεκριμένα, το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους κανόνες και πολιτικές βασίζεται σε ένα πλαίσιο διαχείρισης πολιτικών που αποτελείται από πέντε κύρια συστατικά και στηρίζεται στο πρότυπο XACML (Extensible Access Control Markup Language) (Khan, Parkinson and Qin, 2017):

1. *Μηχανισμός λήψης αποφάσεων πολιτικών (Policy Decision Engine - PDE):* Λαμβάνει αποφάσεις βάσει προκαθορισμένων κανόνων πολιτικής.
2. *Διαχειριστής Εφαρμογών (Application Administrator - AA):* Διαχειρίζεται την πολλαπλή μίσθωση σε ένα περιβάλλον ομίχλης μέσω προκαθορισμένων πολιτικών και κανόνων για την κατανομή των πόρων, την διαχείριση της πρόσβασης και την εξασφάλιση της απομόνωσης μεταξύ των διαφορετικών μισθωτών.
3. *Ανάλυση Πολιτικής (Policy Resolver - PR):* Αποτελεί το συστατικό που είναι υπεύθυνο για την υλοποίηση πιστοποίησης χρηστών βάσει χαρακτηριστικών (attribute-based authentication). Η πιστοποίηση χρηστών συνδέεται με την ανάλυση πολιτικής, καθώς η διαδικασία αυτή βασίζεται στην αξιολόγηση των χαρακτηριστικών του χρήστη σύμφωνα με τις ισχύουσες πολιτικές, ώστε να αποφασιστεί αν και πως ο χρήστης έχει δικαίωμα πρόσβασης στους πόρους ή τις υπηρεσίες. Έτσι, η ανάλυση πολιτικής διασφαλίζει ότι η πρόσβαση παρέχεται μόνο σε χρήστες που πληρούν τα κριτήρια που ορίζονται από τις πολιτικές ασφάλειας του συστήματος.
4. *Αποθετήριο Πολιτικής (Policy Repository - PRep):* Αποτελεί το κεντρικό αποθετήριο όπου αποθηκεύονται και οργανώνονται όλοι οι κανόνες και οι πολιτικές που καθορίζουν πως λειτουργεί το σύστημα.
5. *Εφαρμογή Πολιτικής (Policy Enforcer - PE):* Είναι υπεύθυνη για την εφαρμογή των πολιτικών ασφάλειας, εντοπίζοντας τυχόν διαφορές ή αποκλίσεις στην υλοποίηση της πολιτικής και διασφαλίζοντας ότι οι ενέργειες των χρηστών ή των συστημάτων συμμορφώνονται με τους καθορισμένους κανόνες.

Στο παραπάνω πλαίσιο, όταν ένας χρήστης κάνει μια αίτηση για κάποια υπηρεσία, η αίτηση αυτή στέλνεται στον PR, ο οποίος αυθεντικοποιεί τον χρήστη βάσει συγκεκριμένων χαρακτηριστικών και δικαιωμάτων πρόσβασης. Οι πληροφορίες αυτές μεταφέρονται στον PDE, ο οποίος αναλύει

τους κανόνες από το PRep και εφαρμόζει την πολιτική μέσω του PE. (Khan, Parkinson and Qin, 2017). Οι Dsouza κ.α. (2014) εφάρμοσαν το σύστημα διαχείρισης των πόρων με βάση καθορισμένους κανόνες και πολιτικές σε μία μελέτη περίπτωσης που αφορούσε το STLs (Smart Traffic Lights), δηλαδή ένα έξυπνο σύστημα σηματοδότησης (Dsouza, Ahn and Taguinod, 2014). Ορισμένα από τα πλεονεκτήματα και μειονεκτήματά του πλαισίου ασφάλειας διαχείρισης πόρων με βάση καθορισμένους κανόνες και πολιτικές αναφέρονται παρακάτω.

Η εφαρμογή του πλαισίου ασφάλειας διαχείρισης των πόρων με βάση καθορισμένους κανόνες και πολιτικές στον ομιχλώδη προγραμματισμό προσφέρει σημαντικά πλεονεκτήματα. Ένα από τα σημαντικά πλεονεκτήματα η ενισχυμένη ασφάλεια, καθώς η ενσωμάτωση του συστήματος ασφάλειας διαχείρισης πόρων με καθορισμένους πόρους και πολιτικές σε περιβάλλοντα ομιχλώδους προγραμματισμού επιτρέπει την επιβολή πολιτικών ασφάλειας σε πραγματικό χρόνο και συμβάλλει στην επίλυση ζητημάτων ασφάλειας που είναι κρίσιμα για την αρχιτεκτονική του ομιχλώδους προγραμματισμού. Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους κανόνες και πολιτικές εξασφαλίζει την πολύ-επίπεδη συνεργασία και μπορεί να αντιμετωπίσει προβλήματα ασφάλειας, όπως είναι η διαχείριση της αυθεντικοποίησης των χρηστών του συστήματος και η διαχείριση της εξουσιοδοτημένης πρόσβασης σε πόρους του συστήματος του ομιχλώδους προγραμματισμού. Επίσης, παρέχει ισχυρές πολιτικές προστασίας, όπως η κρυπτογράφηση και ο έλεγχος πρόσβασης, διασφαλίζοντας την ακεραιότητα και την εμπιστευτικότητα των δεδομένων που ανταλλάσσονται μεταξύ των κόμβων ομίχλης. Η αυξημένη αποτελεσματικότητα του συστήματος επιτρέπει την λήψη αποφάσεων και την εξυπηρέτηση των αιτημάτων χρηστών σε πραγματικό χρόνο, γεγονός που αποτελεί κρίσιμο πλεονεκτήματα για τις εφαρμογές με υψηλές απαιτήσεις απόδοσης. Παράλληλα, το πλαίσιο αυτό προσφέρει ευελιξία επιτρέποντας την εύκολη ενσωμάτωση και την προσαρμογή νέων μονάδων σε πραγματικό χρόνο, ενισχύοντας την συνολική ασφάλεια του συστήματος. (Dsouza, Ahn and Taguinod, 2014)

Από την άλλη πλευρά, το πλαίσιο διαχείρισης των πόρων με βάση καθορισμένους κανόνες και πολιτικές αντιμετωπίζει ορισμένα μειονεκτήματα και προκλήσεις. Ένα από τα σημαντικά μειονεκτήματα του πλαισίου ασφάλειας διαχείρισης πόρων με βάση καθορισμένους κανόνες και πολιτικές αποτελεί η πολυπλοκότητα του πλαισίου, καθώς αυτή εντείνεται από την ανάγκη για συνεχή αναπροσαρμογή των πολιτικών, προκειμένου να εξυπηρετούν τις ποικίλες και δυναμικά μεταβαλλόμενες ανάγκες των συσκευών και των χρηστών. Επίσης, τα αποτελέσματα της έρευνας των Dsouza κ.α. (2014) έδειξαν ότι οι διαδικασίες των αποφάσεων και η εφαρμογή των πολιτικών ασφάλειας είναι γρήγορες και ανταποκρίνονται άμεσα στις εφαρμογές του συστήματος σε πραγματικό χρόνο, αλλά υπάρχουν και καθυστερήσεις («lag»), εξαιτίας του μεγάλου όγκου δεδομένων σε συνδυασμό με τους πολλαπλούς κανόνες των πολιτικών αποφάσεων που μπορεί να προκαλέσουν επιβράδυνση στην απόδοση του συστήματος του ομιχλώδους προγραμματισμού, αλλά και στην ποιότητα των υπηρεσιών (QoS) του δικτύου. (Dsouza, Ahn and Taguinod, 2014)

5.3.6.4 Honeypots

Το honeypot είναι ένα εργαλείο κυβερνοασφάλειας που έχει σχεδιαστεί για να εντοπίζει, να αποπροσανατολίζει και να αντεπιτίθεται σε απόπειρες μη εξουσιοδοτημένης πρόσβασης σε υπολογιστικά συστήματα και δίκτυα. Το honeypot είναι σαν μια «παγίδα» στον υπολογιστή ή στο δίκτυο που προσελκύει τους επιτιθέμενους, αλλά στην πραγματικότητα είναι μια ψεύτικη ευπάθεια που δεν μπορεί να βλάψει το πραγματικό σύστημα. Όταν οι επιτιθέμενοι προσπαθήσουν να παραβιάσουν το honeypot, οι αναλυτές ασφάλειας μπορούν να παρακολουθήσουν τις κινήσεις τους και να μάθουν τις τακτικές τους, χωρίς να θέσουν σε κίνδυνο τα πραγματικά συστήματα ή τα δεδομένα. Στον ομιχλώδη προγραμματισμό όπου οι υπολογιστικοί πόροι είναι κατανεμημένοι και βρίσκονται πλησιέστερα στους τελικούς χρήστες ή στις IoT συσκευές, τα honeypots μπορούν να αναπτυχθούν σε διάφορα επίπεδα της αρχιτεκτονικής (όπως στις άκρες του δικτύου, στις πύλες κ.λ.π.). (Sapphire, 2024)

Υπάρχουν δύο κύριες κατηγορίες honeypots (Sapphire, 2024):

- **Honeypots για συστήματα παραγωγής**: Αυτά τα honeypots έχουν σχεδιαστεί για να ενσωματωθούν σε ένα ζωντανό περιβάλλον και να μιμούνται φυσικά συστήματα και υπηρεσίες. Μπορούν να εντοπίζουν και να αποτρέπουν ευπάθειες ασφάλειας σε νόμιμα συστήματα που έχουν σχεδιαστεί να προστατεύουν.
- **Honeypots για την έρευνα:** Έχουν σχεδιαστεί για να προσομοιώνουν διάφορα συστήματα και υπηρεσίες, έτσι ώστε να μπορούν να χρησιμοποιηθούν για την μελέτη και την ανάλυση της συμπεριφοράς των επιθέσεων.

Τα honeypots στον ομιχλώδη προγραμματισμό προσφέρουν σημαντικά πλεονεκτήματα στην ανίχνευση και την αντιμετώπιση των κυβερνοεπιθέσεων. Αρχικά, μέσω της πρώιμης ανίχνευσης επιθέσεων στις άκρες του δικτύου, τα honeypots βοηθούν στον εντοπισμό και την αποτροπή της ανεπιθύμητης πρόσβασης πριν προκαλέσει σοβαρή ζημιά. Παράλληλα, τα honeypots παρέχουν πολύτιμες πληροφορίες για τις απειλές που στοχεύουν σε ευάλωτες IoT συσκευές, επιτρέποντας στους οργανισμούς να βελτιώσουν τα μέτρα ασφάλειας και να αναπτύξουν πιο αποτελεσματικές στρατηγικές προστασίας απέναντι σε μελλοντικές επιθέσεις. Επιπλέον, τα honeypots μειώνουν τον κίνδυνο να πληγούν για τα πραγματικά συστήματα του ομιχλώδους προγραμματισμού, αφού οι επιτιθέμενοι μπορεί να παραπλανηθούν και να απομακρυνθούν από αυτά. (Sapphire, 2024)

Ωστόσο, η εφαρμογή των honeypots στον ομιχλώδη προγραμματισμό μπορεί να εμφανίσει κάποια μειονεκτήματα. Πρώτα από όλα, η ανεπαρκής ή εσφαλμένη διαμόρφωση των honeypots μπορεί να αυξήσει την επιφάνεια επίθεσης, επιτρέποντας στους επιτιθέμενους να έχουν πρόσβαση και σε άλλα τμήματα του δικτύου (εφόσον δεν έχει επέλθει το κατάλληλο επίπεδο απομόνωσης). Επίσης, η ανάπτυξη και η συντήρηση των honeypots είναι δαπανηρή και απαιτεί σημαντικούς πόρους. Τέλος, οι εξειδικευμένοι κακόβουλοι χρήστες μπορούν να ανιχνεύσουν και να παρακάμψουν τα honeypots, ενώ η ενσωμάτωση τους σε ένα δυναμικό περιβάλλον ομίχλης απαιτεί προσεκτικό σχεδιασμό, ώστε να μην επηρεαστεί η κανονική λειτουργία των συστημάτων. (Sapphire, 2024)

5.3.6.5 Ασφαλής διαχείριση κλειδιών

Η Ασφαλής Διαχείριση Κλειδιών (Secure Key Management) είναι η διαδικασία που διασφαλίζει ότι τα κρυπτογραφικά κλειδιά, τα οποία είναι απαραίτητα για την ασφαλή κρυπτογράφηση και την μετάδοση των δεδομένων, παραμένουν ασφαλή από κακόβουλες ενέργειες ή μη εξουσιοδοτημένη πρόσβαση, προσφέροντας προστασία στις πληροφορίες που κρυπτογραφούνται (Kaviyazhiny, Bala and Gowri, 2021). Οι Li κ.α. (2021) πρότειναν το Σχέδιο Ασφαλούς Διαχείρισης Κλειδιών (Secure Key Management Scheme), το όποιο στηρίζεται στην τεχνολογία blockchain και επιτρέπει την ασφαλής διαχείριση κλειδιών σε δίκτυα MEC (Mobile Edge Computing). Το Σχέδιο Ασφαλούς Διαχείρισης Κλειδιών είναι επίσης κατάλληλο για ομιχλώδη περιβάλλοντα, καθώς το αποκεντρωμένο περιβάλλον και η χρήση του blockchain για την αποθήκευση των δημόσιων κλειδιών των συσκευών, επιτρέπουν την κρυπτογραφημένη επικοινωνία μεταξύ των συσκευών, καθώς και την γρήγορη αυθεντικοποίηση σε δυναμικά και κατανεμημένα δίκτυα, όπως είναι και τα ομιχλώδη περιβάλλοντα. Τα ιδιωτικά κλειδιά προστατεύονται μέσω άλλων μηχανισμών ασφάλειας, όπως η κρυπτογράφηση ή η αποθήκευση τους σε ασφαλή και κλειστά περιβάλλοντα, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. (Li *et al.*, 2021)

Η εφαρμογή του Σχεδίου Ασφαλούς Διαχείρισης Κλειδιών στον ομιχλώδη προγραμματισμό προσφέρει πολλά πλεονεκτήματα. Αρχικά, η τεχνολογία blockchain παρέχει ένα αποκεντρωμένο περιβάλλον όπου τα δημόσια κρυπτογραφικά κλειδιά αποθηκεύονται με ασφάλεια, εξασφαλίζοντας έτσι την ασφαλή επικοινωνία μεταξύ των συσκευών. Επίσης, χρησιμοποιώντας τις καταχωρίσεις του blockchain, οι συσκευές που μετακινούνται σε άλλες υποδομές μπορούν να αναγνωρίζονται γρήγορα, χωρίς να χρειάζεται νέα διαδικασία δημιουργίας κλειδιών, διευκολύνοντας έτσι την διαδικασία της αυθεντικοποίησης των συσκευών. Επιπλέον, το blockchain εξαλείφει την ανάγκη της ύπαρξης μιας κεντρικής αρχής για την διαχείριση των κλειδιών, μειώνοντας με αυτό τον τρόπο τα σημεία αποτυχίας και τον κίνδυνο των επιθέσεων. Τέλος, το Σχέδιο Ασφαλούς Διαχείρισης Κλειδιών βασίζεται στην ανθεκτικότητα του Proof-of-Work (PoW) και μπορεί να αμυνθεί σε επιθέσεις 51%, όπου οι κακόβουλοι χρήστες προσπαθούν να ελέγξουν το 50% της υπολογιστικής δύναμης του δικτύου. (Li *et al.*, 2021)

Ωστόσο, η εφαρμογή του Σχεδίου Ασφαλούς Διαχείρισης Κλειδιών στον ομιχλώδη προγραμματισμό παρουσιάζει και κάποια μειονεκτήματα. Οι διαδικασίες συναίνεσης PoW του blockchain απαιτούν υψηλή υπολογιστική ισχύ, κάτι που μπορεί να είναι ενεργοβόρο και δύσκολο να υποστηριχθεί σε περιβάλλοντα ομίχλης με περιορισμένους πόρους. Επίσης, η επιβεβαίωση των συναλλαγών, όπως η αποθήκευση νέων κλειδιών στο blockchain, μπορεί να είναι χρονοβόρα σε σύγκριση με πιο απλά συστήματα διαχείρισης κλειδιών. Τέλος, η φύση του blockchain ως βάσης δεδομένων που προσθέτει μόνο (append-only) δεδομένα, απαιτεί μεγαλύτερους αποθηκευτικούς πόρους, καθώς τα παλαιότερα δεδομένα δεν διαγράφονται ή τροποποιούνται. (Li *et al.*, 2021)

5.3.6.6 Σύγκριση αντιμέτρων για την αντιμετώπιση των επιθέσεων που αφορούν τα δεδομένα του ομιχλώδους προγραμματισμού

Τα κριτήρια σύγκρισης που παρουσιάζονται στην ενότητα 5.2 της παρούσας διπλωματικής εργασίας εφαρμόστηκαν για την αξιολόγηση των αντιμέτρων για την αντιμετώπιση των επιθέσεων που αφορούν τα δεδομένα του ομιχλώδους προγραμματισμού, όπως αυτά περιγράφονται στις ενότητες 5.3.6.1-5.3.6.5 της διπλωματικής εργασίας. Η αξιολόγηση αυτή δικαιολογείται παρακάτω, ενώ τα αποτελέσματα της αξιολόγησης παρουσιάζονται συνοπτικά στον Πίνακας 7. Κατόπιν, παρέχονται ορισμένα βασικά συμπεράσματα από τα αποτελέσματα της αξιολόγησης αυτής.

Ανάλυση Πίνακα Σύγκρισης Αντιμέτρων

Κατανάλωση Πόρων

- Η ομομορφική κρυπτογράφηση αξιολογείται με 2, διότι απαιτεί σημαντικούς πόρους για την επεξεργασία, γεγονός που μπορεί να οδηγήσει σε σημαντική μείωση της απόδοσης σε περιβάλλοντα ομίχλης με περιορισμένους πόρους.
- Η απόκρυψη δεδομένων αξιολογείται με 4, διότι καταναλώνει λιγότερους πόρους σε σύγκριση με άλλες τεχνικές, όπως η κρυπτογράφηση είναι σχετικά χαμηλή, αλλά εξακολουθεί να απαιτεί υπολογιστική ισχύ για την επεξεργασία και διαχείριση των τροποποιημένων δεδομένων.
- Η επιβολή πολιτικών αξιολογείται με 2, διότι καταναλώνει παρά πολλούς πόρους λόγω της τοπικής επεξεργασίας, καθώς και της ανάγκης για κρυπτογράφηση και προστασία, επιβαρύνοντας τους κόμβους ομίχλης και τις IoT συσκευές.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 2, διότι το σύστημα είναι αρκετά απαιτητικό ως προς τους πόρους για την συνεχόμενη εφαρμογή των κανόνων πολιτικής.
- Τα honeypots αξιολογούνται από 2-3, διότι απαιτούν σημαντικούς πόρους για την ανάπτυξη και την συντήρηση τους, αλλά η ακριβής τιμή εξαρτάται από την έκταση της προσομοίωσης. Αν τα honeypots προσομοιώνουν μόνο ένα μέρος του συστήματος, καταναλώνουν λιγότερους πόρους και η απόδοση τους δεν επηρεάζεται σημαντικά, κάτι που δικαιολογεί την τιμή 2. Ωστόσο, αν καλύπτουν ολόκληρο το σύστημα, απαιτούν περισσότερους πόρους και μπορεί να επηρεάσουν την απόδοση του συστήματος, όποτε η τιμή 3 είναι πιο κατάλληλη σε αυτές τις περιπτώσεις.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 1, διότι η υψηλή υπολογιστική ισχύς που απαιτείται το PoW, καθιστά το σύστημα ενεργοβόρο, ιδιαίτερα σε περιβάλλοντα ομίχλης με περιορισμένους πόρους.

Κλιμακωσιμότητα

- Η ομομορφική κρυπτογράφηση αξιολογείται με 2, διότι όταν αυξάνεται ο φόρτος επεξεργασίας, η ανάγκη για περισσότερη επεξεργαστική ισχύ και μνήμη μπορεί να οδηγήσει σε σημαντική πτώση της απόδοση του συστήματος, ιδιαίτερα σε περιβάλλοντα ομίχλης με περιορισμένους πόρους.

- Η απόκρυψη δεδομένων αξιολογείται με 3, διότι η απόδοση μειώνεται με γραμμικό τρόπο όσο αυξάνονται τα δεδομένα.
- Η επιβολή πολιτικών αξιολογείται με 4, διότι μπορεί να διαχειριστεί το αυξημένο φόρτο εργασίας χωρίς να μειώνεται αισθητά η απόδοση του αντιμέτρου, ιδίως λόγω της κατανεμημένης αρχιτεκτονικής του.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 4, διότι λόγω της κατανεμημένης αρχιτεκτονικής του μπορεί να επιλέγεται ποιο συστατικό θα κλιμακωθεί ανάλογα τον φόρτο εργασίας που έχει την εκάστοτε χρονική στιγμή.
- Τα honeypots αξιολογούνται με 4, διότι μπορούν να κλιμακωθούν σχετικά εύκολα και να διατηρήσουν την απόδοση τους, ακόμη και όταν αυξάνεται ο φόρτος εργασίας, εφόσον είναι σωστά διαμορφωμένα.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 2, διότι το blockchain δεν είναι ιδιαίτερα κλιμακώσιμο σε συνθήκες αυξημένου φόρτου εργασίας, γεγονός που επηρεάζει αρνητικά την απόδοση του αντιμέτρου.

Ασφάλεια δεδομένων

- Η ομομορφική κρυπτογράφηση αξιολογείται με 4, διότι προσφέρει υψηλό επίπεδο προστασίας σε συνδυασμό με το ECC, διασφαλίζοντας την ιδιωτικότητα των δεδομένων σε οποιοδήποτε στάδιο επεξεργασίας, ωστόσο δεν διασφαλίζει πλήρως την ακεραιότητα των δεδομένων, καθώς η τροποποίηση τους παραμένει εφικτή. Επίσης, δεν καλύπτονται όλες οι δυνατές επιθέσεις.
- Η απόκρυψη δεδομένων αξιολογείται με 3, διότι εξαρτάται από την μέθοδο απόκρυψης δεδομένων που χρησιμοποιείται και δεν είναι απόλυτα αδιαπέραστη σε εξειδικευμένες επιθέσεις, όπως οι επιθέσεις συσχέτισης δεδομένων, οι οποίες θα μπορούσαν να οδηγήσουν σε αποκάλυψη ευαίσθητης πληροφορίας.
- Η επιβολή πολιτικών αξιολογείται με 4, διότι το PEFM προσφέρει υψηλό επίπεδο ασφάλειας, εξασφαλίζοντας την προστασία τους σε όλα τα σημεία του κύκλου ζωής τους μέσω της κρυπτογράφησης και των άλλων πολιτικών ασφάλειας.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 4, διότι παρέχει πολύ ισχυρά μέτρα ασφάλειας, όπως η κρυπτογράφηση και ο έλεγχος πρόσβασης, εξασφαλίζοντας την προστασία των δεδομένων.
- Τα honeypots αξιολογούνται με 3, καθώς αποσπούν τους επιτιθέμενους από τα πραγματικά συστήματα προσφέροντας κάποια προστασία, άλλα η εσφαλμένη διαμόρφωσή τους μπορεί να δημιουργήσει ευπάθειες. Επιπλέον, η αποτελεσματικότητα τους εξαρτάται από το αν ο επιτιθέμενος παραπλανηθεί. Αν αντιληφθεί το honeypot ή επιλέξει να επιτεθεί σε κανονικό σύστημα, δεν προσφέρουν προστασία, ενώ δεν έχουν σχεδιαστεί για να ανιχνεύουν ή να αποτρέπουν επιθέσεις στο κεντρικό σύστημα.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 4 ως προς την ασφάλεια της διαχείρισης κλειδιών, διότι παρέχει υψηλή ασφάλεια μέσω της χρήσης του blockchain και του PoW, καθιστώντας εξαιρετικά δύσκολες τις κακόβουλες επιθέσεις. Ωστόσο, αυτή η αξιολόγηση δεν καλύπτει όλα τα είδη επιθέσεων, καθώς η προστασία αφορά τα κρυπτογραφικά κλειδιά και τα δεδομένα.

Ευκολία χρήσης

- Η ομομορφική κρυπτογράφηση αξιολογείται με 4, διότι η εκτέλεση ενός έτοιμου αλγορίθμου αυτού του είδους κρυπτογράφησης είναι αρκετά απλοποιημένη για τους τελικούς χρήστες.
- Η απόκρυψη δεδομένων αξιολογείται με 3, διότι αν και η διαχείριση και η εφαρμογή της απόκρυψης δεδομένων είναι πιο εύκολη σε σύγκριση με την κρυπτογράφηση, η εφαρμογή της εξακολουθεί να είναι σύνθετη. Απαιτεί εξειδικευμένες ρυθμίσεις και τεχνογνωσία, καθώς η τεχνική πρέπει να διαμορφώνεται ανάλογα με την κρισιμότητα και τους τύπους των δεδομένων, κάτι που μπορεί να είναι πιο περίπλοκο από την εφαρμογή ενός αλγορίθμου με απλοϊκές παραμέτρους.
- Η επιβολή πολιτικών αξιολογείται με 3, διότι η χρήση του συστήματος απαιτεί εξειδικευμένη γνώση, ιδίως όσον αναφορά την ρύθμιση πολιτικών ασφάλειας και την ενσωμάτωση του στα υπάρχοντα συστήματα κάτι που το καθιστά μέτρια εύχρηστο.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 4, διότι αν και η πολυπλοκότητα του συστήματος και οι απαιτήσεις αναπροσαρμογής των πολιτικών μπορεί να δημιουργούν προκλήσεις, η χρήση γενικών και κοινών πολιτικών είναι πλέον ευρέως διαδεδομένη. Αυτό διευκολύνει την χρήση τους, καθώς η γνώση είναι πλέον κοινή και τα υπάρχοντα πλαίσια βελτιώνονται συνεχώς ως προς την ευχρηστία τους.
- Τα honeypots αξιολογούνται με 2-3, διότι η διαχείριση και η χρήση των honeypots εξαρτάται από το είδος τους. Για απλά ελαφριά honeypots, υπάρχουν έτοιμα εργαλεία που διευκολύνουν την χρήση ακόμη και για λιγότερους εμπείρους χρήστες και παίρνουν τιμή 3 στο παρόν κριτήριο. Ωστόσο, για πιο σύνθετα honeypots, όπως αυτά που προσομοιώνουν ολόκληρα συστήματα, η ευχρηστία μειώνεται και ο φόρτος διαχείρισης αυξάνεται, οπότε παίρνουν τιμή 2 στο παρόν κριτήριο.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 2, διότι η άμεση υιοθέτηση του blockchain είναι τεχνικά περίπλοκη και απαιτεί εξειδικευμένες γνώσεις.

Εκπαίδευση χρηστών

- Η ομομορφική κρυπτογράφηση αξιολογείται με 3, διότι απαιτεί εξειδικευμένη εκπαίδευση, αλλά η βασική χρήση ενός ανεπτυγμένου αλγορίθμου δεν είναι ιδιαίτερα περίπλοκη, ειδικά για την απλή εκτέλεση υπολογισμών σε κρυπτογραφημένα δεδομένα.
- Η απόκρυψη δεδομένων αξιολογείται με 3, διότι απαιτεί κάποια εκπαίδευση για την σωστή χρήση και την διαχείριση των τεχνικών απόκρυψης δεδομένων, ιδίως για τους διαχειριστές των συστημάτων και τους προγραμματιστές που θα πρέπει να γνωρίζουν τις ιδιαιτερότητες των εργαλείων.
- Η επιβολή πολιτικών αξιολογείται με 2, διότι το σύστημα απαιτεί σημαντική εκπαίδευση των χρηστών για την σωστή διαχείριση και την ρύθμιση των πολιτικών, καθώς και γνώση των πρωτοκόλλων ασφάλειας.

- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 2, διότι απαιτείται σημαντική εκπαίδευση για την κατανόηση και την διαχείριση του συστήματος λόγω της πολυπλοκότητας του.
- Τα honeypots αξιολογούνται με 2-3, διότι εξαρτάται από το είδος του honeypot. Στην περίπτωση των απλών honeypots, η εκπαίδευση είναι περιορισμένη, καθώς τα εργαλεία είναι εύκολα στην χρήση και κατανοητά και παίρνουν τιμή 3 σε αυτή την περίπτωση. Αντίθετα, για πιο σύνθετα honeypots, όπως αυτά που προσομοιώνουν ολόκληρα συστήματα, απαιτείται εκτεταμένη εκπαίδευση για την κατανόηση και την σωστή διαχείριση τους και παίρνουν τιμή 2 σε αυτή την περίπτωση.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 2, διότι η τεχνολογία blockchain απαιτεί σημαντική εκπαίδευση και εξοικείωση από τους χρήστες του συστήματος.

Αντίκτυπος Χρήστη

- Η ομομορφική κρυπτογράφηση αξιολογείται με 4, διότι ο αντίκτυπος στον χρήστη δεν είναι σημαντικός σε σχέση με την χρήση της κανονικής κρυπτογράφησης. Επομένως, η εμπειρία του χρήστη βελτιώνεται, καθώς μειώνονται οι καθυστερήσεις. Στην αρχική φάση της εφαρμογής της ομομορφικής κρυπτογράφησης δεν απαιτούνται εξειδικευμένες ρυθμίσεις πέρα από αυτές που θα χρειάζονταν ούτως ή άλλως για την κρυπτογράφηση των δεδομένων, επομένως δεν υπάρχει κάποια σημαντική αλλαγή στην ευχρηστία ή την εκπαίδευση.
- Η απόκρυψη δεδομένων αξιολογείται με 4, καθώς συμβάλλει στην βελτίωση της εμπειρίας του τελικού χρήστη, ειδικότερα σε σύγκριση με την χρήση της κρυπτογράφησης, δεδομένου ο τελικός χρήστης δεν αντιλαμβάνεται την απόκρυψη των δεδομένων άμεσα. Επηρεάζει μόνο τα δεδομένα που αποθηκεύονται ή μεταδίδονται, αλλά μπορεί να υπάρξουν επιπτώσεις στην αποδοτικότητα ή την λειτουργικότητα των δεδομένων σε συγκεκριμένα σενάρια.
- Η επιβολή πολιτικών αξιολογείται με 3, διότι η πολυπλοκότητα του συστήματος, η ανάγκη για επεξεργασία στους κόμβους ομίχλης και η διαχείριση των πολιτικών μπορεί να επιβαρύνουν την απόδοση του συστήματος, μειώνοντας έτσι την εμπειρία του χρήστη.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 3, διότι ο χρήστης επωφελείται από την αυξημένη ασφάλεια, αλλά μπορεί να επηρεάζεται από κάποιες καθυστερήσεις στην απόδοση του συστήματος λόγω της χρήσης του αντιμέτρου.
- Τα honeypots αξιολογούνται με 3, διότι λειτουργούν στο προσκήνιο και δεν επηρεάζουν άμεσα τους χρήστες, εκτός αν υπάρχει εσφαλμένη διαμόρφωση που μπορεί να επηρεάσει την κανονική λειτουργία του συστήματος. Όμως, καταναλώνουν πόρους που κανονικά θα μπορούσαν να είχαν διατεθεί για την επίτευξη καλύτερης απόδοσης στις εφαρμογές ομίχλης.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 2, διότι οι καθυστερήσεις που προκαλούνται στο σύστημα εξαιτίας της πολυπλοκότητας του blockchain, δημιουργούν αρνητικό αντίκτυπο στον χρήστη.

Εφαρμοσιμότητα

- Η ομομορφική κρυπτογράφηση αξιολογείται με 3, διότι η εφαρμογή της στα υπάρχοντα περιβάλλοντα ομίχλης απαιτεί πρόσθετους πόρους και απαιτήσεις για ενοποίηση, γεγονός που καθιστά την διαδικασία απαιτητική σε επίπεδο υποδομών.
- Η απόκρυψη δεδομένων αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε πολλά περιβάλλοντα ομιχλώδους προγραμματισμού, αλλά απαιτεί προσαρμογή και ενσωμάτωση με τις υπάρχουσες υποδομές, αν και η διαδικασία αυτή είναι πιο ελαφριά σε σχέση με άλλες τεχνικές, όπως η ομομορφική κρυπτογράφηση, λόγω των λιγότερων απαιτήσεων σε πόρους.
- Η επιβολή πολιτικών αξιολογείται με 2, διότι το PEFM μπορεί να εφαρμοστεί σε διάφορα περιβάλλοντα ομίχλης, όμως θα πρέπει να γίνει ενσωμάτωση ανεξάρτητων μονάδων στους κόμβους του συστήματος που επιβάλλουν τις πολιτικές ιδιωτικότητας / απορρήτου, καθιστώντας την εφαρμογή και την ενσωμάτωση του σε όλη την υποδομή ομίχλης απαιτητική.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 2, διότι μπορεί να εφαρμοστεί στα υπάρχοντα ομιχλώδη περιβάλλοντα, αλλά απαιτεί σημαντική δέσμευση πόρων και την ενσωμάτωση ανεξάρτητων μονάδων στους κόμβους του συστήματος που επιβάλλουν τις πολιτικές ιδιωτικότητας / απορρήτου. Αυτό καθιστά την εφαρμογή και την ενσωμάτωση του σε όλη την υποδομή ομίχλης πιο απαιτητική και δύσκολή.
- Τα honeypots αξιολογούνται με 3, διότι μπορεί να εφαρμοστούν σε περιβάλλοντα ομίχλης, αλλά απαιτείται πρόσθετη ενοποίηση και πόρους για να λειτουργήσουν σωστά, γεγονός που αυξάνει την δυσκολία υλοποίησης.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 2, διότι η εφαρμογή του blockchain σε ομιχλώδη περιβάλλοντα μπορεί να είναι δύσκολη λόγω της απαίτησης σε επιπλέον πόρους και σε υποδομή.

Βαθμός κάλυψης

- Η ομομορφική κρυπτογράφηση αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε πολλά περιβάλλοντα, αλλά τα είδη επεξεργασίας που μπορούν υποστηριχτούν είναι περιορισμένα. Επίσης, περιορίζεται σε περιβάλλοντα με υψηλές απαιτήσεις υπολογιστικής ισχύος ή με περιορισμένους πόρους, όπως τα IoT περιβάλλοντα.
- Η απόκρυψη δεδομένων αξιολογείται με 3, διότι είναι εφαρμόσιμη σε πολλά περιβάλλοντα, αλλά δεν καλύπτει όλα τα σενάρια, ειδικά αυτά που απαιτούν πλήρη αναγνωσιμότητα των δεδομένων.
- Η επιβολή πολιτικών αξιολογείται με 3, διότι το PERM μπορεί να εφαρμοστεί σε διάφορα IoT περιβάλλοντα και περιβάλλοντα ομίχλης, άλλα η εφαρμογή του σε περιβάλλοντα με περιορισμένους πόρους ενδέχεται να είναι πιο δύσκολη.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε πολλά περιβάλλοντα και σενάρια και προσφέρει ευελιξία και στις πολιτικές και στην διαχείριση των πόρων.

- Τα honeypots αξιολογούνται με 3, διότι μπορούν να εφαρμοστούν σε πολλά διαφορετικά σενάρια και περιβάλλοντα. Αλλά ενέχουν κάποιο υπολογιστικό και διαχειριστικό κόστος που δεν είναι αμελητέο, ειδικά για περιβάλλοντα με σημαντικούς περιοριστικούς πόρους.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε αρκετά περιβάλλοντα και σενάρια, όμως μπορεί να υπάρχουν σημαντικές απαιτήσεις σε πόρους, έτσι ώστε να μην καλύπτονται διάφορα περιβάλλοντα με περιορισμένη διαθεσιμότητα πόρων.

Επεκτασιμότητα

- Η ομομορφική κρυπτογράφηση αξιολογείται με 3, διότι η έλλειψη σημαντικών εξελίξεων στον τομέα περιορίζει την πιθανότητα επέκτασης και την εισαγωγή νέων ειδών επεξεργασίας στο μέλλον, ακόμη και αν υπάρχει η κατάλληλη υποδομή.
- Η απόκρυψη δεδομένων αξιολογείται με 3, διότι επιτρέπεται η εισαγωγή νέων λειτουργιών, αλλά η πολυπλοκότητα των τροποποιημένων δεδομένων μπορεί να δημιουργήσει δυσκολίες στην εισαγωγή επιπλέον χαρακτηριστικών και λειτουργιών.
- Η επιβολή πολιτικών αξιολογείται με 4, διότι το PEFM είναι αρκετά επεκτάσιμο, καθώς η κατανεμημένη αρχιτεκτονική του επιτρέπει την εύκολη προσθήκη νέων λειτουργιών.
- Το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές αξιολογείται με 3, διότι το πλαίσιο αυτό υποστηρίζει την δυνατότητα εισαγωγής νέων λειτουργιών και κανόνων, αλλά η πολυπλοκότητα που προστίθεται μπορεί να δημιουργήσει επιπλέον προκλήσεις κατά την ενσωμάτωση αυτών των νέων στοιχείων.
- Τα honeypots αξιολογούνται με 4, διότι μπορούν να επεκταθούν με νέες λειτουργίες χωρίς να αλλάζουν ριζικά την υπάρχουσα υποδομή. Ωστόσο, η προσθήκη νέων λειτουργιών απαιτεί ανακατανομή των πόρων, αφαιρώντας τους από τις κανονικές εφαρμογές και υπηρεσίες προς τα honeypots, γεγονός που μπορεί να επηρεάσει την συνολική απόδοση του συστήματος.
- Η ασφαλής διαχείριση κλειδιών αξιολογείται με 3, διότι το blockchain υποστηρίζει την δυνατότητα της εφαρμογής νέων λειτουργιών. Όμως η εφαρμογή και η συντήρηση της υποδομής blockchain απαιτεί σημαντικούς πόρους και δεν είναι πλήρως βελτιστοποιημένη για όλα τα περιβάλλοντα, γεγονός που περιορίζει την πλήρη αξιοποίηση των δυνατοτήτων του.

Πίνακας 7 - Πίνακας σύγκρισης των αντιμέτρων για την αντιμετώπιση των επιθέσεων που αφορούν τα δεδομένα του ομιχλώδους προγραμματισμού

Αντίμετρα	**Κατανάλωση Πόρων**	**Κλιμακωσιμότητα**	**Ασφάλεια δεδομένων**	**Ευκολία Χρήσης**	**Εκπαίδευση χρηστών**	**Αντίκτυπος στον χρήστη**	**Εφαρμοσι-μότη-τα**	**Βαθμος κάλη ψυς**	**Επεκτασιμότητα**

Ομομορφική Κρυπτογράφηση	2	2	4	4	3	4	3	3	3
Απόκρυψη Δεδομένων	4	3	3	3	3	4	4	3	3
Επιβολή Πολιτικής	2	4	4	3	2	3	2	3	4
Πλαίσιο διαχείρισης των πόρων με βάση καθορισμένους κανόνες και πολιτικές	2	4	4	4	2	3	3	3	3
Honeypots	2-3	3	4	2-3	2-3	3	3	3	4
Ασφαλής διαχείριση κλειδιών	1	2	4	2	2	2	2	3	3

Με βάση τον παραπάνω πίνακα έχουμε μπορούμε να προχωρήσουμε σε ανάλυση των καλύτερων και των χειρότερων αντιμέτρων για κάθε κριτήριο:

Ανάλυση καλύτερου και χειρότερου αντιμέτρου ανά κριτήριο: Θα εντοπίσουμε ποιο/-α αντίμετρο/-α έχει την καλύτερη και την χειρότερη απόδοση σε κάθε κριτήριο αξιολόγησης:

- Κατανάλωση πόρων:
  - Καλύτερο: Απόκρυψη δεδομένων (3)
  - Χειρότερο: Ασφαλής διαχείριση κλειδιών (1)
- Κλιμακωσιμότητα:
  - Καλύτερο: Επιβολή πολιτικών, πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές (4)
  - Χειρότερο: Ομομορφική κρυπτογράφηση, ασφαλής διαχείριση κλειδιών (2)
- Ασφάλεια δεδομένων:
  - Καλύτερο: Ομομορφική κρυπτογράφηση, επιβολή πολιτικών, πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές, ασφαλής διαχείριση κλειδιών (4)
  - Χειρότερο: Απόκρυψη δεδομένων (3)
- Ευκολία χρήσης:

- Καλύτερο: Ομομορφική κρυπτογράφηση, πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές (4)
- Χειρότερο: Ασφαλής διαχείριση κλειδιών (2)

❖ Εκπαίδευση χρηστών:
- Καλύτερο: Ομομορφική κρυπτογράφηση, απόκρυψη δεδομένων (3)
- Χειρότερο: Ασφαλής διαχείριση κλειδιών, Επιβολή πολιτικών, πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές (2)

❖ Αντίκτυπος στον χρήστη:
- Καλύτερο: Ομομορφική κρυπτογράφηση, απόκρυψη δεδομένων (4)
- Χειρότερο: αμφίδρομη επικύρωση ζεύξης (2)

❖ Εφαρμοσιμότητα:
- Καλύτερο: απόκρυψη δεδομένων (4)
- Χειρότερο: Επιβολή πολιτικών, αμφίδρομη επικύρωση ζεύξης (2)

❖ Βαθμός κάλυψης:
- Όλα τα αντίμετρα έχουν τον ίδιο βαθμό.

❖ Επεκτασιμότητα:
- Καλύτερο: Επιβολή πολιτικών, honeypots (4)
- Χειρότερο: Ομομορφική κρυπτογράφηση, απόκρυψη δεδομένων (3)

Καλύτερο και χειρότερο αντίμετρο συνολικά (στην κατηγόρια): ομομορφική κρυπτογράφηση: 28, απόκρυψη δεδομένων: 30, επιβολή πολιτικών: 27, πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές: 28, honeypots: 26-29, ασφαλής διαχείριση κλειδιών: 21. Επομένως, η απόκρυψη δεδομένων με συνολική βαθμολογία 30 είναι τα καλύτερα αντίμετρα συνολικά, ενώ το χειρότερο αντίμετρο συνολικά είναι η ασφαλής διαχείριση κλειδιών με βαθμολογία 21.

Αντίμετρο με καλύτερη και χειρότερη απόδοση: Για την καλύτερη και χειρότερη απόδοση, πρέπει να εξετάσουμε την απόδοση των αντιμέτρων σε κάθε κριτήριο και να καταλήξουμε στο καλύτερο και το χειρότερο αντίμετρο βασιζόμενοι στο ποσοστό των υψηλών ή των χειρότερων βαθμολογίων τους που έχουν λάβει στα κριτήρια. Θεωρούμε υψηλές τιμές το 4 και 5 και χειρότερες τιμές το 1 και 2. Στον παρών υπολογισμό δεν συμπεριλαμβάνονται τα αντίμετρα που οι τιμές τους είναι με το εύρος τιμών.

Ποσοστά υψηλών και χαμηλών βαθμολογιών:

- Ομομορφική κρυπτογράφηση:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 2/9 = 22,2 %
- Απόκρυψη δεδομένων:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 0/9 = 0 %
- Επιβολή πολιτικών:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 3/9 = 33,3 %

- Πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 2/9 = 22,2 %
- Honeypots:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 3/9 = 33,3 %
- Ασφαλής διαχείριση κλειδιών:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 6/9 = 66,7 %

Το αντίμετρο με την καλύτερη απόδοση είναι η απόκρυψη δεδομένων με 33,3 % (επιλέγετε αυτό το αντίμετρο σε σχέση με τα αντίμετρα, όπως η ομομορφική κρυπτογράφηση, επιβολή πολιτικών και το πλαίσιο ασφάλειας διαχείρισης πόρων με βάση καθορισμένους πόρους και πολιτικές που έχουν και αυτά απόδοση 33,3 %, διότι η απόκρυψη δεδομένων δεν έχει καμία χαμηλή τιμή). Το αντίμετρο με την χειρότερη απόδοση είναι η ασφαλής διαχείριση κλειδιών, καθώς έχει ποσοστό 66,7 % χαμηλότερων βαθμολογίων.

5.3.7 Αντίμετρα για τις επιθέσεις κακόβουλου λογισμικού στον ομιχλώδη προγραμματισμό

Για την αντιμετώπιση των επιθέσεων κακόβουλου λογισμικού στον ομιχλώδη προγραμματισμό μπορούν να εφαρμοστούν αντίμετρα, όπως η διόρθωση τρωτοτήτων (vulnerability patching), το Αντιβιοτικό 2.0, τα αντίγραφα ασφαλείας με το DropStore, το DRTHIS και το MacLeR. (Khan, Parkinson and Qin, 2017)

5.3.7.1 Διόρθωση τρωτοτήτων

Στον ομιχλώδη προγραμματισμό, η διόρθωση τρωτοτήτων (vulnerability patching) είναι ένας μηχανισμός ασφάλειας που αναφέρεται στην εφαρμογή επιδιορθώσεων σε ευάλωτους ξενιστές (host), τόσο πάνω στο υλικό όσο και στο λογισμικό που φιλοξενείται από αυτούς, καθώς και στην εφαρμογή επιδιορθώσεων σε συσκευές δικτύωσης, δηλαδή στο ενδιάμεσο επίπεδο του ομιχλώδους προγραμματισμού. Αυτή η διαδικασία περιλαμβάνει διάφορους τύπους επιδιορθώσεων, οι οποίοι είναι γενικοί και περιλαμβάνουν ενδεικτικά, την αναβάθμιση λογισμικού ή τρίτων βιβλιοθηκών, την αναβάθμιση (δηλαδή την αλλαγή της έκδοσης) του λειτουργικού συστήματος, την εφαρμογή επιδιορθώσεων ασφάλειας σε γνωστά σφάλματα (bugs), καθώς και την τροποποίηση της διαμόρφωσης του λογισμικού. Η εφαρμογή των διορθώσεων τρωτοτήτων λογισμικού ή / και υλικολογισμικού στους ξενιστές συντελεί στην βελτίωση της ασφάλειας τους, διορθώνοντας άμεσα ευπάθειες που ενδέχεται να εκμεταλλευτούν οι επιτιθέμενοι, ενώ ταυτόχρονα ενισχύει την συνολικά ασφάλεια του ομιχλώδους προγραμματισμού, προστατεύοντας από γνωστές επιθέσεις και κενά ασφάλειας. Παρακάτω αναλύονται τα πλεονεκτήματα και τα μειονεκτήματα από την εφαρμογή της διόρθωσης τρωτοτήτων στον ομιχλώδη προγραμματισμό. (An *et al.*, 2022)

Η διόρθωση τρωτοτήτων λογισμικού ή/και υλικολογισμικού σε έναν ξενιστή προστατεύει όχι μόνο την συγκεκριμένη συσκευή, αλλά και ολόκληρο το δίκτυο του ομιχλώδους προγραμματισμού. Συστήματα (π.χ. βιομηχανικά ή υγειονομικά) που απαιτούν εξεργασία δεδομένων σε πραγματικό χρόνο επωφελούνται ιδιαίτερα από την μείωση του κίνδυνου μέσω της διόρθωσης γνωστών ευπαθειών. Επίσης, η εφαρμογή της διόρθωσης τρωτοτήτων περιορίζει τις πιθανές διαδρομές επίθεσης μέσα στο δίκτυο, εμποδίζοντας τους επιτιθέμενους να αποκτήσουν πρόσβαση σε άλλες συσκευές ή κόμβους του δικτύου του ομιχλώδους προγραμματισμού. Αυτό είναι ιδιαίτερα σημαντικό στον ομιχλώδη προγραμματισμό, λόγω της αλληλεξάρτησης των συσκευών, όπου σε περίπτωση που συμβεί μια επίθεση σε μια συσκευή αυτή μπορεί να επηρεάσει πολλές άλλες (συσκευές). (An *et al.*, 2022)

Ωστόσο, η διόρθωση τρωτοτήτων μπορεί να προκαλέσει διακοπές στην λειτουργία (downtime) των συσκευών / κόμβων ομίχλης, κάτι που είναι κρίσιμο για ομιχλώδη περιβάλλοντα που απαιτούν συνεχή συνδεσιμότητα, άμεση απόκριση, ενώ μπορεί να οδηγήσει σε περαιτέρω κόστος για τον οργανισμό. Αν και τεχνικές, όπως οι επιδιορθώσεις εν κίνηση (hot patching) μπορούν να μειώσουν ή να αποφύγουν τις διακοπές λειτουργίας, δεν είναι πάντα εφαρμόσιμες σε όλα τα περιβάλλοντα ομίχλης ή σε συσκευές ομίχλης, γεγονός που μπορεί να περιορίσει την ευελιξία στην εφαρμογή τους. Τέλος, η διόρθωση τρωτοτήτων ενδέχεται να επιλύσει ευπάθειες μόνο σε συγκριμένες εκδόσεις λογισμικού ή λειτουργικών συστημάτων. Αυτό μπορεί να δημιουργήσει προβλήματα συμβατότητας ή να απαιτεί συχνές αναβαθμίσεις σε διαφορετικές συσκευές του ομιχλώδους προγραμματισμού, ενώ ορισμένες ευπάθειες ενδέχεται να μην έχουν καθόλου λύσεις, ή οι λύσεις να μην είναι ολοκληρωμένες ή κατάλληλες (π.χ. να προέρχονται από μη έμπιστα τρίτα μέρη). Αυτό σημαίνει πως δεν θα είναι δυνατόν να αφαιρεθούν οι ευπάθειες σε αυτές τις περιπτώσεις είτε πλήρως είτε και καθόλου. (An *et al.*, 2022)

5.3.7.2 Αντιβιοτικό 2.0

Το Αντιβιοτικό 2.0 (Antibiotic 2.0) αποτελεί μια προηγμένη λύση ανίχνευσης και αντιμετώπισης κακόβουλου λογισμικού (anti-malware), ειδικά σχεδιασμένη για την προστασία των IoT συσκευών, αξιοποιώντας την αρχιτεκτονική του ομιχλώδους προγραμματισμού. Αποτελεί εξέλιξη του προηγμένου μοντέλου, του Αντιβιοτικού 1.0, με βελτιώσεις που αντιμετωπίζουν κρίσιμα ζητήματα, όπως η νομιμότητα και η πρακτική εφαρμογή. Στην αρχιτεκτονική του Αντιβιοτικού 2.0, η οποία στηρίζεται στην αρχιτεκτονική του ομιχλώδους προγραμματισμού, οι αντιβιοτικοί κόμβοι ομίχλης (antibiotic fog nodes) παίζουν ένα σημαντικό κεντρικό ρόλο. Οι κόμβοι αυτοί επιλέγονται με βάση κριτηρίων, όπως την γεωγραφική τους τοποθεσία, την διαθεσιμότητα πόρων και την δυνατότητα επεξεργασίας δεδομένων σε πραγματικό χρόνο. Σε περίπτωση μόλυνσης ενός κόμβου, το σύστημα μπορεί να ενεργοποιήσει μηχανισμούς απομόνωσης ή αποκατάστασης, διασφαλίζοντας ότι η μόλυνση δεν εξαπλώνεται. Ο φόρτος εργασίας κατανέμεται δυναμικά μεταξύ των κόμβων, με βάση την τρέχουσα κατάσταση της ασφάλειας και των πόρων κάθε κόμβου, έτσι ώστε να διατηρείται η αποδοτικότητα και η ασφάλεια του συστήματος. Ειδικότερα, είναι υπεύθυνοι για συλλογή, την ανάλυση και την προστασία των δεδομένων των IoT συσκευών, καθώς και για την ανίχνευση κακόβουλου λογισμικού που μπορεί να επηρεάσει τόσο τα δεδομένα όσο και τα εκτελέσιμα αρχεία.

Η προστασία εκτείνεται όχι μόνο στις IoT συσκευές άλλα και στους κόμβους ομίχλης, με στόχο την ασφάλεια όλου του δικτύου, περιλαμβανομένων των αντιβιοτικών και των υπόλοιπων στοιχειών του συστήματος. (De Donno, Felipe and Dragoni, 2019)

Ένα από τα κύρια πλεονεκτήματα του Αντιβιοτικού 2.0 είναι η νομιμότητα κα ο έλεγχος που εξασφαλίζει. Το Αντιβιοτικό 2.0 λειτουργεί με την συγκατάθεση του χρήστη, κάτι που λύνει το νομικό πρόβλημα που υπήρχε στο Αντιβιοτικό 1.0, όπου η παρέμβαση στις συσκευές γινόταν χωρίς άδεια. Ένα άλλο σημαντικό πλεονέκτημα είναι ότι το Αντιβιοτικό 2.0 βασίζεται στην κατανεμημένη διαχείριση των πόρων του ομιχλώδους προγραμματισμού, όπου οι κόμβοι ομίχλης αναλαμβάνουν την επεξεργασία δεδομένων, ειδικά αυτών που προορίζονται για την ανίχνευση ιών, αντί όλα τα δεδομένα να στέλνονται στο νέφος. Αυτό έχει ως αποτέλεσμα την μείωση του υπολογιστικού φόρτου που μπορεί να υπάρχει στο νέφος, βελτιώνοντας τόσο την απόδοση όσο και την ταχύτητα απόκρισης σε επιθέσεις, κάνοντας με αυτό τον τρόπο το Αντιβιοτικό 2.0 πιο αποδοτικό και ασφαλές. Επίσης, η επεκτασιμότητα του Αντιβιοτικού 2.0 είναι καθοριστική, καθώς αυτό το σύστημα μπορεί να κλιμακωθεί με ευκολία, αφού μπορεί να συνδέονται παρά πολύ κόμβοι ομίχλης μεταξύ τους με ευκολία με σκοπό να διαχειριστούν τον μεγάλο αριθμό συσκευών που υπάρχουν σε ομιχλώδη περιβάλλοντα. Αυτή η δυνατότητα καθιστά το Αντιβιοτικό 2.0 σύστημα ιδιαίτερα ευέλικτο και ικανό να ανταποκριθεί σε αυξημένες απαιτήσεις. Επιπλέον, το Αντιβιοτικό 2.0 προσφέρει την δυνατότητα της συλλογής και της επεξεργασίας δεδομένων σε πραγματικό χρόνο για τον εντοπισμό νέων απειλών. Η ενσωμάτωση τεχνικών στο Αντιβιοτικό 2.0, όπως η μηχανική μάθηση ενισχύει την ικανότητα ανίχνευσης και της πρόληψης των επιθέσεων, συμβάλλοντας στην ενίσχυση της ασφάλειας του ομιχλώδους προγραμματισμού. Τέλος, η εύκολη εγκατάσταση και η διαχείριση του Αντιβιοτικού 2.0 δεν καθιστά υποχρεωτική την συνεχομένη αλληλεπίδραση και την χειροκίνητη ρύθμιση του συστήματος από τον χρήστη. (De Donno, Felipe and Dragoni, 2019)

Ωστόσο, το Αντιβιοτικό 2.0 παρουσιάζει ορισμένα μειονεκτήματα που σχετίζονται με την υποδομή του ομιχλώδους προγραμματισμού. Πρωταρχικό ζήτημα είναι η ανάγκη για ύπαρξη πλήρους εμπιστοσύνης σε έναν κόμβο ομίχλης. Αν παραβιαστεί ένας οποιοδήποτε κόμβος ομίχλης, τότε η ασφάλεια όλων των συνδεδεμένων συσκευών τίθεται σε κίνδυνο. Επίσης, το Αντιβιοτικό 2.0 εξαρτάται από την σταθερότητα του δικτύου. Ο κόμβος ομίχλης πρέπει να διατηρεί συνεχή και σταθερή σύνδεση με τις IoT συσκευές και το υπολογιστικό νέφος για να λειτουργεί σωστά. Τυχόν αστάθεια στη σύνδεση μπορεί να επηρεάσει την λειτουργικότητα και την ασφάλεια του Αντιβιοτικού 2.0. Τέλος, η σύνθετη διαχείριση πολλαπλών κόμβων ομίχλης και IoT συσκευών αποτελεί μια σημαντική πρόκληση, ιδιαίτερα σε περιβάλλοντα με ετερογενείς συσκευές, όπως τα ομιχλώδη περιβάλλοντα. Η πολυπλοκότητα αυξάνεται όταν απαιτείται ο συντονισμός μεταξύ των διαφορετικών τύπων συσκευών, κάτι που μπορεί να οδηγήσει σε δυσκολίες στην λειτουργία και την υποστήριξη του Αντιβιοτικού 2.0. (De Donno, Felipe and Dragoni, 2019)

5.3.7.3 Αντίγραφα ασφαλείας με το DropStore

Το DropStore είναι ένα σύστημα δημιουργίας αντιγράφων ασφαλείας που συνδυάζει τις τεχνολογίες των πολλαπλών νεφών (multi-cloud) και του ομιχλώδους προγραμματισμού για την

αποθήκευση και την προστασία των δεδομένων. Ουσιαστικά, το DropStore αποθηκεύει τα δεδομένα σε πολλαπλά νέφη και σε πολλαπλούς κόμβους ομίχλης, χρησιμοποιώντας έναν εμπεριστατωμένο μηχανισμό που εξασφαλίζει την ικανοποίηση συγκεκριμένων διαμορφώσιμων ιδιοτήτων, όπως η διαθεσιμότητα και η ανθεκτικότητα των δεδομένων. Η διαδικασία αυτή ελέγχεται από έναν κόμβο ομίχλης, το Droplet, μια τοπική συσκευή την οποία διαχειρίζεται πλήρως ο χρήστης. Έτσι δεν υπάρχει εξάρτηση από τρίτους για την διαχείριση της ασφάλειας. Το DropStore προσφέρει αρκετά πλεονεκτήματα όσον αναφορά την ασφάλεια και την απόδοση των δεδομένων, ενώ παρουσιάζει κάποια μειονεκτήματα λόγω της πολυπλοκότητας της διαχείρισης και της εξάρτησης από το υλικό που βρίσκεται στον ομιχλώδη προγραμματισμό. (Maher and Nasr, 2021)

Ένα από τα βασικά πλεονεκτήματα του Drostore είναι η μειωμένη καθυστέρηση, καθώς η χρήση των κοντινών κόμβων ομίχλης επιτρέπει την τοπική μεταφορά και την επεξεργασία των δεδομένων, μειώνοντας δραστικά τις καθυστερήσεις σε σύγκριση με την απομακρυσμένη επεξεργασία σε διακομιστές νέφους Επίσης, οι κόμβοι ομίχλης παρέχουν αυξημένη ιδιωτικότητα και ασφάλεια, εφόσον βρίσκονται υπό τον έλεγχο του χρήστη, καθώς οι συσκευές, όπως το Droplet επιτρέπουν στον χρήστη να διαχειρίζεται τοπικά τα δεδομένα του, χωρίς να εξαρτάται από τρίτους παρόχους για την ασφάλεια και την προστασία των δεδομένων του. Ωστόσο, σε περιβάλλον πολλαπλής μίσθωσης, η προστασία αυτή μπορεί να περιορίζεται, καθώς ο χρήστης ενδέχεται να εξαρτάται από τρίτους παρόχους για τη διαχείριση της ασφάλειας και της προστασίας των δεδομένων του. Ακόμα, η τοπική επεξεργασία των δεδομένων στο Droplet εξασφαλίζει μεγαλύτερη σταθερότητα και αξιοπιστία του συστήματος, καθώς μειώνει την εξάρτηση από τα κεντρικά δίκτυα, κάνοντας το λιγότερο επιρρεπές σε καθυστερήσεις και αποτυχίες λόγω της υπερφόρτωσης των κεντρικών δικτύων. Τέλος, οι κόμβοι ομίχλης καταναλώνουν λιγότερη ενέργεια σε σύγκριση με την διαρκή χρήση των υποδομών του νέφους, βελτιώνοντας με αυτό τον τρόπο την κατανάλωση της ενέργειας και την χρήση των δικτύων. (Maher and Nasr, 2021)

Ωστόσο, υπάρχουν και μειονεκτήματα που σχετίζονται με την υλοποίηση του DropStore. Ένα σημαντικό ζήτημα είναι οι περιορισμένοι πόροι των κόμβων ομίχλης και του Droplet, οι οποίοι διαθέτουν μικρή υπολογιστική ισχύ και χωρητικότητα, κάτι που μπορεί να περιορίσει την απόδοση σε απαιτητικές εργασίες. Επίσης, η αυξημένη πολυπλοκότητα διαχείρισης που προκύπτει από την συνδυασμένη χρήση του ομιχλώδους προγραμματισμού και των πολλαπλών νεφών απαιτεί περισσότερο συντονισμό για τον συγχρονισμό και την αποθήκευση των δεδομένων, γεγονός που μπορεί να οδηγήσει σε πιο περίπλοκα σενάρια ανάπτυξης και συντήρησης του συστήματος. Τέλος, η πολυπλοκότητα ασφάλειας αυξάνεται, καθώς η προστασία των δεδομένων κατά την μεταφορά τους μεταξύ των κόμβων ομίχλης και των παροχών νέφους γίνεται πιο απαιτητική, αυξάνοντας τις πιθανότητες παραβίασης ασφάλειας λόγω των πολλαπλών σημείων επικοινωνίας. (Maher and Nasr, 2021)

5.3.7.4 DRTHIS

Οι Humayoun κ.α. (2019) πρότειναν το DRTHIS (Deep ransomware threat hunting and intelligence system), ένα σύστημα ανίχνευσης και ταυτοποίησης επιθέσεων λυτρισμικού (ransomware),

σχεδιασμένο να λειτουργεί στο επίπεδο ομίχλης (fog layer). Το DRTHIS χρησιμοποιεί προηγμένες τεχνικές βαθιάς μάθησης, όπως το LSTM (Long Short-Term Memory) και CNN (Convolutional Neural Network) για να ξεχωρίσει επιθέσεις λυτρισμικού από τα κανονικά προγράμματα, καθώς και να εντοπίσει σε ποια κατηγορία λυτρισμικού ανήκουν. (Homayoun *et al.*, 2019)

Ένα από τα βασικά πλεονεκτήματα του DRTHIS είναι η χαμηλή καθυστέρηση και η ταχεία ανίχνευση. Δεδομένου ότι ο ομιχλώδης προγραμματισμός επεξεργάζεται τα τοπικά δεδομένα κοντά στις IoT συσκευές, το DRTHIS μπορεί να εντοπίζει επιθέσεις λυτρισμικού σε πραγματικό χρόνο, κάτι που είναι ζωτικής σημασίας για την γρήγορη απόκριση του συστήματος. Επίσης, το DRTHIS βοηθά στην άμεση προστασία των τοπικών συστημάτων και δεδομένων χωρίς να χρειάζεται να αποσταλούν ευαίσθητα δεδομένα στο νέφος, μειώνοντας έτσι τον κίνδυνο διαρροών των ευαίσθητων δεδομένων κατά την μετάδοση τους. Ακόμα, το DRTHIS λειτουργεί αυτόνομα στο επίπεδο ομίχλης και παρέχει υποστήριξη για την προστασία των κόμβων ομίχλης, καθώς και των IoT συσκευών, μέσω της ανίχνευσης επιθέσεων, χωρίς να απαιτείται η άμεση ανθρώπινη παρέμβαση. Τέλος, το DRTHIS μπορεί να επεκτείνεται και να προστατεύει περισσότερους κόμβους σε διαφορετικές τοποθεσίες, διατηρώντας την αποτελεσματικότητα του όσο μεγαλώνει το δίκτυο. (Homayoun *et al.*, 2019)

Ωστόσο, η εφαρμογή του DRTHIS στον ομιχλώδη προγραμματισμό έχει και ορισμένα μειονεκτήματα. Αρχικά, το DRTHIS απαιτεί ξεχωριστό έλεγχο και παρακολούθηση για κάθε μεμονωμένο κόμβο ομίχλης, καθώς είναι υπεύθυνο για την προστασία και την ανίχνευση των επιθέσεων λυτρισμικού σε αυτούς τους κόμβους, κάτι που καθιστά την διαχείριση του συστήματος πιο περίπλοκη. Επίσης, το DRTHIS χρησιμοποιεί αλγόριθμους βαθιάς μάθησης, οι οποίοι μπορεί να απαιτούν σημαντικούς υπολογιστικούς και αποθηκευτικούς πόρους, κάτι που μπορεί να μην μπορεί να υποστηριχθεί από τους κόμβους ομίχλης. Ακόμα, το DRTHIS εξαρτάται από δεδομένα υψηλής ποιότητας για την εκπαίδευση των αλγορίθμων βαθιάς μάθησης, καθώς τα ελλιπή ή κακής ποιότητας δεδομένα ενδέχεται να μειώσουν την απόδοσή του. (Homayoun *et al.*, 2019)

5.3.7.5 MacLeR

Το MacLeR (Machine Learning-based Run-Time Hardware Trojan Detection) είναι ένα σύστημα που χρησιμοποιεί μηχανική μάθηση για να ανιχνεύει δούρειους ίππους στο υλικό (hardware trojan) των IoT συσκευών κατά την λειτουργία τους σε πραγματικό χρόνο. Το MacLeR χρησιμοποιεί πολυεπίπεδα νευρωνικά δίκτυα (multi-layer perceptron - MLP) για να μελετήσει τις αλλαγές στην κατανάλωση ενεργείας του SoC (system-on-chip) των IoT συσκευών και αν εντοπίσει κάτι ασυνήθιστο, το αναγνωρίζει ως μια κρυφή απειλή, όπως είναι οι δούρειοι ίπποι στο υλικό. (Khalid *et al.*, 2020)

Η εφαρμογή του MacLeR προσφέρει πολλά πλεονεκτήματα στις IoT συσκευές που βρίσκονται στην άκρη του δικτύου του ομιχλώδους περιβάλλοντος. Πρώτον, το MacLeR έχει σχεδιαστεί για συσκευές με περιορισμένους πόρους, όπως αυτές που χρησιμοποιούνται στον ομιχλώδη προγραμματισμό. Επίσης, το MacLeR μπορεί να ανιχνεύσει τους δούρειους ίππους στο υλικό με

96% ακρίβεια, κάτι που σημαίνει ότι προσφέρει υψηλό επίπεδο ασφάλειας με τον εντοπισμό κακόβουλων τροποποιήσεων στο υλικό. Ωστόσο, επικεντρώνεται κυρίως στο υλικό και όχι σε περιπτώσεις όπου μπορεί να έχει πειραχθεί το firmware. Επιπλέον, το MacLeR μπορεί να εφαρμοστεί σε διάφορες αρχιτεκτονικές SoC, κάτι που το καθιστά για την χρήση σε ετερογενή δίκτυα ομιχλώδους προγραμματισμού με διαφορετικούς τύπους υλικού. (Khalid *et al.*, 2020)

Ωστόσο, η εφαρμογή του MacLeR στα ομιχλώδη περιβάλλοντα παρουσιάζει ορισμένα μειονεκτήματα. Ένα βασικό μειονέκτημα του MacLeR είναι ότι ενώ έχει σχεδιαστεί για να λειτουργεί σε συσκευές με περιορισμένους πόρους, η εκπαίδευση και η εφαρμογή των αλγορίθμων μηχανικής μάθησης απαιτούν περισσότερους πόρους από αυτούς που μπορεί να προσφέρει μια συσκευή, η οποία ανήκει σε έναν περιβάλλον ομίχλης. Επίσης, η μονή θύρα συλλογής ισχύος (ένα σημείο παρακολούθησης της κατανάλωσης ενέργειας των ηλεκτρονικών κυκλωμάτων ή συσκευών, όπως τα εξαρτήματα του υλικού των IoT συσκευών) μπορεί να περιορίσει την αποτελεσματικότητα της ανίχνευσης δούρειων ίππων στο υλικό των IoT συσκευών. Όταν οι δούρειοι ίπποι σε υλικό μπορούν να ενεργοποιούνται σε σύντομο χρονικό διάστημα προκαλούν μικρές και γρήγορες αλλαγές στην κατανάλωση ενεργείας, τις οποίες η θύρα δεν προλαβαίνει να καταγράψει πριν επιτρέψει την κατανάλωση στα κανονικά επίπεδα. Ως αποτέλεσμα, αυτές οι γρήγορες μεταβολές είναι δύσκολο να εντοπιστούν, καθιστώντας την ανίχνευση του δούρειου ίππου πιο δύσκολη. Ακόμα, με την πάροδο του χρόνου, η «γήρανση» των συσκευών, δηλαδή η φυσική φθορά των συσκευών μπορεί να επηρεάσει την απόδοση του συστήματος με την αύξηση της κατανάλωσης της ενέργειας ή προκαλώντας αστάθειες στο σύστημα, χωρίς όμως να υποδηλώνει την παρουσία δούρειου ίππου στο λογισμικό, κάτι που θα ήταν ψευδές. (Khalid *et al.*, 2020)

5.3.7.6 Συγκριτική ανάλυση αντιμέτρων για την αντιμετώπιση κακόβουλου λογισμικού στον ομιχλώδη προγραμματισμό

Στις ενότητες 5.3.7.1-5.3.7.5 της παρούσας διπλωματικής εργασίας είδαμε τα κύρια πλεονεκτήματα και μειονεκτήματα των αντιμέτρων για την αντιμετώπιση κακόβουλου λογισμικού στον ομιχλώδη προγραμματισμό, όπως είναι οι διορθώσεις τρωτοτήτων, το Αντιβιοτικό 2.0, των αντιγράφων ασφαλείας με το DropStore, το DRTHIS και το MacLeR. Παρακάτω ακολουθεί ο πίνακας σύγκρισης των αντιμέτρων αυτών με βάση τα κριτήρια αξιολόγησης της ενότητας 5.2. Το περιεχόμενο του πίνακα δικαιολογείται επίσης πλήρως ενώ αναδεικνύονται και τα πιο σημαντικά αποτελέσματα.

Ανάλυση κριτηρίων αξιολόγησης του πίνακα

Κατανάλωση Πόρων

- Η διόρθωση τρωτοτήτων αξιολογείται με 3-4, καθώς δεν απαιτείται συνεχομένη κατανάλωση πόρων, ενώ οι διορθώσεις γίνονται είτε με περιοδικό τρόπο είτε κατ' απαίτηση (π.χ. όταν κάποια νέα έκδοση ή επίσημη διόρθωση υπάρχουσας έκδοσης είναι διαθέσιμη

συνήθως ανά αραιά χρονικά διαστήματα ανάλογα βέβαια με την συχνότητα ανανέωσης του εκάστοτε συστατικού ή βιβλιοθήκης).

- Το Αντιβιοτικό 2.0 αξιολογείται με 2, διότι η κατανάλωση πόρων είναι συνεχής και μη αμελητέα, και αυτό επηρεάζει αρνητικά την απόδοση του συστήματος.
- Το DropStore αξιολογείται με 2, διότι υπάρχει μεγάλη κατανάλωση εύρους ζώνης λόγω της ανάγκης μεταφοράς και αποθήκευσης των δεδομένων σε πολλαπλούς παρόχους, και αυτό επηρεάζει αρνητικά την απόδοση του συστήματος.
- Το DRTHIS αξιολογείται με 2, διότι η χρήση αλγόριθμών βαθιάς μάθησης, όπως ο LSTM και ο CNN απαιτούν υψηλή κατανάλωση πόρων για την εκπαίδευση τους, κάτι που επηρεάζει αρνητικά την απόδοση στο σύστημα.
- Το MacLeR αξιολογείται με 3, διότι αν και το αντίμετρο αυτό έχει σχεδιαστεί για συσκευές με περιορισμένους πόρους, η εφαρμογή των αλγόριθμών μηχανικής μάθησης απαιτούν σημαντικούς πόρους για την εκπαίδευση τους, αν και αυτή πραγματοποιείται αρχικά μια φορά και στην συνεχεία εφόσον υπάρχουν αλλαγές στα δεδομένα γίνεται περιοδικά. Επίσης, η κατανάλωση πόρων του αντιμέτρου επηρεάζεται από την πολυπλοκότητα των συστατικών του.

Κλιμακωσιμότητα

- Η διόρθωση τρωτοτήτων αξιολογείται με 4, διότι μπορεί να διατηρεί το επίπεδο απόδοσης, αν και σε ορισμένες περιπτώσεις οι τεχνικές επιδιόρθωσης επηρεάζουν το σύστημα υπό αυξημένο φορτίο, χωρίς όμως να προκαλούν σημαντικά προβλήματα στην απόδοση του.
- Το Αντιβιοτικό 2.0 αξιολογείται με 3, διότι το σύστημα διατηρεί την απόδοση του, καθώς ο φόρτος εργασίας αυξάνεται, χάρις την κατανεμημένη αρχιτεκτονική του. Ωστόσο, η υψηλή κατανάλωση πόρων αποτελεί μειονέκτημα, καθώς όταν ο αριθμός των χρηστών ή των δεδομένων ξεπεράσει ένα όριο, η περαιτέρω κλιμάκωση μπορεί να μην υποστηρίζεται επαρκώς, με αρνητική επίπτωση στην απόδοση του συστήματος (οι κόμβοι ομίχλης ενδέχεται να υπερφορτωθούν), καθώς μόνο ορισμένοι κόμβοι συμμετέχουν στην λειτουργά του συστήματος.
- Το DropStore αξιολογείται με 4, διότι μπορεί να διατηρεί ικανοποιητικά την απόδοση του με την αύξηση του φόρτου εργασίας, λόγω της κατανεμημένης αρχιτεκτονικής του.
- Το DRTHIS αξιολογείται με 4, διότι φαίνεται να διατηρεί την απόδοση του με την αύξηση του αριθμού των κόμβων.
- Το MacLeR αξιολογείται με 4, διότι η απόδοση αυτού μπορεί να διατηρηθεί σε μεγάλο βαθμό όταν αυξάνεται ο φόρτος εργασίας, αλλά το κόστος σε πόρους μπορεί να αυξηθεί ανάλογα με το πλήθος των συσκευών.

Ασφάλεια Δεδομένων

- Η διόρθωση τρωτοτήτων αξιολογείται με 3, διότι δεν καλύπτονται όλες οι τρωτότητες και υπάρχει πιθανότητα να υπάρχουν τρωτότητες που δεν έχουν ανιχνευτεί. Αυτό σημαίνει ότι ενδεχομένως πολλές επιθέσεις, ιδιαίτερα σύνθετες, να είναι δυνατές και μόνο απλές απειλές να αντιμετωπίζονται αποτελεσματικά.

- Το Αντιβιοτικό 2.0 αξιολογείται με 4, διότι με την χρήση σύγχρονων τεχνικών καλύπτονται συνθέτες επιθέσεις και κακόβουλο λογισμικό, αλλά η παραβίαση ενός κόμβου ομίχλης μπορεί να θέσει σε κίνδυνο ολόκληρο το σύστημα.
- Το DropStore αξιολογείται με 3, διότι προσφέρει υψηλή διαθεσιμότητα δεδομένων μέσω της κρυπτογραφημένης και της κατανεμημένης αποθήκευσης. Ωστόσο, αν και η ακεραιότητα δεν επηρεάζεται άμεσα, η εμπιστευτικότητα επηρεάζεται όταν τα δεδομένα γίνονται διαθέσιμα σε μη εξουσιοδοτημένους χρήστες. Επιπλέον το αντίμετρο είναι κυρίως αντιδραστικό, καθώς δεν αναχαιτίζει άμεσα τις απειλές. Σε σενάριο επίθεσης με μη εξουσιοδοτημένη πρόσβαση και τροποποίηση των δεδομένων σε όλα τα αντίγραφα, η ακεραιότητα των δεομένων ενδέχεται να επηρεαστεί, καθώς διατηρείται μόνο μια έκδοση για λόγους εξοικονόμησης χώρου αποθήκευσης.
- Το DRTHIS αξιολογείται με 3, διότι η τοπική επεξεργασία των δεδομένων μειώνει τον κίνδυνο διαρροών ευαίσθητων δεδομένων, διατηρώντας την ασφάλεια κατά την ανίχνευση επιθέσεων λυτρισμικού, όμως και το αντίμετρο δεν καλύπτει εξίσου αποτελεσματικά όλες τις πιθανές απειλές.
- Το MacLeR αξιολογείται με 3, διότι αν και προσφέρει υψηλή αποτελεσματικότητα ανίχνευσης (96%) σε δούρειους ίππους στο υλικό, το αντίμετρο δεν καλύπτει εξίσου αποτελεσματικά όλες τις πιθανές απειλές.

Ευκολία χρήσης

- Η διόρθωση τρωτοτήτων αξιολογείται με 2-4, καθώς το αντίμετρο εφαρμόζεται με διαφορετικό τρόπο ανάλογα με το συστατικό προς επιδιόρθωση ή αναβάθμιση, η ευκολία χρήσης μπορεί παίρνει τιμές από 2 έως 4, ανάλογα με την περίπτωση. Σε περιπτώσεις με που απαιτούν εκτενείς ή χαρακτηρίζονται από ασαφείς οδηγίες, η ευκολία χρήσης μειώνεται.
- Το Αντιβιοτικό 2.0 αξιολογείται με 4, διότι η εύκολη εγκατάστασή του και η ελάχιστη ανάγκη για συνεχή αλληλεπίδραση του χρήστη με το σύστημα το καθιστούν φιλικό προς τον χρήστη. Επιπλέον, όλοι οι πλέον διαχειριστές έχουν εξοικείωση με την χρήση αντιβιοτικών. Ωστόσο, μπορεί να προκύψουν ζητήματα πολυπλοκότητας η επαγρύπνησης, καθώς ο διαχειριστής μπορεί να χρειάζεται να συμβουλεύεται το αντίμετρο, να το ρυθμίζει κατάλληλα, να ελέγχει περιοδικά την λειτουργία του και να το αναβαθμίζει ή να το διορθώνει όταν χρειάζεται.
- Το DropStore αξιολογείται με 3, διότι οι διαδικασίες διαμόρφωσης του αντιμέτρου και η επαναφορά των δεδομένων απαιτούν εξειδικευμένες γνώσεις και είναι πολύπλοκες και απαιτούν εξειδικευμένες γνώσεις, οπότε επηρεάζουν αρνητικά την συνολική εμπειρία του χρήστη.
- Το DRTHIS αξιολογείται με 4, διότι λειτουργεί αυτόνομα και δεν απαιτείται ο χρήστης να το χειρίζεται συνέχεια παρά μόνο όταν χρειάζεται να παρακολουθήσει την απόδοση του συστήματος.
- Το MacLeR αξιολογείται με 3, διότι οφείλεται στην πολυπλοκότητα που προκαλεί η χρήση της μηχανικής μάθησης, η οποία μπορεί να δυσκολεύει τη χρήση από μη εξειδικευμένους χρήστες.

Εκπαίδευση χρηστών

- Η διόρθωση τρωτοτήτων αξιολογείται με τιμή να κυμαίνεται από 3-4, διότι εξαρτάται από την διαδικασία που πρέπει να ακολουθήσει, η οποία διαφοροποιείται ανάλογα με το λογισμικό. Κάποιες διαδικασίες μπορεί να είναι εύκολες ή γνωστές, ενώ άλλες μπορεί να είναι εξειδικευμένες, εκτενείς ή / και ασαφείς, απαιτώντας εκπαίδευση των χρηστών, κυρίως για τους διαχειριστές, ώστε να κατανοήσουν τη διαδικασία εφαρμογής των επιδιορθώσεων και να παρακολουθήσουν τυχόν ενημερώσεις.
- Το Αντιβιοτικό 2.0 αξιολογείται με 3, διότι οι διαχειριστές δεν διαθέτουν τις απαραίτητες γνώσεις και απαιτείται η απόκτηση των βασικών δεξιοτήτων για την αρχική διαχείριση του συστήματος.
- Το DropStore αξιολογείται με 3, διότι παρόλο που οι βασικές ρυθμίσεις είναι απλές, δεν καλύπτουν όλες τις περιπτώσεις, ειδικά όσον αναφορά τις ανάγκες ενός οργανισμού. Επομένως, οι χρήστες χρειάζονται μέτρια εκπαίδευση για να ρυθμίζουν σωστά το σύστημα, ανάλογα με το είδος των δεδομένων προς προστασία και την κρισιμότητας τους
- Το DRTHIS αξιολογείται με 2, διότι οι χρήστες πρέπει να εκπαιδευτούν στη χρήση των αλγόριθμων βαθιάς μάθησης και ιδιαιτέρα στη διαδικασία εκπαίδευσης των αλγορίθμων αυτών. Αν και τα μοντέλα βαθιάς μάθησης λειτουργούν ως black-box και δεν απαιτούν ερμηνεία των αποτελεσμάτων, οι διαχειριστές χρειάζεται να επεμβαίνουν και να διασφαλίζουν ότι τα αποτελέσματα της ανίχνευσης είναι ακριβή, προσδιορίζοντας αν κάποια δραστηριότητα αποτελεί απόπειρα ή πραγματική επίθεση λυτρισμικού.
- Το MacLeR αξιολογείται με 2, διότι χρειάζεται ειδική γνώση για την κατανόηση και την παρακολούθηση της λειτουργίας του, καθώς και εξοικείωση με την διαδικασία εκπαίδευσης των αλγορίθμων, κυρίως λόγω των περίπλοκων αλγορίθμων που περιλαμβάνει.

Αντίκτυπος χρήστη

- Η διόρθωση τρωτοτήτων αξιολογείται με 3, διότι μπορεί να έχει από μικρό έως σημαντικό αρνητικό αντίκτυπο στον χρήστη λόγω τον διακοπών λειτουργίας που μπορεί να προκαλέσει. Αλλά επειδή η διόρθωση τρωτοτήτων δεν γίνεται συνεχώς, η εμπειρία του χρήστη επηρεάζεται αρνητικά σε ορισμένες μόνο περιπτώσεις, ενώ ενδέχεται να βελτιώνεται έπειτα λόγω της χρήσης πιο αξιόπιστων εκδόσεων του (επιδιορθωμένου / ανανεωμένου) λογισμικού.
- Το Αντιβιοτικό 2.0 αξιολογείται με 3, διότι ενώ η λειτουργία του συστήματος με την συγκατάθεση του χρήστη μπορεί να βελτιώνει την εμπειρία του διαχειριστή, υπάρχουν πιθανά αρνητικά αποτελέσματα. Πιο συγκεκριμένα, ενδέχεται να υπάρξουν αρνητικές επιπτώσεις στην απόδοση του συστήματος, ενόχληση των τελικών χρηστών λόγω του αποκλεισμού των ενεργειών τους αν το Αντιβιοτικό 2.0 τις θεωρήσει κατά λάθος κακόβουλες, ή προβλήματα στην λειτουργία των εφαρμογών αν οι συμπεριφορές τους «κόβονται» λανθασμένα από το αντιβιοτικό.
- Το DropStore αξιολογείται με 2, διότι έχει αρνητικό στον χρήστη εξαιτίας των προβλημάτων που δημιουργούνται στην κίνηση του δικτύου, ιδιαίτερα αν πρέπει να γίνει

ταυτόχρονη διαχείριση / αποθήκευση πολλών δεδομένων. Αποθηκευτικά μπορεί επίσης να δημιουργήσει προβλήματα και να μη υπάρχει αρκετός χώρος διαθέσιμος στους κόμβους ομίχλης για την σωστή λειτουργία των εφαρμογών.

- Το DRTHIS αξιολογείται με 2, διότι αν και το σύστημα λειτουργεί αυτόνομα, υπάρχουν περιπτώσεις όπου οι χρήστες ή οι διαχειριστές θα πρέπει να εμπλακούν, όπως η αντιμετώπιση των ειδοποιήσεων ή την παρακολούθηση της απόδοσης. Επιπλέον, μπορεί να υπάρξει αρνητικός αντίκτυπος στην απόδοση του συστήματος, καθώς εξαρτάται από το μέγεθος του μοντέλου και την υπολογιστική ισχύ που απαιτείται για την συνεχιζόμενη εφαρμογή του. Αυτό μπορεί να επηρεάσει τις εφαρμογές, ιδιαίτερα όταν το σύστημα εκτελείται σε πολλές συσκευές ή κόμβους. Επιπλέον, οι πολλές λανθασμένες ειδοποιήσεις, λόγω π.χ. λανθασμένης εκπαίδευσης των αλγόριθμών, μπορεί να προκαλέσουν εκνευρισμό στους χρήστες.
- Το MacLeR αξιολογείται με 3, διότι μπορεί να δημιουργήσει αρνητικό αντίκτυπο στον χρήστη εξαιτίας των καθυστερήσεων που μπορεί να προκληθούν σε περιβάλλοντα ομίχλης με περιορισμένους πόρους. Ωστόσο, ο αντίκτυπος αυτός είναι μικρός, καθώς οι καθυστερήσεις δεν είναι αρκετά σημαντικές ώστε να επηρεάζουν ουσιαστικά την εμπειρία του χρήστη.

Εφαρμοσιμότητα

- Η διόρθωση τρωτοτήτων αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε πολλά υπάρχοντά περιβάλλοντα ομίχλης, αλλά οι μεγάλες απαιτήσεις σε πόρους μπορεί να δημιουργήσει κάποιες δυσκολίες σε πιο σύνθετα συστήματα.
- Το Αντιβιοτικό 2.0 αξιολογείται με 2, διότι σε περιβάλλοντα ομίχλης στηρίζεται σε πράγματα που είτε δεν ισχύουν πάντοτε (π.χ. σταθερή συνδεσιμότητα) είτε απαιτούν επιπρόσθετους μηχανισμούς για να υποστηριχθούν (π.χ. ένας μηχανισμός παρακολούθησης εμπιστοσύνης των κόμβων). Επιπλέον, το αντίμετρο μπορεί να θεωρηθεί ότι δεν πρέπει να εγκατασταθεί σε ένα περιβάλλον ομίχλης, διότι δεν προστατεύει τους κόμβους ομίχλης και αν αυτοί παραβιαστούν, θα οδηγήσει σε πολύ αρνητικές επιπτώσεις στην ασφάλεια του συστήματος.
- Το DropStore αξιολογείται με 2, διότι η πολυπλοκότητα και οι απαιτήσεις σε πόρους μπορούν να δυσκολέψουν την εφαρμογή σε υπάρχοντα περιβάλλοντα ομίχλης, απαιτώντας πολλές προσαρμογές του συστήματος.
- Το DRTHIS αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε περιβάλλοντα ομίχλης, αλλά οι απαιτήσεις σε πόρους και υποδομή που απαιτούν οι αλγόριθμοι βαθιάς μάθησης για την συνεχή εκπαίδευση των μοντέλων ενδέχεται να περιορίζουν την υλοποίηση σε όλα τα περιβάλλοντα ομίχλης.
- Το MacLeR αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε πολλά περιβάλλοντα ομίχλης, άλλα η ανάγκη για επιπλέον πόρους και η πολυπλοκότητα στη διαχείριση και συντήρηση του αντιμέτρου μπορεί να αυξήσει τις δυσκολίες εφαρμογής.

Βαθμός κάλυψης

- Η διόρθωση τρωτοτήτων αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε πολλά διαφορετικά περιβάλλοντα και σενάρια, καλύπτοντας τις περισσότερες περιπτώσεις. Αν και μπορεί να υπάρχουν λίγες περιπτώσεις όπου η διακοπή υπηρεσίας δεν είναι ανεκτή, ιδιαίτερα εφόσον πραγματοποιείται για μεγάλο χρονικό διάστημα, αλλά αυτό το ζήτημα μπορεί να αντιμετωπιστεί μέσω της σταδιακής εφαρμογής των επιδιορθώσεων και των ανανεώσεων, που είναι μια γνωστή πρακτική για την αποφυγή μεγάλων διακοπών και την εύκολη επιστροφή στην προηγούμενη κατάσταση σε περίπτωση αποτυχίας.
- Το Αντιβιοτικό 2.0 αξιολογείται με 3, διότι καλύπτει πολλά περιβάλλοντα και διαφορετικά σενάρια, αλλά περιορίζεται όταν εμπλέκονται πολλές ετερογενείς συσκευές και συγκεκριμένα δεν προστατεύει πάντα τους κόμβους ομίχλης.
- Το DropStore αξιολογείται με 4, διότι μπορεί να εφαρμοστεί σε ποίκιλλα περιβάλλοντα, αλλά απαιτείται σωστός συντονισμός των πόρων για την πλήρη εκμετάλλευση των δυνατοτήτων του.
- Το DRTHIS αξιολογείται με 4, διότι το σύστημα μπορεί να προσαρμοστεί σε διάφορα περιβάλλοντα και σενάρια με IoT συσκευές και κόμβους ομίχλης, καλύπτοντας αρκετές περιπτώσεις χρήσης.
- Το MacLeR αξιολογείται με 3, διότι μπορεί να εφαρμοστεί σε ποίκιλες αρχιτεκτονικές SoC και περιβάλλοντα, αλλά δεν είναι εξίσου αποτελεσματικό σε όλα τα σενάρια (π.χ. όταν οι δούρειοι ίπποι ενεργοποιούνται στιγμιαία), καθώς και η περιορισμένη ακρίβειά του δεν είναι πάντοτε (π.χ. λόγω γήρανσης των συσκευών).

Επεκτασιμότητα

- Η διόρθωση τρωτοτήτων αξιολογείται με 4, διότι διάφορες επεκτάσεις της λειτουργικότητας μπορούν να γίνουν στο μέλλον για την κάλυψη διαφορετικών απαιτήσεων (όπως η έξυπνη εκφόρτωση των νέων εκδόσεων).
- Το Αντιβιοτικό 2.0 αξιολογείται με 5, διότι επιτρέπει την ενσωμάτωση νέων λειτουργιών και μπορεί να προσαρμοστεί σε νέες απαιτήσεις.
- Το DropStore αξιολογείται με 3, διότι η υπάρχουσα υποδομή καλύπτει τις βασικές ανάγκες χωρίς να προσφέρει σημαντικές προοπτικές για περαιτέρω ενσωμάτωση νέων λειτουργιών. Ωστόσο, θα μπορούσαν να γίνουν κάποιες επεκτάσεις, αν και αυτές ενδέχεται να απαιτούν σημαντικό χρόνο για την υλοποίηση τους. Παραδείγματα αυτών των επεκτάσεων περιλαμβάνουν την έξυπνη διαμόρφωση του αντιμέτρου, την ικανότητα αυτό-διαμόρφωσης ανάλογα με τις συνθήκες και την έξυπνη επιλογή του κατάλληλου αντιγράφου για την επαναφορά.
- Το DRTHIS αξιολογείται με 3, διότι, ενώ έχει την ικανότητα να προσφέρει βελτιώσεις στο υπάρχον σύστημα, η εστίαση γίνεται σε συγκεκριμένο είδος επιθέσεων, κάτι που περιορίζει τη δυνατότητα προσθήκης νέων λειτουργιών. Αντί για νέες λειτουργίες, μπορεί να γίνει χρήση επιπλέον δεδομένων για την καλύτερη αντιμετώπιση αυτών των επιθέσεων.
- Το MacLeR αξιολογείται με 3, διότι μπορεί να εισάγει νέες λειτουργίες και να επεκτείνεται μελλοντικά, αλλά μπορεί να είναι περίπλοκη και χρονοβόρα η επέκταση αυτή λόγω των ιδιαίτερων χαρακτηριστικών των IoT συσκευών.

Πίνακας 8 - Πίνακας σύγκρισης των αντιμέτρων για την αντιμετώπιση κακόβουλου λογισμικού στον ομιχλώδη προγραμματισμό

Αντίμετρα	**Κατανά-λωση πόρων**	**Κλιμακω-σιμότητα**	**Ασφάλεια δεδομένων**	**Ευκολία χρήσης**	**Εκπαίδευση χρηστών**	**Αντίκ-τυπος στον χρήστη**	**Εφαρμο-ιμότητα**	**Βαθμός κάλυψης**	**Επεκασιμότητα**
Διόρθω-σεις τρωτοτήτων	3-4	4	3	2-4	3-4	3	4	4	4
Αντιβιοτικό 2.0	2	3	4	4	3	3	2	3	5
DropStore	2	4	3	3	3	2	2	4	3
DRTHIS	2	4	3	4	2	2	3	4	3
MacLeR	3	4	3	3	2	3	3	3	3

Με βάση τον παραπάνω πίνακα έχουμε μπορούμε να προχωρήσουμε σε ανάλυση των καλύτερων και των χειρότερων αντιμέτρων για κάθε κριτήριο:

Ανάλυση καλύτερου και χειρότερου αντιμέτρου ανά κριτήριο: Θα εντοπίσουμε ποιο/-α αντίμετρο/-α έχει την καλύτερη και την χειρότερη απόδοση σε κάθε κριτήριο αξιολόγησης:

- Κατανάλωση πόρων:
  - Καλύτερο: διόρθωση τρωτοτήτων (3-4)
  - Χειρότερο: Αντιβιοτικό 2.0, DropStore, DRTHIS (2)
- Κλιμακωσιμότητα:
  - Καλύτερο: διόρθωση τρωτοτήτων, DropStore, DRTHIS, MacLeR (4)
  - Χειρότερο: Αντιβιοτικό 2.0 (3)
- Ασφάλεια δεδομένων:
  - Καλύτερο: Αντιβιοτικό 2.0 (4)
  - Χειρότερο: διόρθωση τρωτοτήτων, DRTHIS, MacLeR (3)
- Ευκολία χρήσης:
  - Καλύτερο: Αντιβιοτικό 2.0, DRTHIS (4)
  - Χειρότερο: DropStore, MacLeR (3)
- Εκπαίδευση χρηστών:
  - Καλύτερο: Αντιβιοτικό 2.0, DropStore (3)
  - Χειρότερο: MacLeR, DRTHIS (2)
- Αντίκτυπος στον χρήστη:
  - Καλύτερο: διόρθωση τρωτοτήτων, Αντιβιοτικό 2.0, MacLeR (3)

- Χειρότερο: DropStore, DRTHIS (2)

❖ Εφαρμοσιμότητα:
- Καλύτερο: διόρθωση τρωτοτήτων (4)
- Χειρότερο: Αντιβιοτικό 2.0, DropStore (2)

❖ Βαθμός κάλυψης:
- Καλύτερο: διόρθωση τρωτοτήτων, DRTHIS, DropStore (4)
- Χειρότερο: Αντιβιοτικό 2.0, MacLeR (3)

❖ Επεκτασιμότητα:
- Καλύτερο: Αντιβιοτικό 2.0 (5)
- Χειρότερο: DropStore, DRTHIS, MacLeR (3)

Καλύτερο και χειρότερο αντίμετρο συνολικά (στην κατηγόρια): διόρθωση τρωτοτήτων: 30-34, Αντιβιοτικό 2.0: 29, DropStore: 26, DRTHIS: 27, MacLeR: 27. Επομένως, η διόρθωση τρωτοτήτων με εύρος τιμών 30-34 είναι το καλύτερο αντίμετρο συνολικά, ενώ το χειρότερο αντίμετρο συνολικά είναι το DropStore με βαθμολογία 26.

Αντίμετρο με καλύτερη και χειρότερη απόδοση: Για την καλύτερη και χειρότερη απόδοση, πρέπει να εξετάσουμε την απόδοση των αντιμέτρων σε κάθε κριτήριο και να καταλήξουμε στο καλύτερο και το χειρότερο αντίμετρο βασιζόμενοι στο ποσοστό των υψηλών ή των χειρότερων βαθμολογίων τους που έχουν λάβει στα κριτήρια. Θεωρούμε υψηλές τιμές το 4 και 5 και χειρότερες τιμές το 1 και 2. Τα εύρη τιμών δεν συμπεριλαμβάνονται στον παρών υπολογισμό.

Ποσοστά υψηλών και χαμηλών βαθμολογιών:

- Διόρθωση τρωτοτήτων:
  - Υψηλές: 4/9 = 44,4 %
  - Χαμηλές: 0/9 = 0 %
- Αντιβιοτικό 2.0:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 2/9 = 22,2 %
- DropStore:
  - Υψηλές: 2/9 = 22,2 %
  - Χαμηλές: 3/9 = 33,3 %
- DRTHIS:
  - Υψηλές: 3/9 = 33,3 %
  - Χαμηλές: 3/9 = 33,3 %
- MacLeR:
  - Υψηλές: 1/9 = 11,1 %
  - Χαμηλές: 1/9 = 11,1 %

Το αντίμετρο με την καλύτερη απόδοση είναι η διόρθωση τρωτοτήτων, καθώς έχει ποσοστό 44,4 % υψηλών βαθμολογίων. Το αντίμετρο με την χειρότερη απόδοση είναι το DropStore, καθώς έχει ποσοστό 33,3 % χαμηλότερων βαθμολογίων.

5.3.8 Καθολική σύγκριση

Σε έναν κόσμο που οι τρωτότητες, οι απειλές και οι επιθέσεις στον ομιχλώδη προγραμματισμό αυξάνονται, η επιλογή των κατάλληλων αντιμέτρων για την αντιμετώπιση των επιθέσεων είναι κρίσιμη. Η αποτελεσματικότητα των αντιμέτρων εξαρτάται από την ισορροπία που αυτά επιτυγχάνουν μεταξύ της ασφάλειας, της αποδοτικότητας και της πρακτικής εφαρμοσιμότητας. Ορισμένα βασικά κριτήρια που επηρεάζουν την επιλογή των αντιμέτρων περιλαμβάνουν την κατανάλωση πόρων, την επεκτασιμότητα, τον αντίκτυπο στον χρήστη και η ευκολία χρήσης. Στην συνέχεια αναλύονται τα καλύτερα και τα χειρότερα αντίμετρα με βάση τα κριτήρια σύγκρισης που έχουμε θέσει, καθώς και τα κριτήρια σύγκρισης που επιδεικνύουν την μέγιστη και την ελάχιστη απόδοση σε καθολικό επίπεδο, δηλαδή ανεξάρτητα από την εκάστοτε κατηγόρια ένταξης των αντιμέτρων.

Αρχικά, τα αντίμετρα που βασίζονται στην διαχείριση πρόσβασης, όπως το RBAC και το ABAC θεωρούνται από τα πλέον αποδοτικά εργαλεία προστασίας. Αυτά τα συστήματα διαχείρισης πρόσβασης παρέχουν υψηλά επίπεδα ασφάλειας δεδομένων και ευελιξία, ενώ παράλληλα είναι σε θέση να κλιμακωθούν αποτελεσματικά σε μεγάλα και πολυσύνθετα δίκτυα. Ειδικότερα, το RBAC προσφέρει σαφή δομή στη διαχείριση της πρόσβασης, βασισμένο σε ρόλους που ανατίθενται σε χρήστες, κάτι που το καθιστά ιδανικό για περιβάλλοντα με πολλά επίπεδα εξουσιοδότησης. Από την άλλη πλευρά, το ABAC, το οποίο βασίζεται σε ιδιότητες παρέχει ακόμη μεγαλύτερη ευελιξία και λεπτομερή έλεγχο πρόσβασης, καθιστώντας το εξαιρετικά αποτελεσματικό σε περίπλοκα περιβάλλοντα. Αυτά τα δύο συστήματα διασφαλίζουν ότι μόνο οι κατάλληλοι χρήστες έχουν πρόσβαση σε κρίσιμα δεδομένα, μειώνοντας έτσι τον κίνδυνο των εσωτερικών και των εξωτερικών απειλών.

Αντίθετα, υπάρχουν αντίμετρα που δεν αποδεικνύονται εξίσου αποτελεσματικά. Το IoTCop και η τεχνική MLTKNN αποτελούν δύο αντίμετρα που παρουσιάζουν σημαντικές αδυναμίες στην εφαρμογή τους, ιδίως όταν χρησιμοποιούνται σε περιβάλλοντα που απαιτούν γρήγορη αντίδραση για την αντιμετώπιση των απειλών και ευελιξία. Ενώ και τα δύο αυτά αντίμετρα έχουν σχεδιαστεί με σκοπό την ενίσχυση της ασφάλειας των συστημάτων, στην πράξη συχνά αποδεικνύονται αναποτελεσματικά, καθώς δεν καταφέρνουν να καλύψουν πλήρως τις απαιτήσεις των σύγχρονων δικτύων. Η εφαρμογή τους μπορεί να προκαλέσει καθυστερήσεις και να περιορίσει την απόδοση του συστήματος, ενώ ταυτόχρονα δεν παρέχουν την απαιτούμενη ασφάλεια σε υψηλού επιπέδου επιθέσεις. Αυτή η αποτυχία στην αποτελεσματικότητα των λύσεων δημιουργεί πρόσθετα προβλήματα στους οργανισμός, οι οποίοι χρειάζονται γρήγορες και αξιόπιστες λύσεις για την προστασία των δεδομένων τους.

Όσον αφορά τα κριτήρια με την καλύτερη δυνατή απόδοση, ένα από τα ισχυρότερα στοιχεία σε πολλές λύσεις είναι η ασφάλεια των δεδομένων. Πολλά από τα εξεταζόμενα αντίμετρα, όπως τα υβριδικά IDS και το MFA, προσφέρουν υψηλή ασφάλεια, γεγονός που καθιστά ανεκτίμητα για τους οργανισμούς που δίνουν προτεραιότητα στην προστασία των ευαίσθητων πληροφοριών τους. Η υψηλή απόδοση στο κριτήριο της ασφάλειας των δεδομένων προκύπτει από την ικανότητα των

σύγχρονων αντιμέτρων να ανταποκριθούν στις αυξημένες απαιτήσεις προστασίας των πληροφοριών. Οι λύσεις που εστιάζουν στην ασφάλεια των δεδομένων αξιοποιούν πολυδιάστατες τεχνικές ανίχνευσης και πρόληψης, ενσωματώνοντας ενισχυμένα συστήματα ελέγχου και παρακολούθησης σε όλα επίπεδα του δικτύου του ομιχλώδους προγραμματισμού. Αυτό επιτρέπει την γρήγορη αναγνώριση των απειλών και την εξάλειψη των δεδομένων. Επομένως, οι οργανισμοί που επικεντρώνονται στην ασφάλεια των δεδομένων μπορούν να επωφεληθούν από μια περισσότερο ανθεκτική υποδομή, η οποία ενισχύει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, προστατεύοντας τα ευαίσθητα στοιχεία τους από μη εξουσιοδοτημένη πρόσβαση ή επιθέσεις.

Αντίθετα, το κριτήριο της κατανάλωσης πόρων εμφανίζεται συχνά ως ένας από τους πιο περιοριστικούς παράγοντες για πολλά αντίμετρα, καθώς απαιτούν σημαντική υπολογιστική ισχύ και μνήμη για να λειτουργήσουν αποτελεσματικά. Αυτό συμβαίνει, διότι πολλές τεχνικές ασφάλειας βασίζονται σε σύνθετους αλγορίθμους ή διαδικασίες που απαιτούν συνεχείς υπολογισμούς και συχνή ανάλυση δεδομένων. Καθώς οι πόροι του συστήματος (όπως η CPU και η μνήμη) είναι περιορισμένοι, η αυξημένη κατανάλωση τους μπορεί να προκαλέσει επιβράδυνση της απόδοσης του συστήματος ή ακόμα και να το καθιστά μη βιώσιμο για οργανισμούς που διαθέτουν περιβάλλοντα ομίχλης με περιορισμένους πόρους. Αυτό, περιορίζει την ευχρηστία των λύσεων αυτών, ιδίως σε μικρότερες επιχειρήσεις ή σε περιβάλλοντα με απαιτήσεις απόδοσης και ταχύτητας. Για παράδειγμα, τα αντίμετρα, όπως τα IPS και η ομομορφική κρυπτογράφηση απαιτούν μεγάλη επεξεργαστική ισχύ και υψηλή κατανάλωση πόρων για να λειτουργήσουν αποτελεσματικά. Παρόλο που τα αντίμετρα, όπως είδαμε παρέχουν υψηλό επίπεδο ασφάλειας, ορισμένα από αυτά συχνά δεν είναι βιώσιμα για μικρότερες επιχειρήσεις ή οργανισμούς με περιβάλλοντα που διαθέτουν περιορισμένους πόρους.

Η ευκολία χρήσης είναι ένα άλλο κριτήριο που επηρεάζει την απόδοση ορισμένων αντιμέτρων, ειδικότερα όταν η απόδοση δεν είναι αναμενόμενη εξαιτίας της πολυπλοκότητας της εφαρμογής ή της διαχείρισης των αντιμέτρων αυτών. Όταν ένα αντίμετρο απαιτεί εξειδικευμένες γνώσεις ή πολύπλοκες διαδικασίες για την εφαρμογή και την διαχείριση του, η υιοθέτηση του γίνεται πιο δύσκολη και χρονοβόρα. Σε πολλές περιπτώσεις, αυτό μπορεί να οδηγήσει σε καθυστερήσεις στην αντίδραση και στην αποδοτικότητα του συστήματος, καθώς οι οργανισμοί που δεν διαθέτουν επαρκή τεχνογνωσία ή εξειδικευμένο προσωπικό ενδέχεται να μην μπορούν να εκμεταλλευτούν πλήρως τα διαθέσιμα εργαλεία ασφάλειας. Επιπλέον, η έλλειψη κατάλληλης εκπαίδευσης για την χρήση αυτών των συστημάτων μπορεί να μειώσει την ταχύτητα ανίχνευσης και απόκρισης στις επιθέσεις, επηρεάζοντας τελικά την αποτελεσματικότητα και την αποδοτικότητα του συνολικού συστήματος. Για αυτόν τον λόγο, όταν τα αντίμετρα παρουσιάζουν χαμηλή απόδοση σε αυτό το κριτήριο, οι οργανισμοί μπορεί να βρουν δύσκολη την συνεχιζόμενη χρήση ή την ενσωμάτωση τους στην καθημερινή λειτουργία τους, γεγονός που μπορεί να καταστήσει την εφαρμογή τους μη βιώσιμη σε βάθος χρόνου.

Η επιλογή των κατάλληλων αντιμέτρων είναι καθοριστικής σημασίας για την προστασία των πληροφοριακών συστημάτων στον ομιχλώδη προγραμματισμό. Λύσεις, όπως το RBAC και το

ABAC, προσφέρουν μια σταθερή ισορροπία μεταξύ της ασφάλειας και της ευκολίας χρήσης, καθιστώντας τα ιδανικά για την προστασία μεγάλων δικτύων. Αντίθετα, η κατανάλωση πόρων και η ευκολία χρήσης εξακολουθούν να αποτελούν προκλήσεις για ορισμένα εξειδικευμένα αντίμετρα, αναδεικνύοντας την σημασία της προσαρμοσμένης επιλογής λύσεων που μπορούν να ανταποκριθούν στις ανάγκες και τους περιορισμούς κάθε οργανισμού.

Ωστόσο, είναι σημαντικό να σημειώσουμε ότι, για την αποτελεσματική προστασία, είναι αναγκαία η χρήση πολλαπλών αντιμέτρων, δημιουργώντας έτσι μια πολύ-επίπεδη άμυνα. Κάθε αντίμετρο μπορεί να εξειδικεύεται σε διαφορετικές απειλές και επιθέσεις, αλλά αυτό μπορεί να οδηγήσει αυξημένη κατανάλωση πόρων, μειωμένη κλιμακωσιμότητα και προκλήσεις στην εφαρμοσιμότητα. Ο συνδυασμός αυτών των παραμέτρων μπορεί να επιβαρύνει το σύστημα, καθιστώντας την απόδοση των αντιμέτρων λιγότερο ικανοποιητική σε μεγάλη κλίμακα. Συνεπώς, η έρευνα πρέπει να επικεντρωθεί είτε στην βελτίωση του συνδυασμού των αντιμέτρων, ώστε να περιοριστούν οι αρνητικές επιπτώσεις στην απόδοση, είτε στην ανάπτυξη νέων αντιμέτρων με καλύτερη συνολική απόδοση, που θα είναι σε θέση να καλύψουν μια ευρύτερη γκάμα επιθέσεων και απειλών χωρίς να επιβαρύνουν υπερβολικά τους πόρους του συστήματος.

6 *Προκλήσεις*

Η ασφάλεια έχει ζωτική σημασία σε όλους τους τομείς. Για να εξασφαλίσουμε την αποστολή και αποθήκευση δεδομένων με ασφάλεια απαιτείται η συμμόρφωση με προκαθορισμένα πρωτόκολλα ασφάλειας και η λήψη μέτρων για την προστασία των συστημάτων από διάφορες επιθέσεις. Ωστόσο, η έρευνα στο μέλλον καλείται να αντιμετωπίσει σημαντικές προκλήσεις που σχετίζονται με την ολοένα και αυξανόμενη πολυπλοκότητα των συστημάτων ασφάλειας και των απειλών. Μεταξύ των βασικών προκλήσεων είναι η διαχείριση της ασφάλειας σε αποκεντρωμένα περιβάλλοντα, όπως τα περιβάλλοντα ομίχλης, καθώς και η αντιμετώπιση επιθέσεων που χρησιμοποιούν την μηχανική μάθηση. Παράλληλα, οι ερευνητικές κατευθύνσεις που φαίνονται πιο υποσχόμενες περιλαμβάνουν την ανάπτυξη καινοτόμων τεχνικών ανίχνευσης απειλών, την ενίσχυση της ιδιωτικότητας μέσω προηγμένων κρυπτογραφικών μεθόδων, καθώς και την διασφάλιση της ακεραιότητας και της διαθεσιμότητας των δεδομένων σε ομιχλώδη περιβάλλοντα. Οι τεχνικές που αναφέρονται σε αυτό το κεφάλαιο φαίνεται ότι έχουν ήδη προταθεί και εφαρμόζονται ευρέως, επομένως δεν μπορούν να θεωρηθούν «ερευνητικές κατευθύνσεις». Επιπλέον, η προστασία των συστημάτων ομιχλώδους προγραμματισμού από διάφορες επιθέσεις προϋποθέτει την εφαρμογή αυστηρών κανόνων και πολιτικών ασφάλειας. Στο παρόν κεφάλαιο της διπλωματικής εργασίας παρουσιάζονται τόσο οι βασικές προκλήσεις που παραμένουν στην έρευνα (ενότητες 6.1-6.8) και ερευνητικές κατευθύνσεις αντιμετώπισης τους, καθώς και ορισμένες ερευνητικές κατευθύνσεις γενικής φύσεως (ενότητα 6.9), οι οποίες μπορεί να επιτρέψουν την ταυτόχρονη αντιμετώπιση πολλών προκλήσεων. (Kaviyazhiny, Bala and Gowri, 2021).

6.1 Κοστοβόρα κρυπτογράφηση δεδομένων

Οι βασικές προκλήσεις που θα πρέπει να αντιμετωπίσει η μελλοντική έρευνα στον τομέα της κρυπτογράφησης δεδομένων στον ομιχλώδη προγραμματισμό περιλαμβάνουν αρκετούς κρίσιμους παράγοντες. Καταρχάς, οι περιορισμοί επεξεργαστικής ισχύς των IoT συσκευών αποτελούν έναν κρίσιμο παράγοντα, καθώς οι συσκευές αυτές δεν διαθέτουν επαρκή μνήμη για την τοπική αποθήκευση δεδομένων, ενώ η κρυπτογράφηση εντός των IoT συσκευών δεν συνιστάται. Μια ακόμη σημαντική πρόκληση είναι η επιλογή των δεδομένων προς κρυπτογράφηση. Μόνο τα απαραίτητα ή τα ευαίσθητα δεδομένα θα πρέπει να υποβάλλονται σε κρυπτογράφηση, διότι η κρυπτογράφηση όλων των δεδομένων μπορεί να επιφέρει αρνητικές επιπτώσεις στην αποδοτικότητα του συστήματος. Επιπλέον, η ανάγκη για ισορροπία μεταξύ της λειτουργίας των κόμβων και των τεχνικών ασφάλειας είναι κρίσιμη, καθώς η κρυπτογράφηση δεδομένων απαιτεί αρκετή επεξεργαστική ισχύ και αποθηκευτικό χώρο, γεγονός που μπορεί να επηρεάσει την συνολική απόδοση σε όλα τα επίπεδα. (Kaviyazhiny, Bala and Gowri, 2021)

Οι ερευνητικές κατευθύνσεις που φαίνονται πολλά υποσχόμενες για την αντιμετώπιση αυτών των προκλήσεων που σχετίζονται με την κρυπτογράφηση των δεδομένων στον ομιχλώδη προγραμματισμό περιλαμβάνουν την βελτιστοποίηση των αλγόριθμων κρυπτογράφησης, όπως είναι ο AES και ECC. Αυτή η κατεύθυνση, εφόσον ευδοκιμήσει, θα είναι ιδιαίτερα αποδοτική, καθώς οι επεξεργαστές που χρησιμοποιούνται στα IoT συστήματα απαιτούν χαμηλούς πόρους. Η εστίαση στην αποδοτικότητα των αλγορίθμων κρυπτογράφησης είναι κρίσιμη, έτσι ώστε να εξασφαλιστεί ότι οι περιορισμένες δυνατότητες των IoT συσκευών δεν θα επηρεαστούν αρνητικά. Επίσης, η εφαρμογή πρωτοκόλλων ασφάλειας, όπως το TLS, είναι καθοριστική για την εξασφάλιση της ασφαλούς επικοινωνίας μεταξύ του πελάτη και του διακομιστή, αν και είναι σημαντικό τα πρωτόκολλα αυτά να βελτιστοποιούνται συνεχώς ώστε να απαιτούν μικρότερη υπολογιστική ισχύ και άρα να γίνουν πιο ελαφριά. Η ενίσχυση των μηχανισμών ασφάλειας μέσω των πρωτοκόλλων επικοινωνίας είναι επιτακτική προκειμένου να προστατευτούν τα ευαίσθητα δεδομένα κατά την διάρκεια της μεταφοράς τους. Μια σημαντική κατεύθυνση για το μέλλον θα μπορούσε να περιλαμβάνει την ανάπτυξη μεθόδων συμπίεσης για τα κρυπτογραφημένα δεδομένα, έτσι ώστε να μειωθεί το μέγεθος των δεδομένων που αποστέλλονται και να σωθεί το εύρος ζώνης, αλλά και χώρος που απαιτείται για την αποθήκευση τους, λαμβάνοντας όμως υπόψη την πιθανή επίπτωση στη δυνατότητα επερώτησης αυτών των δεδομένών. Παρά την πρόκληση αυτή, η χρήση κρυπτογραφικών ευρετηρίων μπορεί να προσφέρει μια λύση. Τα κρυπτογραφικά ευρετήρια (cryptographic indexes[7]) επιτρέπουν την διατήρηση της δυνατότητας επερώτησης κρυπτογραφημένων δεδομένων, επιτρέποντας γρήγορη και αποδοτική αναζήτηση χωρίς να απαιτείται η αποκρυπτογράφηση του συνόλου των δεδομένων (Muddumadappa, Anjanappa and Srikantaswamy, 2022). Αυτή η προσέγγιση όχι μόνο θα διευκολύνει την διαχείριση του αποθηκευτικού χώρου των κρυπτογραφημένων δεδομένων, αλλά θα βελτιώσει και την συνολική αποδοτικότητα του συστήματος του ομιχλώδους προγραμματισμού. (Kaviyazhiny, Bala and Gowri, 2021)

6.2 Μη κλιμακώσιμη & αναποτελεσματική παρακολούθηση δικτύου

Στα πλαίσιο του ομιχλώδους προγραμματισμού η παρακολούθηση του δικτύου αποτελεί μια καίρια διαδικασία για την έγκαιρη ανίχνευση κακόβουλων επιθέσεων και την εξασφάλιση της ακεραιότητας των δικτύων. Η συνεχής αύξηση του αριθμού των IoT συσκευών και των δεδομένων που παράγονται από αυτές δημιουργεί σημαντικές προκλήσεις για την αποτελεσματική και

[7] Τα κρυπτογραφικά ευρετήρια είναι μηχανισμοί που επιτρέπουν την αποδοτική εκτέλεση ερωτημάτων σε κρυπτογραφημένα δεδομένα βάσεων δεδομένων, όπως στο μοντέλο Database-as-a-Service. Τα κρυπτογραφικά ευρετήρια χρησιμοποιούν την πιθανότητα εμφάνισης κάθε ερώτησης (query probability) για να οργανώσουν τα δεδομένα σε ξεχωριστές κατηγορίες (buckets), τα οποία επιστρέφουν κάποια ενδιάμεσα αποτελέσματα που φιλτράρονται για εξαχθούν τα τελικά σωστά αποτελέσματα, μειώνοντας έτσι τα σφάλματα, αυξάνοντας την αποδοτικότητα των ερωτημάτων και για να βελτιώσουν την ταχύτητα εκτέλεσης των κρυπτογραφικών ερωτημάτων. (Wei *et al.*, 2009)

κλιμακώσιμη παρακολούθηση και την διαχείριση των δικτυακών πόρων. (Kaviyazhiny, Bala and Gowri, 2021)

Μια από τις κύριες προκλήσεις σχετικά με την παρακολούθηση του δικτύου στα πλαίσια του ομιχλώδους προγραμματισμού αφορά την διαχείριση του μεγάλου αριθμού των κόμβων ομίχλης και των δεδομένων που παράγονται από τις IoT συσκευές. Αν και η ποσότητα των δεδομένων που παράγεται από κάθε IoT συσκευή είναι σχετικά μικρή, ο τεράστιος όγκος δεδομένων που προκύπτει από τον συνδυασμό πολλών IoT συσκευών και κόμβων ομίχλης, καθιστά την συνολική διαχείριση και την επεξεργασία των δεδομένων ιδιαιτέρως απαιτητική από την άποψη των υπολογιστικών πόρων και της ταχύτητας επεξεργασίας. Επιπλέον, η συνεχής παρακολούθηση του δικτύου για την ανίχνευση πιθανών ανωμαλιών αποτελεί μία ακόμη πρόκληση, δεδομένου ότι το επίπεδο ομίχλης διαχειρίζεται ευαίσθητα και ιδιωτικά δεδομένα. Αυτό καθιστά αναγκαία την αυτοματοποιημένη επιβολή βέλτιστων κανόνων και πολιτικών ασφάλειας, προκειμένου να αποτρέπονται οι κακόβουλες ενέργειες και να διασφαλίζεται η προστασία των δεδομένων. (Kaviyazhiny, Bala and Gowri, 2021)

Σε ότι αφορά τις ερευνητικές κατευθύνσεις, η ενσωμάτωση των τεχνητών νευρικών δικτύων ANN (Artificial Neural Networks) και των τεχνικών ανίχνευσης κακόβουλης συμπεριφοράς μέσω κανόνων αναδεικνύεται ως μια πολλά υποσχόμενη προσέγγιση για την ανίχνευση απειλών σε μεγάλα και ετερογενή δίκτυα. Αυτή η μέθοδος ενισχύει την ακρίβεια και την αποτελεσματικότητα της ανίχνευσης, καθώς τα ANN δεν είναι μόνο κλιμακώσιμα αλλά μπορούν να αναγνωρίζουν πρότυπα ανωμαλιών και νέων απειλών, ενώ οι τεχνικές αντιστοίχισης κανόνων βοηθούν στην άμεση ταυτοποίηση γνωστών κακόβουλων ενεργειών. Ακόμα, η υλοποίηση εικονικών ιδιωτικών δικτύων (Virtual Private Networks -VPNs) θεωρείται κρίσιμη για την απομόνωση του δικτύου σε εξωτερικές απειλές. Τα VPNs συμβάλλουν σημαντικά στην ενίσχυση της ασφάλειας και της προστασίας των δεδομένων, διασφαλίζοντας την ακεραιότητα του δικτύου και την αποτροπή εξωτερικών επιθέσεων. Τέλος, για την αντιμετώπιση της συνεχής παρακολούθησης του δικτύου για την ανίχνευση πιθανών ανωμαλιών απαιτείται η ανάγκη ανάπτυξης μιας μεθόδου αυτοματοποιημένης επιβολής βέλτιστων κανόνων και πολιτικών ασφάλειας, προκειμένου να αποτρέπονται οι κακόβουλες ενέργειες και να διασφαλίζεται η προστασία των δεδομένων (Kaviyazhiny, Bala and Gowri, 2021)

6.3 Ανεπαρκής προστασία από κακόβουλο λογισμικό

Η προστασία από κακόβουλο λογισμικό σε περιβάλλοντα ομίχλης αναδεικνύει σημαντικές προκλήσεις, καθώς και προοπτικές για μελλοντική έρευνα. Οι σύγχρονες επιθέσεις κακόβουλου λογισμικού γίνονται ολοένα και πιο περίπλοκες, καθιστώντας δύσκολη την ανίχνευση τους και την ανάπτυξη αποδοτικών αμυντικών μηχανισμών. Η έλλειψη σύγχρονων και αποδοτικών μεθόδων ανίχνευσης απειλών μειώνει την ικανότητα των συστημάτων ομιχλώδους προγραμματισμού να αντιμετωπίσουν νέες μορφές κακόβουλου λογισμικού, γεγονός που αυξάνει την ευπάθεια τους. Επιπλέον, οι κίνδυνοι που σχετίζονται με κενά ασφάλειας, όπως είναι οι επιθέσεις μηδενικής ημέρας (zero day), που δεν έχουν ακόμη αναγνωριστεί και η δυνατότητα εκμετάλλευσης τους από

επιτιθέμενους, μπορούν να οδηγήσουν σε έκχυση κακόβουλου λογισμικού, αποτελώντας σοβαρούς κινδύνους για την ασφάλεια των περιβαλλόντων ομίχλης. Η πολυμορφία και η κατανομή των συνδεδεμένων συσκευών, όπως κινητών τηλεφώνων και τάμπλετ, αυξάνουν την πιθανότητα μόλυνσης και της διάδοσης κακόβουλου λογισμικού, καθιστώντας την προστασία τους πιο περίπλοκη. Πολλά συστήματα ομιχλώδους προγραμματισμού δεν διαθέτουν αρκετούς μηχανισμούς προστασίας από κακόβουλο λογισμικό, κυρίως λόγω της ανάγκης για συνεχή κατανομή υπολογιστικών και δικτυακών πόρων, κάτι που μπορεί να μην είναι εφικτό σε κάθε περίπτωση. (Khan, Parkinson and Qin, 2017)

Από την άλλη πλευρά, οι υποσχόμενες ερευνητικές κατευθύνσεις περιλαμβάνουν την ανάπτυξη φυσικών συσκευών ανίχνευσης κακόβουλου λογισμικού, οι οποίες μπορούν να τοποθετηθούν σε κομβικά σημεία του δικτύου ομίχλης με χαμηλό κόστος αγοράς και εγκατάστασης. Αυτές οι συσκευές προσφέρουν λύσεις με ισχυρές υπολογιστικές δυνατότητες, οι οποίες απαιτούν ελάχιστους πόρους από τον ομιχλώδη προγραμματισμό, ενισχύοντας με αυτόν τον τρόπο την ασφάλεια των συστημάτων χωρίς να επιβαρύνουν την υποδομή τους. Η χρήση τεχνικών μηχανικής μάθησης διαθέτει την ικανότητα να ανιχνεύουν επιθέσεις μηδενικής ημέρας με μεγαλύτερη ακρίβεια λόγω της εστίασης τους στη δυναμική συμπεριφορά, αποτρέποντας την έκχυση κακόβουλου λογισμικού ή σε περιπτώσεις που αυτό δεν είναι εφικτό, εντοπίζοντας την ύπαρξη του στο σύστημα (π.χ. σε έναν κόμβο) ώστε να ακολουθήσει η εξάλειψη ή η μεταφορά του σε καραντίνα. Αυτές οι τεχνικές ουσιαστικά εκπαιδεύουν αλγόριθμους, όπως είναι οι Μηχανές Διανυσμάτων Υποστήριξής (Support Vectors Machines - SVMs), με ένα μοντέλο κανονικού λογισμικού και στην συνέχεια οποιαδήποτε ανώμαλη συμπεριφορά (από ένα λογισμικό) μπορεί να προκαλέσει την ενεργοποίηση του μηχανισμού ανίχνευσης. Επομένως, είναι σημαντικό να πραγματοποιείται συνεχής έλεγχος για κακόβουλο λογισμικό ή ακόμη και για κακόβουλους κόμβους ομίχλης και να αναπτύσσονται μηχανισμοί ασφάλειας για την αποτροπή κακόβουλων κόμβων και συσκευών από τελικούς χρήστες του ομιχλώδους περιβάλλοντος, προκειμένου να διασφαλιστεί η καλύτερη προστασία του περιβάλλοντος και των IoT συσκευών. Ιδιαίτερα, στον τομέα της υγειονομικής περίθαλψης, η εφαρμογή ισχυρών ελέγχων ακεραιότητας και η απομόνωση του συστήματος σε περίπτωση κακόβουλης δραστηριότητας είναι καίριας σημασίας για την προστασία κρίσιμων δεδομένων. Τέλος, η χρήση αντιβιοτικών και αντιϊκών νέας γενιάς με βελτιώσεις όσον αφορά την αποδοτικότητα στην κατανάλωση πόρων, θα μπορούσε να αποτελέσει μια πολλά υποσχόμενη κατεύθυνση για το μέλλον.(Khan, Parkinson and Qin, 2017)

6.4 Ανασφάλεια ασύρματων δικτύων

Η ταχεία ανάπτυξη του ομιχλώδους προγραμματισμού και η ενσωμάτωση των IoT συσκευών σε κρίσιμες εφαρμογές, όπως είναι η υγειονομική περίθαλψη, δημιουργούν νέες προκλήσεις στον τομέα της ασφάλειας των ασύρματων δικτύων των περιβαλλόντων ομίχλης. Οι IoT συσκευές, όπως είναι οι αισθητήρες και οι κάμερες, συνδέονται σε περιβάλλοντα ομίχλης, έτσι ώστε να στείλουν τα δεδομένα τους σε κοντινούς κόμβους ομίχλης κυρίως με ασύρματο τρόπο. Αυτή η κατανεμημένη φύση των δικτύων του ομιχλώδους προγραμματισμού ενέχει κινδύνους, όπως οι παρεμβολές στις επικοινωνίες, οι επιθέσεις DDoS, η εισαγωγή κακόβουλων κόμβων κ.α.. Συνεπώς, η ασφάλεια των

δεδομένων και των σημείων πρόσβασης (access point) των περιβαλλόντων ομίχλης μειώνεται και άρα γίνονται αυτά ακόμη πιο ευάλωτα σε επιθέσεις. (Kaviyazhiny, Bala and Gowri, 2021)

Μια από τις βασικότερες προκλήσεις αφορά την ασφάλεια των ασύρματων δικτύων των περιβαλλόντων ομίχλης. Τα σημεία πρόσβασης είναι ορατά σε όλες τις κοντινές συσκευές γεγονός που τα καθιστά ευάλωτα σε επιθέσεις, όπως είναι οι σύβυλες επιθέσεις (sybil attacks) και οι επιθέσεις πλημμύρας (flood attacks). Οι επιθέσεις αυτές όχι μόνο διαταράσσουν την λειτουργία του δικτύου, αλλά επιβαρύνουν και το εύρος ζώνης του δικτύου, προκαλώντας σημαντική υποβάθμιση της ποιότητας των υπηρεσιών του. Η αδυναμία εξασφάλισης ασφαλών σημείων πρόσβασης αποτελεί σοβαρό κίνδυνο για το συνολικό σύστημα του ομιχλώδους προγραμματισμού. Πιο συγκεκριμένα, η ύπαρξη ενός αδύνατου σημείου πρόσβασης αυξάνει την πιθανότητα εισβολής, δημιουργώντας τρωτά σημεία που μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. (Kaviyazhiny, Bala and Gowri, 2021)

Η ασφάλεια των δεδομένων σε κρίσιμες εφαρμογές, όπως η παρακολούθηση της υγείας, αποτελεί μία ακόμα πρόκληση. Τα δεδομένα των ασθενών είναι πολύ ευαίσθητα και η μετάδοση τους μέσω μη ασφαλών δικτύων μπορεί να έχει σοβαρές συνέπειες. Μικρές αλλοιώσεις ή παραποιήσεις των δεδομένων υγείας μπορούν να οδηγήσουν σε λανθασμένες διαγνώσεις ή και λήψη αποφάσεων που θέτουν σε κίνδυνο την ζωή των ασθενών. Τέλος, η διατήρηση της ασφάλειας σε ένα περιβάλλον ομίχλης είναι δύσκολη, λόγω της διασποράς των συσκευών που αποτελούν το δίκτυο. (Kaviyazhiny, Bala and Gowri, 2021)

Προκειμένου να αντιμετωπιστούν οι παραπάνω προκλήσεις, η μελλοντική έρευνα πρέπει να εστιάσει σε συγκεκριμένες ερευνητικές κατευθύνσεις που εμφανίζονται ως οι πιο υποσχόμενες. Η μελλοντική έρευνα πρέπει να επικεντρωθεί στην ανάπτυξη ασφαλών πρωτοκόλλων και τεχνικών, προκειμένου να αντιμετωπιστούν αυτές οι προκλήσεις. Πρώτον, η χρήση ισχυρότερων, αλλά ελαφρύτερων αλγορίθμων ασφάλειας σε Wi-Fi δίκτυα που θα διασφαλίσουν την κρυπτογράφηση των δεδομένων κατά την μετάδοση τους, είναι ιδιαίτερα σημαντική σε κρίσιμους τομείς όπως η υγεία, όπου η ακρίβεια και η ακεραιότητα των δεδομένων είναι ύψιστης σημασίας. Μια άλλη πολλά υποσχόμενη ερευνητική κατεύθυνση είναι η μείωση της εσωτερικής και της εξωτερικής ασύρματης επικοινωνίας μεταξύ των τελικών συσκευών και της πλατφόρμας ομίχλης. Η μείωση των ασύρματων μεταδόσεων μπορεί να συμβάλλει σημαντικά στην ελαχιστοποίηση των τρωτών σημείων που εκτίθενται σε πιθανές επιθέσεις, προσφέροντας παράλληλα βελτιωμένη απόδοση και αποτελεσματικότητα στο σύστημα. Ωστόσο, αυτή η προσέγγιση ενέχει και ορισμένους κινδύνους, όπως η ενδεχόμενη επιδείνωση της υποστήριξης της κινητικότητας, καθώς και η πιθανότητα απομόνωσης των IoT συσκευών σε περιπτώσεις που απαιτείται συνεχής σύνδεση. Επίσης, η μείωση των ασύρματων μεταδόσεων μπορεί να περιορίσει το συνολικό εύρος ζώνης του δικτύου, γεγονός που μπορεί να είναι επιβλαβές σε περιπτώσεις με υψηλές απαιτήσεις σε εύρος ζώνης. Τέλος, η απόκρυψη των δεδομένων και η ενίσχυση της ασφάλειας του επιπέδου ομίχλης μέσω της εφαρμογής κρυπτογράφησης και της επαλήθευσης ταυτότητας αποτελεί μια ακόμη κρίσιμη ερευνητική κατεύθυνση. (Kaviyazhiny, Bala and Gowri, 2021)

Η ανάγκη για καλύτερη προστασία στο επίπεδο ομίχλης και των IoT συσκευών που το περιβάλλουν είναι προφανής δεδομένου της πολυπλοκότητας και της διασποράς του δικτύου του ομιχλώδους προγραμματισμού. Ωστόσο, οι προτεινόμενες λύσεις επικεντρώνονται κυρίως στην ασφαλή επικοινωνία των IoT συσκευών και των κόμβων ομίχλης, χωρίς να καλύπτουν επαρκώς την επικοινωνία μεταξύ των κόμβων ομίχλης. Επομένως, είναι αναγκαίο να αναπτυχθούν τεχνολογίες, οι οποίες θα κρύβουν το επίπεδο ομίχλης από πιθανές απειλές, καθώς και τεχνικές που θα ενισχύουν την προστασία μέσω κρυπτογράφησης και ελέγχων πρόσβασης, είναι ακόμη μια ερευνητική κατεύθυνση. Ωστόσο, για να διασφαλιστεί η πλήρης ασφάλεια του δικτύου, απαιτείται η ανάπτυξη επιπλέον μηχανισμών και στρατηγικών που θα καλύπτουν τα κενά προστασίας και θα ενισχύουν την άμυνα έναντι των επιθέσεων. Επίσης, μια σημαντική ερευνητική κατεύθυνση είναι η διασφάλιση της ασφαλούς επικοινωνίας και της μετάδοσης δεδομένων στους κόμβους ομίχλης μέσω ασύρματων δικτύων, καθώς σε αυτό το επίπεδο είναι κρίσιμο να αποφεύγονται επιθέσεις, να προστατεύονται τα δεδομένα που μεταδίδονται ασύρματα και να εξασφαλίζεται η ασφαλής μεταφορά των μεταβιβάσεων εργασιών (task handoffs) μεταξύ των κόμβων ομίχλης. Επομένως, πρέπει να αναπτυχθούν μηχανισμοί που στοχεύουν στην συνεργατική και στην ασφαλή εκτέλεση των συστατικών των εφαρμογών σε αυτό το επίπεδο, προκειμένου να διασφαλιστεί η ακεραιότητα, η εμπιστευτικότητα και η σωστή λειτουργεία του συστήματος, προστατεύοντας το παράλληλα από ενδεχόμενους κινδύνους και επιθέσεις. (Kaviyazhiny, Bala and Gowri, 2021)

6.5 Επισφαλής εικονικοποίηση

Στο πλαίσιο της μελλοντικής έρευνας στον τομέα της ασφαλής πολλαπλής μίσθωσης του ομιχλώδους προγραμματισμού αναδεικνύονται πολλές προκλήσεις. Αυτές οι προκλήσεις, οι οποίες αφορούν την προστασία των δεδομένων και την διαχείριση των πόρων, είναι κρίσιμες για την βιωσιμότητα και την αποτελεσματικότητα αυτής της τεχνολογίας. (Kaviyazhiny, Bala and Gowri, 2021)

Μια από τις κύριες προκλήσεις είναι η διατήρηση της ασφάλειας και της εμπιστευτικότητας. Ως εικονικό περιβάλλον που υποστηρίζει την πολλαπλή μίσθωση, ο ομιχλώδης προγραμματισμός πρέπει να αντιμετωπίσει ζητήματα που σχετίζονται με την προστασία και την ιδιωτικότητα των χρηστών, καθώς πολλοί χρήστες μοιράζονται τους ίδιους πόρους. Αυτή η συνύπαρξη πολλών χρηστών σε ένα κοινό περιβάλλον δημιουργεί την ανάγκη για την εφαρμογή αξιόπιστων μηχανισμών προστασίας, οι οποίοι θα πρέπει να προσφέρουν κατάλληλο επίπεδο απομόνωσης ώστε να διασφαλίζουν ότι τα δεδομένα κάθε χρήστη παραμένουν ασφαλή και ιδιωτικά, ακόμα και όταν οι πόροι χρησιμοποιούνται από κοινού. Μια ακόμη πρόκληση αποτελεί η δίκαιη κατανομή των πόρων, η οποία είναι κρίσιμη σε περιβάλλοντα ομίχλης που υποστηρίζουν την πολλαπλή μίσθωση. Μία κακή κατανομή πόρων μπορεί να οδηγήσει σε μη ασφαλή πρόσβαση και καταχρήσεις από κακόβουλους χρήστες καθώς και σε περιπτώσεις, λόγω έλλειψης πόρων, όπου ένα συστατικό εφαρμογής δυσλειτουργεί, δημιουργώντας «παράθυρο» για επιθέσεις στα δεδομένα που μεταδίδονται. Αυτό τονίζει την ανάγκη για την ανάπτυξη αποτελεσματικών μηχανισμών κατανομής. Μια τρίτη πρόκληση είναι η δυσκολία συντήρησης, καθώς ο αριθμός των χρηστών που μοιράζονται τους πόρους σε ένα επίπεδο ομίχλης ολοένα και αυξάνεται. Εφόσον η τρέχουσα

υποδομή δεν επαρκεί, τίθεται το ζήτημα της επέκτασης και της δυναμικής κατανομής των πόρων, ώστε να υποστηρίζεται η αυξανόμενη ζήτηση. Η διαχείριση και η συντήρηση της υποδομής του ομιχλώδους προγραμματισμού γίνεται ολοένα και πιο περιπλοκή, γεγονός που μπορεί να οδηγήσει σε προβλήματα απόδοσης, καθώς και σε προκλήσεις όσον αφορά την ορθή διαχείριση των ταυτοτήτων των χρηστών και την διασφάλιση της ασφάλειας των δεδομένων. (Kaviyazhiny, Bala and Gowri, 2021)

Για την αντιμετώπιση αυτών των προκλήσεων, προτείνονται διάφορες ερευνητικές κατευθύνσεις που θεωρούνται πολλά υποσχόμενες. Πρώτα απ' όλα, οι μηχανισμοί ασφάλειας, όπως ο λογικός διαχωρισμός των δεδομένων (logical data segregation) θα μπορούσαν να βελτιώσουν την ασφάλεια και την ιδιωτικότητα στα περιβάλλοντα ομίχλης που υποστηρίζουν την πολλαπλή μίσθωση. Η εφαρμογή της πολλαπλής αυθεντικοποίησης διασφαλίζει ότι οι χρήστες είναι αξιόπιστοι, ενώ η εφαρμογή του λογικού διαχωρισμού των δεδομένων μειώνει την πιθανότητα παραβίασης ή ανεπιθύμητης πρόσβασης σε δεδομένα από κακόβουλους χρήστες. Επίσης, η ανάπτυξη ανθεκτικών δικτύων (resilient networking) μπορεί να βοηθήσει στην βελτίωση της σταθερότητας και της ασφάλειας των δικτύων ομιχλώδους προγραμματισμού. Η προσαρμογή της τοπολογίας του δικτύου σε ένα περιβάλλον ομίχλης, σε συνδυασμό με την χρήση της εικονικοποίησης, όπως η κοκκοποίηση (granulation) του δικτύου και της υποδομής, αποτελούν βασικά χαρακτηριστικά των ανθεκτικών δικτύων, προσφέροντας μεγαλύτερη ευελιξία στην διαχείριση των πόρων και διευκολύνοντας την αντοχή σε επιθέσεις ή αστοχίες, ενώ παράλληλα ενσωματώνει τεχνικές για την αντιμετώπιση των περιορισμών που μπορεί να επιφέρει η εικονικοποίηση. Ακόμα, η κλιμάκωση μπορεί να απαιτεί την υιοθέτηση τεχνικών, όπως την αυτόματη προσαρμογή της υποδομής ανάλογα με τις ανάγκες των χρηστών, την εξισορρόπηση του φόρτου εργασίας μεταξύ διαφορετικών κόμβων ομίχλης, καθώς και την αξιοποίηση έξυπνων αλγορίθμων για την βέλτιστη κατανομή των πόρων σε πραγματικό χρόνο. (Kaviyazhiny, Bala and Gowri, 2021)

Μια άλλη ερευνητική κατεύθυνση που θα μπορούσε να αντιμετωπίσει σημαντικές προκλήσεις είναι η βελτίωση των τεχνολογιών εικονικοποίησης. Η χρήση της τεχνολογίας των δοχείων (containers) προσφέρει καλύτερη απομόνωση και μειωμένες τρωτότητες μπορεί να ενισχύσουν την ασφάλεια στα περιβάλλοντα ομίχλης, καθώς αυτά τα συστήματα είναι πιο αποδοτικά και ευέλικτα σε σχέση με την παραδοσιακή εικονικοποίηση. Επίσης, η πιο κατάλληλη και ακριβής παρακολούθηση εικονικών μηχανών με λιγότερους πόρους που να εντοπίζει επιθέσεις θα μπορούσε να είναι μια άλλη κατεύθυνση. (Kaviyazhiny, Bala and Gowri, 2021)

6.6 Επικινδυνότητα απώλειας δεδομένων

Τα περιβάλλοντα ομίχλης αποτελούν μια αναδυόμενη τεχνολογία στον χώρο πληροφορικής, τα οποία χαρακτηρίζονται με υψηλή συχνότητα διεκπεραίωσης δεδομένων και με σχετικά περιορισμένη δυνατότητα μακροχρόνιας αποθήκευσης πληροφοριών. Παρά τα σημαντικά πλεονεκτήματα που υπάρχουν στον ομιχλώδη προγραμματισμό, παρουσιάζονται σημαντικές προκλήσεις, ιδίως στον τομέα της δημιουργίας αντιγράφων ασφαλείας (back up) και της ανάνηψης (recovery) των δεδομένων. (Khan, Parkinson and Qin, 2017)

Στα περιβάλλοντα ομίχλης υπάρχει ο κίνδυνος της απώλειας των δεδομένων σε περιπτώσεις, όπως είναι οι φυσικές καταστροφές, η αποτυχία των συστημάτων ή των κυβερνοεπιθέσεων, γεγονός που καθιστά απαραίτητη την ύπαρξη αντιγράφων ασφαλείας. Μια από τις κύριες προκλήσεις είναι το υψηλό κόστος που συνεπάγεται η διαδικασία των αντιγράφων ασφαλείας, γιατί απαιτεί την προσεκτική επιλογή των δεδομένων προς αντιγραφή, την χαρτογράφηση των συστημάτων, τη δοκιμή της διαδικασίας επαναφοράς, καθώς και τον καθορισμό κατάλληλων ρόλων πρόσβασης. Ένα άλλο ζήτημα αποτελεί η ύπαρξη διπλο-εγγραφών που τυχόν υπάρχουν στα δεδομένα πριν από την διαδικασία των αντιγράφων ασφαλείας, καθώς αυτό σημαίνει σπατάλη χώρου κατά την δημιουργία των αντιγράφων για αυτά τα δεδομένα. Επιπλέον, η βελτίωση της απόδοσης, της συνέπειας και του συντονισμού της διαδικασίας αντιγράφων ασφαλείας και της ανάνηψης των δεδομένων αποτελεί μια ακόμη πρόκληση. Στο πλαίσιο αυτό, σημαντικό ρόλο παίζει η ρύθμιση της συχνότητας δημιουργίας των αντιγράφων ασφαλείας, η οποία θα πρέπει να ισχυροποιεί την απόδοση του δικτύου χωρίς να το επιβαρύνει υπερβολικά. Η συχνότητα αυτή εξαρτάται από τις ανάγκες κάθε εφαρμογής και απαιτεί κατάλληλη ισορροπία, ώστε να μην διαταράσσεται η απόδοση του δικτύου ή των εφαρμογών. Επιπρόσθετα, ένα άλλο κρίσιμο ζήτημα είναι ο τόπος αποθήκευσης των αντιγράφων ασφαλείας , είτε στην ομίχλη (fog) είτε στο νέφος (cloud). Εάν επιλεγεί η ομίχλη, θα πρέπει να εξεταστεί αν υπάρχει επαρκής χώρος, δεδομένου ότι αυτός μπορεί να καταλαμβάνεται από τα πρωτότυπα δεδομένα που μεταφέρονται για επεξεργασία στο επίπεδο της ομίχλης. Τέλος, μια ακόμα σημαντική πρόκληση σχετίζεται με τις δυσκολίες που αντιμετωπίζουν οι κινητές και οι ασύρματες πλατφόρμες ομίχλης στην αποτελεσματική διαχείριση των διαδικασιών δημιουργίας αντιγράφων ασφαλείας, όπως η περιορισμένη διαθέσιμη μνήμη, η αστάθεια της σύνδεσης και η καθυστέρηση στην μεταφορά των δεδομένων. (Khan, Parkinson and Qin, 2017)

Οι ερευνητικές κατευθύνσεις για την αντιμετώπιση των προκλήσεων του ομιχλώδους προγραμματισμού επικεντρώνονται σε διάφορους τομείς που σχετίζονται με την βελτίωση των διαδικασιών δημιουργίας αντιγράφων ασφαλείας και ανάνηψης των δεδομένων. Πρωταρχική κατεύθυνση αποτελεί η ανάπτυξη προηγμένων τεχνολογιών, όπως είναι η Υψηλής Ασφάλειας Διανομής και Τεχνολογία Ανάκτησης[8] (High Security Distribution and Rake Technology), οι οποίες στοχεύουν στην βελτίωση της συνέπειας, του συντονισμού και της απόδοσης των διαδικασιών της δημιουργίας αντιγράφων ασφαλείας και της ανάκτησης δεδομένων. Ιδιαίτερη έμφαση θα πρέπει να δοθεί στην ανάπτυξη στρατηγικών για κινητές και ασύρματες πλατφόρμες ομίχλης, που στοχεύουν στην βελτιστοποίηση φορητών συστημάτων αποθήκευσης και η ενίσχυση του εύρους ζώνης του δικτύου για την αποστολή των δεδομένων. Επιπλέον, η έρευνα πρέπει να εξετάσει την ενίσχυση της ανθεκτικότητας των συστημάτων ομιχλώδους προγραμματισμού απέναντι σε φυσικές καταστροφές

[8] Το σύστημα High Security Distribution and Rake Technology (HS-DRT) είναι μια καινοτόμος τεχνολογία δημιουργίας αντιγράφων ασφαλείας που κρυπτογραφεί τα δεδομένα, τα διασπά σε τμήματα και τα διανέμει σε πελάτες με τυχαίο τρόπο για ασφαλή αποθήκευση. Κατά την ανάκτηση, τα κρυπτογραφημένα τμήματα συλλέγονται από διαφορετικούς πελάτες, αποκωδικοποιούνται και ανακατασκευάζονται για να ανακτηθούν τα αρχικά δεδομένα. (Franklin *et al.*, 2018)

και σε κυβερνοεπιθέσεις, καθώς και την διασφάλιση της ύπαρξης αξιόπιστων πρωτογενών και δευτερογενών αντιγράφων ασφαλείας. Τέλος, σημαντικές βελτιώσεις μπορούν να επιτευχθούν στις διαδικασίες δημιουργίας αντιγράφων ασφαλείας με την βοήθεια βάσεων δεδομένων που βασίζονται σε SSD (Solid-state drive), καθώς και με την βοήθεια εικόνων εικονικών μηχανών (VM images). Αυτές οι τεχνολογίες μπορούν να ενσωματωθούν στην αρχιτεκτονική των υποδομών ομίχλης και νέφους, τοποθετούμενες σε κατάλληλα επίπεδα αποθήκευσης και διαχείρισης δεδομένων, ενισχύοντας την αποδοτικότητα της διαδικασίας δημιουργίας αντιγράφων ασφαλείας και την ανθεκτικότητα των συστημάτων. (Khan, Parkinson and Qin, 2017)

6.7 Ασφάλεια και αποδοτικότητα

Η ανάπτυξη και η λειτουργία ενός περιβάλλοντος ομίχλης αντιμετωπίζει σημαντικές προκλήσεις, καθώς απαιτείται εξισορρόπηση μεταξύ της ασφάλειας και της απόδοσης, σε ένα περιβάλλον όπου οι πόροι είναι συχνά περιορισμένοι και οι απαιτήσεις συνεχώς αυξάνονται (Khan, Parkinson and Qin, 2017).

Μια από τις κύριες προκλήσεις είναι η περιορισμένη δυνατότητα κλιμάκωσης των υπολογιστικών πόρων σε ορισμένες πλατφόρμες ομίχλης. Αν και κάποια συστήματα ομιχλώδους προγραμματισμού μπορούν να αυξήσουν τους πόρους τους (όπως την επεξεργαστική ισχύ και την αποθήκευση) ανάλογα με τις ανάγκες τους, αυτό εξαρτάται από την ύπαρξη επαρκών πόρων στο σύστημα. Ωστόσο, αυτό δεν ισχύει για όλες τις πλατφόρμες ομίχλης, καθώς σε περιπτώσεις περιορισμένων πόρων η δυναμική κλιμάκωση δεν είναι εφικτή. Αυτή η έλλειψη ομοιομορφίας αναδεικνύεται ως μια από τις βασικές δυσκολίες στον τομέα της ασφάλειας του ομιχλώδους προγραμματισμού. Το ζήτημα αυτό καθιστά σαφή τη σημασία του σχεδιασμού και της οργάνωσης των περιβαλλόντων ομίχλης, όπου απαιτείται είτε ένα μοντέλο κλιμάκωσης σε πραγματικό χρόνο με επαρκείς πόρους, είτε ένας αποτελεσματικός τρόπος διαμοιρασμού και κατανομής των διαθέσιμων πόρων, ώστε να μπορούν να καλύπτονται οι απαιτήσεις κάθε συστήματος / εφαρμογής όταν αυτές προκύπτουν. (Khan, Parkinson and Qin, 2017).

Ένα άλλο σημαντικό ζήτημα είναι η ισορροπία μεταξύ της ασφάλειας και της απόδοσης. Η υιοθέτηση ισχυρών μηχανισμών ασφάλειας μπορεί να υποβαθμίζει την λειτουργικότητα και την απόδοση του συστήματος, δημιουργώντας την ανάγκη για περαιτέρω έρευνα σχετικά με την επίτευξη αυτής της ισορροπίας. Η πρόκληση αυτή έγκειται στην ανάγκη για την εφαρμογή κατάλληλων μέτρων ασφάλειας χωρίς να θυσιάζεται η αποτελεσματικότητα και η ταχύτητα του συστήματος του ομιχλώδους προγραμματισμού. Επιπλέον, η ενσωμάτωση των ετερογενών IoT συσκευών αποτελεί μια επιπλέον πρόκληση, καθώς τα δίκτυα επικοινωνίας που υπάρχουν σε περιβάλλοντα ομίχλης καλούνται να διαχειριστούν την ασφαλή επικοινωνία μεταξύ των διαφορετικών συσκευών, καθεμιά από τις οποίες ξεχωριστά διαθέτει μοναδικές προδιαγραφές βάσει του σχεδιασμού του κατασκευαστής της. Αυτή η πολυπλοκότητα της διασύνδεσης αυτών των ετερογενών IoT συσκευών υφίσταται κυρίως λόγω της ετερογένειας των συσκευών, η οποία δημιουργεί σημαντικά ζητήματα, όπως οι διαφορετικές αρχιτεκτονικές, τα ασύμβατα πρωτόκολλα επικοινωνίας και οι ποικίλες απαιτήσεις ασφάλειας. Αυτές οι διαφορές καθιστούν δύσκολη την ομαλή και την ασφαλή επικοινωνία μεταξύ των συσκευών, καθιστώντας τη διασφάλιση των

επικοινωνιών και την αποτελεσματική λειτουργία των δικτύων των περιβαλλόντων ομίχλης κρίσιμα ζητήματα. (Khan, Parkinson and Qin, 2017).

Για την αντιμετώπιση των παραπάνω προκλήσεων η έρευνα θα πρέπει να επικεντρωθεί σε διάφορες κατευθύνσεις. Μια σημαντική ερευνητική κατεύθυνση στον τομέα του ομιχλώδους προγραμματισμού αποτελεί η ανάπτυξη ελαφριών και αποδοτικών μηχανισμών ασφάλειας, οι οποίοι μπορούν να ενσωματωθούν απευθείας στο λογισμικό του ομιχλώδους προγραμματισμού, χωρίς να επιβαρύνουν τους διαθέσιμους πόρους του συστήματος. Οι λύσεις αυτές θα πρέπει να επιτυγχάνουν την ισορροπία μεταξύ υψηλής απόδοσης και αποτελεσματικής ασφάλειας, εξασφαλίζοντας την συνεχή λειτουργία του συστήματος χωρίς σημαντική επίπτωση στην απόδοση του. Επίσης, η βελτιστοποίηση της χρήσης των διαθέσιμων πόρων μέσω της δυναμικής κατανομής τους στις εφαρμογές, με την παροχή μόνο των πλέον απαραίτητων πόρων και την κλιμάκωση τους μόνο όταν αυξάνονται οι ανάγκες των εφαρμογών, αναδεικνύεται ως μια σημαντική ερευνητική κατεύθυνση. Αυτό στοχεύει στην αποτελεσματική διαχείριση των πόρων του ομιχλώδους προγραμματισμού, εξασφαλίζοντας ότι οι πόροι καταναλώνονται με τον πιο αποδοτικό τρόπο. Επιπλέον, η δυναμική κλιμάκωση των υπολογιστικών πόρων αναμένεται να αποτελέσει κεντρικό σημείο της έρευνας. Οι πόροι του ομιχλώδους προγραμματισμού θα πρέπει να μπορούν να προσαρμόζονται σε πραγματικό χρόνο ανάλογα με τις απαιτήσεις της ασφάλειας και της απόδοσης, εξασφαλίζοντας την συνεχή λειτουργία του συστήματος υπό μεταβαλλόμενες συνθήκες, αλλά παράλληλα θα πρέπει να εξασφαλίζεται η ανθεκτικότητα του συστήματος σε πιθανές απειλές και επιθέσεις. Τέλος, η συνεργασία μεταξύ του ομιχλώδους προγραμματισμού και του υπολογιστικού νέφους μπορεί να οδηγήσει σε καλύτερη κατανομή των φορτίων εργασίας και στην αποδοτικότερη χρήση των διαθέσιμων πόρων, καθώς και στην εξισορρόπηση των υπολογιστικών αναγκών και των απαιτήσεων ασφάλειας, συμβάλλοντας στην αποδοτική λειτουργία ολόκληρης της υποδομής του ομιχλώδους προγραμματισμού. (Khan, Parkinson and Qin, 2017).

6.8 Διαχείριση εμπιστοσύνης

Η διαχείριση της εμπιστοσύνης σε περιβάλλοντα ομίχλης παρουσιάζει σημαντικές προκλήσεις, καθώς απαιτεί την ανάπτυξη μηχανισμών που να εξασφαλίζουν την αμφίδρομη εμπιστοσύνη και την διατήρηση αξιόπιστων σχέσεων μεταξύ των κόμβων του δικτύου. Η ανάπτυξη αυτών των μηχανισμών είναι πρόκληση για διάφορους λόγους, όπως η δυσκολία στον καθορισμό και την ανίχνευση κακόβουλης συμπεριφοράς, η ανάγκη για συνεχείς αξιολογήσεις στην εμπιστοσύνη σε κατανεμημένα περιβάλλοντα και η έλλειψη ενσωματωμένων ασφάλειας στα ομιχλώδη περιβάλλοντα. Παρά τις δυσκολίες, δεν υπάρχει εύκολη λύση για την ανάπτυξη ενός κεντρικού αξιόπιστου μέρους που να μπορεί να ρυθμίζει την αξιοπιστία των υπηρεσιών και την σταθερότητα του δικτύου, λόγω του κινδύνου διαφθοράς ή κακής συμπεριφοράς από τους κόμβους (Κρητικός, 2023). Επίσης, η προστασία της ιδωτικότητας είναι μια σημαντική πρόκληση, καθώς η προστασία των ευαίσθητων δεδομένων και η αποτροπή από μη εξουσιοδοτημένη πρόσβαση απαιτούν την ανάπτυξη κατάλληλων μηχανισμών, οι οποίοι ακόμα βρίσκονται σε πρώιμο στάδιο. Επιπλέον, η διαχείριση της ενέργειας είναι κρίσιμη, καθώς οι IoT συσκευές και οι κόμβοι ομίχλης έχουν περιορισμένους πόρους, γεγονός που απαιτεί την ανάπτυξη ελαφρών μηχανισμών διαχείρισης

εμπιστοσύνης με χαμηλή κατανάλωση ενέργειας. Επιπρόσθετα, η κινητικότητα των συσκευών, η οποία είναι ένα χαρακτηριστικό των περιβαλλόντων ομίχλης εντείνει τις προκλήσεις της διαχείρισης εμπιστοσύνης, καθώς η εμπιστοσύνη θα πρέπει να προσαρμόζεται συνεχώς στις μεταβαλλόμενες θέσεις και συνθήκες του δικτύου. Τέλος, η κλιμάκωση του συστήματος και η προσαρμογή της διαχείρισης της εμπιστοσύνης σε περιβάλλοντα ομίχλης με εκατομμύρια συσκευές παραμένει ένα ανοιχτό ερευνητικό ζήτημα (Nikravan and Kashani, 2022).

Μια προτεινομένη κατεύθυνση για την αντιμετώπιση αυτών των προβλημάτων είναι η χρήση της τεχνολογίας blockchain. Το blockchain μπορεί να αποτελέσει ένα αξιόπιστο και αμετάβλητο μέσο για την αποθήκευση κα την ανάλυση των καταχωρήσεων των κόμβων, διευκολύνοντας την ανίχνευση κακών συμπεριφορών και την διαχείριση των τιμωριών και των εξαργυρώσεων (redemption) φήμης. Μέσω αυτής της τεχνολογίας, θα είναι δυνατόν να εξασφαλιστεί μια διαφανής και ασφαλής διαδικασία καταγραφής και αξιολόγησης της εμπιστοσύνης στους κόμβους του δικτύου, βελτιώνοντας έτσι την συνολική σταθερότητα και την ασφάλεια του συστήματος (Κρητικός, 2023). Επίσης, η ενσωμάτωση τεχνολογιών SDN και NFV μπορεί να ενισχύσουν την ευελιξία και την αποδοτικότητα της διαχείρισης της εμπιστοσύνης, διευκολύνοντας την ανάπτυξη νέων προσεγγίσεων διαχείρισης εμπιστοσύνης. Επιπλέον, η πολυδιάστατη βελτιστοποίηση (multi-objective optimization) αποτελεί κρίσιμη ερευνητική κατεύθυνση, με στόχο τον σχεδιασμό λύσεων που να εξισορροπούν διάφορους παράγοντες, όπως η αξιοπιστία, η ασφάλεια και η απόδοση. Ένα άλλο σημαντικό πεδίο έρευνας είναι η αντιμετώπιση της ετερογένειας των συσκευών των περιβαλλόντων ομίχλης, διασφαλίζοντας ότι τα συστήματα διαχείρισης εμπιστοσύνης μπορούν να διαχειριστούν αποτελεσματικά την ποικιλία των συσκευών με διαφορετικές ικανότητες και χαρακτηριστικά (Nikravan and Kashani, 2022).

6.9 Μελλοντικές κατευθύνσεις

Πέρα από τις υπάρχουσες προκλήσεις του ομιχλώδους προγραμματισμού υπάρχει περαιτέρω περιθώριο για έρευνα στον τομέα του ομιχλώδους προγραμματισμού, ειδικότερα όσον αναφορά την δημιουργία μεγάλων σε κλίμακα δοκιμαστικών περιβαλλόντων (testbeds) και την ανάπτυξη δυναμικών λύσεων. Οι νέες τάσεις, όπως η ομοσπονδιακή μάθηση (federated learning) και η κβαντική υπολογιστική, αναμένεται να ενισχύσουν σημαντικά την υιοθέτηση του ομιχλώδους προγραμματισμού σε πραγματικές εφαρμογές στο εγγύς μέλλον. Οι προτεινόμενες μελλοντικές κατευθύνσεις στοχεύουν να κάνουν πιο εύκολη την εφαρμογή και να βελτιώσουν την προσβασιμότητα τόσο της τεχνολογίας IoT όσο και του ομιχλώδους προγραμματισμού, ενισχύοντας έτσι την διάδοση και την αξιοποίηση των λύσεων που βασίζονται σε αυτές τις τεχνολογίες. (Srirama, 2023)

6.9.1 Σχέδιο δράσης για την δημιουργία μεγάλης κλίμακας πειραματικών περιβαλλόντων και δοκιμών σε περιβάλλοντα ομίχλης

Οι εφαρμογές του ομιχλώδους προγραμματισμού έχουν παρουσιαστεί σε διάφορες μικρής κλίμακα πιλοτικές μελέτες σε διαφορετικούς τομείς, κυρίως λόγω της έλλειψης επαρκούς υποδομής. Η απουσία καταλλήλων δοκιμαστικών περιβαλλόντων (testbeds) μεγάλης κλίμακας, είτε εμπορικά είτε ακαδημαϊκά, περιορίζει την παρουσίαση και την αξιολόγηση τέτοιων πρότυπών. Τέτοια δοκιμαστικά περιβάλλοντα είναι δοκιμασμένα και κοινά στον τομέα των τηλεπικοινωνίων, με την συνεργασία ακαδημαϊκών και βιομηχανικών φορέων. Για παράδειγμα, οι Midoglu κ.α. (2021) μελέτησαν την ταχύτητα των δικτύων κινητής ευρυζωνικότητας (Mobile Broadband - MBB) στο δοκιμαστικό περιβάλλον MONROE (Measuring Mobile Broadband Networks in Europe) (Midoglu *et al.*, 2021). (Srirama, 2023)

Στο τομέα του υπολογιστικού νέφους υπάρχουν προσπάθειες, όπως το ELIXIR, το οποίο χρησιμοποιείται από την κοινότητα βιοπληροφορικής και υπηρεσιών στην Ευρώπη. Αντίστοιχες προσπάθειες μπορούν να πραγματοποιηθούν για την δημιουργία δοκιμαστικών περιβαλλόντων που αφορούν συστήματα ομιχλώδους προγραμματισμού. Με αρκετές εφαρμογές του ομιχλώδους προγραμματισμού να είναι εφικτές σε οικοσυστήματα, όπως το IIoT, τις έξυπνες πόλεις και τα αυτόνομα οχήματα, η δημιουργία μιας κοινοπραξίας μεταξύ των κυβερνήσεων, των βιομηχανικών και των ακαδημαϊκών φορέων για την εγκαθίδρυση δοκιμαστικών περιβαλλόντων μεγάλης κλίμακας θα πρέπει να εξεταστεί σοβαρά. Τέτοιες πρωτοβουλίες μπορεί να προωθήσουν περαιτέρω την έρευνα στον ομιχλώδη προγραμματισμό, επιτρέποντας την διαλειτουργικότητα και την μεταβίβαση εργασιών, στα δίκτυα του ομιχλώδους προγραμματισμού, τα οποία αυτή την στιγμή μελετώνται θεωρητικά και παρουσιάζονται μόνο μέσω προσομοιωτών. (Srirama, 2023)

6.9.2 Δυναμική ανάπτυξη υπηρεσιών ομίχλης συμβατή με πρότυπα

Αυτή την στιγμή, οι υπηρεσίες ομίχλης αναπτύσσονται σε συσκευές που παρουσιάζουν ετερογένεια και διαθέτουν περιορισμένους πόρους, χρησιμοποιώντας ιδιόκτητες λύσεις. Η μεθοδολογία DevOps ενσωματώνει και αυτοματοποιεί την ανάπτυξη λογισμικού και τις λειτουργίες πληροφορικής, χρησιμοποιώντας σχετικά εργαλεία, μειώνοντας έτσι τον κύκλο ζωής ανάπτυξης λογισμικού. Πρότυπα, όπως είναι το OASIS – TOSCA (Topology and Orchestration Specification for Cloud Applications) έχουν αναπτυχθεί για να καθορίσουν την διαμόρφωση των εφαρμογών. Οι συμβατοί με TOSCA ενορχηστρωτές (orchrestrators) μπορούν να αναπτύξουν τις εφαρμογές για πολλαπλά νέφη, διευκολύνοντας την μεταφορά τους μεταξύ διαφορετικών πάροχων. (Srirama, 2023)

Ωστόσο, η αυτοματοποιημένη ανάπτυξη και η εφαρμογή του DevOps στον ομιχλώδη προγραμματισμό δεν έχουν εξερευνηθεί αρκετά. Η ενορχηστρωμένη διαχείριση δοχείων (π.χ. Docker Swarm, k3s) μπορεί να εξασφαλίσει ότι οι συσκευές ομίχλης (fog devices) μπορούν να συνεργάζονται και να λειτουργούν αποτελεσματικά μαζί, ανεξάρτητα από την υποκείμενη πλατφόρμα ή το λειτουργικό σύστημα που χρησιμοποιούν. Πρώτες προσπάθειες προσαρμογής του

TOSCA για τον ομιχλώδη προγραμματισμό έχουν γίνει στο πλαίσιο του FogDEFT. Αυτό το πλαίσιο απλοποιεί τις διάφορες πολυπλοκότητες και προσφέρει μια πιο φιλική προς τον χρήστη μέθοδο για την μοντελοποίηση και την δυναμική ανάπτυξη υπηρεσιών ομίχλης, κατόπιν αιτήματος σε πραγματικό χρόνο από απομακρυσμένα συστήματα. Χρειάζεται ακόμη περισσότερη δουλειά για να προχωρήσει αυτή η προσέγγιση σε επίπεδο τυποποίησης. (Srirama, 2023)

6.9.3 Ομοσπονδιακή μάθηση

Η ομοσπονδιακή μάθηση (federated learning - FL) είναι μια αναδυόμενη τεχνική μηχανικής μάθησης που εκπαιδεύει μοντέλα σε συσκευές ομίχλης με περιορισμένους πόρους χρησιμοποιώντας μόνο τοπικά δεδομένα. Οι τοπικές εκπαιδευόμενες παράμετροι του μοντέλου μηχανικής μάθησης από κάθε κόμβο συγκεντρώνονται και συνδυάζονται σε έναν κεντρικό μοντέλο, το οποίο στη συνέχεια αποστέλλεται πίσω στους κόμβους για περαιτέρω εκπαίδευση. Αυτή η διαδικασία συνεχίζεται μέχρι το μοντέλο να φτάσει σε ένα σταθερό αποτέλεσμα, δηλαδή να επιτευχθεί η σύγκλιση. Η ομοσπονδιακή μάθηση χρησιμοποιείται σε διαφορές εφαρμογές του ομιχλώδους προγραμματισμού, όπως οι έξυπνες πόλεις, η έξυπνη υγειονομική περίθαλψη και τα αυτόνομα οχήματα. Επιπλέον, η ομοσπονδιακή μάθηση βοηθά στην αντιμετώπιση του ομιχλώδους προγραμματισμού, όπως είναι η ασφάλεια και η προστασία της ιδιωτικότητας με την χρήση διαφόρων τεχνικών, όπως η διαφορική ιδιωτικότητα (differential privacy). Οι πιο πρόσφατες εξελίξεις στην ομοσπονδιακή μάθηση περιλαμβάνουν την Μεταφερομένη Μάθηση (Transfer Learning) δηλαδή την εκπαίδευση σε σύνολα δεδομένων που μοιράζονται πολλοί συμμετέχοντες, όπως είναι οι κόμβοι ομίχλης, και την Διασκορπισμένη Ομοσπονδιακή Μάθηση (Dispersed FL) όπου το μοντέλο εκπαιδεύεται σε ομάδες και στην συνέχεια ενοποιείται σε ένα μεγαλύτερο μοντέλο. Αυτές οι τεχνικές επιτρέπουν την συνεργατική μάθηση σε πολλά επίπεδα στην ιεραρχική αρχιτεκτονική του ομιχλώδους προγραμματισμού. Τα τελευταία χρόνια, η ομοσπονδιακή μάθηση διερευνάται εκτενώς. (Srirama, 2023)

Η ομοσπονδιακή μάθηση προσθέτει επιπλέον φόρτο στις συσκευές ομίχλης, οι οποίες συχνά διαθέτουν περιορισμένους πόρους. Γι’ αυτό, η μελλοντική έρευνα πρέπει να επικεντρωθεί στην ανάπτυξη πιο ελαφριών μοντέλων μηχανικής μάθησης και στην βελτιστοποίηση των αλγορίθμων FL, λαμβάνοντας υπόψιν περιορισμούς, όπως είναι η ακρίβεια του τοπικού μοντέλου μηχανικής μάθησης που διαθέτει κάθε συσκευή ομίχλης, οι ενεργειακές απαιτήσεις, η διαθεσιμότητα των υπολογιστικών πόρων κ.α.. Επιπλέον, είναι ενδιαφέρον να μελετηθεί αν η ομοσπονδιακή μάθηση μπορεί να προσφέρεται ως υπηρεσία από τους κόμβους ομίχλης, κάτι που θα μπορούσε να οδηγήσει σε νέα οικονομικά μοντέλα και την ευρύτερη υιοθέτηση του ομιχλώδους προγραμματισμού. (Srirama, 2023)

6.9.4 Το κβαντικό υπολογιστικό νέφος και οι επιπτώσεις του στον ομιχλώδη προγραμματισμό

Μια άλλη τεχνολογία που αναπτύσσεται γρήγορα είναι η κβαντική υπολογιστική, η οποία χρησιμοποιεί τους νόμους της κβαντομηχανικής για να λύσει προβλήματα που είναι πολύ περίπλοκα για τους κλασικούς υπολογιστές. Αν οι ισχυροί κβαντικοί υπολογιστές γίνουν ευρέως διαθέσιμοι στο μέλλον, θα μπορούσαν να οδηγήσουν στην εξέλιξη του κβαντικού υπολογιστικού νέφους (quantum cloud computing). Αυτές οι εξελίξεις θα προσφέρουν λύσεις, όπως είναι οι ασφαλείς κβαντικοί υπολογισμοί που αντέχουν σε σφάλματα, καθώς και οι κβαντικές τεχνικές για κρυπτογράφηση, επαλήθευση και τον έλεγχο πρόσβασης στο υπολογιστικό νέφος. Οι πελάτες του κβαντικού υπολογιστικού νέφους θα πρέπει να επικοινωνούν με το νέφος μέσω ενός κβαντικού συνδέσμου για να μεταφέρουν τα καθήκοντά τους και τα σχετικά qubits (κβαντικά bits). Ήδη έχουν γίνει αρχικές προσπάθειες προς αυτή την κατεύθυνση. (Srirama, 2023)

Καθώς ο ομιχλώδης προγραμματισμός θεωρείται ως μια μορφή υπολογιστικού νέφους που βρίσκεται κοντά στους χρήστες, είναι πιθανό το κβαντικό υπολογιστικό νέφος να επηρεάσει τον ομιχλώδη προγραμματισμό. Η μελλοντική έρευνα θα πρέπει να ξεκινήσει να διερευνά τις ευκαιρίες που μπορεί να προσφέρει το κβαντικό υπολογιστικό νέφος. Για παράδειγμα, αν συνδυαστεί η τεχνολογία Blockchain με το κβαντικό ιντερνέτ μπορεί να βελτιωθεί η ταχύτητα επικοινωνίας, καθώς και να προσφέρει την απαιτούμενη ασφάλεια, έτσι ώστε να εκτελούνται με ασφάλεια οι διάφορες εργασίες, όπως είναι η ανάλυση των δεδομένων και η ομοσπονδιακή μάθηση που πραγματοποιούνται συνεχόμενα μεταξύ του άκρου και του νέφους (edge-cloud). (Srirama, 2023)

7 Συμπεράσματα

7.1 Συνεισφορά διπλωματικής

Η παρούσα διπλωματική εργασία πραγματοποίησε μια ενδελεχή ανάλυση των ζητημάτων ασφάλειας που προκύπτουν στα περιβάλλοντα ομίχλης. Μελετώντας συστηματικά τις τρωτότητες, τις απειλές και τις επιθέσεις που χαρακτηρίζουν αυτά τα περιβάλλοντα ομίχλης, η αναφορά αυτή προσφέρει μια ολοκληρωμένη κατηγοριοποίηση των κινδύνων και προτείνει μια συγκριτική αξιολόγηση των υπαρχουσών τεχνικών αντιμετώπισης. Τα αποτελέσματα της συγκριτικής ανάλυσης των αντιμέτρων έδειξαν ότι η επιλογή των κατάλληλων αντιμέτρων στον ομιχλώδη προγραμματισμό είναι κρίσιμη, καθώς η πολυπλοκότητα των συστημάτων απαιτεί λύσεις που προσφέρουν την ιδανική ισορροπία μεταξύ της ακρίβειας, της αποτελεσματικότητας και της απόδοσης. Η ανάλυση έδειξε ότι λύσεις, όπως το RBAC και το ABAC είναι ιδιαίτερα αποδοτικές και αποτελεσματικές, προσφέροντας υψηλή ακρίβεια στην προστασία των δεδομένων, ενώ παράλληλα διατηρούν την απόδοση σε υψηλά επίπεδα, καθιστώντας τις ιδανικές για μεγάλα και σύνθετα δίκτυα. Αντίθετα, το IoTCoP και η τεχνική MLTKNN είναι οι χειρότερες λύσεις όπως προέκυψε από την ανάλυση. Αυτές οι δύο λύσεις ενώ παρέχουν ικανοποιητική ασφάλεια σε διαφορετικά επίπεδα, μπορεί να μην θεωρούνται «εξαιρετικές» σε όλες συνθήκες ή για όλες τις απειλές. Επιπλέον, το IoTCoP και η τεχνική MLTKNN επιβαρύνουν τους πόρους του συστήματος και απαιτούν υψηλή υπολογιστική ισχύ, γεγονός που περιορίζει την απόδοση τους σε περιβάλλοντα με περιορισμένους υπολογιστικούς πόρους.

Η κυριότερη συνεισφορά της διπλωματικής εργασίας περιλαμβάνει την ιεραρχική κατηγοριοποίηση των τρωτοτήτων, των επιθέσεων και των κινδύνων / επιπτώσεων στον ομιχλώδη προγραμματισμό. Εκτός από την κατηγοριοποίηση των παραπάνω παραγόντων, η εργασία προτείνει επίσης μια κατηγοριοποίηση των αντιμέτρων που μπορούν να εφαρμοστούν για την αντιμετώπιση των συγκεκριμένων απειλών. Αυτή η κατηγοριοποίηση προσφέρει μια δομημένη και οργανωμένη προσέγγιση, επιτρέποντας την καλύτερη κατανόηση και την διαχείριση των κινδύνων που αντιμετωπίζουν τα συστήματα ομίχλης. Η ιεραρχία αυτή βοηθά στην αναγνώριση των πιο κρίσιμων σημείων αδυναμίας και της επίδρασης των επιθέσεων, κάτι που επιτρέπει την εφαρμογή πιο στοχευμένων και αποτελεσματικών αντιμέτρων. Τέλος, η διπλωματική εργασία συνείσφερε στην συγκριτική ανάλυση των αντιμέτρων με βάση ένα κατάλληλο σύνολο από κριτήρια που επιλέχθηκαν προσεκτικά από την βιβλιογραφία.

Τα πλεονεκτήματα αυτής της προσέγγισης είναι πολλαπλά. Πρώτα από όλα, διευκολύνει την επιλογή των κατάλληλων λύσεων ασφάλειας με βάση τις ειδικές ανάγκες του κάθε περιβάλλοντος ομίχλης, αυξάνοντας την αποδοτικότητα της προστασίας. Επίσης, παρέχει την δυνατότητα για πιο

ευέλικτη προσαρμογή των αντιμέτρων, καθώς επιτρέπει την άμεση αναγνώριση των διαφορετικών επιπέδων κίνδυνου και την εφαρμογή δυναμικών λύσεων. Τέλος, η ιεραρχική κατηγοριοποίηση ενισχύει την διαδικασία αξιολόγησης και σύγκρισης των διαφορετικών αντιμέτρων, προσφέροντας ένα εργαλείο για τη συνεχιζόμενη βελτίωση και αναβάθμιση των μηχανισμών ασφάλειας στον ομιχλώδη προγραμματισμό.

Παράλληλα, εντοπίστηκαν σημαντικά κενά στην υπάρχουσα βιβλιογραφία που σχετίζονται με την χαμηλή αξιολόγηση των προτεινόμενων αντιμέτρων ιδιαίτερα στην ικανότητα τους να αντιμετωπίζουν αποτελεσματικά συγκεκριμένους τύπους επιθέσεων. Η σύγκριση μεταξύ των ήδη υπαρχόντων αντιμέτρων του ομιχλώδους προγραμματισμού έδειξε ότι ενώ υπάρχουν διάφορες τεχνικές που μπορούν να εφαρμοστούν, καμία δεν αποτελεί μια ολοκληρωμένη λύση. Η επιλογή του κατάλληλου αντιμέτρου εξαρτάται από τον συγκεκριμένο τύπο απειλής, τις ιδιαιτερότητες του περιβάλλοντος και τους επιχειρησιακούς στόχους. Σε πολλές περιπτώσεις, απαιτείται ο συνδυασμός διαφορετικών αντιμέτρων για την επίτευξη μιας πιο ολοκληρωμένης λύσης ασφάλειας που έχει ως στόχο την ενίσχυση της προστασίας των δεδομένων και των περιβαλλόντων ομιχλώδους προγραμματισμού, καθώς οι επιθέσεις συχνά στοχεύουν σε πολλαπλές πτυχές του συστήματος και ένα μόνο αντίμετρο μπορεί να μην επαρκεί για την αντιμετώπιση τους. Επιπλέον, η έλλειψη ενός ενιαίου πλαισίου αξιολόγησης των αντιμέτρων καθιστά δύσκολη την επιλογή της βέλτιστης λύσης σε περιβάλλοντα ομιχλώδη προγραμματισμού. Ωστόσο, η παρούσα διπλωματική εργασία επιχειρεί να καλύψει αυτό το κενό, προσφέροντας ένα πλαίσιο αξιολόγησης που αναδεικνύει της καλύτερες λύσεις, αλλά και τις σημαντικότερες αδυναμίες τους.

7.2 Μελλοντικές κατευθύνσεις

Ο ομιχλώδης προγραμματισμός ως μια αποκεντρωμένη αρχιτεκτονική, παρουσιάζει πολλές προκλήσεις που πρέπει να αντιμετωπιστούν για την ευρεία υιοθέτηση του. Μια από τις κύριες προκλήσεις είναι η ασφάλεια των δεδομένων και η προστασία της ιδιωτικότητας. Η διαχείριση των δεδομένων σε κατανεμημένα συστήματα καθιστά την διασφάλιση της ασφαλούς αποθήκευσης και μετάδοσης των δεδομένων πολύπλοκη. Χωρίς τους κατάλληλους μηχανισμούς κρυπτογράφησης και της αποτελεσματικής διαχείρισης των δικαιωμάτων πρόσβασης τα δεδομένα παραμένουν ευάλωτα σε επιθέσεις και κακόβουλες ενέργειες. Ακόμη, η κλιμάκωση του συστήματος αποτελεί μια σοβαρή πρόκληση καθώς η ανάγκη για διαρκή εξισορρόπηση του φορτιού και την κατανομή των πόρων σε πραγματικό χρόνο μπορεί να επηρεάσει την απόδοση του συστήματος, δημιουργώντας προβλήματα ασφάλειας λόγω μη βέλτιστων ρυθμίσεων και υποδομών. Επιπλέον, οι συνεχείς εξελισσόμενες απειλές απαιτούν την εφαρμογή ευέλικτων και δυναμικών μηχανισμών άμυνας, ικανών να προσαρμοστούν στις νέες συνθήκες και τις εξελισσόμενες απειλές.

Η έρευνα στον ομιχλώδη προγραμματισμό συνεχίζει να εστιάζει στην βελτίωση των μηχανισμών ασφάλειας μέσω της αξιοποίησης καινοτόμων τεχνολογιών, όπως η ομοσπονδιακή μάθηση και η κβαντική υπολογιστική. Η ομοσπονδιακή μάθηση επιτρέπει την συνεργατική εκμάθηση μοντέλων χωρίς την μεταφορά δεδομένων, ενισχύοντας την ιδιωτικότητα των χρηστών. Παράλληλα, η ανάπτυξη ελαφριών λύσεων κρυπτογράφησης και η ενσωμάτωση δυναμικών μηχανισμών

ασφάλειας που προσαρμόζονται ανάλογα με το φορτίο και τις επιθέσεις, θα βελτιώσει σημαντικά την αποδοτικότητα των συστημάτων ομιχλώδους προγραμματισμού. Η αξιολόγηση αυτών των λύσεων μέσω δοκιμαστικών περιβαλλόντων (testbeds) σε ρεαλιστικά σενάρια είναι κρίσιμη για την εμπειρική επαλήθευση της αποτελεσματικότητας τους. Επιπλέον, θα πρέπει να αναπτυχθούν ευέλικτα προγνωστικά μοντέλα βασισμένα σε τεχνικές μηχανικής μάθησης ικανά να προβλέπουν τις υπάρχουσες και τις νεοεμφανιζόμενες απειλές. Αυτές οι προκλήσεις και οι μελλοντικές κατευθύνσεις δείχνουν ότι η ασφάλεια στον ομιχλώδη προγραμματισμό είναι μια δυναμική και συνεχώς εξελισσόμενη διαδικασία που απαιτεί τη ενσωμάτωση καινοτόμων τεχνολογιών, την βελτιστοποίηση των υπαρχόντων συστημάτων και την προσαρμογή σε νέες απειλές και απαιτήσεις των χρηστών.

7.3 Προσωπική εμπειρία

Κατά τη διάρκεια της εκπόνησης της διπλωματικής εργασίας, αποκομίσαμε πολύτιμες γνώσεις και δεξιότητες στον τομέα της ασφάλειας των συστημάτων ομιχλώδους προγραμματισμού. Η ενδελεχής μελέτη των τρωτοτήτων, των απειλών και των επιθέσεων σε συνδυασμό με την συγκριτική ανάλυση των υπαρχουσών τεχνικών αντιμετώπισης, μας επέτρεψε να κατανοήσουμε σε βάθος τις ιδιαιτερότητες και τις προκλήσεις που υπάρχουν σε αυτό το πεδίο. Η ανακάλυψη σημαντικών κενών στην υπάρχουσα βιβλιογραφία μας ώθησε να αναπτύξουμε κριτική σκέψη. Οι γνώσεις που αποκομίσαμε θα μας βοηθήσουν να αντιμετωπίσουμε με επιτυχία τις προκλήσεις της ασφάλειας σε περιβάλλοντα ομιχλώδους προγραμματισμού, τόσο στην ακαδημαϊκή μας πορεία όσο και σε επαγγελματικό επίπεδο. Επιπλέον, η εμπειρία που απεκτήσαμε ως προς την εκπόνηση της διπλωματικής εργασίας ενίσχυσε της δεξιότητές μας στην ανάλυση των δεδομένων, στην σύνθεση πληροφοριών και στην επιστημονική συγγραφή, οι οποίες αποτελούν εφόδια για τον κάθε ερευνητή.

Βιβλιογραφία

Aazam, M. and Huh, E.-N. (2015) 'Dynamic resource provisioning through fog micro datacenter', in *2015 IEEE international conference on pervasive computing and communication workshops (PerCom workshops)*. IEEE, pp. 105–110.

Abbasi, B.Z. and Shah, M.A. (2017) 'Fog computing: Security issues, solutions and robust practices', in *2017 23rd international conference on automation and computing (ICAC)*. IEEE, pp. 1–6.

Abdel-Basset, M. *et al.* (2020) 'Deep-IFS: Intrusion detection approach for industrial internet of things traffic in fog environment', *IEEE Transactions on Industrial Informatics*, 17(11), pp. 7704–7715.

Aguzzi, C. *et al.* (2020) 'From cloud to edge: Seamless software migration at the era of the web of things', *IEEE Access*, 8, pp. 228118–228135.

Ahmadi, F. *et al.* (2021) 'Multi-factor biometric authentication approach for fog computing to ensure security perspective', in *2021 8th international conference on computing for sustainable global development (INDIACom)*. IEEE, pp. 172–176.

Al Harbi, S., Halabi, T. and Bellaiche, M. (2020) 'Fog computing security assessment for device authentication in the internet of things', in *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, pp. 1219–1224.

Alam, T. (2023) 'A reliable communication framework and its use in internet of things (IoT)', *Authorea Preprints* [Preprint].

Aleisa, M.A., Abuhussein, A. and Sheldon, F.T. (2020) 'Access control in fog computing: Challenges and research agenda', *IEEE Access*, 8, pp. 83986–83999.

Al-Fuqaha, A. *et al.* (2015) 'Internet of things: A survey on enabling technologies, protocols, and applications', *IEEE communications surveys & tutorials*, 17(4), pp. 2347–2376.

Al-Hasnawi, A., Carr, S.M. and Gupta, A. (2019) 'Fog-based local and remote policy enforcement for preserving data privacy in the Internet of Things', *Internet of Things*, 7, p. 100069.

Al-Hasnawi, A. and Lilien, L. (2017) 'Pushing data privacy control to the edge in IoT using policy enforcement fog module', in *Companion Proceedings of the10th International Conference on Utility and Cloud Computing*, pp. 145–150.

Al-Hasnawi, A., Mohammed, I. and Al-Gburi, A. (2018) 'Performance evaluation of the policy enforcement fog module for protecting privacy of IoT data', in *2018 IEEE International Conference on Electro/Information Technology (EIT)*. IEEE, pp. 0951–0957.

Ali, A. *et al.* (2020) 'Security and Privacy Issues in Fog Computing', in A. Zomaya, A. Abbas, and S. Khan (eds) *Fog Computing*. 1st edn. Wiley, pp. 105–137. Available at: https://doi.org/10.1002/9781119551713.ch5.

Aljumah, A. and Ahanger, T.A. (2018) 'Fog computing and security issues: A review', in *2018 7th international conference on computers communications and control (ICCCC)*. IEEE, pp. 237–239.

Al-Musib, N.S. *et al.* (2023) 'Business email compromise (BEC) attacks', *Materials Today: Proceedings*, 81, pp. 497–503.

Alrawais, A. *et al.* (2017) 'Fog computing for the internet of things: Security and privacy issues', *IEEE Internet Computing*, 21(2), pp. 34–42.

Alwakeel, A.M. (2021) 'An overview of fog computing and edge computing security and privacy issues', *Sensors*, 21(24), p. 8226.

Alzoubi, Y.I. *et al.* (2021) 'Fog computing security and privacy for the Internet of Thing applications: State-of-the-art', *Security and Privacy*, 4(2), p. e145.

An, X. *et al.* (2018) 'Hypergraph clustering model-based association analysis of DDOS attacks in fog computing intrusion detection system', *EURASIP Journal on Wireless Communications and Networking*, 2018(1), pp. 1–9.

Antonakakis, M. *et al.* (2017) 'Understanding the mirai botnet', in *26th USENIX security symposium (USENIX Security 17)*, pp. 1093–1110.

Archana Lisbon, A. and Kavitha, R. (2017) 'A study on cloud and fog computing security issues and solutions', *International Journal of Innovative Research in Advanced Engineering (IJIRAE)*, (03), pp. 17–22.

Arora, A. (2018) 'Preventing wireless deauthentication attacks over 802.11 Networks'. arXiv. Available at: https://doi.org/10.48550/arXiv.1901.07301.

Atlam, H.F., Walters, R.J. and Wills, G.B. (2018) 'Fog computing and the internet of things: A review', *big data and cognitive computing*, 2(2), p. 10.

Azarkasb, S.O. and Khasteh, S.H. (2023) 'Advancing Intrusion Detection in Fog Computing: Unveiling the Power of Support Vector Machines for Robust Protection of Fog Nodes against XSS and SQL Injection Attacks', *Journal of Engineering Research and Reports*, 25(3), pp. 59–84.

Badger, M.L. *et al.* (2012) *Cloud computing synopsis and recommendations*. National Institute of Standards & Technology.

Banday, M.T. (2019) *Cryptographic Security Solutions for the Internet of Things*. IGI Global.

Banerjee, R. *et al.* (2020) 'Detection of XSS in web applications using Machine Learning Classifiers', in *2020 4th international conference on electronics, materials engineering & nano-technology (IEMENTech)*. IEEE, pp. 1–5.

Basir, R. *et al.* (2019) 'Fog computing enabling industrial internet of things: State-of-the-art and research challenges', *Sensors*, 19(21), p. 4807.

Bhushan, B. *et al.* (eds) (2023) *5G and Beyond*. Singapore: Springer Nature Singapore (Springer Tracts in Electrical and Electronics Engineering). Available at: https://doi.org/10.1007/978-981-99-3668-7.

black hole in The Network Encyclopedia (no date a). Available at: http://www.thenetworkencyclopedia.com/entry/black-hole/ (Accessed: 7 December 2024).

black hole in The Network Encyclopedia (no date b). Available at: http://www.thenetworkencyclopedia.com/entry/black-hole/ (Accessed: 7 December 2024).

Boneh, D. and Boyen, X. (2008) 'Short signatures without random oracles and the SDH assumption in bilinear groups', *Journal of cryptology*, 21(2), pp. 149–177.

Bonomi, F. *et al.* (2012) 'Fog computing and its role in the internet of things', in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13–16.

Bowman, K. (2024) *Data Obfuscation Techniques*. Available at: https://pathlock.com/learn/data-obfuscation/ (Accessed: 21 November 2024).

Brady, K. *et al.* (2020) 'Docker container security in cloud computing', in *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, pp. 0975–0980.

Butani, B., Shukla, P.K. and Silakari, S. (2014) 'An exhaustive survey on physical node capture attack in WSN', *International Journal of Computer Applications*, 95(3), pp. 32–39.

Cagalj, M. *et al.* (2006) 'Integrity (I) codes: Message integrity protection and authentication over insecure channels', in *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, pp. 15-pp.

Cao, Y. *et al.* (2015) 'FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation', in *2015 IEEE international conference on networking, architecture and storage (NAS)*. IEEE, pp. 2–11.

Carlin, S. and Curran, K. (2012) 'Cloud Computing Technologies', *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, 1(2), pp. 59–65. Available at: https://doi.org/10.11591/closer.v1i2.486.

Chandramohan, D. *et al.* (2019) 'Fog enabled secure and privacy obfuscation for IoT services', *Jour. of Adv. Research in Dynamical & Control Systems*, 11(Special Issue-08), pp. 1604–1610.

Chang, V. *et al.* (2022) 'A survey on intrusion detection systems for fog and cloud computing', *Future Internet*, 14(3), p. 89.

Chaudhary, D., Bhushan, K. and Gupta, B.B. (2018) 'Survey on DDoS Attacks and Defense Mechanisms in Cloud and Fog Computing':, *International Journal of E-Services and Mobile Applications*, 10(3), pp. 61–83. Available at: https://doi.org/10.4018/IJESMA.2018070104.

Chen, C. *et al.* (2014) '{cTPM}: A cloud {TPM} for {Cross-Device} trusted applications', in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*.

Chen, Y. (2023) *Creating a Data as a Service (DaaS) Platform: Building RESTful APIs with Swagger 2 Documentation using Spring Boot*, *Medium*. Available at: https://medium.com/@dynotes/creating-a-data-as-a-service-daas-platform-building-restful-apis-with-swagger-2-documentation-80ac12cd392 (Accessed: 2 June 2024).

Chen, Y. and Yang, J. (2012) 'Defending against identity-based attacks in wireless networks', *Handbook on Securing Cyber-Physical Critical Infrastructure*, pp. 191–222.

Chiba, Z. *et al.* (2022) 'A deep study of novel intrusion detection systems and intrusion prevention systems for Internet of Things networks', *Procedia Computer Science*, 210, pp. 94–103.

Chowdhury, A. and A Raut, S. (2019) 'Benefits, challenges, and opportunities in adoption of industrial IoT', *International Journal of Computational Intelligence & IoT*, 2(4).

Cisco (2015) 'Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are'. Available at: https://www.researchgate.net/profile/Mohamed-Mourad-Lafifi/post/Is_there_any_simulation_tool_for_fog_computing/attachment/59d638c079197b8077995f4c/AS%3A398883160117248%401472112564706/download/Fog+Computing+and+the+Internet+of+Things++Extend+the+Cloud+to+Where+the+Things+Are.pdf.

Cisco (2024) *Cisco Locator/ID Separation Protocol (LISP)*, *Cisco*. Available at: https://www.cisco.com/c/en/us/products/ios-nx-os-software/locator-id-separation-protocol-lisp/index.html (Accessed: 7 August 2024).

Cloudflare (2024) *What is DNS cache poisoning?* Available at: https://www.cloudflare.com/learning/dns/dns-cache-poisoning/ (Accessed: 6 December 2024).

Coyne, E. and Weil, T.R. (2013) 'ABAC and RBAC: Scalable, flexible, and auditable access management.', *IT professional*, 15(3).

CSRC NIST (2024) *security service*. Available at: https://csrc.nist.gov/glossary/term/security_service (Accessed: 14 January 2025).

CSRC NIST, C.C. (2024) *security control*. Available at: https://csrc.nist.gov/glossary/term/security_control (Accessed: 14 January 2025).

Das, R. and Inuwa, M.M. (2023) 'A review on fog computing: issues, characteristics, challenges, and potential applications', *Telematics and Informatics Reports*, 10, p. 100049.

De Donno, M., Felipe, J.M.D. and Dragoni, N. (2019) 'ANTIBIOTIC 2.0: A fog-based anti-malware for Internet of Things', in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, pp. 11–20.

De Vivo, M. *et al.* (1999) 'Internet vulnerabilities related to TCP/IP and T/TCP', *ACM SIGCOMM Computer Communication Review*, 29(1), pp. 81–85.

Diaz-Sanchez, D. *et al.* (2019) 'TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications', *IEEE Communications Surveys & Tutorials*, 21(4), pp. 3502–3531.

Diro, A., Mahmood, A. and Chilamkurti, N. (2021) 'Collaborative intrusion detection schemes in fog-to-things computing', *Fog/edge computing for security, privacy, and applications*, pp. 93–119.

Dsouza, C., Ahn, G.-J. and Taguinod, M. (2014) 'Policy-driven security management for fog computing: Preliminary framework and a case study', in *Proceedings of the 2014 IEEE 15th international conference on information reuse and integration (IEEE IRI 2014)*. IEEE, pp. 16–23.

Dwyer, O.P. *et al.* (2019) 'Profiling iot-based botnet traffic using dns', in *2019 IEEE global communications conference (GLOBECOM)*. IEEE, pp. 1–6.

Elmansy, H., Metwally, K. and Badran, K. (2023) 'Reinforcement learning-based security schema mitigating man-in-the-middle attacks in fog computing', *International Journal of Electrical and Computer Engineering (IJECE)*, 13(5), pp. 5908–5921.

Farhadi, M. *et al.* (2020) 'A systematic approach toward security in Fog computing: Assets, vulnerabilities, possible countermeasures', *Software: Practice and Experience*, 50(6), pp. 973–997.

Firdhous, M., Ghazali, O. and Hassan, S. (2014) 'Fog computing: Will it be the future of cloud computing?', in. The Third International Conference on Informatics & Applications (ICIA2014).

Fiveable (2024) *Hypervisor attack - (Network Security and Forensics) - Vocab, Definition, Explanations*. Available at: https://library.fiveable.me/key-terms/network-security-and-forensics/hypervisor-attack (Accessed: 28 October 2024).

Fortinet (2024a) *What is Attack Surface ?*, *Fortinet*. Available at: https://www.fortinet.com/resources/cyberglossary/attack-surface (Accessed: 26 March 2024).

Fortinet (2024b) *What Is Spyware? Definition, Types And Protection*. Available at: https://www.fortinet.com/resources/cyberglossary/spyware (Accessed: 29 October 2024).

Franklin, I.B. *et al.* (2018) 'A Survey on Data Recovery Approaches in Cloud Computing Environment', *International Journal of Computer Sciences and Engineering*, 6(5), pp. 440–447. Available at: https://doi.org/10.26438/ijcse/v6i5.440447.

GeeksforGeeks (2022) *Hardware Trojan*. Available at: https://www.geeksforgeeks.org/hardware-trojan/ (Accessed: 3 January 2025).

Goldberg, I. *et al.* (1996) 'A secure environment for untrusted helper applications: Confining the wily hacker', in *Proceedings of the 1996 USENIX Security Symposium*. USENIX Association Berkeley.

Gonzales, H. *et al.* (2010) 'Practical defenses for evil twin attacks in 802.11', in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE, pp. 1–6.

Goyal, S. (2014) 'Public vs private vs hybrid vs community-cloud computing: a critical review', *International Journal of Computer Network and Information Security*, 6(3), pp. 20–29.

Graz University of Technology (2018) *Meltdown and Spectre*. Available at: https://meltdownattack.com/ (Accessed: 30 November 2024).

Guan, Y. *et al.* (2018) 'Data Security and Privacy in Fog Computing', *IEEE Network*, 32(5), pp. 106–111. Available at: https://doi.org/10.1109/MNET.2018.1700250.

Gulatas, I. *et al.* (2023) 'Malware threat on edge/fog computing environments from Internet of Things devices perspective', *IEEE Access*, 11, pp. 33584–33606.

Hassan, S.R. and Rashad, M. (2023) *Cloud Computing to Fog Computing: A Paradigm Shift*, *IntechOpen*. Available at: https://www.intechopen.com/chapters/86772 (Accessed: 11 July 2024).

Homayoun, S. *et al.* (2019) 'DRTHIS: Deep ransomware threat hunting and intelligence system at the fog layer', *Future Generation Computer Systems*, 90, pp. 94–104.

Hu, P. *et al.* (2017) 'Survey on fog computing: architecture, key technologies, applications and open issues', *Journal of network and computer applications*, 98, pp. 27–42.

Hu, V.C. *et al.* (2013) 'Guide to attribute based access control (abac) definition and considerations (draft)', *NIST special publication*, 800(162), pp. 1–54.

Hu, Y.-C., Perrig, A. and Johnson, D.B. (2003) 'Packet leashes: a defense against wormhole attacks in wireless networks', in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*. IEEE, pp. 1976–1986.

Ibrahim, A.S., Hamlyn-Harris, J. and Grundy, J. (2016) 'Emerging security challenges of cloud virtual infrastructure', *arXiv preprint arXiv:1612.09059* [Preprint].

IGI GLOBAL (2024) *What is Partial/Selective Encryption*, *IGI GLOBAL*. Available at: https://www.igi-global.com/dictionary/partial-selective-encryption/21909 (Accessed: 6 August 2024).

Imperva (2024a) *What is Data Obfuscation*. Available at: https://www.imperva.com/learn/data-security/data-obfuscation/ (Accessed: 21 November 2024).

Imperva (2024b) *What is Slowloris?* Available at: https://www.imperva.com/learn/ddos/slowloris/ (Accessed: 4 December 2024).

Infocean (2024) *Threat/Vulnerability Management*. Available at: https://www.infocean.com/solutions/threat-vulnerability-management/ (Accessed: 14 October 2024).

Iorga, M. *et al.* (2017) *The nist definition of fog computing*. National Institute of Standards and Technology.

Ioulianou, P. (2021) *Protecting IoT networks against routing attacks*. PhD Thesis. University of York.

Ishiguro, K. and Kono, K. (2018) 'Hardening hypervisors against vulnerabilities in instruction emulators', in *Proceedings of the 11th European workshop on systems security*, pp. 1–6.

Jian, Z. and Chen, L. (2017) 'A defense method against docker escape attack', in *Proceedings of the 2017 International Conference on Cryptography, Security and Privacy*, pp. 142–146.

Jiang, S., Jiang, T. and Wang, L. (2017) 'Secure and efficient cloud data deduplication with ownership management', *IEEE Transactions on Services Computing*, 13(6), pp. 1152–1165.

Johnston, A.B. (2015) *SIP: understanding the session initiation protocol*. Artech House.

Juggernaut Pentesting Blog (2024) *Weak File Permissions*. Available at: https://juggernaut-sec.com/weak-file-permissions/#How_Permissions_Work_in_Linux (Accessed: 20 October 2024).

Junejo, A.K. (2019) *A secure integrated framework for fog-enabled cyber physical systems*. City, University of London.

Kalaria, R. *et al.* (2021) 'A Secure Mutual authentication approach to fog computing environment', *Computers & security*, 111, p. 102483.

Karagiannis, V. and Schulte, S. (2021) 'Distributed algorithms based on proximity for self-organizing fog computing systems', *Pervasive and Mobile Computing*, 71, p. 101316.

Katal, A. and Sethi, V. (2022a) 'Communication protocols in fog computing: a survey and challenges', in *Fog computing*. Chapman and Hall/CRC, pp. 153–170.

Katal, A. and Sethi, V. (2022b) 'Communication protocols in fog computing: a survey and challenges', in *Fog computing*. Chapman and Hall/CRC, pp. 153–170.

Katbi, A., Hammad, M. and Ksantini, R. (2023) 'A Survey on IOT Firmware Security', *International Journal of Computing and Digital Systems*, 14(1), pp. 190–199.

Kaur, J., Garg, U. and Bathla, G. (2023) 'Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review', *Artificial Intelligence Review*, 56(11), pp. 12725–12769.

Kaviyazhiny, C., Bala, P.S. and Gowri, A. (2021) 'Fog computing perspective: technical trends, security practices, and recommendations', *The Smart Cyber Ecosystem for Sustainable Development*, pp. 323–351.

Kayes, A. *et al.* (2020) 'A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues', *Sensors*, 20(9), p. 2464.

Khalid, F. *et al.* (2020) 'MacLeR: machine learning-based runtime hardware trojan detection in resource-constrained IoT edge devices', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(11), pp. 3748–3761.

Khan, S., Parkinson, S. and Qin, Y. (2017) 'Fog computing security: a review of current applications and security solutions', *Journal of Cloud Computing*, 6, pp. 1–22.

Khan, Z.A. and Namin, A.S. (2022) 'A survey of DDoS attack detection techniques for IoT systems using Blockchain technology', *Electronics*, 11(23), p. 3892.

Khater, B.S. *et al.* (2021) 'Classifier performance evaluation for lightweight IDS using fog computing in IoT security', *Electronics*, 10(14), p. 1633.

Kolias, C. *et al.* (2017) 'DDoS in the IoT: Mirai and other botnets', *Computer*, 50(7), pp. 80–84.

Koshkin, D. (2024) *Advantages And Disadvantages Of Cloud Deployment Models*. Available at: https://sam-solutions.us/insights/advantages-and-disadvantages-of-cloud-deployment-models/ (Accessed: 10 June 2024).

Krombholz, K. *et al.* (2015) 'Advanced social engineering attacks', *Journal of Information Security and applications*, 22, pp. 113–122.

Kumar, R.A. (2019) 'Possible solutions on security and privacy issues in fog computing'.

Kumarasamy, S. and Gowrishankar, A. (2012) 'An active defense mechanism for TCP SYN flooding attacks', *arXiv preprint arXiv:1201.2103* [Preprint].

Le, A. *et al.* (2013) 'The impact of rank attack on network topology of routing protocol for low-power and lossy networks', *IEEE Sensors Journal*, 13(10), pp. 3685–3692.

Li, Jiaxing *et al.* (2021) 'Blockchain-based secure key management for mobile edge computing', *IEEE Transactions on Mobile Computing*, 22(1), pp. 100–114.

Liu, J. *et al.* (2013) 'An experimental study of data retention behavior in modern DRAM devices: Implications for retention time profiling mechanisms', *ACM SIGARCH Computer Architecture News*, 41(3), pp. 60–71.

Loffi, L. *et al.* (2019) 'Mutual authentication for IoT in the context of fog computing', in *2019 11th International Conference on Communication Systems & Networks (COMSNETS)*. IEEE, pp. 367–374.

Loffi, L. *et al.* (2021) 'Mutual authentication with multi-factor in IoT-Fog-Cloud environment', *Journal of Network and Computer Applications*, 176, p. 102932.

Lu, Y. *et al.* (2021) 'Secure deduplication-based storage systems with resistance to side-channel attacks via fog computing', *IEEE Sensors Journal*, 22(18), pp. 17529–17541.

Lynn, T. *et al.* (2014) 'Towards a framework for defining and categorising business Process-As-A-Service (BPaaS)', in *21st International Product Development Management Conference*.

Mahadevappa, P. and Murugesan, R.K. (2021) 'Study of container-based virtualisation and threats in fog computing', in *Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2*. Springer, pp. 535–549.

Maher, R. and Nasr, O.A. (2021) 'DropStore: A secure backup system using multi-cloud and fog computing', *IEEE Access*, 9, pp. 71318–71327.

Mallick, S.R. *et al.* (2024) 'Fog-Assisted Blockchain-IoMT Healthcare Framework with Role-Based Access Control for Critically Ill Patients', *SN Computer Science*, 5(6), p. 658.

Manor, G.L. (2024) *MAC vs. DAC: Comparing Access Control Fundamentals*, *Permit.io*. Available at: https://www.permit.io/blog/mac-vs-dac-comparing-access-control-fundamentals (Accessed: 3 November 2024).

Manzoor, A. *et al.* (2022) 'Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges', *International Journal of Communication Systems*, 35(12), p. e4033.

Mao, Z., Li, N. and Molloy, I. (2009) 'Defeating cross-site request forgery attacks with browser-enforced authenticity protection', in *Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers 13*. Springer, pp. 238–255.

Mell, P. and Grance, T. (2011) *SP 800-145, The NIST Definition of Cloud Computing*, *NIST*. Available at: https://csrc.nist.gov/pubs/sp/800/145/final (Accessed: 5 May 2024).

Midoglu, C. *et al.* (2021) 'Large scale "speedtest" experimentation in mobile broadband networks', *Computer Networks*, 184, p. 107629.

Mishra, P. and Yadav, S.K. (2020) 'Threats and vulnerabilities to IoT end devices architecture and suggested remedies', *International Journal of Recent Technology and Engineering (IJRTE)*, 8, pp. 5712–5718.

Mohammed, M.A. *et al.* (2023) 'Bio-inspired robotics enabled schemes in blockchain-fog-cloud assisted IoMT environment', *Journal of King Saud University-Computer and Information Sciences*, 35(1), pp. 1–12.

Möller, B., Duong, T. and Kotowicz, K. (2014) 'This POODLE bites: exploiting the SSL 3.0 fallback', *Security Advisory*, 21, pp. 34–58.

Muddumadappa, P., Anjanappa, S. and Srikantaswamy, M. (2022) 'An efficient reconfigurable cryptographic model for dynamic and secure unstructured data sharing in multi-cloud storage server', *J. Intell Syst. Control*, 1(1), pp. 68–78.

Murkomen, T. (2023a) 'Privacy and security issues in fog-to-fog communication: A survey', *World Journal of Advanced Research and Reviews*, 20(3), pp. 466–491.

Murkomen, T. (2023b) 'Privacy and security issues in fog-to-fog communication: A survey', *World Journal of Advanced Research and Reviews*, 20(3), pp. 466–491.

Murugesan, A. *et al.* (2021) 'Analysis on homomorphic technique for data security in fog computing', *Transactions on Emerging Telecommunications Technologies*, 32(9), p. e3990.

Naha, R.K. *et al.* (2018) 'Fog computing: Survey of trends, architectures, requirements, and research directions', *IEEE access*, 6, pp. 47980–48009.

Naik, C. *et al.* (2019) 'Location privacy using data obfuscation in fog computing', in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, pp. 1286–1291.

Nath, S.B. *et al.* (2018) 'A survey of fog computing and communication: current researches and future directions', *arXiv preprint arXiv:1804.04365* [Preprint].

Neerugatti, V. and Mohan Reddy, A.R. (2019) 'Machine learning based technique for detection of rank attack in RPL based internet of things networks', *Machine Learning Based Technique for*

Detection of Rank Attack in RPL based Internet of Things Networks (July 10, 2019). International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN, pp. 2278–3075.

Ni, J. *et al.* (2017) 'Securing fog computing for internet of things applications: Challenges and solutions', *IEEE Communications Surveys & Tutorials*, 20(1), pp. 601–628.

Nikravan, M. and Kashani, M.H. (2022) 'A review on trust management in fog/edge computing: Techniques, trends, and challenges', *Journal of Network and Computer Applications*, 204, p. 103402.

NIST (2011) 'Final Version of NIST Cloud Computing Definition Published', *NIST* [Preprint]. Available at: https://doi.org/10/final-version-nist-cloud-computing-definition-published.

Numan, M. *et al.* (2020) 'A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks', *IEEE Access*, 8, pp. 65450–65461. Available at: https://doi.org/10.1109/ACCESS.2020.2983091.

Okta (2024) *Session Hijacking Attack: Definition, Damage & Defense*. Available at: https://www.okta.com/identity-101/session-hijacking/ (Accessed: 4 December 2024).

Ometov, A. *et al.* (2022) 'A survey of security in cloud, edge, and fog computing', *Sensors*, 22(3), p. 927.

Open University (2024) *Risk management*. Available at: https://www.open.edu/openlearn/mod/oucontent/view.php?id=88999&section=6.2 (Accessed: 29 November 2024).

Packetlabs (2024) *What Are Oracle Attacks?* Available at: https://www.packetlabs.net/posts/what-are-oracle-attacks/ (Accessed: 7 December 2024).

Paganini, P. (2020) *Mozi Botnet is responsible for most of the IoT Traffic*, *Cyber Defense Magazine*. Available at: https://www.cyberdefensemagazine.com/mozi-botnet-is-responsible-for-most-of-the-iot-traffic/ (Accessed: 9 December 2024).

Pakmehr, A. *et al.* (2023) 'Security challenges for cloud or fog computing-based ai applications', *arXiv preprint arXiv:2310.19459* [Preprint].

Patel, V.H. and Patel, S. (2020) 'A Review on IoT Security: Challenges and Solution using Lightweight Cryptography and Security Service Mechanisms Offloading at Fog'.

Patil, A. and Gaikwad, R. (2015) 'Comparative analysis of the prevention techniques of denial of service attacks in wireless sensor network', *Procedia Computer Science*, 48, pp. 387–393.

Patwary, A.A.-N. *et al.* (2020) 'Authentication, access control, privacy, threats and trust management towards securing fog computing environments: A review', *arXiv preprint arXiv:2003.00395* [Preprint].

Patwary, A.A.-N., Hossain, N. and Sami, M.A. (2019) 'A detection approach for finding rogue fog node in fog computing environments', *Am. J. Eng. Res*, 8, pp. 2320–0847.

Pék, G., Buttyán, L. and Bencsáth, B. (2013) 'A survey of security issues in hardware virtualization', *ACM Computing Surveys (CSUR)*, 45(3), pp. 1–34.

Pervez, S., Alandjani, G. and Babar, F. (no date) 'An Efficient Cloud Model with integrated Services by addressing Major Security Challenges'.

Point Monitor Corporation (2024) *What Are The 4 Types Of Security Controls*. Available at: https://pointmonitor.com/what-are-the-4-types-of-security-controls-point-monitor-corporation/ (Accessed: 29 November 2024).

Popoola, O. *et al.* (2023) 'A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: problems, challenges and solutions', *Blockchain: Research and Applications*, p. 100178.

Posey, B. (2022) *What is device as a service (DaaS)?* Available at: https://www.techtarget.com/searchvirtualdesktop/definition/device-as-a-service (Accessed: 3 June 2024).

Poston, H. (2020) *Cryptography-based Vulnerabilities in Applications*, *Infosec*. Available at: https://www.infosecinstitute.com/resources/secure-coding/cryptography-based-vulnerabilities-in-applications/ (Accessed: 24 October 2024).

Prajapati, P. *et al.* (2021) 'A review on recent intrusion detection systems and intrusion prevention systems in IoT', in *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, pp. 588–593.

Preneel, B. (2011) 'Collision Attack', in H.C.A. Van Tilborg and S. Jajodia (eds) *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US, pp. 220–221. Available at: https://doi.org/10.1007/978-1-4419-5906-5_564.

Promon (2024) *Device cloning*. Available at: https://promon.co/resources/security-software-glossary/device-cloning (Accessed: 9 December 2024).

Pure Storage (2024) *Emulation vs. Virtualization: What's the Difference?*, *Pure Storage*. Available at: https://blog.purestorage.com/purely-educational/emulation-vs-virtualization/ (Accessed: 22 July 2024).

Puthal, D. *et al.* (2019) 'Fog computing security challenges and future directions [energy and security]', *IEEE Consumer Electronics Magazine*, 8(3), pp. 92–96.

Qureshi, R. *et al.* (2023) 'A Survey on Security Issues and Attacks of Fog Computing', *VFAST Transactions on Software Engineering*, 11(1), pp. 1–11.

Radware (2024a) *The Story of the Mirai Botnet*, *Radware*. Available at: https://www.radware.com/security/ddos-knowledge-center/ddospedia/mirai/ (Accessed: 24 June 2024).

Radware (2024b) *What is an HTTP Flood Attack?* Available at: https://www.radware.com/cyberpedia/application-security/http-flood/ (Accessed: 28 October 2024).

Rahman, F.H. *et al.* (2019) 'A performance study of high-end fog and fog cluster in ifogsim', in *Computational Intelligence in Information Systems: Proceedings of the Computational Intelligence in Information Systems Conference (CIIS 2018) 3*. Springer, pp. 87–96.

Rahman, G. and Wen, C.C. (2018) 'Fog computing, applications, security and challenges, review', *International Journal of Engineering & Technology*, 7(3), pp. 1615–1621.

Rajendran, G. *et al.* (2023) 'Pushing the limits of generic side-channel attacks on LWE-based KEMs-parallel PC oracle attacks on Kyber KEM and beyond', *IACR Transactions on Cryptographic Hardware and Embedded Systems* [Preprint].

Rashidi, L. *et al.* (2021) 'More than a Fair Share: Network Data Remanence Attacks against Secret Sharing-based Schemes.', in *NDSS*.

Rastogi, A. (2010) 'A model based approach to implement cloud computing in e-Governance', *International Journal of Computer Applications*, 9(7), pp. 15–18.

Rawat, R. *et al.* (2022) 'Rooted learning model at fog computing analysis for crime incident surveillance', in *2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*. IEEE, pp. 1–9.

Rehman, S.-U. *et al.* (2013) 'Vehicular ad-hoc networks (VANETs): an overview and challenges', *Journal of Wireless Networking and communications*, 3(3), pp. 29–38.

Riggs, H. *et al.* (2023) 'Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure', *Sensors*, 23(8), p. 4060.

Roman, R., Lopez, J. and Mambo, M. (2018) 'Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges', *Future Generation Computer Systems*, 78, pp. 680–698.

Rosencrance, L. (2021) *SaaS vs. IaaS vs. PaaS: Differences, Pros, Cons and Examples*, *TechTarget*. Available at: https://www.techtarget.com/whatis/SaaS-IaaS-PaaS-Comparing-Cloud-Service-Models (Accessed: 13 May 2024).

Rupanetti, D. and Kaabouch, N. (2024) 'Combining Edge Computing-Assisted Internet of Things Security with Artificial Intelligence: Applications, Challenges, and Opportunities', *Applied Sciences*, 14(16), p. 7104.

Saad, M. (2018) 'Fog Computing and Its Role in the Internet of Things: Concept, Security and Privacy Issues', *International Journal of Computer Applications*, 180(32), pp. 7–9. Available at: https://doi.org/10.5120/ijca2018916829.

Sahota, J. and Vlajic, N. (2021) 'Mozi IoT malware and its botnets: From theory to real-world observations', in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, pp. 698–703.

Sánchez, D.D. *et al.* (2018) 'Dns-based dynamic authentication for microservices in IOT', in *Proceedings*. MDPI, p. 1233.

Sane, B.O., Niang, I. and Fall, D. (2018) 'A review of virtualization, hypervisor and vm allocation security: Threats, vulnerabilities, and countermeasures', in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, pp. 1317–1322.

Sapphire (2024) *What Are Honeypots? Types, Benefits, Risks, and Best Practices*. Available at: https://www.sapphire.net/blogs-press-releases/what-are-honeypots/ (Accessed: 21 November 2024).

Sarwar, K. *et al.* (2021) 'A survey on privacy preservation in fog-enabled internet of things', *ACM Computing Surveys (CSUR)*, 55(1), pp. 1–39.

ScienceDirect (2024) *Security Mechanism*. Available at: https://www.sciencedirect.com/topics/computer-science/security-mechanism (Accessed: 29 November 2024).

Securiti (2024) *What is Countermeasure?* Available at: https://securiti.ai/glossary/countermeasure/ (Accessed: 29 November 2024).

Selim, I. and Sadek, R. (2021) 'A Review of Intrusion Detection and Prevention Systems in Fog Computing Environment', *FCI-H Informatics Bulletin*, 3(2), pp. 17–22.

Sendhil, R. and Amuthan, A. (2020) 'A descriptive study on homomorphic encryption schemes for enhancing security in fog computing', in *2020 International Conference on Smart Electronics and Communication (ICOSEC)*. IEEE, pp. 738–743.

Seshadri, S.S. *et al.* (2020) 'IoTCop: A blockchain-based monitoring framework for detection and isolation of malicious devices in Internet-of-Things systems', *IEEE Internet of Things Journal*, 8(5), pp. 3346–3359.

Seth, D., Najana, M. and Ranjan, P. (2024) 'Compliance and regulatory challenges in cloud computing: a sector-wise analysis', *International Journal of Global Innovations and Solutions (IJGIS)* [Preprint].

Shirey, R. (2000) *RFC 2828 - Internet Security Glossary*, *Datatracker*. Available at: https://datatracker.ietf.org/doc/html/rfc2828 (Accessed: 27 March 2024).

Simmon, E. and others (2018) 'Evaluation of cloud computing services based on NIST SP 800-145', *NIST Special Publication*, 500(322), pp. 500–322.

Song, S., Choi, B.-Y. and Kim, D. (2016) 'Selective encryption and component-oriented deduplication for mobile cloud data computing', in *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, pp. 1–5.

Srirama, S.N. (2024) 'A decade of research in fog computing: relevance, challenges, and future directions', *Software: Practice and Experience*, 54(1), pp. 3–23.

Stallings, W. and Brown, L. (2015) *Computer security: principles and practice*. Pearson.

Standaert, F.-X. (2010) 'Introduction to Side-Channel Attacks', in I.M.R. Verbauwhede (ed.) *Secure Integrated Circuits and Systems*. Boston, MA: Springer US (Integrated Circuits and Systems), pp. 27–42. Available at: https://doi.org/10.1007/978-0-387-71829-3_2.

Stanik, A., Hovestadt, M. and Kao, O. (2012) 'Hardware as a Service (HaaS): Physical and virtual hardware on demand', in *4th IEEE international conference on cloud computing technology and science proceedings*. IEEE, pp. 149–154.

Strom, D. (2019) *Exploring multifactor authentication benefits and technology*, *TechTarget*. Available at: https://www.techtarget.com/searchsecurity/feature/The-fundamentals-of-MFA-Multifactor-authentication-in-the-enterprise (Accessed: 6 July 2024).

Su, J. *et al.* (2015) 'Steiner tree based optimal resource caching scheme in fog computing', *China Communications*, 12(8), pp. 161–168.

Suryateja, P. (2018) 'Threats and vulnerabilities of cloud computing: a review', *International Journal of Computer Sciences and Engineering*, 6(3), pp. 297–302.

Syed, M.H., Fernandez, E.B. and Silva, P. (2017) 'The secure software container pattern', in *Proceedings of the 23rd Conference on Pattern Languages of Programs (PLoP 2017). Vancouver, Canada*.

Tekiner, E. *et al.* (2021) 'SoK: cryptojacking malware', in *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, pp. 120–139.

The Network Encyclopedia (2024) *Black hole*. Available at: http://www.thenetworkencyclopedia.com/entry/black-hole/ (Accessed: 7 December 2024).

Valadares, D.C.G. *et al.* (2021) 'Trusted Execution Environments for Cloud/Fog-based Internet of Things Applications.', in *CLOSER*, pp. 111–121.

Vaquero, L.M. and Rodero-Merino, L. (2014) 'Finding your way in the fog: Towards a comprehensive definition of fog computing', *ACM SIGCOMM computer communication Review*, 44(5), pp. 27–32.

Velte, A.T., Velte, T.J. and Elsenpeter (2010) *Cloud Computing Μια Πρακτική Προσέγγιση*.

Vishwanath, A., Peruri, R. and He, J. (Selena) (2016) *Security in fog computing through encryption*. DigitalCommons@ Kennesaw State University Kennesaw, Georgia, USA.

Volokyta, A., Kokhanevych, I. and Ivanov, D. (2012) 'Secure virtualization in cloud computing', in *Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science*. IEEE, pp. 395–395.

Wan, J., Waqas, M., Tu, S., Mudassir Hussain, S., *et al.* (2021) 'An Efficient Impersonation Attack Detection Method in Fog Computing', *Computers, Materials & Continua*, 68(1), pp. 267–281. Available at: https://doi.org/10.32604/cmc.2021.016260.

Wan, J., Waqas, M., Tu, S., Hussain, S.M., *et al.* (2021) 'An efficient impersonation attack detection method in fog computing', *CMC-Comput Mater Cont*, 68(1), pp. 267–281.

Wei, Z. *et al.* (2009) 'A cryptography index technology and method to measure information disclosure in the DAS model', *WSEAS Transactions on Information Science and Applications*, 6(9), pp. 1443–1452.

Weng, C.-Y. *et al.* (2021) 'A lightweight anonymous authentication and secure communication scheme for fog computing services', *IEEE Access*, 9, pp. 145522–145537.

Wikipedia (2024a) *Cyberattack*. Available at: https://en.wikipedia.org/wiki/Cyberattack (Accessed: 27 March 2024).

Wikipedia (2024b) *Data as a service*, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Data_as_a_service (Accessed: 16 May 2024).

Wikipedia (2024c) *Sandbox (computer security)*. Available at: https://en.wikipedia.org/wiki/Sandbox_%28computer_security%29 (Accessed: 18 May 2024).

Wikipedia (2024d) *Spectre (security vulnerability)*. Available at: https://en.wikipedia.org/wiki/Spectre_(security_vulnerability) (Accessed: 30 November 2024).

Wikipedia (2024e) *Verifiable computing*. Available at: https://en.wikipedia.org/wiki/Verifiable_computing (Accessed: 15 August 2024).

Wilson, D. (2020) 'IoT is Creating Massive Growth Opportunities', *Cisco Systems*, 23.

Wong, A.Y. *et al.* (2023) 'On the security of containers: Threat modeling, attack analysis, and mitigation strategies', *Computers & Security*, 128, p. 103140.

WordReference (2024) *batch processing*. Available at: https://www.wordreference.com/engr/batch%20processing (Accessed: 20 June 2024).

Xie, X. *et al.* (2019) 'Sql injection detection for web applications based on elastic-pooling cnn', *IEEE Access*, 7, pp. 151475–151481.

Yaseen, Q. *et al.* (2016) 'A fog computing based system for selective forwarding detection in mobile wireless sensor networks', in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W)*. IEEE, pp. 256–262.

YELER, B. (2021) *How to Tell the Difference that Vulnerability, Threat, and Risk?*, *Medium*. Available at: https://bugrayeler.medium.com/how-to-tell-the-difference-that-vulnerability-threat-or-risk-4a96117f8f26 (Accessed: 10 May 2024).

Yi, S., Li, C. and Li, Q. (2015a) 'A survey of fog computing: concepts, applications and issues', in *Proceedings of the 2015 workshop on mobile big data*, pp. 37–42.

Yi, S., Li, C. and Li, Q. (2015b) 'A survey of fog computing: concepts, applications and issues', in *Proceedings of the 2015 workshop on mobile big data*, pp. 37–42.

Yousefpour, A., Ishigaki, G. and Jue, J.P. (2017) 'Fog computing: Towards minimizing delay in the internet of things', in *2017 IEEE international conference on edge computing (EDGE)*. IEEE, pp. 17–24.

Zahid, A. (2023) *(26) Understanding Insecure Design Vulnerability: An Overview of Risks and Solutions*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/understanding-insecure-design-vulnerability-overview-risks-zahid-ali/ (Accessed: 25 October 2024).

Zahra, F.T., Bostanci, Y.S. and Soyturk, M. (2024) 'Security of Wireless IoT in Smart Manufacturing: Vulnerabilities and Countermeasures', in *Intelligent Secure Trustable Things*. Springer, pp. 419–441.

Zahra, S.R. and Chishti, M.A. (2023) 'Fuzzy logic and fog based secure architecture for internet of things (flfsiot)', *Journal of ambient intelligence and humanized computing*, pp. 1–25.

Zenarmor (2024) *Multi-Tenancy Explained. From Fundamentals to Implementation (Pros, Cons, Security, and Examples)*. Available at: https://www.zenarmor.com/docs/network-basics/what-is-multi-tenancy (Accessed: 18 May 2024).

Zhang, J. (2019) *The Importance of Effective Correlation for Threat Intelligence Users*. Available at: https://www.securitymagazine.com/articles/90996-the-importance-of-effective-correlation-for-threat-intelligence-users (Accessed: 20 October 2024).

Zhang, P. *et al.* (2018) 'A survey on access control in fog computing', *IEEE Communications Magazine*, 56(2), pp. 144–149.

Zimba, A. and Chama, V. (2018) 'Cyber attacks in cloud computing: modelling multi-stage attacks using probability density curves', *International Journal of Computer Network and Information Security*, 14(3), p. 25.

Zwayed, F.A. *et al.* (2021) 'Intrusion Detection Systems in Fog Computing–A Review', in *Advances in Cyber Security: Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers 3*. Springer, pp. 481–504.

Γκρίτζαλης, Δ. (2013) *Ασφάλεια Πληροφοριακών Συστημάτων και Υποδομών: Εννοιολογική Θεμελίωση*, *Εκδόσεις Νέων Τεχνολογίων*. Available at: https://newtech-pub.com/wp-content/uploads/2013/10/kef-asf.plhr_.sust_.pdf (Accessed: 7 May 2024).

Δασυγένης, Μ. (2013) *Τμήμα Μηχανικών Πληροφορικής & Τηλεπικοινωνιών Συστήματα Παράλληλης & Κατανεμημένης Επεξεργασίας Ενότητα 14: Cloud Computing*. Available at: https://docplayer.gr/48412825-Systimata-parallilis-katanemimenis-epexergasias.html (Accessed: 31 May 2024).

Zimperium (2024) *What is Certificate Pinning?* Available at: https://www.zimperium.com/glossary/certificate-pinning/ (Accessed: 16 August 2024).

Κάτσικας, Σ. (2014) *Διαχείριση της ασφάλειας πληροφοριών*. Πεδίο. Αθήνα.

Κιουντούζης, Ε. (2004) *Διαχείριση Έργων Πληροφορικής*.

Κοντόπουλος, Ι. and Ματσαρίδης, Π. (2013) 'Cloud Computing Συστήματα Παρ. & Κατ. Επεξεργασίας'. *Τμήμα Μηχανικών Πληροφορικής & Τηλεπικοινωνιών Πολυτεχνική Σχολή Κοζάνης Πανεπιστήμιο Δυτικής Μακεδονίας*, 17 July. Available at: https://arch.icte.uowm.gr/docs/CloudComputing_Parallel_Distributed_Dasygenis_Matsaridhs_Kontopoulous.pdf.

Κρητικός, Κ. (2023) '234 Ασφάλεια & Ιδιωτικότητα στο Διαδίκτυο του Μέλλοντος Κυριάκος Κρητικός Αναπλ . Καθηγητής Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων Ασφάλεια Ομιχλώδους Υπολογισμού (Fog Computing Security)'.

Κρητικός, Κυριάκος (2023) '234 Ασφάλεια & Ιδιωτικότητα στο Διαδίκτυο του Μέλλοντος Κυριάκος Κρητικός Αναπλ . Καθηγητής Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων ΕΙΣΑΓΩΓΗ'.

Νταρζάνος, Π. (2016) *Τεχνοοικονομική Μελέτη των Ultra-Dense Deployments σε Κινητά Δίκτυα 5G*, *ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ*. Available at: https://telematics.upatras.gr/telematics/system/files/bouras_site/ergasies/diplwmatikes/ntarzanos_5g.pdf?language=el (Accessed: 12 May 2024).