FOG COMPUTING: ΑΝΑΛΥΣΗ ΘΕΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Η Διπλωματική Εργασία

παρουσιάστηκε ενώπιον

του Διδακτικού Προσωπικού του

Πανεπιστημίου Αιγαίου

Σε Μερική Εκπλήρωση

των Απαιτήσεων για το Δίπλωμα του

Μηχανικού Πληροφοριακών και Επικοινωνιακών Συστημάτων

του

Θεόδωρου Μπερμπερίδη

ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2020

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΔΙΔΑΣΚΟΝΤΩΝ ΕΠΙΚΥΡΩΝΕΙ

ΤΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΤΟΥ ΘΕΟΔΩΡΟΥ ΜΠΕΡΜΠΕΡΙΔΗ:

Καρύδα Μαρία, Αναπληρώτρια Καθηγήτρια, Επιβλέπουσα
Ημερομηνία 6/02/2020

Τμήμα Μηχανικών Πληροφοριακών και

Επικοινωνιακών Συστημάτων

Κοκολάκης Σπύρος, Καθηγητής, Μέλος

Τμήμα Μηχανικών Πληροφοριακών και

Επικοινωνιακών Συστημάτων

Ελισάβετ Κωνσταντίνου, Μόνιμη Επίκουρος, Μέλος

Τμήμα Μηχανικών Πληροφοριακών και

Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΧΕΙΜΕΡΙΝΟ ΕΞΑΜΗΝΟ 2020

ΠΕΡΙΛΗΨΗ

Ο κόσμος των υπολογιστών έχει δει μια μεγάλη μεταστροφή από την παραδοσιακή προσωπική υπολογιστική, στην σημερινή επικοινωνία ανάμεσα σε πελάτες και εξυπηρετητές, λόγω και των εξελίξεων στην δικτύωση των υπολογιστών. Η επικοινωνία client – server έχει εξελιχθεί ολοκληρωτικά στο Cloud Computing, το οποίο παρέχει προσαρμοστικότητα, υψηλό επίπεδο διαθεσιμότητας και ανοχή στα λάθη. Λόγω όμως της γρήγορης εξάπλωσης των συσκευών του Internet of Things (IoT), απαιτείται μεγαλύτερη υποστήριξη σε θέματα καθυστερήσεων, κάτι το οποίο το cloud δεν μπορεί να προσφέρει. Για τον λόγο αυτό, τα τελευταία χρόνια έχει προταθεί ένα νέο είδος υπολογιστικής πλατφόρμας, το Fog Computing, στο οποίο οι υπολογισμοί αναθέτονται σε συσκευές στο άκρο του δικτύου και οι οποίες με τη σειρά τους αλληλοεπιδρούν με τον εξυπηρετητή του cloud για να προσφέρουν μεγαλύτερη ποιότητα υπηρεσιών στους τελικούς χρήστες.

Καθώς το Fog Computing θεωρείται μια σημαντική εξέλιξη και επέκταση του Cloud, είναι φυσικό να μπορούμε να αναφέρουμε πως τα περισσότερα ζητήματα ασφάλειας του Cloud «κληρονομούνται» και στο Fog Computing. Ωστόσο, λόγω των μοναδικών χαρακτηριστικών που προσφέρει το Fog Computing και τα οποία το διαφοροποιούν από το Cloud, εμφανίζονται και περαιτέρω προκλήσεις σε ότι αφορά στο θέμα της ασφάλειας και της ιδιωτικότητας. Εάν αυτά τα θέματα δεν αναγνωριστούν, τότε η εξέλιξη και η προώθηση του Fog Computing θα καθυστερήσει σημαντικά.

Στην συγκεκριμένη διπλωματική εργασία, θα αναφερθούμε αρχικά στον ορισμό του Fog Computing, στην αρχιτεκτονική του καθώς και στις διαφορές που το διέπουν με το Cloud computing. Έπειτα, θα παρουσιάσουμε ορισμένα παραδείγματα εφαρμογών του που ήδη εφαρμόζονται και κυκλοφορούν στο εμπόριο. Στη συνέχεια, θα παρουσιάσουμε εκτενώς τα διάφορα θέματα που σχετίζονται με την ασφάλεια και την ιδιωτικότητα: από τις απαιτήσεις ασφάλειας και τις αδυναμίες, έως τις απειλές και τα μέσα προστασίας τους. Τέλος, καταλήγουμε με την ανάλυση ενός συγκεκριμένου σεναρίου χρήσης που αναφέρεται στον περιορισμό της υποκλοπής των εσωτερικών δεδομένων.

.

Λέξεις-κλειδιά: Fog Computing, Cloud Computing, Internet of Things, Ασφάλεια, Ιδιωτικότητα.

ABSTRACT

The computing word has seen a great shift from the traditional, personal computing, to the communication between clients and servers, with the advancements of the computing networking. The communication between clients and servers has completely evolved to Cloud Computing, which provides flexibility, high level of availability and fault tolerance. However, due to the fact that the use of Internet of Things devices have greatly expanded, a latency – sensitive support is required, which a cloud cannot provide. For this reason, nowadays, a new kind of computing platform has been produced, Fog Computing, in which the computation is assigned to devices at the edge of the network, and these devices interplay with the server of the cloud to provide better quality of service to the end users.

As Fog Computing is considered a significant evolution and extension of Cloud, it is only natural to assume that most of the security issues of Cloud are inherited to Fog Computing. However, because of the fact that Fog Computing has some unique features that differentiate it from Cloud, new challenges are presented in terms of security and privacy. If these challenges are not identified, thus the evolution and promotion of Fog Computing will significantly be delayed.

In this thesis, we will first discuss about the definition of Fog Computing, its architecture and the differences that differentiate it from Cloud Computing. Furthermore, we will present some examples of applications that are already in use and are available on the market. Moreover, we will thoroughly analyze the security and privacy issues: from the security challenges and weaknesses, to the threats and their countermeasures. Finally, this thesis will conclude with the analysis of a certain use – case scenario, that refers to the limitation of the insider data theft.

.

Keywords: Fog Computing, Cloud Computing, Internet of Things, Security, Privacy.

Theodoros Bermperidis

Department of Information and Communication Systems Engineering

UNIVERSITY OF THE AEGEAN

ΕΥΧΑΡΙΣΤΙΕΣ – ΑΦΙΕΡΩΣΕΙΣ

Αρχικά θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια, κυρία Καρύδα Μαρία, για την ανάθεση της συγκεκριμένης διπλωματικής εργασίας, την καθοδήγησή της και την υπομονή της καθ' όλη τη διάρκεια της διεκπεραίωσης της. Οι συμβουλές της, οι οδηγίες καθώς και οι διορθώσεις ήταν πάντα ακριβής και σαφής για την βελτίωση της συγκεκριμένης εργασίας.

Τέλος, οφείλω ένα μεγάλο ευχαριστώ στην οικογένεια μου, στη γυναίκα μου και στους αγαπημένους φίλους μου που με στήριξαν όλα τα χρόνια της φοιτητικής μου σταδιοδρομίας, καθώς και για την ηθική υποστήριξη που μου παρείχαν σε κάθε βήμα της ζωής μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

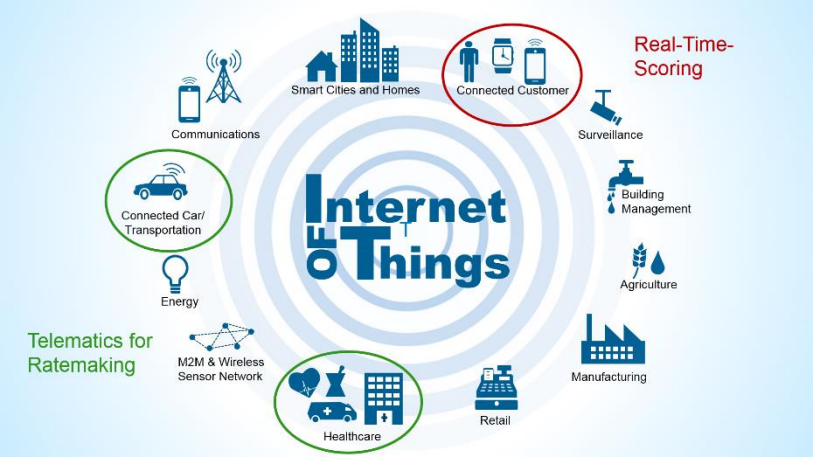
ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΕΦΑΛΑΙΟ 1 - ΕΙΣΑΓΩΓΗ

1.1 Internet of Things (IoT)

Το «Διαδίκτυο των Πραγμάτων», ή αλλιώς Internet of Things, αποτελεί μια νέα επανάσταση στο χώρου του διαδικτύου. Το κύριο χαρακτηριστικό του είναι πως μπορεί να οδηγήσει τα διάφορα αντικείμενα να αποκτήσουν νοημοσύνη, να επικοινωνούν πληροφορίες σχετικά με αυτά αλλά και να έχουν πρόσβαση σε πληροφορίες οι οποίες έχουν συλλεχθεί από άλλα αντικείμενα. Σε γενικότερο πλαίσιο, το Internet of Things επιτρέπει τους ανθρώπους και τα πράγματα να συνδέονται οποτεδήποτε, οπουδήποτε αλλά και με τον οποιονδήποτε, χρησιμοποιώντας κάθε λογής δίκτυα και υπηρεσίες.

Κατά τη διάρκεια των χρόνων έχουν γίνει αρκετές προσπάθειες για να δοθεί ένας συγκεκριμένος ορισμός για το Internet of Things και τα συστήματά του. Ένας από αυτούς προέρχεται από το περιοδικό του IEEE (IEEE, Internet of Things, 2014). Σύμφωνα με τον ορισμό αυτό "Ένα σύστημα IoT είναι ένα δίκτυο από δίκτυα όπου, τυπικά, ένας τεράστιος αριθμός από αντικείμενα/πράγματα/αισθητήρες/συσκευές συνδέονται μέσα από υποδομές επικοινωνιών και πληροφοριών για να παρέχουν αξιόπιστες υπηρεσίες μέσω της επεξεργασίας και της διαχείρισης ευφυών δεδομένων, για διαφορετικές εφαρμογές. Γενικότερα, το Internet of Things (IoT) είναι μια υπολογιστική έννοια που περιγράφει ένα μέλλον όπου τα καθημερινά αντικείμενα θα συνδέονται στο Διαδίκτυο και θα μπορούν να αναγνωρίζονται από άλλες συσκευές. Ο όρος αυτός μπορεί να συνδεθεί με το RFID[1] ως τη μέθοδο επικοινωνίας, ωστόσο μπορεί να περιλαμβάνει και άλλες τεχνολογίες, όπως τεχνολογίες αισθητήρων, ασύρματες, κωδικούς QR κτλ."



Εικόνα 1 - Internet Of Things **(**Source: SAS Blogs – IoT Trends 2017: Digital Twins /Edge Analytics schon spruchreif?**)**

[1] RFID (Radio Frequency Identification): Η απόδοση του όρου στα ελληνικά ορίζεται ως «ταυτοποίηση μέσω ραδιοσυχνοτήτων». Τα συστήματα αυτά αποτελούν ένα υποσύνολο των Συστημάτων Αυτόματου Προσδιορισμού (Automatic Identification Systems). Λειτουργεί ως γενικός όρος των τεχνολογιών που χρησιμοποιούν ραδιοκύματα για να προσδιορίσουν αυτόματα ανθρώπους ή αντικείμενα και αποτελεί την τεχνολογική εξέλιξη των ραβδωτών κωδικών (barcode).

Από όλες τις παραπάνω περιγραφές, μπορούμε να εκλάβουμε πως το Internet of Things παρέχει μορφές αλληλεπίδρασης ανάμεσα στο φυσικό και τον εικονικό κόσμο. Οι φυσικές συσκευές κατέχουν αντίστοιχες ψηφιακές οντότητες, μέσω των οποίων μπορούν να συνδέονται, να επικοινωνούν και να ανταλλάσσουν γνώσεις και δεδομένα με άλλες. Επιπλέον, οι άμεσες και κατάλληλες αποκρίσεις στις φυσικές οντότητες μπορούν να δοθούν μέσω της χρήσης ευφυών αλγορίθμων για λήψεις αποφάσεων στις προγραμματιστικές εφαρμογές, οι οποίοι με τη σειρά τους βασίζονται στις πληροφορίες που συλλέχθηκαν, είτε τις τελευταίες είτε βάσει ιστορικού, και για την ίδια οντότητα αλλά και για διαφορετικές. Τα παραπάνω έχουν συντελέσει στο να ανοίξει ο δρόμος για νέες διαστάσεις εφαρμογής του IoT, όπως είναι η διαχείριση της εφοδιαστικής αλυσίδας, οι μεταφορές, η ενέργεια, τα έξυπνα περιβάλλοντα (σπίτια, κτίρια, υποδομές), η γεωργία κ. ά.

Πίνακας 1 - Τομείς Εφαρμογών IoT

Τομέας	Περιγραφή	Εφαρμογές
Κοινωνία	Ενέργειες για την βελτίωση και την ανάπτυξη της κοινωνίας, των πόλεων και των ανθρώπων	Έξυπνες Πόλεις, Έξυπνη Γεωργία, Ιατροφαρμακευτική Περίθαλψη, Τηλεπικοινωνίες
Περιβάλλον	Ενέργειες που σχετίζονται με την προστασία, την επίβλεψη και την ανάπτυξη όλων των φυσικών πόρων	Έξυπνο Περιβάλλον, Έξυπνη Ανακύκλωση Νερού, Ειδοποιήσεις Έκτακτης Ανάγκης
Βιομηχανία	Ενέργειες που σχετίζονται με την οικονομία, τις εμπορικές συναλλαγές ανάμεσα σε εταιρείες, οργανισμούς και άλλες οντότητες	Λιανικό εμπόριο, Εφοδιασμός, Διαχείριση Εφοδιαστικής Αλυσίδας, Εναέριος χώρος και Αεροπλοΐα, Βιομηχανικός Έλεγχος

1.2 Στόχος της εργασίας

Η φήμη των εφαρμογών του IoT, καθώς και η αύξηση της ψηφιοποίησης των δομών της κοινωνίας, όπου εκατομμύρια έξυπνες συσκευές (πχ. Έξυπνα σπίτια, έξυπνα οχήματα, ασύρματα δίκτυα αισθητήρων μεγάλης έκτασης) ανταλλάσσουν συνεχώς πληροφορίες διαμέσου του Διαδικτύου, έχουν ως αποτέλεσμα την απαίτηση για την επεξεργασία και διαχείριση ενός τεράστιου όγκου δεδομένων. Για να επιτευχθεί αυτό, μια δημοφιλής επιλογή καθίσταται το Cloud Computing, λόγω της ελαστικότητας του, της υπολογιστικής ικανότητας και της αποθήκευσης, καθώς και άλλων δυνατοτήτων για την υποστήριξη της παροχής πόρων, σύμφωνα πάντα με τις ανάγκες των χρηστών. Παρ' όλα αυτά, τα τελευταία χρόνια, έχει προταθεί μια δομή για την επέκταση του Cloud computing από τον πυρήνα προς τα άκρα του δικτύου. Η δομή αυτή ορίζεται ως Fog Computing. Αυτή η δομή παρουσιάζει μια υψηλού επιπέδου εικονική πλατφόρμα, η οποία παρέχει υπηρεσίες υπολογισμών, δικτύωσης και αποθήκευσης ανάμεσα στο Cloud Computing και τις τερματικές συσκευές.

Στην εργασία αυτή θα εμβαθύνουμε περισσότερο στην καταγραφή και ανάλυση των θεμάτων ασφαλείας που διέπουν το fog computing. Αρχικά, στο πρώτο κομμάτι της εργασίας, δίνεται μια

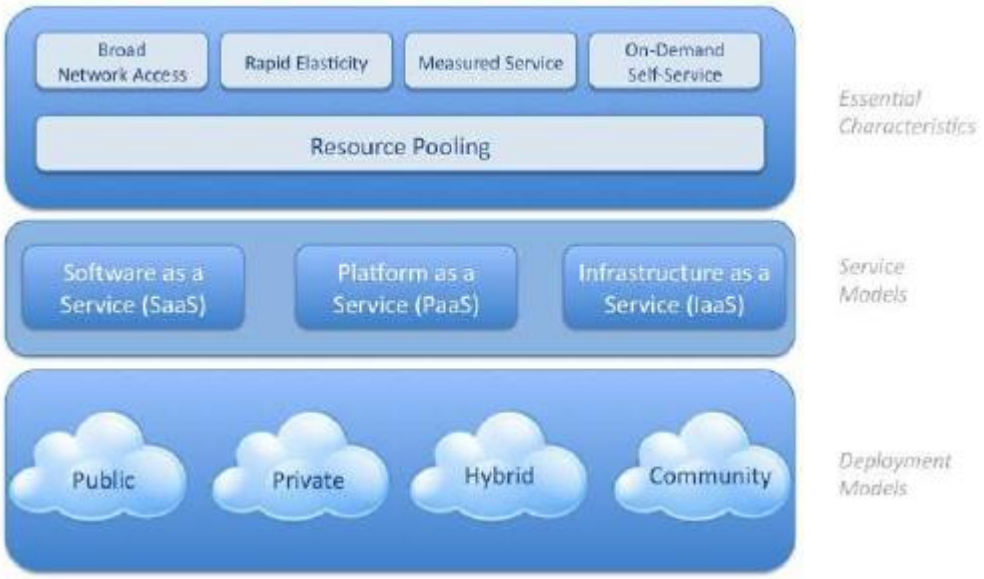
περιγραφή των βασικών χαρακτηριστικών των Cloud και Fog Computing, καθώς και των διαφορών τους. Έπειτα, παρουσιάζονται κάποια βασικά στοιχεία που αφορούν τις διαφορές των Cloud και Fog Computing πάνω στο θέμα της ενεργειακής κατανάλωσης, ενώ παράλληλα συζητούνται και ορισμένες κύριες παράμετροι που μπορούν να συνδράμουν στην εξοικονόμηση ενέργειας κατά την χρήση της πλατφόρμας του Fog Computing. Στη συνέχεια, παρουσιάζονται τα κύρια στοιχεία και οι προκλήσεις σε ότι αφορά την εφαρμογή της πλατφόρμας του Fog Computing, ενώ γίνεται αναφορά και σε εφαρμογές οι οποίες έχουν ήδη κυκλοφορήσει στο εμπόριο. Στο τέταρτο κομμάτι της εργασίας γίνεται μια εκτενής αναφορά στα βασικά θέματα ασφάλειας και ιδιωτικότητας που εμφανίζονται στο Fog Computing, ξεκινώντας με τις προκλήσεις για την σχεδίαση ασφαλών συστημάτων του Fog Computing, ενώ συνεχίζουμε με τις αναφορές για τις αδυναμίες και τις απειλές απέναντι στην πλατφόρμα. Έπειτα, στο πέμπτο κεφάλαιο της εργασίας αναφερόμαστε ειδικά σε μέσα προστασίας, τα οποία μπορούν να βοηθήσουν πρακτικά στην αντιμετώπιση αυτών των απειλών. Τέλος, η εργασία αυτή καταλήγει με την περιγραφή ενός σεναρίου χρήσης που αναφέρεται στην εφαρμογή ενός μοντέλου αντιμετώπισης επιθέσεων κλοπής δεδομένων στο fog computing, το οποίο έχει προταθεί.

ΚΕΦΑΛΑΙΟ 2 - ΠΕΡΙΓΡΑΦΗ ΤΟΥ FOG COMPUTING

Πριν να προχωρήσουμε στην αναλυτική περιγραφή του Fog Computing, είναι συνετό να ξεκινήσουμε δίνοντας μια βασική περιγραφή του Cloud Computing και των βασικών χαρακτηριστικών του, ούτως ώστε να μπορέσουμε να καταστήσουμε ευκολότερη την σύνδεση με το Fog Computing, καθώς και να αναγνωρίσουμε τις διαφορές που υφίστανται ανάμεσα στις δύο τεχνολογίες.

2.1 Ορισμός Cloud Computing

Σύμφωνα με το NIST (Mell and Grance, 2011: 2), το Cloud Computing χαρακτηρίζεται ως "ένα μοντέλο για την ενεργοποίηση μιας ευρείας, πρακτικής και κατ' αίτηση (on-demand) διαδικτυακής πρόσβασης σε μια κοινή ομάδα από επεξεργάσιμους υπολογιστικούς πόρους (π.χ. δίκτυα, εξυπηρετητές, αποθηκευτικούς χώρους, εφαρμογές και υπηρεσίες) που μπορούν να προβλεφθούν και να απελευθερωθούν άμεσα, με την ελάχιστη διαχειριστική προσπάθεια ή αλληλεπίδραση του παρόχου υπηρεσιών. Αυτό το μοντέλο cloud αποτελείται από 5 βασικά χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης''.



Εικόνα 2 - Ψηφιακό μοντέλο του Nist για τον ορισμό του Cloud Computing (Source: Researcher's Blog – NIST- Visual Model of Cloud Computing Definition)

2.2 Βασικά Χαρακτηριστικά

2.2.1 Αυτό-εξυπηρέτηση κατ' αίτηση (On-demand self-service).

Ένας καταναλωτής μπορεί μονόπλευρα να προβλέψει τις υπολογιστικές ικανότητες, όπως ο χρόνος του εξυπηρετητή και ο αποθηκευτικός χώρος του δικτύου, εφόσον χρειάζονται, αυτόματα, χωρίς την επίδραση του ανθρώπου με κάθε πάροχο υπηρεσίας.

2.2.2 Ευρεία δικτυακή πρόσβαση (Broad Network Access).

Οι υπολογιστικές δυνατότητες είναι διαθέσιμες στο δίκτυο και είναι προσβάσιμες μέσω συγκεκριμένων μηχανισμών που προωθούν την χρήση από ετερογενείς αδύνατες ή πυκνές πλατφόρμες πελατών (πχ. Κινητά τηλέφωνα, tablet, φορητοί υπολογιστές).

2.2.3 Ομαδοποίηση Πόρων (Resource pooling).

Οι υπολογιστικοί πόροι του παρόχου ομαδοποιούνται για να εξυπηρετήσουν πολλαπλούς καταναλωτές χρησιμοποιώντας ένα μοντέλο πολλαπλής ενοικίασης (multi-tenant), με διαφορετικούς φυσικούς και εικονικούς πόρους να θέτονται και να αναθέτονται δυναμικά, ανάλογα με τις απαιτήσεις των πελατών. Υπάρχει μια αίσθηση ανεξάρτητης τοποθέτησης, καθώς ο καταναλωτής, γενικά, δεν έχει κανέναν έλεγχο ή γνώση για την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να είναι σε θέση να προσδιορίσει την τοποθεσία σε υψηλότερο επίπεδο αφαίρεσης (π.χ. χώρα, περιφέρεια ή κέντρο δεδομένων). Παραδείγματα τέτοιων πόρων αποτελούν ο αποθηκευτικός χώρος, η επεξεργασία, η μνήμη και το εύρος ζώνης του δικτύου.

2.2.4 Άμεση ελαστικότητα (Rapid Elasticity).

Οι ικανότητες μπορούν να προβλεφθούν και να απελευθερωθούν «ελαστικά», και σε κάποιες περιπτώσεις αυτόματα, για να εξισορροπηθούν οι εξερχόμενες και οι εισερχόμενες, ισάξια, κατά απαίτηση. Για τον καταναλωτή, οι ικανότητες που είναι διαθέσιμες για πρόβλεψη συχνά εμφανίζονται ως απεριόριστες και μπορούν να διατεθούν σε οποιαδήποτε ποσότητα, την οποιαδήποτε στιγμή.

2.2.5 Measured Service

Τα συστήματα Cloud ελέγχουν και βελτιστοποιούν αυτόματα την χρήση πόρων αξιοποιώντας μια ικανότητα μέτρησης, σε κάποιο επίπεδο αφαίρεσης, κατάλληλη σύμφωνα με τον τύπο της υπηρεσίας (π.χ. αποθηκευτικός χώρος, επεξεργασία, εύρος ζώνης και ενεργοί λογαριασμοί χρηστών). Η χρήση πόρων μπορεί να ελεγχθεί, να παρακολουθείται και να καταγράφεται, παρέχοντας διαφάνεια και για τον πάροχο και για τον καταναλωτή της αξιοποιήσιμης υπηρεσίας.

2.3 Μοντέλα Υπηρεσιών

2.3.1 Λογισμικό ως Υπηρεσία (Software as a Service - SaaS).

Η δυνατότητα που παρέχεται στον καταναλωτή είναι η χρήση των εφαρμογών του παρόχου που τρέχουν πάνω σε μια υποδομή cloud (cloud infrastracture)[2]. Οι εφαρμογές είναι προσβάσιμες από διάφορες συσκευές, δια μέσου είτε μιας λεπτής υποδομής του πελάτη, όπως ενός προγράμματος περιήγησης (web browser) είτε ενός προγράμματος διεπαφής. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποβόσκουσα υποδομή cloud, συμπεριλαμβανομένου του δικτύου, των εξυπηρετητών, του λειτουργικού συστήματος, του αποθηκευτικού χώρου, ή ακόμα και ανεξάρτητων δυνατοτήτων των εφαρμογών, με πιθανή εξαίρεση τις περιορισμένες ρυθμίσεις των εφαρμογών που σχετίζονται με τον χρήστη.

2.3.2 Πλατφόρμα ως Υπηρεσία (Platform as a Service - PaaS).

Η δυνατότητα που παρέχεται στον καταναλωτή είναι η ανάπτυξη, πάνω στην υποδομή του cloud, εφαρμογών που κατασκευάστηκαν από τον ίδιο τον καταναλωτή ή εφαρμογών που αποκτήθηκαν και οι οποίες είναι κατασκευασμένες χρησιμοποιώντας γλώσσες προγραμματισμού, βιβλιοθήκες, υπηρεσίες και εργαλεία που υποστηρίζονται από τον πάροχο[3]. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποβόσκουσα υποδομή cloud, συμπεριλαμβανομένου του δικτύου, των εξυπηρετητών, του λειτουργικού συστήματος και του αποθηκευτικού χώρου, αλλά έχει έλεγχο πάνω στις αναπτυχθείσες εφαρμογές και πιθανώς στις ρυθμίσεις παραμέτρων για το περιβάλλον φιλοξενίας των εφαρμογών.

2.3.3 Υποδομή ως Υπηρεσία (Infrastracture as a Service - IaaS).

Η δυνατότητα που παρέχεται στον καταναλωτή είναι η πρόβλεψη της επεξεργασίας, του αποθηκευτικού χώρου, του δικτύου και άλλων θεμελιωδών υπολογιστικών πόρων, όπου ο καταναλωτής έχει την δυνατότητα της αξιοποίησης και της λειτουργίας αυθαίρετου λογισμικού, το οποίο μπορεί να περιλαμβάνει λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν διαχειρίζεται ή ελέγχει την υποβόσκουσα υποδομή του cloud, αλλά έχει έλεγχο πάνω στα λειτουργικά συστήματα, τον αποθηκευτικό χώρο και τις αξιοποιήσιμες εφαρμογές και πιθανώς

---

[2] Cloud infrastructure (υποδομή cloud): είναι η συλλογή υλικού και λογισμικού που ενεργοποιεί τα πέντε βασικά χαρακτηριστικά του cloud computing. Η υποδομή μπορεί να προβληθεί, καθώς περιέχει και φυσικό επίπεδο και επίπεδο αφαίρεσης. Το φυσικό επίπεδο αποτελείται από υλικούς πόρους που είναι απαραίτητοι για τις παρεχόμενες υπηρεσίες cloud, ενώ περιλαμβάνει δομικά στοιχεία εξυπηρετητών, αποθηκευτικού χώρου και δικτύου. Το επίπεδο αφαίρεσης αποτελείται από το λογισμικό που εφαρμόζεται κατά μήκος του φυσικού επιπέδου, το οποίο αναδεικνύει τα βασικά χαρακτηριστικά του cloud. Εννοιολογικά, το επίπεδο αφαίρεσης βρίσκεται πάνω από το φυσικό επίπεδο.

[3] Η δυνατότητα αυτή δεν απαγορεύει απαραίτητα την χρήση συμβατών γλωσσών προγραμματισμού, βιβλιοθηκών, υπηρεσιών και εργαλείων από άλλες πηγές.

περιορισμένο έλεγχο σε επιλεγμένα στοιχεία δικτύου, όπως για παράδειγμα τα τείχη προστασίας του host.

2.4 Μοντέλα Ανάπτυξης

2.4.1 Ιδιωτικό Cloud (Private Cloud).

Η υποδομή του cloud προβλέπεται για αποκλειστική χρήση από ένα μοναδικό οργανισμό, αποτελούμενο από πολλαπλούς καταναλωτές. Μπορεί να βρίσκεται στην κατοχή, να διαχειρίζεται και να λειτουργεί από τον οργανισμό, από εξωτερικούς συνεργάτες ή από ένα συνδυασμό αυτών, ενώ μπορεί να υπάρχει εντός ή εκτός των εγκαταστάσεων.

2.4.2 Κοινοτικό Cloud (Community Cloud).

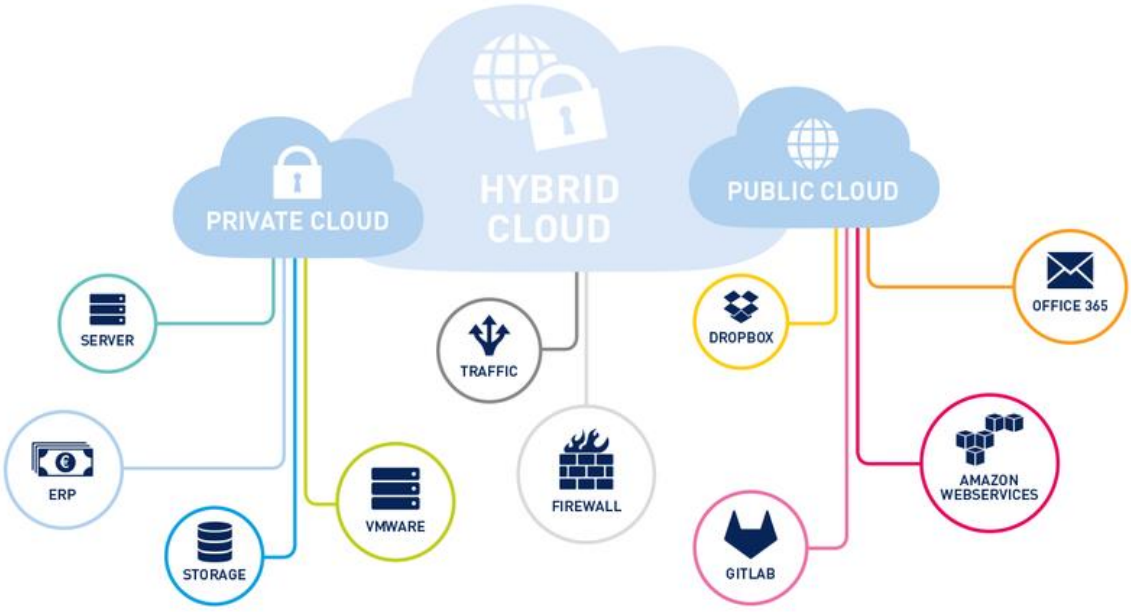
Η υποδομή του cloud προβλέπεται για αποκλειστική χρήση από μια συγκεκριμένη κοινότητα καταναλωτών, από οργανισμούς που έχουν κοινά ενδιαφέροντα (αποστολή, απαιτήσεις ασφάλειας, πολιτικές). Μπορεί να κατέχεται, να διαχειρίζεται και να λειτουργεί από έναν ή περισσότερους οργανισμούς στην κοινότητα, από εξωτερικό συνεργάτη ή συνδυασμό αυτών, ενώ μπορεί να υπάρχει εντός ή εκτός των εγκαταστάσεων.

2.4.3 Δημόσιο Cloud (Public Cloud).

Η υποδομή του cloud προβλέπεται για ανοικτή χρήση από το κοινό. Μπορεί να κατέχεται, να διαχειρίζεται και να λειτουργεί από έναν επιχειρηματικό, ακαδημαϊκό ή κυβερνητικό οργανισμό, ή από κάποιον συνδυασμό τους. Προϋπάρχει στις εγκαταστάσεις του παρόχου του cloud.

2.4.4 Υβριδικό Cloud (Hybrid Cloud).

Η υποδομή του cloud είναι μια σύνθεση δύο ή περισσότερων διαφορετικών υποδομών cloud (ιδιωτικού, κοινοτικού ή δημόσιου) που παραμένουν μοναδικές οντότητες, αλλά δεσμεύονται μεταξύ τους από μια ενοποιημένη ή ιδιόκτητη τεχνολογία που παρέχει την δυνατότητα φορητότητας των δεδομένων και των εφαρμογών.



Εικόνα 3 - Δομή Hybrid Cloud (Source: Cloudoye – Approaches to Tackle Compliance and Security Challenges in Hybrid Cloud Environments)

2.5 Ορισμός Fog Computing

Από την οπτική γωνία της Cisco, η οποία ήταν η πρώτη εταιρεία που χρησιμοποίησε τον όρο (White paper of Cisco, Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are, 2015), το Fog Computing χαρακτηρίζεται ως μια επέκταση του Cloud Computing από τον πυρήνα του δικτύου στο άκρο του δικτύου. Αποτελεί μια υψηλά ψηφιοποιημένη πλατφόρμα που παρέχει υπολογιστική ικανότητα, αποθηκευτικό χώρο και δικτυακές υπηρεσίες ανάμεσα σε τερματικές συσκευές και παραδοσιακούς εξυπηρετητές cloud (cloud servers). Από την σκοπιά της μελέτης (L. M. Vaquero and L. Rodero-Merino, Finding your way in the fog: Towards a comprehensive definition of fog computing, 2014), το fog computing ορίζεται ως «ένα σενάριο όπου ένας μεγάλος αριθμός ετερογενών (ασύρματων και ορισμένες φορές αυτόνομων), ευρέων και αποκεντρωμένων συσκευών επικοινωνούν και ενδεχομένως συνεργάζονται μεταξύ τους και με το δίκτυο, έτσι ώστε να εκτελούν αποθηκευτικές και επεξεργαστικές εργασίες, χωρίς την παρεμβολή τρίτων. Αυτές οι εργασίες μπορεί να υποστηρίζουν βασικές δικτυακές λειτουργίες ή νέες υπηρεσίες και εφαρμογές που τρέχουν σε ένα κλειστό περιβάλλον. Για τον λόγο αυτό, δίνεται το κίνητρο στους χρήστες να ενοικιάζουν μέρη των δικών τους συσκευών για αυτές τις υπηρεσίες». Παρ' όλο που αυτός ο ορισμός είναι ακόμα προς συζήτηση, πιστεύεται έντονα πως χρειάζεται ένας ορισμός που να διαφέρει το fog computing από αντίστοιχες τεχνολογίες, από την στιγμή που οποιαδήποτε από αυτές τις υποκείμενες τεχνικές μπορεί να μας προσφέρει μια λάθος οπτική του fog computing.

Επιπρόσθετα, υπάρχουν και κάποιοι όροι που είναι παρόμοιοι με το fog computing, όπως mobile cloud computing, mobile edge computing κτλ. Στη συνέχεια θα εξηγήσουμε κάθε έναν από αυτούς.

1) ***Local Cloud (Τοπικό Σύννεφο)***: Το τοπικό cloud είναι ένα cloud το οποίο δημιουργείται σε ένα τοπικό δίκτυο. Απαρτίζεται από λογισμικό με δυνατότητες cloud, το οποίο τρέχει σε τοπικούς εξυπηρετητές (servers) και υποστηρίζει, κυρίως, την αλληλεπίδραση με απομακρυσμένα cloud. Το τοπικό cloud είναι

συμπληρωματικό του απομακρυσμένου εκτελώντας ειδικές υπηρεσίες τοπικά, έτσι ώστε βελτιώσει τον έλεγχο της ιδιωτικότητας των δεδομένων.

2) ***Cloudlet:*** Το Cloudlet είναι ένα «κέντρο δεδομένων σε κουτί», το οποίο ακολουθεί το παράδειγμα του cloud computing με πιο επικεντρωμένη ματιά και βασίζεται σε υψηλού όγκου εξυπηρετητές. Το Cloudlet εστιάζεται περισσότερο στο να προσφέρει υπηρεσίες σε κοντινής περιοχής εφαρμογές, που είναι ευαίσθητες ως προς την καθυστέρηση και περιορισμένες σε εύρος ζώνης.
3) ***Mobile Edge Computing:*** Είναι αρκετά παρόμοιο με το Cloudlet, με την εξαίρεση ότι κυρίως είναι τοποθετημένοι σε σταθμούς κινητής βάσης.
4) ***Mobile Cloud Computing (MCC):*** Αποτελεί μια υποδομή όπου και η αποθήκευση δεδομένων και η επεξεργασία τους συμβαίνει εκτός των κινητών συσκευών, αναθέτοντας τους υπολογισμούς και την αποθήκευση δεδομένων από τα κινητά τηλέφωνα στο cloud. Λόγω της τάσης του να προωθείται το cloud στις άκρες, το MCC έχει ξεκινήσει να εξελίσσεται σε Mobile Edge Computing.

Σύμφωνα, λοιπόν, με όλα τα παραπάνω, μπορούμε να διακρίνουμε σε τι διαφέρει τελικά το Fog Computing από τους σχετικούς όρους. Η αρχική διαφορά του Fog Computing με το Edge Computing είναι ότι το πρώτο αποτελεί μια υψηλού επιπέδου ψηφιοποιημένη πλατφόρμα που παρέχει υπολογιστική ικανότητα, αποθηκευτικό χώρο, καθώς και δικτυακές υπηρεσίες ανάμεσα στις τερματικές συσκευές (end devices) και στα κέντρα δεδομένων του Cloud Computing. Αντίθετα, και τα δύο απαιτούν την ώθηση της ευφυίας και των επεξεργαστικών δυνατοτήτων εκτός των συγκεντρωτικών κέντρων δεδομένων, αλλά ακόμα πιο κοντά στις τερματικές συσκευές, όπως είναι οι αισθητήρες IoT, οι μηχανές κτλ. Η κύρια, όμως, διαφορά εμφανίζεται στο που τοποθετούνται η ευφυία και η υπολογιστική δύναμη. Το Fog ωθεί την ευφυία στο επίπεδο του τοπικού δικτύου (LAN), ενώ η επεξεργασία δεδομένων ωθείται σε κατάλληλους κόμβους. Αντίθετα, το Edge Computing ωθεί την ευφυία, την υπολογιστική δύναμη και τις δυνατότητες επικοινωνίας ακόμα πιο κάτω, στο επίπεδο των τερματικών συσκευών.

2.6 Αρχιτεκτονική Fog Computing

Η αρχιτεκτονική του Fog Computing αποτελείται από τρία κύρια συστατικά:

- «*Κάθετα» στοιχεία του Internet of Things (IoT)*
- *Επίπεδο «Ενορχήστρωσης» (**Orchestration Layer**)*
- *Επίπεδο Αφαίρεσης (**Abstraction Layer**)*

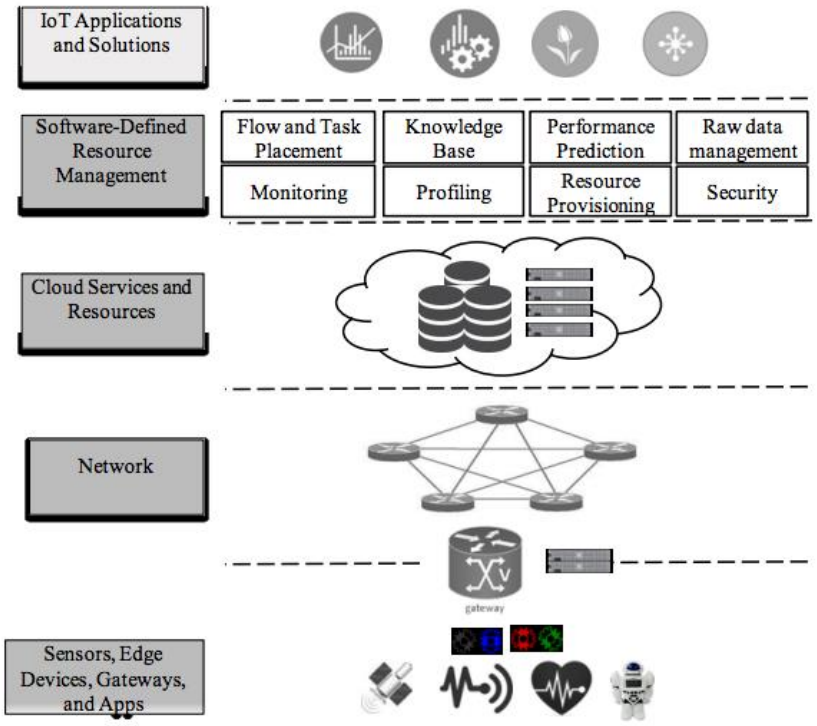
Κάθε επίπεδο αποτελείται εξίσου από ψηφιακά και φυσικά συστατικά, τα οποία συμβάλλουν στην αποδοτική και δυναμική λειτουργία ενός συστήματος fog. Πιο συγκεκριμένα, τα «κάθετα» IoT στοιχεία ορίζονται ως μισθωτές εφαρμογές ή προϊόντα τα οποία ενοικιάζονται προς χρήση. Δοθείσας της ευελιξίας μιας fog computing πλατφόρμας και της διαλειτουργικής της φύσης, η πολλαπλή ενοικίαση (multi - tenancy) αποτελεί ένα μοναδικό και εξαιρετικά επιθυμητό χαρακτηριστικό που υποστηρίζεται από ένα fog computing περιβάλλον. Το χαρακτηριστικό της πολλαπλής ενοικίασης επιτρέπει σε πολλαπλούς χρήστες (clients) να φιλοξενούν τις εφαρμογές τους σε ένα και μόνο αναφορικό σημείο του fog computing (fog instance).

Επιπλέον, το δεύτερο επίπεδο (Orchestration Layer) υποστηρίζει την συγκέντρωση δεδομένων, αποφάσεων, την διανομή και «μετανάστευση» δεδομένων (migration), καθώς και την διαχείριση των πολιτικών για το fog computing. Τέλος, το τρίτο και τελευταίο επίπεδο (Abstraction Layer) είναι υπεύθυνο για την έκθεση ενός ενιαίου και προγραμματιστικού περιβάλλοντος διεπαφής (interface) προς τον πελάτη, καθώς επίσης και για την απόκρυψη της ετερογένειας της πλατφόρμας.

Στο σημείο αυτό μπορούμε να παρουσιάσουμε δύο πολύ κύρια χαρακτηριστικά του fog computing, τα οποία στοχεύουν όχι μόνο στο να υποστηρίζουν συγκεκριμένα σενάρια περιπτώσεων χρήσης (use – case scenarios), αλλά να παρέχουν και μια γενική κατεύθυνση στο να υποστηρίζουν ένα μεγάλο εύρος χρηστών και επαναχρησιμοποιήσιμων συστημάτων:

- ***Fog Node*** (FN) ορίζονται ως ετερογενή ημι-εικονικά δομικά στοιχεία τα οποία αναπτύσσονται σε πληθώρα περιβαλλόντων. Αυτοί οι κόμβοι μπορούν να χρησιμοποιηθούν στα κύρια προσβάσιμα δίκτυα και τερματικά ενός fog περιβάλλοντος με ποικίλα προγραμματιστικά στοιχεία. Ο πρωτεύον στόχος των FN είναι να διευκολύνουν την συνεχή και ομοιόμορφη διαχείριση των πόρων, συμπεριλαμβανομένων της διαχείρισης του δικτύου, καθώς και την υπολογιστική και αποθηκευτική κατανομή κάθε κόμβου. Κάθε κόμβος μπορεί να είναι ένα «Μικρό Cloud» παρέχοντας βραχυπρόθεσμη υποστήριξη στους χρήστες και στις αιτήσεις εφαρμογών. Ο σχεδιασμός ενός FN πρέπει να είναι σε δομημένη μορφή με δυνατότητα σύνδεσης ή εγκατάστασης νέου κόμβου όταν ο τωρινός αποτυγχάνει.
- ***Fog Instance*** (FI) είναι μια εικονική αναφορά ως ένα υποστηρικτικό μοντέλο για τα FN, ως προς την διαχείριση των πόρων και τις αιτήσεις υπηρεσιών. Τα FI προκύπτουν δυναμικά και βασιζόμενα σε απαιτήσεις πόρων και προορίζονται στο να προσφέρουν υπολογιστικές, δικτυακές και βραχυπρόθεσμες υπηρεσίες αποθήκευσης.

2.6.1 Βασικά Δομικά Στοιχεία Αρχιτεκτονικής



Εικόνα 4 - Γενική Αρχιτεκτονική Fog Computing (Source: Amir Vahid Dastjerdi κ.ά, Fog Computing: Principles, Architectures and Applications)

Η εικόνα 3 παρουσιάζει μια γενική αρχιτεκτονική του Fog Computing. Στην ενότητα αυτή θα αναλύσουμε περαιτέρω τα παραπάνω επίπεδα, καθώς και τις εφαρμογές που προκύπτουν από αυτά. Στο τελευταίο επίπεδο βρίσκονται οι τερματικές συσκευές (sensors) καθώς και ευφυείς συσκευές και πύλες δικτύου. Το επίπεδο αυτό περιλαμβάνει, επίσης, εφαρμογές οι οποίες μπορούν να εγκατασταθούν στις τερματικές συσκευές για να βελτιώσουν την λειτουργικότητά τους. Τα στοιχεία από το επίπεδο αυτό χρησιμοποιούν το επόμενο επίπεδο, το δίκτυο (**Network**), για την επικοινωνία μεταξύ τους αλλά και την επικοινωνία μεταξύ αυτών και του cloud. Στη συνέχεια, το επόμενο επίπεδο (Cloud Services and Resources) περιλαμβάνει τις υπηρεσίες του cloud και τους πόρους που υποστηρίζουν την διαχείριση των πόρων αυτών και την επεξεργασία εργασιών του IoT (Internet of Things) που φτάνουν έως το cloud. Πάνω από τον επίπεδο του Cloud βρίσκεται το λογισμικό διαχείρισης πόρων, το οποίο διαχειρίζεται ολόκληρη την υποδομή και ενεργοποιεί την ποιότητα των υπηρεσιών στις εφαρμογές του Fog Computing. Τέλος, το υψηλότερο επίπεδο περιλαμβάνει τις εφαρμογές που αξιοποιούν το fog computing, έτσι ώστε να διανέμουν καινοτόμες και ευφυείς εφαρμογές στους τελικούς χρήστες.

Κοιτώντας στο εσωτερικό του επιπέδου λογισμικού διαχείρισης πόρων (Software – Defined Resource Management), παρατηρούμε ότι εφαρμόζει πολλές ενδιάμεσες (middleware) υπηρεσίες που βελτιστοποιούν την χρήση του cloud και των Fog εφαρμογών, εκ μέρους των εφαρμογών. Ο στόχος των υπηρεσιών αυτών είναι να μειώσουν το κόστος της χρήσης του cloud την στιγμή που η απόδοση των εφαρμογών φτάνει σε αποδεκτά επίπεδα καθυστέρησης, ωθώντας την εκτέλεση των διεργασιών στους κόμβους (Fog Nodes). Αυτό επιτυγχάνεται με μια σειρά υπηρεσιών που συνεργάζονται μεταξύ τους, όπως θα παρουσιαστούν παρακάτω.

- ***Ροή και τοποθέτηση εργασιών (Flow and Task Placement):*** τα στοιχεία αυτά παρακολουθούν την κατάσταση του διαθέσιμου cloud, του Fog και των δικτυακών πόρων (οι πληροφορίες παρέχονται από την υπηρεσία παρακολούθησης – **Monitoring Service**) για να αναγνωρίσουν τους καλύτερους υποψήφιους για να κρατήσουν εισερχόμενες εργασίες και ροές προς εκτέλεση. Το στοιχείο αυτό επικοινωνεί με την υπηρεσία Παροχής Πόρων (**Resource Provisioning Service**) για να υποδείξουν τον τρέχοντα αριθμό ροών και εργασιών, που μπορούν να αποτελέσουν έναυσμα για νέους γύρους κατανομής εάν θεωρηθούν πολύ υψηλά.
- ***Βάση Γνώσεων (Knowledge Base):*** Το στοιχείο αυτό αποθηκεύει πληροφορίες ιστορικού για απαιτήσεις εφαρμογών και πόρων που μπορούν να χρησιμοποιηθούν από άλλες υπηρεσίες για να υποστηρίξουν την δική τους διαδικασία υλοποίησης αποφάσεων.
- ***Πρόγνωση Απόδοσης (Performance Prediction):*** Η υπηρεσία αυτή αξιοποιεί πληροφορίες από την υπηρεσία της Βάσης Γνώσεων για να εκτιμήσει την απόδοση των διαθέσιμων πόρων cloud. Οι πληροφορίες αυτές χρησιμοποιούνται από την υπηρεσία Παροχής Πόρων (Resource Provisioning) για να αποφασιστεί η ποσότητα των πόρων που θα παρασχεθούν. Αυτό συμβαίνει κυρίως σε περιόδους όπου υπάρχει μεγάλος αριθμός εργασιών και ροών σε χρήση ή όταν η απόδοση δεν είναι ικανοποιητική.
- ***Διαχείριση Ακατέργαστων Δεδομένων (Raw Data Management):*** Η υπηρεσία αυτή έχει άμεση πρόσβαση στις πηγές δεδομένων και παρέχει «εικόνες» από τα δεδομένα για τις άλλες υπηρεσίες. Μερικές φορές, οι «εικόνες» αυτές μπορούν να αποκτηθούν μέσω απλής υποβολής ερωτημάτων (querying – πχ. SQL, NOSQL REST APIs), ενώ σε διαφορετικές περιπτώσεις μπορεί να απαιτηθεί πιο πολύπλοκη διαδικασία (πχ. MapReduce). Σε κάθε περίπτωση, η συγκεκριμένη μέθοδος για παραγωγή «εικόνων» αποκόπτεται μακριά από τις υπόλοιπες υπηρεσίες.
- ***Επίβλεψη (Monitoring):*** Η συγκεκριμένη υπηρεσία παρακολουθεί την απόδοση και την κατάσταση των εφαρμογών και των υπηρεσιών και παρέχει αυτές τις πληροφορίες σε άλλες υπηρεσίας, εφόσον απαιτηθούν.
- ***Σκιαγράφηση Προφίλ (Profiling):*** Η υπηρεσία αυτή δημιουργεί προφίλ πόρων και εφαρμογών βασιζόμενα σε πληροφορίες που πάρθηκαν από τις υπηρεσίες της **Βάσης Γνώσεων (Knowledge Base)** και της **Επίβλεψης (Monitoring)**.
- ***Παροχή Πόρων (Resource Provisioning):*** Η υπηρεσία αυτή είναι υπεύθυνη για την απόκτηση cloud, Fog και δικτυακών πόρων για την φιλοξενία των εφαρμογών. Η κατανομή αυτή είναι δυναμική, καθώς οι απαιτήσεις των εφαρμογών αλλά και ο αριθμός των φιλοξενούμενων εφαρμογών αλλάζουν με την πάροδο του χρόνου. Η απόφαση για τον αριθμό των πόρων λαμβάνεται με βάση τις πληροφορίες που παρέχονται από άλλες υπηρεσίες (όπως οι υπηρεσίες Σκιαγράφησης Προφίλ, Πρόβλεψης Απόδοσης και Επίβλεψη), ενώ οι απαιτήσεις χρήστη που αφορούν την καθυστέρηση (latency) και τα διαπιστευτήρια (credentials) διαχειρίζονται από την υπηρεσία Ασφάλειας (Security). Για παράδειγμα, το τμήμα οδηγεί τις εργασίες με χαμηλές απαιτήσεις καθυστέρησης στο άκρο του δικτύου, μόλις γίνουν διαθέσιμοι κάποιοι ελεύθεροι πόροι.
- ***Ασφάλεια (Security):*** Η υπηρεσία αυτή παρέχει αυθεντικοποίηση, εξουσιοδότηση και κρυπτογράφηση, εφόσον απαιτηθούν, από υπηρεσίες και εφαρμογές.

Αξίζει να σημειωθεί πως όλα τα στοιχεία και οι υπηρεσίες που περιγράψαμε παραπάνω είναι μόνο ενδεικτικά στοιχεία. Ολοκληρωμένες στοίβες fog (fog stacks) και εφαρμογές μπορούν επίσης να

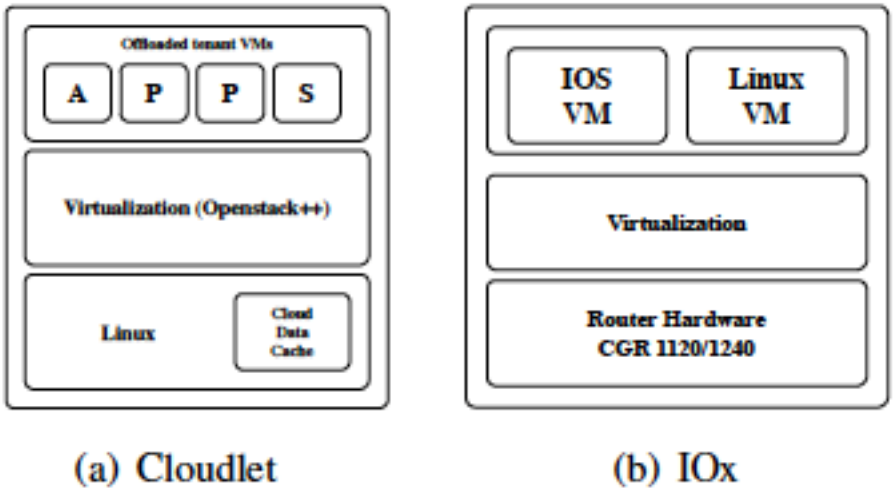
κατασκευαστούν χωρίς την χρήση όλων αυτών των στοιχείων, ή ακόμα και να κατασκευαστούν με άλλα στοιχεία και υπηρεσίες, τα οποία δεν περιγράφονται στην Εικόνα 1.

2.7 Σχεδιασμός και Εφαρμογή

Οι υπάρχουσες μελέτες έχουν στοχεύσει στον σχεδιασμό και την εφαρμογή κόμβων του fog computing (fog nodes) όπως το Cloudlet (M. Satyanarayanan, P. Bahl, R. Caceres and N. Davies, The Case for VM-Based Cloudlets in Mobile Computing, 2009), IOx (Cisco DevNet, iox-docs) και ParaDrop (Willis, Dale & Dasgupta, Arkodeb & Banerjee, Suman, ParaDrop: A multi-tenant platform to dynamically install third party services on wireless gateways, 2014). Το Cloudlet, όπως φαίνεται στην εικόνα 3, αναφέρεται ως ένα πρότυπο εφαρμογής fog κόμβων με πλούσιο επίπεδο πόρων. Κατέχει έναν σχεδιασμό τριών στρωμάτων, από τα οποία το χαμηλότερο επίπεδο είναι Linux και απόκρυψη δεδομένων από το cloud, το μεσαίο στρώμα είναι η «εικονοποίηση» (virtualization) με μια σειρά από λογισμικά cloud, όπως το OpenStack, ενώ το υψηλότερο στρώμα αποτελείται από εφαρμογές, απομονωμένες από διαφορετικές περιπτώσεις εικονικών μηχανών (VMs).

Η αρχιτεκτονική του IOx παρουσιάζεται στην εικόνα 3β, η οποία είναι ένας δρομολογητής (router) από την Cisco. Δουλεύει φιλοξενώντας εφαρμογές σε «φιλοξενούμενα» λειτουργικά συστήματα, που τρέχουν πάνω στο υλικό ενός δρομολογητή δικτύου. Η πλατφόρμα υποστηρίζει τους προγραμματιστές να τρέχουν scripts, να μεταγλωττίζουν κώδικα, καθώς και να εγκαθιστούν το δικό τους λειτουργικό σύστημα. Το σημαντικό μειονέκτημα αυτής της πλατφόρμας είναι πως δεν είναι ανοιχτή στο κοινό και βασίζεται σε ακριβό υλικό (hardware).

Το ParaDrop εφαρμόζεται σε πύλες εισόδου (σημείο πρόσβασης Wi-Fi ή σε set-top box στο σπίτι), το οποίο είναι μια ιδανική επιλογή κόμβου fog, λόγω της κοντινής του απόστασης με τον τελικό χρήστη. Ωστόσο, έχει σχεδιασθεί για σενάρια χρήσης σε σπίτια και δεν χαρακτηρίζεται από μεγάλη αποκέντρωση, καθώς όλοι οι εξυπηρετητές εφαρμογών απαιτείται να χρησιμοποιούν έναν εξυπηρετητή ParaDrop (ParaDrop Server) ως σημείο εισόδου σε υπηρεσίες που παρέχονται από τις πύλες εισόδου. Για τον λόγο αυτό, το ParaDrop θεωρείται μια συμπληρωματική εφαρμογή πλατφόρμας fog computing για σενάρια ελαφρών εργασιών.



Εικόνα 5 - Αρχιτεκτονική Cloudlet και IOx (Source: Shanhe Yi κ.ά: Fog Computing: Platform and Applications)

Σύμφωνα με τα παραπάνω, πιστεύεται πως το πρώτο βήμα για την μελέτη και την έρευνα του Fog Computing είναι ο σχεδιασμός και η εφαρμογή μιας ικανοποιητικής και επαρκής πλατφόρμας fog computing, η οποία μπορεί να χρησιμοποιηθεί ως ένα βασικό περιβάλλον ανάπτυξης πρωτότυπου.

2.7.1 Στόχοι Σχεδιασμού

Υπάρχουν μερικοί βασικοί στόχοι για τον σχεδιασμό μιας πλατφόρμας fog computing. Παρακάτω θα εξηγήσουμε μερικούς από τους σημαντικότερους από αυτούς.

- **Καθυστέρηση (Latency)**. Αποτελεί βασική αρχή για μια πλατφόρμα fog computing να προσφέρει εφαρμογές και υπηρεσίες με εγγυημένη μικρή καθυστέρηση στους τελικούς χρήστες. Η καθυστέρηση προκύπτει από τον χρόνο εκτέλεσης μιας εργασίας, από τον χρόνο «φόρτωσης» της εργασίας, από τον χρόνο ψηφιακής συλλογής και ταχύτητας λήψης αποφάσεων κτλ.
- **Αποδοτικότητα (Efficiency)**. Παρ' ότι με την πρώτη ματιά η αποδοτικότητα μπορεί να έχει την δική της επίδραση στην καθυστέρηση, εδώ είναι περισσότερο συνδεδεμένη με την αποδοτική εφαρμογή των πόρων και της ενέργειας. Οι λόγοι είναι προφανείς και σχετικά διαφορετικοί με τους αντίστοιχους σε σενάρια cloud computing: 1) δεν είναι όλοι οι κόμβοι fog πλούσιοι σε πόρους: μερικοί από αυτούς έχουν περιορισμένη υπολογιστική ισχύ, μνήμη και αποθηκευτικό χώρο. 2) Οι περισσότεροι από τους κόμβους fog και τους πελάτες τους βασίζονται στην δύναμη των μπαταριών, όπως συσκευές που μπορούν να φορεθούν, ασύρματες μονάδες αισθητήρων κ.α.
- **Γενικότητα (Generality)**. Λόγω της ετερογένειας των κόμβων fog και των πελατών, χρειάζεται να παρέχουμε το ίδιο επίπεδο πληροφοριών σε εφαρμογές και υπηρεσίες υψηλού επιπέδου για τους fog πελάτες. Πρέπει να παρέχονται γενικές προγραμματιστικές διεπαφές εφαρμογών (APIs), έτσι ώστε να έρχονται σε συμφωνία με τα υπάρχοντα πρωτόκολλα και τα APIs (π.χ πρωτόκολλα μηχανής Machine-2, APIs για συσκευές έξυπνων οχημάτων κτλ.).

2.7.2 Προκλήσεις

Για την επίτευξη των παραπάνω στόχων, είναι αναγκαίο να αναγνωρίζουμε και κάποιες βασικές προκλήσεις, όσον αφορά τον σχεδιασμό και την εφαρμογή μιας πλατφόρμας fog computing. Στην συνέχεια θα αναφερθούμε σε κάποιες από αυτές τις βασικές προκλήσεις και δυσκολίες.

- ***Επιλογή Τεχνολογίας «Εικονικοποίησης» (Virtualization)***: Η εικονοποίηση είναι η κύρια μέθοδος για την παροχή απομονωμένων περιβαλλόντων σε fog computing, καθώς και ο κύριος παράγοντας απόδοσης των κόμβων fog. Για τον λόγο αυτό προκύπτει ένα πολύ σημαντικό ερώτημα: «**Hypervisor**[4] vs container, ποιο από τα δύο να επιλέξουμε;». Όπως γνωρίζουμε, το Cloudlet είναι μια τεχνική εφαρμογής hypervisor εικονικοποίησης, ενώ το ParaDrop χρησιμοποιεί μια «ελαφρότερη» λύση: το container, όπως για παράδειγμα η εικονοποίηση σε επίπεδο λειτουργικού συστήματος. Η επιλογή σχεδιασμού γίνεται διαφορετικά, αφού τα υλικά τους κατέχουν διαφορετικές δυνατότητες. Παρ' όλα αυτά, ένα μειονέκτημα σε σύγκριση με την εικονοποίηση που είναι βασισμένη σε container, είναι η απώλεια ευελιξίας. Για παράδειγμα, αδυνατεί να φιλοξενήσει διαφορετικά είδη λειτουργικών συστημάτων σε μια ενιαία δομή κόμβου. Συνεπώς, προτιμούμε τεχνικές εικονικοποίησης hypervisor από τις τεχνικές που βασίζονται σε container.
- ***Πρόκληση Καθυστέρησης***: Υπάρχουν πολλοί παράγοντες που μπορούν να εισάγουν την υψηλή καθυστέρηση εφαρμογών ή απόδοσης υπηρεσιών σε μια πλατφόρμα fog computing. Η υψηλή καθυστέρηση μπορεί να καταστρέψει την εμπειρία και την ικανοποίηση του χρήστη, από την στιγμή που το fog computing στοχεύει σε εφαρμογές και υπηρεσίας με ευαισθησία στην καθυστέρηση. Παρουσιάζονται αρκετές πιθανότητες στην εισαγωγή καθυστέρησης στο fog computing:
    - *Συγκέντρωση Δεδομένων*: Η φύση της γεωγραφικής κατανομής του παραδείγματος του fog computing καθορίζει πως θα υπάρχει καθυστέρηση εάν η συλλογή δεδομένων δεν ολοκληρωθεί πριν την επεξεργασία αυτών. Ωστόσο, υπάρχουν αρκετοί τρόποι μετρίασης του προβλήματος, όπως η εφαρμογή φιλτραρίσματος/κατατόμισης και η εφαρμογή γειτνίασης σε ιεραρχία για την μείωση του όγκου των υπολογισμών σε υψηλότερο στρώμα.
    - *Παροχή πόρων*: Είναι γνωστό πως θα υπάρξει καθυστέρηση στην παροχή πόρων για συγκεκριμένες εργασίες, ειδικά για κόμβους περιορισμένων πόρων. Στην περίπτωση αυτή ίσως απαιτηθεί ο προσεκτικός σχεδιασμός προγράμματος, χρησιμοποιώντας μοντέλα προτεραιότητας και κίνησης.
    - *Μετακίνηση, αποτυχία, χτύπημα κόμβων*: Το Fog Computing χρειάζεται να είναι ανθεκτικό ως προς την μετακίνηση, την αποτυχία και την περίπτωση χτυπήματος του κόμβου. Ο έλεγχος του συστήματος καθώς και η υπηρεσία τοποθεσίας θα συνεργάζονται μαζί, προκειμένου να παρέχουν πληροφορίες για να βοηθούν στην επιλογή στρατηγικών άμβλυνσης, όπως επαναπρογραμματισμός και αντιγραφή, εφαρμογή σημείου ελέγχου κ.α.
- ***Διαχείριση Δικτύου***: Η διαχείριση δικτύου θα αποτελεί ένα βάρος για το fog computing, εκτός εάν επωφεληθούμε από τα προνόμια της εφαρμογής των τεχνικών SDN και NFV. Ωστόσο, η απρόσκοπτη εφαρμογή των SDN και NFV στο fog computing δεν αποτελεί εύκολη υπόθεση και σίγουρα θα είναι μια δυνατή πρόκληση. Οι δυσκολίες εμφανίζονται

[4] Hypervisor: είναι ένα λογισμικό ή υλικό ή πρόγραμμα της Rom ενός υπολογιστή που δημιουργεί και τρέχει εικονικές μηχανές (virtual machines). Διαφορετικά ονομάζεται και Virtual Machine Monitor (VMM).

από τον επανασχεδιασμό των βόρειων, νότιων, δυτικών και ανατολικών APIs για την εισαγωγή πρωτότυπων στοιχείων του fog computing. Μια αφελής ενσωμάτωσή τους μπορεί να μην οδηγήσει στην επίτευξη των στόχων για την καθυστέρηση και την αποδοτικότητα.

2.8 Σύγκριση Cloud Computing Fog Computing

Από τις παραπάνω αναφορές, μπορούμε να διακρίνουμε πως τεχνικά το Fog Computing είναι αρκετά όμοιο με το Cloud Computing, με το σκεπτικό ότι και τα δύο αποτελούν ψηφιακά συστήματα που παρέχουν την ελαστικότητα στην κατά παραγγελία (on demand) παροχή υπολογιστικής ικανότητας, αποθηκευτικού χώρου και δικτυακών πόρων. Σε αντίθεση, όμως, με το cloud, το fog εφαρμόζεται πολύ κοντά στους τελικούς χρήστες. Στο κομμάτι αυτό θα ασχοληθούμε με τις ομοιότητες και τις διαφορές των δύο αυτών τεχνολογιών, ακολουθώντας το σκεπτικό των απαιτήσεων των αναπτυσσόμενων τάσεων στην δικτύωση.

Στον επόμενο πίνακα παρουσιάζονται κάποιες βασικές ομοιότητες και διαφορές ανάμεσα στις δύο τεχνολογίες. Από τον πίνακα μπορούμε να διακρίνουμε πως τα χαρακτηριστικά του Cloud Computing παρουσιάζουν σημαντικούς περιορισμούς όσον αφορά την ποιότητα των υπηρεσιών που απαιτούνται από εφαρμογές πραγματικού χρόνου, απαιτώντας παράλληλα και άμεση δράση από τον εξυπηρετητή (server).

Πίνακας 2 - Cloud Computing vs Fog Computing

Requirement	Cloud Computing	Fog Computing
Καθυστέρηση (Latency)	Υψηλή	Χαμηλή
Διακύμανση Καθυστέρησης (Delay Jitter)	Υψηλή	Πολύ χαμηλή
Τοποθεσία Κόμβων Εξυπηρετητών (Location of Server Nodes)	Στο εσωτερικού του Διαδικτύου	Στο άκρο του τοπικού δικτύου
Απόστασης ανάμεσα σε πελάτη και εξυπηρετητή (Distance Between the client and server)	Πολλαπλά βήματα (hops)	Ένα βήμα (hop)
Ασφάλεια (Security)	Απροσδιόριστη	Μπορεί να προσδιορισθεί
Επίθεση σε δρομολογημένα δεδομένα (Attack on data en route)	Υψηλή πιθανότητα	Πολύ χαμηλή πιθανότητα
Επίγνωση τοποθεσίας (Location Awareness)	Όχι	Ναι
Γεωγραφική κατανομή (Geographical distribution)	Συγκεντρωτική	Κατανεμημένη

Αριθμός κόμβων εξυπηρετητών(No. Of server nodes)	Μικρός	Πολύ μεγάλος
Υποστήριξη Κινητικότητας (Support for Mobility)	Περιορισμένη	Υποστηριζόμενη
Αλληλεπίδραση πραγματικού χρόνου (Real time interactions)	Υποστηρίζει	Υποστηρίζει
Τύπος επικοινωνίας «τελευταίου μιλίου» (Type of last mile connectivity)	Μισθωμένη γραμμή (Leased line)	Ασύρματα

Το Διαδίκτυο των Πραγμάτων (Internet of Things) οραματίζεται να τοποθετήσει μια IP διεύθυνση σε κάθε συσκευή, έτσι ώστε να συνδέονται στο Internet. Τα δίκτυα οχημάτων (Vehicular networks), ένα ειδικού τύπου αναπτυσσόμενο κινητό δίκτυο, αποτελούν ένα σημαντικό κομμάτι του αυτού του οράματος (F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its role in the internet of things, 2012). Στα δίκτυα οχημάτων, η επικοινωνία θα διαδραματίζεται ανάμεσα στα οχήματα, ανάμεσα στα οχήματα και τα σημεία πρόσβασης και ανάμεσα σε σημεία πρόσβασης μεταξύ τους, με σκοπό την μεταφορά σημαντικών πληροφοριών ανάμεσα στα αντικείμενα αυτά. Μερικά από τα κύρια χαρακτηριστικά αυτής της επικοινωνίας είναι η επίγνωση της τοποθεσίας, η ασύρματη σύνδεση, η χαμηλή καθυστέρηση, η κινητικότητα και η αλληλεπίδραση σε πραγματικό χρόνο. Για να μπορέσουν, λοιπόν, να επιτευχθούν οι συγκεκριμένες απαιτήσεις, είναι αναγκαίος ένας μεγάλος αριθμός από κόμβους, οι οποίοι θα βρίσκονται πολύ κοντά στους πελάτες -στην προκειμένη περίπτωση στα οχήματα- και θα μπορούν να επικοινωνούν με αυτούς δια μέσου ασύρματων συνδέσεων χαμηλής καθυστέρησης. Για τον παραπάνω λόγο, το fog computing αποτελεί το κατάλληλο μοντέλο επικοινωνίας σε σύγκριση με το cloud, όπου οι επεξεργασία των πληροφοριών διαδραματίζεται πολύ βαθιά μέσα στο Διαδίκτυο.

Παράλληλα, οι αναπτυσσόμενες εφαρμογές πολυμέσων υψηλής ποιότητας, συμπεριλαμβανομένων των διαδραστικών παιχνιδιών, των «κατά παραγγελία» video (video on demand) και των διαδικτυακών μεταδόσεων (streaming), απαιτούν πολύ υψηλές τιμές μεταφοράς δεδομένων με χαμηλή καθυστέρηση, διακύμανση της καθυστέρησης και απώλεια πακέτων (A.Erbad, Real – time support for interactive multimedia applications, 2012). Για την επίτευξη αυτών, κρίνεται απαραίτητο η επεξεργασία των εφαρμογών αυτών να γίνεται πιο κοντά στους τελικούς χρήστες. Από τη στιγμή που τα κέντρα δεδομένων του cloud βρίσκονται, σε γενικότερο πλαίσιο, τοποθετημένα μέσα στο Διαδίκτυο, καθίσταται αρκετά δύσκολο να διαχειριστούν αυτούς τους παράγοντες. Έτσι, το fog computing είναι η πρακτική λύση για αυτού του είδους τις εφαρμογές ευαίσθητης απόδοσης.

Ένα ακόμα σημαντικό στοιχείο αποτελούν τα δίκτυα ασύρματων αισθητήρων, τα οποία έχουν αξιοποιηθεί ευρέως σε πολλές εφαρμογές που σχετίζονται με το περιβάλλον (F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its role in the internet of things, 2012). Τα δίκτυα αυτά χαρακτηρίζονται γενικά από χαμηλή ισχύ, χαμηλό εύρος ζώνης, καθώς και από κόμβους με περιορισμένη επεξεργαστική ικανότητα, οι οποίοι είναι κατανεμημένοι κατά μήκος ευρέων γεωγραφικών εκτάσεων. Επίσης, τα δίκτυα αυτά πρέπει να υποστηρίζονται από χαμηλή καθυστέρηση, επίγνωση τοποθεσίας και κατανεμημένα συστήματα για την επεξεργασία και την διανομή των δεδομένων. Φαίνεται, λοιπόν, πως τα παραπάνω αποτελούν τυπικά χαρακτηριστικά του fog computing παρά του cloud.

Δύο από τα πιο σημαντικά χαρακτηριστικά που απαιτούνται από πολλές Διαδικτυακές εφαρμογές είναι η ασφάλεια των δεδομένων και η ακεραιότητα (J.K Zao κ. ά, Pervasive brain monitoring and data sharing based on multi-tier distributed computing and linked data technology, 2014). Όσο περισσότερο είναι δρομολογημένα τα δεδομένα, τόσο πιο ευάλωτα είναι απέναντι σε επιθέσεις, ακόμα και όταν είναι κρυπτογραφημένα. Έτσι, είναι πάντα επιθυμητό να υπάρχει μικρή απόσταση ανάμεσα στους πελάτες και τους εξυπηρετητές. Το Fog computing παρέχει την μικρότερη δυνατή απόσταση, ενώ παράλληλα παρέχει και όλα τα άλλα πλεονεκτήματα του cloud computing.

Μια σημαντική παράμετρος αποτελεί και οι επιθέσεις απέναντι στα διαθέσιμα συστήματα cloud που βρίσκονται στο εσωτερικού του Διαδικτύου, με την χρήση διαφόρων μεθόδων άρνησης υπηρεσίας (Denial of Service, DoS). Οι επιθέσεις DoS δεν είναι απαραίτητο να γίνουν απευθείας στα τερματικά συστήματα, αλλά μπορούν να στοχεύσουν ακόμα και τις ενδιάμεσες συσκευές, όπως οι δρομολογητές (routers). Από την άλλη μεριά, οι κόμβοι fog (fog nodes) είναι, σε πολύ μεγάλο βαθμό, κατανεμημένοι στα άκρα του δικτύου. Έτσι, για να επιτευχθεί η επίθεση απέναντι στη διαθεσιμότητα των συστημάτων αυτών, απαιτείται μια τεράστια επίθεση σε όλα τα συστήματα τα οποία βρίσκονται κοντά στον πελάτη. Αυτό καθιστά επιτακτική την ανάγκη τεράστιων πόρων και από την μεριά των επιτιθέμενων. Εξάλλου, δεν υπάρχουν πολλές ενδιάμεσες συσκευές που μπορούν να στοχοποιηθούν από τον επιτιθέμενο, καθώς οι κόμβοι είναι τοποθετημένοι πολύ κοντά στους τελικούς χρήστες. Σύμφωνα, λοιπόν, με όλα τα παραπάνω, μπορούμε με ασφάλεια να διαπιστώσουμε ότι τα συστήματα του fog computing είναι λιγότερα επιρρεπή σε επιθέσεις DoS, σε αντίθεση με τα cloud συστήματα.

Από την άλλη μεριά, πρέπει να τονιστεί πως και το cloud computing έχει τα δικά του πλεονεκτήματα. Από τη στιγμή που το fog computing απαιτεί την εφαρμογή σε μια τεράστια γεωγραφική κατανομή, οι απλοί κόμβοι δεν μπορούν να διαθέτουν μεγάλο αριθμό πόρων για οικονομικούς, κυρίως, λόγους. Παρ’ όλα αυτά, επιχειρηματική υπολογισμοί υψηλού επιπέδου, όπως είναι οι εργασίες επεξεργασίας παρτίδων (batch processing jobs), απαιτούν μεγάλο αριθμό πόρων, ενώ παράλληλα δεν είναι πολύ ευαίσθητοι ως προς το θέμα της καθυστέρησης. Αυτού του είδους οι εργασίες μπορούν να έρθουν εις πέρας χρησιμοποιώντας παραδοσιακά συστήματα του cloud computing, πάρα κόμβων του fog. Για τον λόγο αυτό, είναι συνετό να αναφέρουμε πως το fog computing δεν θα μπορέσει να αντικαταστήσει εξ ολοκλήρου το cloud computing και να παραμείνει ως το μοναδικό μοντέλο στο μέλλον. Αντίθετα, μπορούμε να αναφέρουμε με ασφάλεια πως το cloud και το fog θα συνυπάρχουν και θα εξυπηρετούν δύο διαφορετικές κοινότητες, ενώ θα συμπληρώνουν το ένα με το άλλο όποτε αυτό κρίνεται απαραίτητο.

2.9 Fog Computing και οικολογικό IoT

Ακολουθώντας κάποια βασικά στοιχεία από τα προηγούμενα κεφάλαια, ενισχύεται όλο και περισσότερο η άποψη ότι το Fog Computing και το Cloud Computing αποτελούν δύο μοντέλα τα οποία είναι σε μεγάλο βαθμό αλληλένδετα μεταξύ τους. Για την ακρίβεια, συμπληρώνουν το ένα με το άλλο, καθώς η διαχείριση και η αναβάθμιση των συστημάτων Fog μπορούν κάλλιστα να χειρίζονται από το Cloud. Αυτή τη στιγμή, γίνεται μεγάλη προσπάθεια που στοχεύει στο να βελτιωθεί η ασφάλεια, η ιδιωτικότητα, η ευελιξία κ.ά. Παρ' όλα αυτά, δεν έχει δοθεί ιδιαίτερη έμφαση στην ανάπτυξη της κατανάλωσης ενέργειας των εφαρμογών του Διαδικτύου των Πραγμάτων (IoT), παρόλο που πολλές συσκευές απαιτούν υψηλή ισχύ για την συλλογή, την μετάδοση και την ανάλυση των δεδομένων.

Στο κεφάλαιο αυτό, θα συζητήσουμε για την σύγκριση, όσον αφορά την κατανάλωση ισχύος, ανάμεσα σε εφαρμογές που βασίζονται στο Cloud και το Fog, αντίστοιχα. Επίσης, σημειώνουμε και κάποιες στρατηγικές που μπορούν να βοηθήσουν τις εφαρμογές να καταναλώνουν υψηλά ποσοστά ισχύος. Τέλος, επισημαίνουμε τεχνολογίες και παράγοντες που μπορούν να έχουν σημαντική επίδραση στην κατανάλωση ισχύος, όπως είναι ο τύπος του δικτύου πρόσβασης στο Fog, ο χρόνος αδράνειας των εξυπηρετητών που βρίσκονται στο fog, καθώς και η δικτυακή ψηφιοποίηση.

2.9.1 Κατανάλωση ισχύος σε Cloud Vs Fog

2.9.1.1 Επιπρόσθετη κατανάλωση ενέργειας για την ενεργοποίηση συστήματος βασισμένο στο IoT

Το 2016 δημοσιεύθηκε, από τον Διεθνή Οργανισμό Ενέργειας, μια έκθεση βασισμένη στο 4E (Energy Efficient End-Use Equipment), με στόχο να επιδείξει το ρίσκο μιας ουσιαστικής αύξησης στην παγκόσμια κατανάλωση ισχύος μετά την αναμενόμενη εξάπλωση του Διαδικτύου των πραγμάτων και των υπηρεσιών του. Στην έκθεση αυτή, εκτιμάται ότι η ετήσια, παγκόσμια κατανάλωση ισχύος από πέντε σενάρια εφαρμογών του IoT (αυτοματοποίηση οικίας, έξυπνος φωτισμός, έξυπνες οικιακές συσκευές, έξυπνοι δρόμοι και έξυπνη σηματοδότηση) μπορεί να φτάσει τα 45 TWh έως το 2025, με το μερίδιο της αυτοματοποίησης οικίας και των έξυπνων οικιακών συσκευών να αντιστοιχούν στο 78% (36TWh) και 15% (7 TWh) αντίστοιχα. Ωστόσο, η έκθεση αυτή δεν περιλαμβάνει τα επίπεδα ενέργειας για την επικοινωνία ανάμεσα στις σχετιζόμενες εφαρμογές που βασίζονται στο Cloud. Παρ' όλα αυτά, από την στιγμή που οι πύλες, καθώς και άλλες τοπικές συσκευές περιλαμβάνονται στην εκτίμηση, αυτό μπορεί να δώσει μια ένδειξη για την ετήσια κατανάλωση ενέργειας για τις εφαρμογές που βασίζονται στο Fog.

2.9.1.2 Παράμετροι για οικολογικό Fog Computing

Λαμβάνοντας υπόψιν πως το IoT αλλά και η πλατφόρμα του Fog Computing συνεχίζουν να εξελίσσονται, υπάρχουν ακόμα παράγοντες που μπορούν να έχουν επίδραση στο θέμα της κατανάλωσης ισχύος από τις εκάστοτε εφαρμογές που δραστηριοποιούνται πάνω στην πλατφόρμα του Fog. Στην ενότητα αυτή, θα δούμε ορισμένες από αυτές τις παραμέτρους, αλλά και τις διαφορές που υπάρχουν ανάμεσα στο Cloud και το Fog, για το θέμα της κατανάλωσης ισχύος, ενώ θα συζητηθούν και ορισμένες μέθοδοι που έχουν προταθεί για την μείωση της κατανάλωσης ισχύος των εφαρμογών.

2.9.1.2.1 Τεχνολογίες πρόσβασης δικτύου

Θέλοντας να εστιάσουμε στην κατανάλωση ισχύος ανάμεσα στο Fog και το Cloud, μπορούμε να παρατηρήσουμε κάποιες σημαντικές διαφορές ανάμεσα στις δύο αυτές πλατφόρμες. Για παράδειγμα, τα κέντρα δεδομένων του Cloud βρίσκονται, συνήθως, απομακρυσμένα (γεωγραφικά) από τις εκάστοτε δικτυακές συσκευές. Έτσι, η κατανάλωση ισχύος για την μεταφορά στο δίκτυο με τη χρήση του Cloud θα είναι αρκετά μεγαλύτερη σε σχέση με την χρήση του Fog. Ωστόσο, εκείνο που δεν πρέπει να αγνοηθεί είναι το γεγονός ότι, σε ορισμένες περιπτώσεις, η κατανάλωση ισχύος για την μεταφορά στο δίκτυο αποτελεί ένα σημαντικό μερίδιο της γενικότερης κατανάλωσης ισχύος της υπηρεσίας του IoT (F. Jalali κ. ά, Energy Consumption of Content Distribution from Nano Data Centers versus Centralized Data Centers, 2014).

Επιπρόσθετα, ο Gray και άλλοι (C. Gray κ. ά, Power consumption of IoT access network technologies, 2015) παρείχαν ένα μοντέλο για την κατανάλωση ισχύος, για ένα εύρος δικτυακών τεχνολογιών του IoT. Οι συγγραφείς παρείχαν μια λεπτομερή περιγραφή του μοντέλου, καθώς και ανάλυση και σύγκριση της κατανάλωσης ισχύος από διαφορετικές τεχνολογίες πρόσβασης δικτύου. Σύμφωνα με αυτή την σύγκριση διαπιστώθηκε πως εάν η πρόσβαση στο δίκτυο είναι μοιρασμένη σε ένα σεβαστό αριθμό χρηστών ή υπηρεσιών, το μερίδιο ισχύος ανά χρήστη ή ανά υπηρεσία είναι μικρό. Έτσι, με και τις περαιτέρω αναλύσεις, διαπιστώθηκε πως η διαμοιρασμένη επικοινωνία ανάμεσα σε Wi-Fi και πύλες με πρόσβαση σε δίκτυο PON[5] θεωρείται ως η πλέον αποδοτική σε θέματα ισχύος. Παράλληλα, λόγω του ότι η κατανάλωση ισχύος με ενσύρματη πρόσβαση σε δίκτυο κυριαρχείται από την αδράνεια των αντίστοιχων διαμορφωτών (modem), η εφαρμογή τεχνικών που είναι αποδοτικές, όσον αφορά την ισχύ, όπως είναι η κατάσταση ύπνου (sleep mode), καθώς και η λογική επιλογή τεχνολογίας πρόσβασης σε δίκτυο, μπορούν να μειώσουν την κατανάλωση ισχύος των υπηρεσιών που βασίζονται, κυρίως, στο Cloud.

Επιπλέον, αναλύθηκε ακόμα ένα δείγμα κατανάλωσης ισχύος για την πρόσβαση σε δίκτυο, έτσι ώστε να συγκριθεί η τοπική και η απομακρυσμένη επεξεργασία των δεδομένων (F. Jalali κ. ά, Fog Computing May Help to Save Energy in Cloud Computing, 2016). Στην έκθεση αυτή παρατηρήθηκε πως η κατανάλωση ισχύος από εφαρμογές του Fog Computing βασίζονται σε πολύ μεγάλο βαθμό στον τύπο του δικτύου πρόσβασης που συνδέεται με τον/τους εξυπηρετητή/ές ή τις πύλες στο τοπικό δίκτυο. Για παράδειγμα, η κατανάλωση ισχύος για εφαρμογή που έχει τον εξυπηρετητή συνδεδεμένο με 4G, είναι πολύ μεγαλύτερη από την ίδια εφαρμογή με τον εξυπηρετητή σε σύνδεση μέσω Ethernet. Επίσης φανερώνεται ότι, ανάλογα με τον ρυθμό των δεδομένων της υπηρεσίας IoT, οι ενσύρματες τεχνολογίες μπορούν να είναι ή όχι ενεργειακά αποδοτικές σε σύγκριση με τις ασύρματες τεχνολογίες.

[5] Ένα παθητικό οπτικό δίκτυο (Passive Optical Network – PON) είναι μια τεχνολογία τηλεπικοινωνιών που χρησιμοποιείται για την παροχή ινών στον τελικό καταναλωτή, τόσο για οικιακές όσο και για εμπορικές χρήσεις. Το κύριο χαρακτηριστικό του είναι ότι εφαρμόζει μια αρχιτεκτονική «σημεία-σε-πολλά σημεία», στην οποία χρησιμοποιούνται διαχωριστές οπτικών ινών, χωρίς ισχύ, για την ενεργοποίηση μιας μοναδικής οπτικής ίνας που εξυπηρετεί πολλαπλά τελικά σημεία. Το δίκτυο αυτό, συχνά, αναφέρεται ως το «τελευταίο μίλι» ανάμεσα στοn πάροχο δικτύου και τον καταναλωτή.

2.9.1.2.2 Κατανάλωση ισχύος από Fog Servers σε αδράνεια

Μια ακόμα παράμετρος αποτελεί η κατανάλωση ισχύος από τοπικές υπολογιστικές συσκευές που βρίσκονται σε αδράνεια μέσα στο Fog, καθώς και ο ενεργός χρόνος τους. Οι φυσικοί εξυπηρετητές στα κέντρα δεδομένων του Cloud είναι δυναμικά κατανεμημένα ανάμεσα σε πολλές υπηρεσίες και χρήστες. Εάν μια εφαρμογή είναι αδρανής για κάποιο χρόνο, ο εξυπηρετητής μπορεί να διανεμηθεί σε άλλες εργασίες στο κέντρο δεδομένων του Cloud. Η κατανομή αυτή οδηγεί στην μείωση του ποσοστού κατανάλωσης ενέργειας για μια υπηρεσία από έναν αδρανή εξυπηρετητή.

Από την άλλη μεριά, λόγω του σχετικού μεγέθους των κέντρων δεδομένων του Fog, ο παραπάνω βαθμός κατανομής μπορεί να μην είναι εφικτός στο Fog. Συνεπώς, εάν εξυπηρετητές σε ένα κέντρο δεδομένων Fog είναι αδρανείς για μεγάλες χρονικές περιόδους ανάμεσα στις εκάστοτε εργασίες τους, η υπηρεσία IoT μπορεί να είναι λιγότερη αποδοτική σε θέματα ισχύος στο Fog συγκριτικά με το Cloud. Αντίστοιχα, ένα κέντρο δεδομένων του Fog έχει, γενικά, πολύ λιγότερους διαθέσιμους, πόρους (πχ. CPU, RAM, αποθηκευτικό χώρο κτλ.), σε σύγκριση με ένα κέντρο δεδομένων του Cloud. Επομένως, τα κέντρα δεδομένων του Fog μπορεί να είναι λιγότερο ικανά στο να αξιοποιούν στρατηγικές για την εξοικονόμηση ενέργειας που είναι διαθέσιμες σε μεγάλα κέντρα δεδομένων, όπως για παράδειγμα η ψηφιοποίηση καθώς και οι περισσότερο επιθετική χρήση των καταστάσεων ύπνου.

2.9.1.2.3 Τύπος Εφαρμογής

Ένας ακόμα καθοριστικός παράγοντας, όσον αφορά την ενεργειακή κατανάλωση, είναι ο τύπος των εφαρμογών. Σύμφωνα με ορισμένες εκτιμήσεις (F. Jalali κ. ά, Fog Computing May Help to Save Energy in Cloud Computing, 2016) ο αριθμός των ενημερώσεων, ο αριθμός των λήψεων, καθώς και ο αριθμός των δεδομένων που φορτώνονται εξ αρχής, παίζουν σημαντικό ρόλο στην κατανάλωση ισχύος των εφαρμογών. Για παράδειγμα, παρουσιάζεται πως εφαρμογές που απαιτούν περισσότερη υπολογιστική δύναμη μπορεί να είναι πιο αποδοτικές στο Cloud παρά στο Fog. Τα αποτελέσματα των παραπάνω εκτιμήσεων έδειξαν, επίσης, πως οι καλύτερες πρακτικές εξοικονόμησης ενέργειας, χρησιμοποιώντας το Fog, έρχονται από εφαρμογές που παράγουν και διανέμουν τα δεδομένα συνεχόμενα στους τελικούς χρήστες, με χαμηλό ρυθμό πρόσβασης στα δεδομένα έξω από το Fog, καθώς και επαρκείς τοπικούς υπολογισμούς, όπως για παράδειγμα η παρακολούθηση μέσω βίντεο, χωρίς την αναγνώριση προσώπου.

Παράλληλα, σε άλλη μια αντίστοιχη έρευνα (F. Jalali, A. Vishwanath, Julian de Hoog, F. Suits**,** *Interconnecting Fog computing and Microgrids for Greening IoT),* αποφάνθηκε πως οι εφαρμογές του IoT χωρίς υπολογιστική ικανότητα, είναι πιο ενεργειακά αποδοτικές όταν «τρέχουν» στη Fog πλατφόρμα. Αντίστροφα, φάνηκε πως οι εφαρμογές με μεγάλο όγκο υπολογισμών καταναλώνουν περισσότερη ενέργεια στο Fog και συνεπώς είναι προτιμότερο για τις αντίστοιχες υπηρεσίες τους να στέλνονται στο Cloud. Ο λόγος που συμβαίνει αυτό είναι πως κατανάλωση ενέργειας, κατά την διάρκεια αδράνειας, των τοπικών υπολογιστικών πόρων για εφαρμογές με υψηλό αριθμό τοπικών υπολογισμών είναι πολύ υψηλή σε σύγκριση με την κατανάλωση ενέργειας σε αδρανή κέντρα δεδομένων που μπορούν να διαμοιράζονται από πολλές άλλες εφαρμογές.

Επιπλέον, ειδικά οι εφαρμογές που είναι ευαίσθητες στο θέμα της καθυστέρησης, είναι προτιμότερο να παρέχονται χρησιμοποιώντας το Fog computing. Ωστόσο, αυτό μπορεί να οδηγήσει στην αύξηση της κατανάλωσης ενέργειας από την εφαρμογή. Για τον λόγο αυτό, έχει προταθεί (R. Deng κ. ά, Optimal Workload Allocation in Fog-Cloud Computing Towards Balanced Delay and Power Consumption, 2016) μια συνδυασμένη πλατφόρμα Cloud – Fog για την βελτίωση της ανταλλαγής ανάμεσα στην κατανάλωση ισχύος του συστήματος και την εμπειρία καθυστέρησης του τελικού χρήστη. Στην έρευνα αυτή, διαπιστώθηκε πως με τον σχεδιασμό της

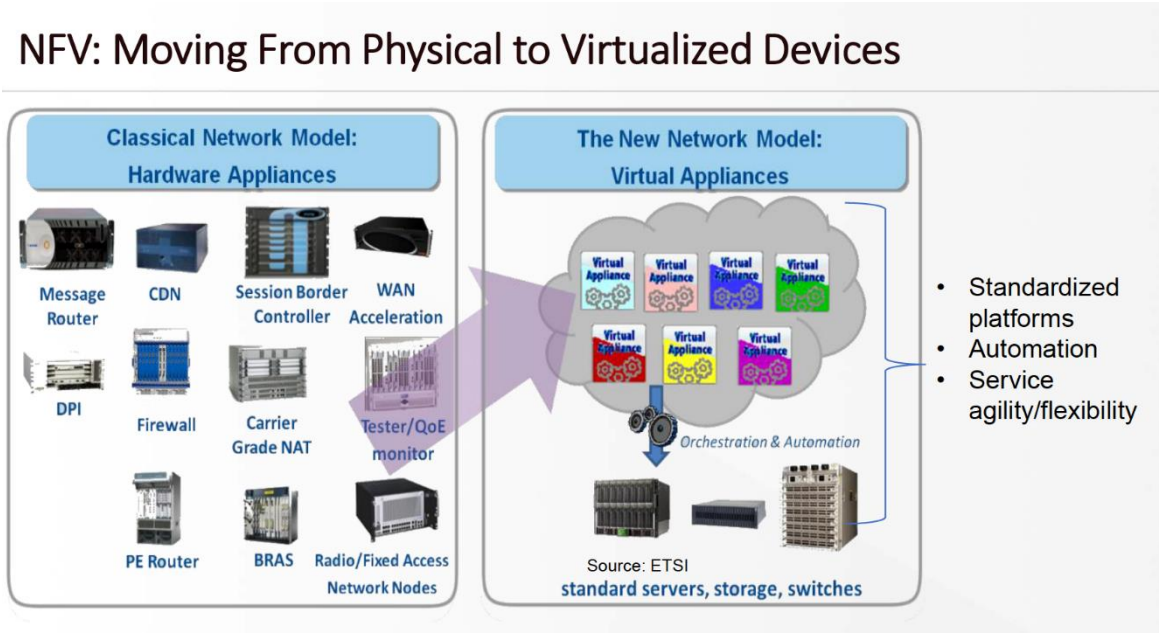
συνδυασμένης αυτής πλατφόρμας και με την τμηματική κατανομή του φόρτου εργασίας τόσο στο Fog όσο και στο Cloud, η καθυστέρηση στο σύστημα μειώνεται αλλά παράλληλα αυξάνεται η κατανάλωση ισχύος. Ο λόγος αυτού του αποτελέσματος είναι πως το Fog computing παρέχει το προνόμιο της κοντινής απόστασης ανάμεσα στους τελικούς χρήστες, κάτι το οποίο προσφέρει αποδοτικότητα ως προς την καθυστέρηση, συγκριτικά με το Cloud, θυσιάζοντας ορισμένους υπολογιστικούς πόρους, ενώ παράλληλα εξοικονομείται και εύρος ζώνης. Αντίθετα, το Cloud Computing είναι πιο ισχυρό υπολογιστικά και ακόμα πιο αποδοτικό ενεργειακά σε σχέση με το Fog, πάντα σε αυτή την συνδυαστική πλατφόρμα.

2.9.1.2.4 Εικονικοποίηση και Διαχείριση δικτύου

Στις μέρες μας, η διαμόρφωση και η διαχείριση των υπολογιστικών δομών του Cloud και του Fog, για την παροχή υπηρεσιών IoT, όπου οι υπηρεσίες «τρέχουν» σε πολλές ετερογενείς συσκευές, καθίσταται μια δύσκολη διαδικασία. Είναι γεγονός πως το Fog απαιτεί η διαχείριση ετερογενών συσκευών και υπηρεσιών να γίνεται ομοιόμορφα, ιδανικά από μια πλήρως αυτοματοποιημένη προγραμματιστική πλατφόρμα. Οι πιο αξιοσημείωτες τεχνολογίες για τον σκοπό αυτό, η **Εικονικοποίηση Δικτυακών Λειτουργιών**[6] (Network Function Virtualization – NFV) καθώς και η **Δικτύωση Καθορισμένου Προγραμματισμού**[7] (Software – Defined Networking –SDN) μπορούν να απλοποιήσουν την εφαρμογή, καθώς και να διαχειριστούν και να μειώσουν τα κόστη σε πολλές διαστάσεις του Fog computing, όπως για παράδειγμα η κατανομή των πόρων.

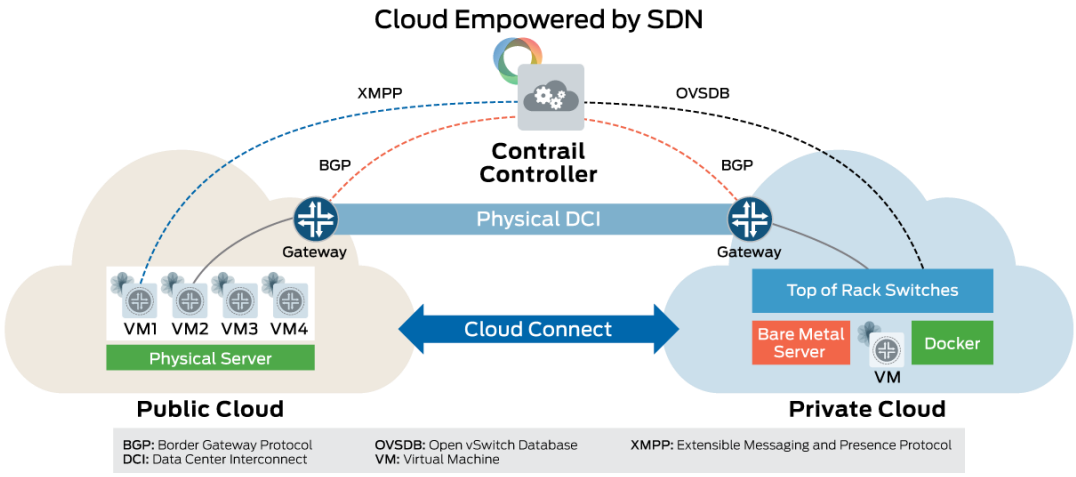
[6] Εικονοποίηση Δικτυακών Λειτουργιών (Network Function Virtualization – NFV): Αποτελεί μια αρχιτεκτονική δικτύου που χρησιμοποιεί τις τεχνολογίες εικονικοποίησης για να εξομοιώσει τις λειτουργίες κόμβων δικτύων σε δομικά στοιχεία που μπορούν να συνδεθούν μαζί για να δημιουργήσουν υπηρεσίες τηλεπικοινωνιών. Τέτοια παραδείγματα λειτουργιών είναι οι εξισορροπητές φόρτου, τα τείχη προστασίας, οι επιταχυντές διαδικτύου κ. ά.

[7] Δικτύωση Καθορισμένου Προγραμματισμού **(**Software – Defined Networking –SDN): Αποτελεί μια προσέγγιση στο Cloud Computing που διευκολύνει την διαχείριση δικτύου και ενεργοποιεί μια προγραμματιστικά αποδοτική διαμόρφωση δικτύου, με σκοπό την βελτίωση της αποδοτικότητας του δικτύου, καθώς και την επίβλεψή του.



Εικόνα 6 - NFV: Μετακίνηση από Φυσικές σε Εικονικοποιήσιμες Συσκευές (Source: TechPlayOn – Network Function [NFV] Architecture)

Πάνω στο θέμα της εξοικονόμησης ενέργειας στο δίκτυο, οι τεχνολογίες NFV και SDN αποτελούν δύο πολλά υποσχόμενες λύσεις. Αρχικά, η NFV προσπαθεί να ενεργοποιήσει μια δυναμική ανάπτυξη των υπηρεσιών χρηστών και δικτύου όπου και όποτε χρειάζονται. Παράλληλα, το SDN αποτελεί ένα στοιχείο «κλειδί» που απαιτείται για την NFV, καθώς ορισμένες δικτυακές υπηρεσίες μπορούν να εκτελεστούν μόνο από προγράμματα. Για παράδειγμα, μερικές πύλες μπορούν να αναπτυχθούν ως εικονικές μηχανές, ενώ η κίνησή των δεδομένων τους μπορεί να ελέγχεται στενά λόγω των δυνατοτήτων της SDN, μέσα σε ένα τοπικό cloud. Γενικά, όπως προκύπτει, ο συνδυασμός των NFV και SDN μπορεί να βοηθήσει στην ελαχιστοποίηση της κατανάλωσης ενέργειας του συνολικού δικτύου και του εξυπηρετητή των κέντρων δεδομένων (S. Yi, C. Li and Q. Li, A Survey of Fog Computing: Concepts, Applications and Issues, 2015).



Εικόνα 7 - Τί είναι το SDN (Source: Juniper Networks – What is SDN?)

ΚΕΦΑΛΑΙΟ 3 - ΕΦΑΡΜΟΓΕΣ

Η πλατφόρμα του fog computing διαθέτει ένα μεγάλο πλήθος εφαρμογών. Ο Bonomi (F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, Fog computing and its role in the internet of things, 2012) έχει παρουσιάσει διάφορα σενάρια του fog computing σε συνδεδεμένα οχήματα, έξυπνα δίκτυα και ασύρματα αναλογιστικά δίκτυα, καθώς και δίκτυα αισθητήρων. Αργότερα, ο Stojmenovic (I. Stojmenovic, Fog computing: A cloud to the ground support for smart things and machine-to-machine networks, 2014) έδωσε έμφαση σε προηγούμενα σενάρια και επεκτάθηκε στο θέμα του fog computing σε έξυπνα κτίρια (smart building). Στην ενότητα αυτή, θα αναφερθούμε σε κάποιες πολύ ενδιαφέρουσες εφαρμογές, που μπορούν να επωφεληθούν από το fog computing.

3.1 Έξυπνο Σπίτι (Smart Home)

Λόγω της ραγδαίας ανάπτυξης του Internet of Things, όλο και περισσότερες έξυπνες συσκευές και αισθητήρες συνδέονται μέσα στο σπίτι. Παρ' όλα αυτά, προϊόντα διαφορετικών προμηθευτών είναι πολλές φορές δύσκολο να δουλέψουν μαζί. Κάποιες εργασίες, οι οποίες απαιτούν μεγάλες ποσότητες υπολογισμών και αποθηκευτικού χώρου, όπως για παράδειγμα η ανάλυση βίντεο σε πραγματικό χρόνο, καθίστανται αδύνατες λόγω των περιορισμένων δυνατοτήτων του υλικού (hardware). Για να επιλυθούν αυτά τα προβλήματα, το fog computing αξιοποιείται για να ενσωματώσει όλα εκείνα τα «συντρίμμια» (ή δομικά στοιχεία), σε μια ενιαία πλατφόρμα και να ενδυναμώσει τις εφαρμογές Έξυπνων Σπιτιών με ελαστικούς πόρους.

Για παράδειγμα, ας δούμε την περίπτωση της εφαρμογής ασφάλειας στο σπίτι. Οι ευρέως αξιοποιήσιμοι αισθητήρες ασφαλείας αποτελούνται από έξυπνες κλειδαριές, συσκευή καταγραφής ήχου/εικόνας, καθώς και διάφορους αισθητήρες παρακολούθησης (πχ αισθητήρας φωτός, χρήσης, κίνησης κτλ.). Εάν τα προϊόντα αυτά δεν είναι του ίδιου προμηθευτή, οι παραπάνω συσκευές ασφαλείας θα είναι δύσκολο να συνδυαστούν. Το Fog Computing μπορεί να προσφέρει εφαρμογές ασφάλειας για το σπίτι, όπως:

- Ενοποιημένο σημείο διεπαφής (interface) για να συνδυάζει όλα τα είδη των ανεξάρτητων συσκευών.
- Ευέλικτους πόρους για την υποστήριξη υπολογισμών και αποθήκευσης.
- Επεξεργασία σε πραγματικό χρόνο και απάντηση με μικρή καθυστέρηση (latency).

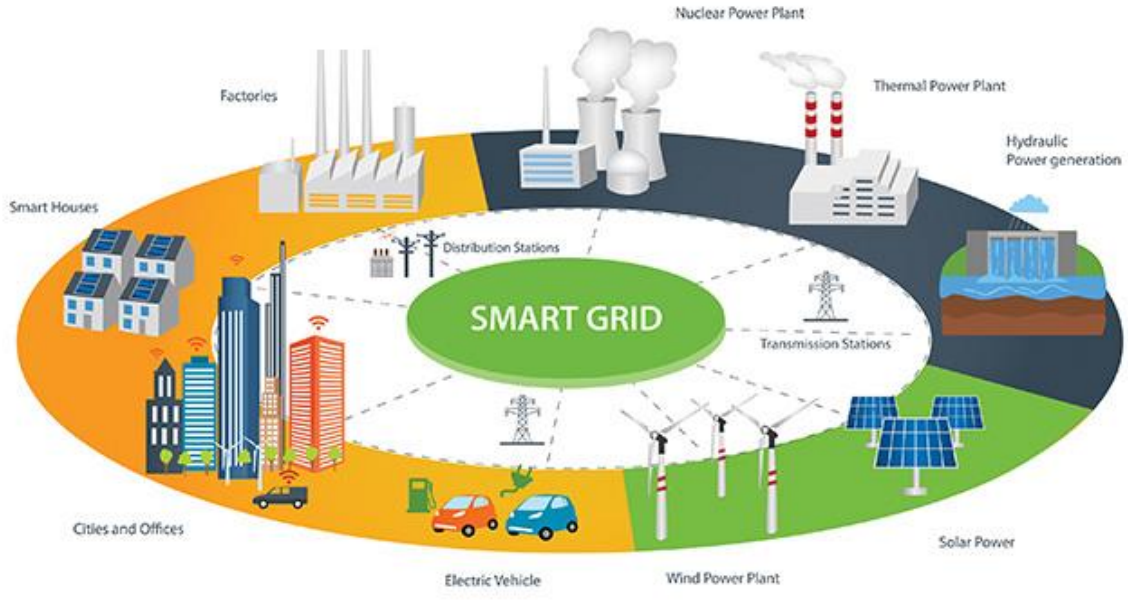
Μόλις η fog πλατφόρμα εγκατασταθεί, κάθε αισθητήρας ασφαλείας συνδέεται ως πελάτης (client). Η αντίστοιχη εφαρμογή εξυπηρετητή (server) μπορεί να εγκατασταθεί σε ανεξάρτητες εικονικές μηχανές (Virtual Machines - VMs). Η λογική των προηγμένων επεξεργασιών μπορεί να εφαρμοσθεί και αυτή σε VMs, οι οποίες μπορούν να επεξεργάζονται δεδομένα, τα οποία μοιράζονται από τις εφαρμογές αισθητήρων ασφαλείας. Για παράδειγμα, ένας αισθητήρας κίνησης εντοπίζει μια ύποπτη κίνηση σε ένα συγκεκριμένο δωμάτιο, οπότε σε ένα ρομπότ καθαρισμού, το οποίο διαθέτει κάμερα για βίντεο, θα δοθεί εντολή να ελέγξει την συγκεκριμένη τοποθεσία. Κατόπιν, τα στατιστικά αναλυτικά στοιχεία του βίντεο, σε πραγματικό χρόνο, θα επεξεργασθούν αυτό το βίντεο και θα επιβεβαιώσουν εάν ήταν ένας εσφαλμένος συναγερμός (false alarm). Τέλος, μια ειδοποίηση και μια αναφορά θα σταλούν στον ιδιοκτήτη του σπιτιού και το σύστημα θα καλέσει την αστυνομία, εάν του έχει εφαρμοσθεί η εντολή αυτή.

Εικόνα 8 - Smart House Network Concept (Source: www.alamy.com – Smart house, home automation and network concept)

3.2 Έξυπνο Δίκτυο (Smart Grid)

Το έξυπνο δίκτυο (smart grid) είναι ένα δίκτυο διανομής ηλεκτρισμού, με έξυπνους μετρητές που χρησιμοποιούνται σε διάφορες τοποθεσίες για να μετράνε την κατάσταση των πληροφοριών σε πραγματικό χρόνο. Ένας συγκεντρωτικός εξυπηρετητής (server), που ονομάζεται σύστημα SCADA, συλλέγει και αναλύει τις καταστάσεις των πληροφοριών και στέλνει εντολές απόκρισης σε κάθε αιτούμενη αλλαγή ή επείγουσα κατάσταση για να σταθεροποιηθεί το ηλεκτρικό δίκτυο.

Το Fog Computing μπορεί να ωφελήσει σε μεγάλο βαθμό το έξυπνο δίκτυο. Με το Fog Computing, ο SCADA μπορεί να συμπληρωθεί με ένα αποκεντρωτικό μοντέλο με μικρά δίκτυα (micro-grids), τα οποία δεν βελτιώνουν μόνο την επεκτασιμότητα, την αποδοτικότητα κόστους, την ασφάλεια και την ραγδαία απόκριση του συστήματος ισχύος, αλλά και να συμπεριλάβει γεννήτριες διανομής ισχύος (αιολικές φάρμες, φωτοβολταϊκά πάνελ και PHEVs) στο κύριο δίκτυο ισχύος. Με το Fog Computing, το έξυπνο δίκτυο θα μετατραπεί σε ένα πολυ-επίπεδο ιεραρχικό σύστημα με αλληλεπίδραση μεταξύ του Fog και του SCADA. Σε ένα τέτοιο σύστημα, ένα fog είναι υπεύθυνο ενός μικρο-δικτύου (micro-grid) και επικοινωνεί με γειτονικά fog και υψηλότερα επίπεδα. Όσο υψηλότερο το επίπεδο, τόσο είναι μεγαλύτερη η καθυστέρηση, καθώς και ευρύτερη η γεωγραφική κάλυψη. Η τελική καθολική κάλυψη παρέχεται από τον SCADA, ο οποίος είναι υπεύθυνος για την μακροπρόθεσμη αποθήκευση και οικονομική αναλυτική.



Εικόνα 9 - Smart Grid Evolution (Source: Eolas Magazine – Smart Grid Evolution)

3.3 Έξυπνο Όχημα (Smart Vehicle)

Το Fog Computing μπορεί να ενσωματωθεί και σε δίκτυα οχημάτων. Ανάλογα με το αν απαιτείται επιπλέον υποδομή, τα σύστημα fog computing για οχήματα μπορούν να κατηγοριοποιηθούν σε δύο τύπους: με βάση την υποδομή και αυτόνομο. Το πρώτο, όπως για παράδειγμα το VTube, βασίζεται σε fog κόμβους (fog nodes) που εφαρμόζονται κατά μήκος του δρόμου (Luan T. H, Cai L. X, Chen J. M, Shen X., Bai F, 2011). Οι κόμβοι αυτοί είναι υπεύθυνοι για την αποστολή/παραλαβή πληροφοριών προς/από τα διερχόμενα οχήματα. Το δεύτερο σύστημα αξιοποιεί τα οχήματα εν κινήσει για να σχηματίσει ένα fog ή cloud, έτσι ώστε να υποστηρίζει κάποιες καταστάσεις επί τόπου, με αποτέλεσμα κάθε fog να μπορεί να επικοινωνεί με τον πελάτη του (client) εσωτερικά, αλλά και με άλλα fog.

Υπάρχουν διάφορες εφαρμογές για συστήματα fog computing για οχήματα, ανεξαρτήτου εάν είναι του πρώτου ή του δεύτερου τύπου. Κάποιες δημοφιλής εφαρμογές είναι: πρόγραμμα των φαναριών, μετριασμός της κυκλοφοριακής συμφόρησης, διαμοίραση μέτρων ασφαλείας, διαχείριση εγκαταστάσεων παρκαρίσματος, διαμοίραση πληροφοριών κίνησης κτλ.

3.4 Επαυξημένη Πραγματικότητα και Ανάλυση Βίντεο σε πραγματικό χρόνο (Augmented Reality and Real-time Video Analytics)

Οι εφαρμογές επαυξημένης πραγματικότητας (AR) είναι αρκετά δημοφιλής σε έξυπνα τηλέφωνα (smart-phones), τάμπλετ και έξυπνα γυαλιά (smart-glasses) καλύπτοντας με μια πληροφοριακή ματιά τον πραγματικό κόσμο (εμφανίζοντας την στο σύστημα εμφάνισης της συσκευής). Μερικά δημοφιλή προϊόντα ή έργα είναι τα Google Glass, Sony SmartEyeGlass και Microsoft HoloLens. Οι εφαρμογές επαυξημένης πραγματικότητας συχνά χρειάζονται υψηλή υπολογιστική ισχύ για την επεξεργασία της ροής βίντεο (video streaming), καθώς και υψηλό εύρος ζώνης για την μετάδοση δεδομένων. Για παράδειγμα, μια φυσιολογική εφαρμογή AR απαιτείται να επεξεργάζεται το πλαίσιο ενός βίντεο σε πραγματικό χρόνο, χρησιμοποιώντας αλγόριθμο εικόνας υπολογιστή, ενώ την ίδια στιγμή πρέπει να επεξεργάζεται εισόδους, όπως την φωνή ή την αίσθηση και, τέλος, να εξάγει έγκαιρο πληροφοριακό περιεχόμενο σε εικόνες. Παρ' όλα αυτά, ο άνθρωπος είναι αρκετά ευαίσθητος σε ότι αφορά την καθυστέρηση στην εκτέλεση των εργασιών. Μια καθυστέρηση στην επεξεργασία μεγαλύτερη της τάξεως των δέκα milliseconds μπορεί να καταστρέψει την εμπειρία του χρήστη και να οδηγήσει σε αρνητική αντίδραση των χρηστών (feedback). Ένα σύστημα AR, υποστηριζόμενο από fog computing, μπορεί να μεγιστοποιήσει την διεκπεραιωτική ικανότητα και να μειώσει την καθυστέρηση στην επεξεργασία και στην μετάδοση.

Συγκεκριμένα, ο K. Ha (K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, M. Satyanarayanan, Mobisys Acm. 2014) σχεδίασε και εφάρμοσε ένα νοητικό βοήθημα που μπορεί να φορεθεί, συνδέοντας τα Google Glass και το Cloudlet, το οποίο μπορεί να προσφέρει σε αυτόν που το φορά, στοιχεία για κοινωνική αλληλεπίδραση μέσω ανάλυσης της σκηνής σε πραγματικό χρόνο. Το σύστημα επιτυγχάνει στενή και περιορισμένη καθυστέρηση από άκρο σε άκρο, ξεφορτώνοντας εργασίες που απαιτούν έντονη και υψηλή υπολογιστική ικανότητα, σε κοντινό Cloudlet. Παράλληλα, η αποτυχία του δικτύου και η μη-διαθεσιμότητα των απομακρυσμένων Cloudlet λαμβάνονται και αυτά υπόψιν, παρέχοντας αυτοματοποιημένες υποβαθμισμένες υπηρεσίες.

Οι πλήρως αξιοποιήσιμοι αισθητήρες κάμερας σε μια πόλη ή κατά μήκος του δρόμου αποτελούν σημαντικό στοιχείο μιας έξυπνης πόλης (smart city) και των έξυπνων οχημάτων, με σκοπό να υποστηρίζουν την παρακολούθηση, την διαχείριση της κίνησης κτλ. Το Fog Computing μπορεί να παρέχει επαρκής πόρους για υπολογισμούς και αποθηκευτικού χώρου, έτσι ώστε να αποθηκεύονται απαθανατιζόμενες ροές βίντεο και επεξεργαζόμενα πλαίσια βίντεο για εργασίες όπως η αναγνώριση αντικειμένου, ο εντοπισμός αντικειμένου, η αλίευση δεδομένων (data mining) κτλ. Αμέσως μετά, μπορούμε απλά να στείλουμε ειδοποιήσεις, καταστάσεις, περιγραφή ή περίληψη βίντεο στους τελικούς χρήστες, σε κεντρικούς εξυπηρετητές ή βάσεις δεδομένων. Με την βοήθεια του fog, μπορούμε να πετύχουμε επεξεργασία, σε πραγματικό χρόνο, και ανάδραση για υψηλής έντασης ροές βίντεο, καθώς και επεκτασιμότητα της υπηρεσίας σε εξαγόμενα δεδομένα χαμηλού εύρους ζώνης. Παράλληλα, τεχνικές διατήρησης της ιδιωτικότητας μπορούν επίσης να εφαρμοσθούν από την πλευρά του fog, έτσι ώστε να μειωθεί η έγνοια για την διαρροή της προσωπικής ιδιωτικότητας σε δημόσια συστήματα παρακολούθησης.

3.5 Μετάδοση Περιεχομένου και Απόκρυψη (Content Delivery and Caching)

Οι παραδοσιακές τεχνολογίες μετάδοσης διαδικτυακού περιεχομένου αδυνατούν να προσαρμοστούν στις απαιτήσεις του χρήστη μετά από την βελτιστοποίηση της διαδικτυακής απόδοσης, στην πλευρά του εξυπηρετητή. Ωστόσο, μικρή γνώση μπορεί να γίνεται γνωστή μόνο στην πλευρά του πελάτη (client) ή κοντά στο δίκτυο του πελάτη, όπως είναι καταστάσεις τοπικού δικτύου ή στατιστικά της κίνησης, τα οποία μπορούν να αξιοποιηθούν για να βελτιστοποιηθεί η διαδικτυακή απόδοση. Για τον λόγο αυτό, ένας fog εξυπηρετητής (Fog Server) μπορεί να παρέχει δυναμική και επεκτάσιμη βελτιστοποίηση βασιζόμενη σε συσκευές πελατών και σε καταστάσεις τοπικού δικτύου. Επιπλέον, αφού ο fog εξυπηρετητής δεν βρίσκεται στην γύρω περιοχή του πελάτη, μπορεί να συλλέξει γνώση από πλευράς του πελάτη και εμπειρία χρηστών, έτσι ώστε να βελτιστοποιήσει την απόδοση μιας ιστοσελίδας. Παρομοίως, μια τεχνική απόκρυψης (caching) μπορεί καλύτερη να αξιοποιηθεί στο εσωτερικά των κόμβων (fog nodes), για να αποθηκεύει ακόμα περισσότερο εύρος ζώνης και να μειώσει την καθυστέρηση για την μεταφορά περιεχομένου.

3.6 Mobile Big Data Analytics

Η επεξεργασία των μεγάλων δεδομένων (Big Data) είναι ένα σημαντικό θέμα όσον αφορά την αρχιτεκτονική μεγάλων δεδομένων στο απλό και κινητό cloud. Το Fog Computing μπορεί να προσφέρει ελαστικούς πόρους για να αυξήσουν την κλίμακα των συστημάτων επεξεργασίας δεδομένων, χωρίς να υποφέρουν από το μειονέκτημα του cloud, το οποίο είναι η υψηλή καθυστέρηση. Στο παράδειγμα του cloud computing, αποτελέσματα ή δεδομένα θα μεταδίδονται στο κέντρο των δεδομένων, εσωτερικά του κυρίως δικτύου και το αποτέλεσμα θα αποστέλλεται πίσω στον τελικό χρήστη, μετά από μια σειρά επεξεργασιών. Μια συνεργασία fog και cloud μπορεί να χειριστεί την απόκτηση, συγκέντρωση και προεπεξεργασία μεγάλων δεδομένων, μειώνοντας την μετακίνηση και αποθήκευση δεδομένων, καθώς και να εξισορροπήσει την υπολογιστική ισχύ πάνω στην επεξεργασία των δεδομένων.

Για παράδειγμα, σε ένα μεγάλο εύρους σύστημα παρακολούθησης περιβάλλοντος, τοπικά και περιφερειακά δεδομένα μπορούν να συγκεντρωθούν και να «αλιευθούν» (mined) σε fog κόμβους, παρέχοντας συνεχή ανάδραση (feedback), ειδικά σε επείγουσες περιπτώσεις, όπως σε έναν συναγερμό τοξικής ρύπανσης. Αυτό μπορεί να γίνει ταυτόχρονα και με λεπτομερή και διεξοδική ανάλυση, καθώς εργασίες έντονης υπολογιστικής μπορούν να προγραμματισθούν στην μεριά του cloud. Για τον λόγο αυτό, πιστεύεται πως η επεξεργασία δεδομένων στην πλευρά του fog θα είναι μια τεχνική κλειδί για να αντιμετωπιστούν τα αναλυτικά στοιχεία σε ένα μεγάλο εύρος δεδομένων, τα οποία παράγονται από εφαρμογές του IoT (Internet of Things).

3.7 Διαχείριση Δεδομένων Υγείας (Health Data Management)

Η διαχείριση δεδομένων υγείας αποτελεί ένα ευαίσθητο ζήτημα για τον λόγο ότι τα δεδομένα υγείας περιέχουν πολύτιμες και προσωπικές πληροφορίες. Με το Fog Computing, είναι δυνατόν να αντιληφθούμε τον κύριο στόχο, ότι ο ασθενής θα πάρει στην κατοχή του τοπικά τα δικά του δεδομένα υγείας. Αυτά τα δεδομένα θα αποθηκεύονται σε fog κόμβο όπως ένα έξυπνο τηλέφωνο ή ένα έξυπνο όχημα. Εφόσον ο ασθενής ζητήσει την βοήθεια ενός ιατρικού εργαστηρίου ή ενός ιατρικού γραφείου, ο υπολογισμός θα ανατεθεί με γνώμονα την ιδιωτικότητα του ασθενή, ενώ η τροποποίηση των δεδομένων συμβαίνει απευθείας σε fog κόμβο, που βρίσκεται στην ιδιοκτησία του ασθενή.

Ένα παράδειγμα συστήματος αποτελεί το FAST, το οποίο προτάθηκε από τον Cao [8]. Το FAST είναι ένα βοηθητικό, κατανεμημένο σύστημα στατιστικής ανάλυσης βασιζόμενο στο fog computing και το οποίο παρακολουθεί την πτώση ασθενών από εγκεφαλικό. Οι συγγραφείς έχουν αναπτύξει μια ομάδα από αλγόριθμους ανίχνευσης πτώσης, συμπεριλαμβανομένων και αλγορίθμων βασιζόμενων σε μετρήσεις επιτάγχυνσης και μεθόδους ανάλυσης χρονικών σειρών, καθώς και τεχνικών φιλτραρίσματος για να την διευκόλυνση της διαδικασίας ανίχνευσης πτώσης. Σχεδίασαν ένα σύστημα ανίχνευσης πτώσης σε πραγματικό χρόνο βασιζόμενο στο fog computing το οποίο διαχωρίζει την εργασία ανίχνευσης της πτώσης μεταξύ των τελικών συσκευών (edge devices) και του cloud. Το προτεινόμενο σύστημα επιτυγχάνει υψηλή ευαισθησία και εξειδίκευση, όταν ελέγχεται απέναντι σε πραγματικά δεδομένα. Την ίδια στιγμή, ο χρόνος απόκρισης και η κατανάλωση ενέργειας βρίσκονται κοντά στις πιο αποδοτικές υπαρκτές προσεγγίσεις.

Μια ακόμη χρήση του fog computing στον τομέα της υγείας δόθηκε από τον Stanchev [9]. Ο συγκεκριμένος πρότεινε μια αρχιτεκτονική τριών επιπέδων για υποδομή έξυπνης πρόληψης υγείας (smart-healthcare), αποτελούμενη από μια πρότυπη, πολυ-επίπεδη αρχιτεκτονική cloud, καθώς και ένα στρώμα fog computing, ούτως ώστε να παρέχει μια αποδοτική αρχιτεκτονική για εφαρμογές πρόληψης υγείας και ηλικιωμένων. Το στρώμα του fog βελτιώνει την αρχιτεκτονική παρέχοντας χαμηλή καθυστέρηση, υποστήριξη κίνησης, αντίληψη τοποθεσίας και μέτρα ασφαλείας. Η ροή διαδικασιών της εφαρμογής πρόληψης υγείας μοντελοποιείται με την χρήση του BMPN (Business Process Modeling Notiation) και στην συνέχεια χαρτογραφείται σε συσκευές μέσω μιας προσέγγισης με γνώμονα τις υπηρεσίες. Η εγκυρότητα του αρχιτεκτονικού μοντέλου αποδείχθηκε μέσω επίδειξης ενός σεναρίου χρήσης ως πρότυπο έξυπνης υποδομής πρόληψης υγείας, βασιζόμενη σε αισθητήρες.

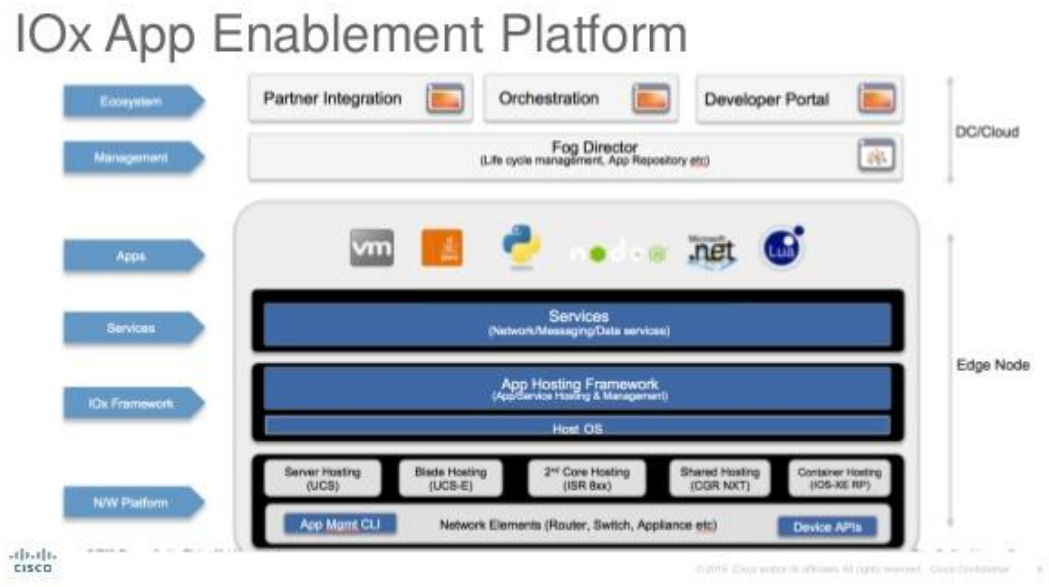
3.8 Εμπορικές Εφαρμογές

Στην ενότητα αυτή, θα αναφερθούμε σε ορισμένα παραδείγματα εμπορικών εφαρμογών, τα οποία έχουν προταθεί ή έχουν διατεθεί ήδη στην αγορά, προκειμένου να εισάγουν ολοένα και περισσότερο την τεχνολογία του fog computing στη καθημερινή ζωή.

3.8.1 Cisco IOx

Η Cisco αποτελεί πρωτοπόρο εταιρεία στον τομέα του fog computing, σε τέτοιο βαθμό έτσι ώστε ο συγκεκριμένος όρος να έχει προταθεί από την ίδια την εταιρεία. Η προσφορά της Cisco στον τομέα του fog computing, γνωστή ως IOx (Cisco, IOx, 2017), είναι ένας συνδυασμός ενός πρωτοπόρου δικτυακού λειτουργικού συστήματος στην βιομηχανία, το IOS, καθώς και του δημοφιλούς λειτουργικού συστήματος ανοιχτού κώδικα Linux. Συγκεκριμένα, οι ανθεκτικοί δρομολογητές (routers) που «τρέχουν» το Cisco IOx δίνουν την δυνατότητα υπολογισμών και αποθήκευσης σε εφαρμογές που φιλοξενούνται σε ένα ξένο λειτουργικό σύστημα, το οποίο με την σειρά του «τρέχει» σε έναν hypervisor μαζί με την εικονική μηχανική του IOS. Επίσης, η Cisco παρέχει ένα app-store, το οποίο επιτρέπει στους χρήστες να «κατεβάζουν» εφαρμογές στις συσκευές IOx, καθώς και μια κονσόλα διαχείρισης εφαρμογών, η οποία έχει σκοπό τον έλεγχο και την παρακολούθηση της απόδοσης μιας εφαρμογής. Χρησιμοποιώντας τις πληροφορίες συσκευών που παρέχονται από διάφορα APIs του Cisco IOx, οι εφαρμογές που λειτουργούν στο fog μπορούν να επικοινωνούν με IoT συσκευές που χρησιμοποιούν οποιοδήποτε πρωτόκολλο. Η φιλοσοφία “δώσε την δική σου διεπαφή” του IOx επιτρέπει την απλή ενσωμάτωση καινοτόμων και εξειδικευμένων τεχνολογιών επικοινωνίας με μια κοινή αρχιτεκτονική IP. Παράλληλα, οι εφαρμογές του fog μπορούν να στέλνουν δεδομένα IoT στο cloud, μεταφράζοντας άτυπα και ιδιόκτητα πρωτόκολλα σε IP.

Το Cisco IOx έχει χρησιμοποιηθεί από μεγάλο αριθμό πελατών στην βιομηχανία του IoT, με σκοπό τον σχεδιασμό καινοτόμων λύσεων για διάφορα προβλήματα. Για παράδειγμα, η εταιρεία Rockwell ανέπτυξε το FactoryTalk AssetCentre (Rockwell Software, FactoryTalk AssetCentre, 2017), ένα συγκεντρωτικό εργαλείο για την ασφαλή παρακολούθηση και διαχείριση χρήσιμων πληροφοριών αυτοματοποίησης, σε όλη την έκταση των εγκαταστάσεων. Επιπλέον, το σύστημα PI της OSIsoft (OSIsoft, PI System, From data to knowledge to transformation, 2017), το οποίο αποτελεί ένα βιομηχανικό πρότυπο στις επιχειρησιακές υποδομές, για την διαχείριση δεδομένων και γεγονότων σε πραγματικό χρόνο, χρησιμοποιεί το IOx της Cisco για την ανάπτυξη και αξιοποίηση των δικών του διεπαφών συλλογής δεδομένων.



Εικόνα 10 -Δομή Πλατφόρμας Cisco IOx (Source: SlideShare – IOx Introduction)

3.8.2 Data in Motion (DMo)

Η Data in Motion της Cisco (Cisco, Data in Motion: The Evolution of Data, 2017) είναι μια τεχνολογία που παρέχει διαχείριση και ανάλυση των δεδομένων στο άκρο του δικτύου. Η DMo της Cisco δημιουργήθηκε γύρω από λύσεις που παρέχονται από την Cisco και τους συνεργάτης της. Η τεχνολογία αυτή παρέχει ένα απλό RESTful API (Wikipedia, Representational state transfer), βασισμένο σε κανόνες, για την κατασκευή εφαρμογών. Οι κανόνες μπορούν να προστεθούν ή να διαγραφούν επι τόπου χωρίς την διακοπή εργασιών. Παράλληλα, η DMo μπορεί να χρησιμοποιηθεί για την εφαρμογή ανάλυσης σε εισερχόμενα δεδομένα, όπως π.χ για την εύρεση συγκεκριμένων δεδομένων, για την σύνοψη δεδομένων, για την παραγωγή νέου αποτελέσματος από δεδομένα κτλ. Η τεχνολογία αυτή έχει ως στόχο την αξιοποίησή της σε συσκευές με κατανεμημένο τρόπο καθώς και το έλεγχο της ροής των δεδομένων που προέρχονται από τις συσκευές IoT.

3.8.3 LocalGrid

Η πλατφόρμα Fog Computing της LocalGrid (LocalGrid, Accelerating IIoT) είναι ένα ενσωματωμένο λογισμικό, εγκατεστημένο σε δικτυακές συσκευές (δρομολογητές, switches) και αισθητήρες. Σταθεροποιεί και ασφαλίζει τις επικοινωνίες μεταξύ των συσκευών όλων των ειδών, από διαφορετικούς προμηθευτές, με στόχο την ελαχιστοποίηση της εξατομίκευσης και του κόστους υπηρεσιών. Η πλατφόρμα αυτή συνυπάρχει σε συσκευές ανάμεσα στο άκρο και το cloud και παρέχει αξιόπιστη M2M επικοινωνία[8], ανάμεσα σε συσκευές, χωρίς να χρειάζεται να περνούν διαμέσου του cloud. Αυτό επιτρέπει στις εφαρμογές να παίρνουν αποφάσεις σε πραγματικό χρόνο,

[8] M2M (Machine to Machine) επικοινωνία: η άμεση επικοινωνία μεταξύ συσκευών με χρήση οποιουδήποτε καναλιού επικοινωνίας, συμπεριλαμβανομένου του ασύρματου ή ενσύρματου.

ακριβώς στο άκρο, χωρίς να έχουν να αντιμετωπίσουν την υψηλή καθυστέρηση λόγω της επικοινωνίας με το cloud. Επιπρόσθετα, όλες οι συσκευές LocalGrid μπορούν να επικοινωνούν με το cloud μέσω ανοιχτών επικοινωνιακών προτύπων, αντιλαμβάνοντας πως η έννοια του fog αποτελεί την επέκταση του cloud. Εφαρμογές που τρέχουν στην πλατφόρμα LocalGrid μπορούν να αξιοποιούν την αλληλεπίδραση μεταξύ του fog και του cloud, με σκοπό την επίλυση περισσότερο περίπλοκων προβλημάτων.

Η παραπάνω πλατφόρμα της LocalGrid έρχεται, επίσης, μαζί με το LocalGrid vRTU, μια εικονική, ασύρματη, τερματική μονάδα βασισμένη σε λογισμικό, η οποία μετατρέπει τις επικοινωνίες μεταξύ των συσκευών στο άκρο, σε συμβατά ανοιχτά πρότυπα. Η vRTU μπορεί να εγκατασταθεί τυποποιημένα, καθώς και ως εξατομικευμένη λύση από διάφορους OEM (Original Equipment Manufacturer)[9], χρηματοδοτώντας συσκευές με δυνατότητες RTU και παρέχοντας ένα μοναδικό σημείο για την διαχείριση όλων των συσκευών, με σκοπό την ελαχιστοποίηση της εξατομίκευσης και του κόστους συντήρησης.

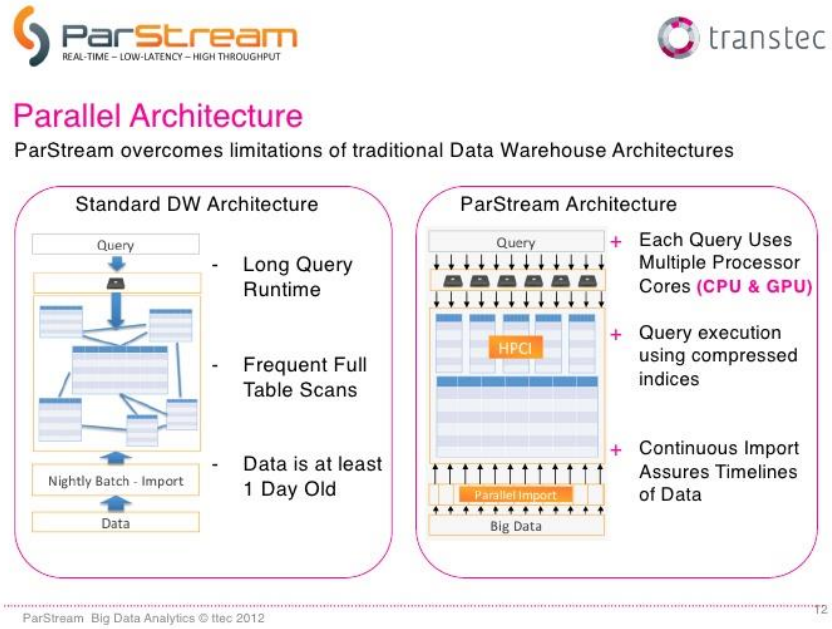
3.8.4 ParStream

Η ParStream είναι μια IoT πλατφόρμα στατιστικών στοιχείων σε πραγματικό χρόνο. Η Cisco και η ParStream (Cisco, Cisco has Completed the Acquisition of ParStream, 2015) εργάζονται μαζί για την κατασκευή μιας γρήγορης, αξιόπιστης και υψηλά επιδεκτικής υποδομής για την ανάλυση στατιστικών στοιχείων στο fog. Η Cisco στοχεύει στην χρήση αυτής της υποδομής για να ενισχύσει τις δικές της λύσεις και να παρέχει νέου τύπου υπηρεσίες.

Η προσφορά της ParStream για μια πλατφόρμα στατιστικής ανάλυσης Μεγάλων Δεδομένων για IoT αποτελεί ένα κομμάτι της πατέντας της τεχνολογίας βάσης δεδομένων, ονόματι ParStream DB. Η ParStream DB αποτελεί μια βάση δεδομένων εσωτερικής μνήμης κατά στήλη (column-based[10]) που διαθέτει μια, υψηλού επιπέδου, παράλληλη και ανεκτική στα σφάλματα αρχιτεκτονική και η οποία κατασκευάζεται χρησιμοποιώντας πατενταρισμένο ευρετήριο και αλγόριθμους συμπίεσης. Εφόσον είναι μια βάση δεδομένων εσωτερικής μνήμης, αποτελεί ιδανική επιλογή για τις fog συσκευές, οι οποίες συνήθως περιόριζαν τον χώρο του δίσκου. Η ParStream μπορεί να «σπρώξει» (push) την εκτέλεση των ερωτημάτων στο άκρο, εκεί όπου τα δεδομένα παράγονται και να εκτελέσει στατιστική ανάλυση με κατανεμημένο τρόπο. Παράλληλα, η ParStream διαθέτει σημαντικά χαμηλό αποτύπωμα (footprint), κάτι το οποίο την κάνει εφικτή στο να αναπτυχθεί σε ενσωματωμένες συσκευές καθώς και σε εφαρμογές που λειτουργούν με βάση το fog, όπως για παράδειγμα το Cisco IOx.

[9] Original Equipment Manufacturer (OEM): επιχείρηση που αγοράζει τα βασικά μέρη ενός υπολογιστή έτοιμα και συνθέτει ένα ολοκληρωμένο υπολογιστή, τον οποίο πουλάει μαζί με άλλες υπηρεσίες, όπως εγγύηση, υποστήριξη κτλ.

[10] Column-Based (Oriented) DBMS: σύστημα διαχείρισης βάσεις δεδομένων που αποθηκεύει πίνακες δεδομένων κατά στήλη παρά κατά γραμμή.



Εικόνα 11 - Αρχιτεκτονική ParStream (Source: SlideShare – Transtec ParStream)

3.8.5 AdLink Vortex (παλαιότερα Prismtech)

Η Vortex (ADLINK, Vortex DDS) είναι μια ευρέως διαδεδομένη πλατφόρμα διαμοιρασμού δεδομένων φτιαγμένη για το Internet of Things. Παρέχει έναν αποδοτικό, ασφαλή και συνεχή τρόπο διαμοίρασης δεδομένων ανάμεσα σε συσκευές που υποστηρίζουν το IoT, τα άκρα, τις πύλες αλλά και το cloud.

Η Vortex αξιοποιεί το πρωτόκολλο DDS 2.0 (Wikipedia, Data Distribution Service) για την διαλειτουργική διανομή δεδομένων, αλλά το επεκτείνει επιπλέον για να υποστηρίζει διαδικτυακής κλίμακας συστήματα, κινητικότητα και εφαρμογές Web 2.0 (Wikipedia, Web 2.0). Η Vortex, επίσης, συμπεριλαμβάνεται μαζί με κοινά IoT πρωτόκολλα αποστολής μηνυμάτων, όπως το MQTT (Wikipedia, MQTT) και το CoAP (Wikipedia, Constained Application Protocol). Επιπλέον, για να αντιμετωπίσει και τις απαιτήσεις ασφάλειας και ιδιωτικότητας, η πλατφόρμα παρέχει υποστήριξη τον έλεγχο πρόσβασης, καθώς και συμμετρική και ασύμμετρη αυθεντικοποίηση.

Κάθε συσκευή IoT είναι συνδεδεμένη σε μια συσκευή άκρου της Vortex η οποία εκτελεί ολόκληρο το λογισμικό της Vortex. Κάθε ένα από αυτά τα λογισμικά εκτελεί μια λειτουργία, η οποία είναι απαραίτητη για την υλοποίηση μιας ευρέως κοινόχρηστης Υπηρεσίας Διανομής Δεδομένων (DDS). Η παραπάνω σύνδεση σχηματίζει έναν τομέα, ο οποίος στην περίπτωση αυτή ονομάζεται fog-τομέας. Εφόσον η Vortex είναι εξοπλισμένη με αυτές τις συσκευές, μπορεί και υποστηρίζει έναν αριθμό μοντέλων ανάπτυξης.

- Fog + Cloud: Συσκευές IoT μέσα σε έναν fog-τομέα επικοινωνούν μεταξύ τους ως peer-to-peer. Οι επιμέρους fog-τομείς πρέπει να επικοινωνούν δια μέσου του cloud.
- Fog + Cloud-link + Cloud: Ομοίως με το προηγούμενο μοντέλο, συσκευές μέσα στον ίδιο fog-τομέα επικοινωνούν ως peer-to-peer, ενώ συσκευές που δεν βρίσκονται στον ίδιο

τομέα ανταλλάσσουν δεδομένα μέσω του cloud, χρησιμοποιώντας ένα Cloud Link[11], το οποίο χειρίζεται τα συσχετιζόμενα ζητήματα ασφαλείας και ελέγχει τις πληροφορίες που εκτίθενται.

- Ενοποιημένο Fog (Federated Fog): Κάθε fog-τομέας κατέχει ένα Vortex Cloud Link, το οποίο «τρέχει» πάνω στην συσκευή Vortex. Το Ενοποιημένο Fog (Federated Fog) είναι μια συλλογή από fog-τομείς, οι οποίοι είναι ενοποιημένοι μέσω Cloud Link. Οι πληροφορίες που ανταλλάσσονται ανάμεσα στους fog-τομείς ελέγχονται από τις Cloud Link καταστάσεις.

[11] Cloud Link: Τεχνολογία, η οποία κρυπτογραφεί, επικυρώνει, ελέγχει και διαχειρίζεται υπολογιστικά συμβάντα μέσα στο cloud.

ΚΕΦΑΛΑΙΟ 4 - ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Καθώς το fog computing θεωρείται ως μια σημαντική επέκταση του cloud, μπορούν να επισημανθούν κάποια ζητήματα ασφάλειας και ιδιωτικότητας, στο γενικότερο πλαίσιο του cloud computing, τα οποία αναπόφευκτα θα έχουν επίδραση πάνω στο fog computing. Εάν δεν αναγνωριστούν αυτά τα ζητήματα, η εξέλιξη και η προώθηση του fog computing θα καθυστερήσει σημαντικά. Καθώς το fog computing βρίσκεται σε πρώιμο στάδιο, παρατηρείται μικρό έργο, έως τώρα, πάνω στα ζητήματα ασφάλειας και ιδιωτικότητας. Από την στιγμή που το fog computing προτείνεται στα πλαίσια του Internet of Things (IoT) και καθώς προέρχεται από το cloud, τα ζητήματα ασφάλειας και ιδιωτικότητας του cloud «κληρονομούνται» στο fog computing. Παράλληλα, ενώ κάποια από αυτά τα ζητήματα μπορούν να αναγνωρισθούν με την χρήση των ήδη υπαρχόντων συστημάτων, υπάρχουν και άλλα ζητήματα που αντιμετωπίζουν νέες προκλήσεις, λόγω των μοναδικών χαρακτηριστικών του fog computing, όπως η ετερογένεση στους fog κόμβους (nodes) και το δίκτυο, η απαίτηση για υποστήριξη κίνησης, οι κόμβοι με τεράστια κλίμακα γεωγραφικής κατανομής, η επίγνωση τοποθεσίας και η χαμηλή καθυστέρηση.

Έτσι, λοιπόν, στο κεφάλαιο αυτό θα αναφερθούμε σε διάφορα ζητήματα ασφάλειας και ιδιωτικότητας στο fog computing, εξετάζοντας το υπάρχον έργο στο fog computing και την σχετική δουλειά στους υποκείμενους τομείς του, έτσι ώστε να αναγνωρίσουμε μερικά προβλήματα που σχετίζονται με την ασφάλεια και την ιδιωτικότητα.

4.1 Απαιτήσεις Ασφάλειας

4.1.1 Εμπιστοσύνη

Τα δίκτυα που σχετίζονται με το Διαδίκτυο των Πραγμάτων (IoT) αναμένεται να παρέχουν αξιόπιστες και ασφαλείς υπηρεσίες στους τελικούς χρήστες. Αυτό απαιτεί από όλες τις συσκευές που ανήκουν στο δίκτυο fog να κατέχουν ένα συγκεκριμένο επίπεδο εμπιστοσύνης ανάμεσά τους. Παράλληλα, η αυθεντικοποίηση παίζει πολύ σημαντικό ρόλο για την εδραίωση των αρχικών σχέσεων ανάμεσα στις συσκευές IoT και τους κόμβους fog στο δίκτυο. Παρ’ όλα αυτά, αυτό δεν είναι επαρκές, καθώς οι συσκευές μπορεί ανά πάσα στιγμή να δυσλειτουργούν, ενώ επίσης μπορούν να είναι ευαίσθητες απέναντι σε κακόβουλες επιθέσεις. Σε ένα τέτοιο σενάριο, η εμπιστευτικότητα παίζει κύριο ρόλο στο να ευνοούνται οι σχέσεις που βασίζονται σε προηγούμενες αλληλεπιδράσεις.

Η εμπιστοσύνη θα πρέπει να παίζει έναν διπλό ρόλο μέσα σε ένα δίκτυο fog. Από την μια, οι fog κόμβοι, οι οποίοι προσφέρουν υπηρεσίες στις συσκευές IoT, θα πρέπει να μπορούν να επιβεβαιώνουν το εάν οι συσκευές που αιτούνται αυτές τις υπηρεσίες είναι αξιόπιστες. Από την άλλη, οι συσκευές IoT που στέλνουν τα δεδομένα, καθώς και άλλα αξιότιμα αιτήματα επεξεργασίας, θα πρέπει να είναι σε θέση να μπορούν να επαληθεύουν το εάν οι επιθυμητοί fog κόμβοι είναι στη πραγματικότητα ασφαλείς. Το γεγονός αυτό απαιτεί ένα σταθερό μοντέλο εμπιστοσύνης που να διασφαλίζει την αξιοπιστία και την ασφάλεια σε ένα δίκτυο fog.

4.1.2 Αυθεντικοποίηση

Μια από τις σημαντικότερες προκλήσεις, όσον αφορά την ασφάλεια, σε ένα δίκτυο fog αποτελεί η αυθεντικοποίηση των δικτυακών συσκευών οι οποίες είναι εγγεγραμμένες στις υπηρεσίες του fog. Μια συσκευή, για να μπορεί να έχει πρόσβαση στις υπηρεσίες ενός δικτύου fog, θα πρέπει πρώτα να γίνει κομμάτι του δικτύου, με το να αυθεντικοποιείται το ίδιο από το δίκτυο. Το γεγονός αυτό είναι απαραίτητο έτσι ώστε να αποτραπεί η είσοδος μη εξουσιοδοτημένων fog κόμβων στο δίκτυο. Το παραπάνω αποτελεί μια μεγάλη πρόκληση, καθώς οι συσκευές που ανήκουν στο δίκτυο περιορίζονται σε διάφορους τομείς, όπως η ισχύς, η επεξεργασία και ο αποθηκευτικός χώρος. Οι παραδοσιακοί μηχανισμοί αυθεντικοποίησης που χρησιμοποιούν πιστοποιητικά και Υποδομές Δημόσιου Κλειδιού (Public – Key Infrastructure – PKI) δεν είναι κατάλληλες λόγω των περιορισμών στον αποθηκευτικό χώρο των IoT συσκευών.

Στην ουσία, η αυθεντικοποίηση θα πρέπει να προσφέρεται ως υπηρεσία, όπως γίνεται και με τις υπηρεσίες αποθήκευσης και επεξεργασίας. Μέσω αυτής, μια συσκευή η οποία χρειάζεται αυτές τις υπηρεσίες θα πρέπει να αυθεντικοποιείται απέναντι στον fog κόμβο, με την βοήθεια ενός μεσάζοντα, ο οποίος μπορεί να είναι η Αρχή Πιστοποίησης (Certifying Authority). Αυτό το μοντέλο διαδικασιών θα μπορούσε να αποτρέπει τους μη εξουσιοδοτημένους κόμβους από το να γίνουν κομμάτια του δικτύου. Επιπρόσθετα, το γεγονός αυτό θα επέτρεπε στους fog κόμβους να περιορίζουν τα αιτήματα υπηρεσιών από τους κακόβουλους / επικίνδυνους κόμβους.

Παρόμοια με το θέμα τις μετακίνησης των τελικών χρηστών, οι fog κόμβοι επίσης εισέρχονται και εξέρχονται από το επίπεδο του fog. Αυτό καθιστά απαραίτητη την εξασφάλιση της αδιάκοπης υπηρεσίας στους εγγεγραμμένους τελικούς χρήστες, κατά την στιγμή που ένας fog κόμβος εισέρχεται (ή εξέρχεται) στο στρώμα του fog. Ο τελικός χρήστης θα πρέπει να είναι σε θέση να μπορεί να αυθεντικοποιηθεί απέναντι στο νέου σχήματος fog στρώμα. Έτσι, η διαδικασία αυτή αποτελεί ακόμα μια σημαντική απαίτηση για την ασφάλεια στο fog δίκτυο.

4.1.3 Ασφαλείς επικοινωνίες στο Fog Computing

Καθώς οι απαιτήσεις επεξεργασίας και αποθήκευσης μπορούν να «ξεφορτώνονται» στους κόμβους fog, το ίδιο δεν μπορεί να ειπωθεί και για τις απαιτήσεις ασφάλειας. Ακόμα και οι IoT συσκευές χρειάζεται να εφαρμόζουν τις απαιτήσεις ασφάλειας. Οι συσκευές αυτές αλληλοεπιδρούν με τους fog κόμβους μόνο στην περίπτωση που απαιτείται να ξεφορτωθούν μια αίτηση επεξεργασίας ή αποθήκευσης. Οποιαδήποτε άλλη αλληλεπίδραση δεν θα πρέπει να θεωρείται ως μέρος του περιβάλλοντος του fog, καθώς έτσι οι επικοινωνίες θα λάμβαναν μέρος ως κομμάτια του δικτύου. Οι κόμβοι αυτοί επικοινωνούν μεταξύ τους όταν απαιτείται η αποτελεσματική διαχείριση δικτυακών πόρων ή ακόμα και η διαχείριση του ίδιου του δικτύου. Μπορούν, επίσης, να λειτουργούν με κατανεμημένο τρόπο έτσι ώστε να εκτελούν μια συγκεκριμένη εργασία. Για τους λόγους αυτούς, για να μπορεί να διασφαλιστεί η επικοινωνία σε ένα περιβάλλον fog computing, θα πρέπει πρώτα να διασφαλίζονται οι επικοινωνίες όπως: επικοινωνίες ανάμεσα σε συσκευές IoT και fog κόμβους, καθώς και οι επικοινωνίες ανάμεσα στους ίδιους τους fog κόμβους.

Συχνά, μια συσκευή IoT μπορεί να ξεκινά την επικοινωνία με οποιονδήποτε από τους κόμβους fog στο δίκτυο, με το να κάνει γνωστή την ανάγκη για επεξεργασία ή αποθήκευση. Στην πραγματικότητα, μια IoT συσκευή μπορεί να μην γνωρίζει καν για την ύπαρξη του δικτύου fog, με συνέπεια τα μηνύματα που στέλνονται από μια τέτοια συσκευή να μην μπορούν να διασφαλιστούν χρησιμοποιώντας τεχνικές συμμετρικής κρυπτογράφησης. Εναλλακτικά, η κρυπτογραφία ασύμμετρου κλειδιού παρουσιάζει τις δικές τις προκλήσεις. Η μεγαλύτερη από αυτές είναι η διατήρηση της PKI, η οποία απαιτείται για την εξασφάλιση μιας ασφαλούς επικοινωνίας. Μια ακόμα πρόκληση αποτελεί η ελαχιστοποίηση του μεγέθους του μηνύματος, έχοντας υπόψιν το

περιορισμένο περιβάλλον στο οποίο λειτουργούν οι συσκευές IoT. Τέλος, οι επικοινωνίες ανάμεσα σε fog κόμβους απαιτούν την ασφάλεια από άκρο-σε-άκρο, καθώς οι κόμβοι που δεσμεύονται σε μονοπάτια πολλαπλών αναπηδήσεων μπορεί να μην είναι αξιόπιστοι.

4.1.4 Ιδιωτικότητα τελικών χρηστών

Το fog computing βασίζεται στην υπολογιστική δύναμη των κατανεμημένων κόμβων με σκοπό την μείωση της πίεσης που ασκείται στο κέντρο δεδομένων. Στο fog computing, η προστασία της ιδιωτικότητας αποτελεί ένα αρκετά απαιτητικό ζήτημα, καθώς οι κόμβοι που βρίσκονται γύρω από τους τελικούς χρήστες συχνά συλλέγουν ευαίσθητα δεδομένα, που αφορούν για παράδειγμα την ταυτότητα, την χρήση των υπηρεσιών ή την τοποθεσία των χρηστών, συγκριτικά με ένα απομακρυσμένο εξυπηρετητή νέφους που βρίσκεται στο κύριο δίκτυο. Παράλληλα, ένας κεντρικός έλεγχος μπορεί να αποδεικνύεται δύσκολος, μιας και οι fog κόμβοι βρίσκονται διασκορπισμένοι σε μεγάλες περιοχές. Ένας κόμβος στο άκρο του δικτύου, ο οποίος μπορεί να μην είναι απόλυτα ασφαλής, μπορεί να θέσει σε κίνδυνο ολόκληρο το δίκτυο, καθώς είναι πιθανό να αποτελέσει την είσοδο για κάποιον εισβολέα στο δίκτυο. Με τη σειρά του, ο εισβολέας, από την στιγμή που βρίσκεται μέσα στο δίκτυο, θα μπορεί να αντλεί και να κλέβει τα ιδιωτικά δεδομένα των χρηστών, τα οποία ανταλλάσσονται ανάμεσα στις οντότητες.

Επιπλέον, η αυξημένη επικοινωνία ανάμεσα στα τρία επίπεδα που απαρτίζουν την αρχιτεκτονική ενός δικτύου fog μπορούν, επίσης, να οδηγήσουν σε διαρροή ιδιωτικών δεδομένων. Για παράδειγμα, η ιδιωτικότητα της τοποθεσίας (M. A. Ferrag κ.ά., Privacy – preserving schemes for ad hoc social networks: A survey, 2016), αποτελεί ένα από τα σημαντικότερα μοντέλα ιδιωτικότητας, καθώς η τοποθεσία εγκατάστασης των συσκευών μπορεί να συνδέεται με τους ιδιοκτήτες. Από την στιγμή που οι fog πελάτες «ξεφορτώνουν» τις εργασίες τους στους πλησιέστερους κόμβους, η τοποθεσία, η πορεία καθώς και οι συνήθειες τις κίνησης μπορούν να αποκαλυφθούν από έναν αντίπαλο. Επιπρόσθετα, οι συνήθειες των χρηστών μπορούν επίσης να αποκαλυφθούν, αναλύοντας τις συνηθέστερες χρήσεις των υπηρεσιών fog, όπως για παράδειγμα σε ένα έξυπνο δίκτυο (smart grid). Όπως έχει περιγραφεί (Y. Hong, W. M. Liu, L. Wang, Privacy preserving smart meter streaming against information leakages, 2017), οι ενδείξεις των έξυπνων μετρητών μπορούν να αποκαλύψουν πληροφορίες για τον χρόνο κατά τον οποίο ένα σπίτι είναι άδειο ή ακόμα και για το ποια τηλεοπτικά προγράμματα βρίσκονται στις προτιμήσεις του τελικού χρήστη.

Παρ’ όλο που τα συστήματα είναι καλά σχεδιασμένα και εφαρμοσμένα με μεγάλο επίπεδο ασφάλειας, μπορούν να αποκαλύψουν σημαντικές πληροφορίες δια μέσου των πλευρικών τους καναλιών. Κάποιες από τις πιθανές διαρροές δεδομένων από τα πλευρικά κανάλια, τα οποία έχουν ήδη αναφερθεί στην βιβλιογραφία, περιλαμβάνουν την ηλεκτρομαγνητική ακτινοβολία, την εμφανή χρονική διάρκεια συγκεκριμένων ενεργειών, την κατανάλωση ισχύος από συγκεκριμένες συσκευές, καθώς και φωτεινές, ακουστικές ή θερμικές εκροές από τον εξοπλισμό (D. Koo, J. Hur, Privacy – preserving deduplication of encrypted data with dynamic ownership management in fog computing, 2017). Όλα τα παραπάνω ζητήματα που σχετίζονται με την ιδιωτικότητα εγείρουν περισσότερο την ανάγκη για τον σχεδιασμό πιο εκλεπτυσμένων λύσεων αλλά και αντίμετρων για την καταπολέμησή τους.

4.1.5 Εικονοποίηση (Virtualization)

Μια σημαντική απαίτηση ασφάλειας στο fog computing αφορά στο χαρακτηριστικό της εικονοποίησης (virtualization). Η εικονοποίηση αποτελεί ένα πολύ σημαντικό χαρακτηριστικό του fog computing, καθώς χωρίς αυτό η ιδέα της χρήσης του fog computing καθίσταται αδύνατη. Για τον λόγο αυτό, είναι απαραίτητο να εξασφαλιστεί και το επίπεδο ασφάλειας ως προς την εικονοποίηση, καθώς θα βοηθήσει αισθητά και στην ομαλή λειτουργία ολόκληρου του συστήματος. Χωρίς την ασφάλεια, οι κακόβουλες εικονικές μηχανές θα μπορούσαν να εκμεταλλεύονται τις υπηρεσίες του fog computing, καθώς επίσης και να αποκτήσουν τον έλεγχο του υποβόσκοντος υλικού και λογισμικού, με σκοπό την εξαπόλυση επιθέσεων.

Όπως είναι γνωστό, οι εικονικές μηχανές (Virtual Machines – VM) λειτουργούν κάτω από το ίδιο υλικό (hardware), ενώ παράλληλα μοιράζονται όλα τα υπολογιστικά στοιχεία, όπως τον επεξεργαστή, την μνήμη και τον αποθηκευτικό χώρο. Ο διαμοιρασμός αυτός έχει ως συνέπεια το να μην είναι αρκετή η απομόνωση των VM, έτσι ώστε να αποτραπεί η παρέμβαση της μιας απέναντι στην άλλη, από τη στιγμή που μοιράζονται τους υπολογιστικούς πόρους, την μνήμη και τον αποθηκευτικό χώρο. Συνεπώς, ένα σοβαρό ζήτημα που προκύπτει είναι η πιθανότητα διαρροής των δεδομένων, όταν αυτά για παράδειγμα βρίσκονται σε καθεστώς αποθήκευσης ή επεξεργασίας. Για τον λόγο αυτό, απαιτείται η απομόνωση στο επίπεδο των VM και του υλικού (επεξεργαστής – μνήμη – αποθηκευτικός χώρος), έτσι ώστε να αποτραπούν τα σενάρια διαρροής ή παραμετροποίησης των δεδομένων.

4.2 Αδυναμίες Ασφάλειας

Καθώς προχωράμε στην ανάλυση του fog computing, αλλά και της συνύπαρξής του με το cloud, μπορούμε, τουλάχιστον, να υποθέσουμε πως η συνύπαρξή τους μπορεί να οδηγήσει σε ορισμένες πολύ σημαντικές βελτιώσεις στο μέλλον, ειδικά όσον αφορά την παροχή υπηρεσιών. Ωστόσο, η συνύπαρξη αυτή μπορεί να οδηγήσει και σε προκλήσεις όσον αφορά τις κυρίαρχες υποθέσεις πάνω στο θέμα της διασφάλισης των υποδομών. Παρ' όλο που, ακόμα, δεν έχουν καθοριστεί πλήρως κάποιες τεχνικές λεπτομέρειες, υπάρχει μεγάλη πιθανότητα στο να μπορούμε να περιγράψουμε κάποιες βασικές αδυναμίες που παρουσιάζει το fog computing, καθώς αυτές, σε αρκετά μεγάλο βαθμό, είναι ταυτόσημες με τις αδυναμίες μιας cloud πλατφόρμας. Έτσι, στην ενότητα αυτή, θα αναλύσουμε κάποιες πιθανές αδυναμίες όσον αφορά την ασφάλεια του fog computing, οι οποίες περιστρέφονται γύρω από ορισμένους βασικούς άξονες.

4.2.1 Εμπιστευτικότητα

Ο όρος εμπιστευτικότητα αναφέρεται στο δικαίωμα που έχουν μόνο τα εγκεκριμένα συστήματα στο να έχουν πρόσβαση σε προστατευόμενα δεδομένα. Σε ότι αφορά την εμπιστευτικότητα, η δομή του fog computing κατέχει δύο αδύναμα σημεία. Το πρώτο από αυτά τα σημεία εκφράζει την αδυναμία πρακτικών για «επι τόπου» αυθεντικοποίηση. Είναι απαραίτητο για τα στοιχεία του fog, αλλά και του cloud, να μπορούν να ταυτοποιούνται πριν την οποιαδήποτε προσπάθεια συναλλαγής (πχ. για την αποδοχή δεδομένων προς επεξεργασία ή την δημοσιοποίηση των ταυτοτήτων των πελατών που συνδέονται ασύρματα). Τα cloud έχουν ήδη αναπτύξει κάποια στοιχειώδη συστήματα για την αυθεντικοποίηση υπολογιστικών κόμβων στους διοικητικούς εξυπηρετητές. Αυτές οι τεχνικές αυθεντικοποίησης καθίστανται επαρκής για τα κέντρα δεδομένων, λόγω του ότι αυτά με τη σειρά τους βρίσκονται κάτω από ένα μοναδικό διαχειριστικό τομέα, ενώ συνυπάρχουν σε ένα κλειστό οικοσύστημα.

Στον αντίποδα, οι παραπάνω τεχνικές εμφανίζουν μια σημαντική αδυναμία στα ανοιχτά περιβάλλοντα. Οι επίδοξοι επιτιθέμενοι μπορούν να εκμεταλλευτούν το σύστημα ταυτοποίησης και να υποδυθούν νόμιμους υπολογιστικούς πόρους. Αυτό συμβαίνει, καθώς δεν υπάρχει κάποιος ισχυρός παράγοντας που να τους το αποτρέπει. Επίσης, λόγω του ότι οι εξυπηρετητές, στα άκρα των αχανών δικτύων, τάσσονται κάτω από διαφορετικούς διαχειριστικούς κλάδους, οι fog κόμβοι θα είναι σε θέση να διανέμουν μικρό αριθμό πληροφοριών, με σκοπό να ταυτοποιούνται ο ένας από τον άλλον. Έτσι, οι επιτιθέμενοι μπορούν να το εκμεταλλευτούν, υποθέτοντας την ταυτότητα των fog κόμβων, καθώς και να προσπαθήσουν να αυθεντικοποιήσουν τους εαυτούς τους στα συστήματα του cloud computing. Εάν το επιτύχουν, θα μπορούν να έχουν πρόσβαση σε πολλές backend λειτουργίες και επεξεργασίες, καθώς και σε ένα τεράστιο όγκο αποθηκευμένων δεδομένων. Εναλλακτικά, οι επιτιθέμενοι μπορούν να στρέψουν την προσοχή τους και προς την μεριά των τελικών χρηστών. Παίζοντας τον ρόλο ενός fog κόμβου, οι επιτιθέμενοι μπορούν να προσφέρουν ασύρματη σύνδεση, καθώς και φαινομενικά νόμιμες υπηρεσίες στους πελάτες. Αυτό με τη σειρά του μπορεί να τους δώσει την ευκαιρία να υποκλέψουν τα στοιχεία σύνδεσης των πελατών. Τέλος, είναι πολύ πιθανό να μπορούν ακόμα και να μεταχειρίζονται αυτόνομες οντότητες, οι οποίες βασίζονται σε κατανεμημένο πρόγραμμα με σκοπό τον έλεγχο και τον συντονισμό.

4.2.2 Ακεραιότητα

Στις μέρες μας, οι διάφοροι χρήστες είναι πιθανό να κατέχουν ένα τεράστιο όγκο προσωπικών αρχείων. Συνεπώς, τα συστήματα των cloud και fog computing παρέχουν την υπηρεσία αποθήκευσης αυτών των αρχείων. Παράλληλα, η πρόσβαση στα αρχεία αυτά μπορεί να γίνεται καθημερινά ή ακόμα και σπάνια. Συνεπώς, είναι επιτακτική η ανάγκη στο να παραμένουν σωστά και αναλλοίωτα.

Η παραπάνω ανάγκη προκαλείται από την ίδια την φύση του fog computing, καθώς τα δεδομένα εξωτερικεύονται σε ένα απομακρυσμένο cloud (ή έναν κοντινό fog κόμβο), το οποίο όμως με τη σειρά του μπορεί να είναι μη ασφαλές και αναξιόπιστο. Στο σημείο αυτό εμφανίζεται και μια σημαντική αδυναμία που σχετίζεται με την ακεραιότητα των δεδομένων και των υπηρεσιών. Από τη στιγμή που το cloud ή ακόμα και οι fog κόμβοι μπορεί να είναι αναξιόπιστοι, τα δεδομένα μπορούν είτε να χαθούν είτε να μεταβληθούν από μη εξουσιοδοτημένους χρήστες. Παράλληλα, σε πολλές περιπτώσεις, τα δεδομένα μπορούν να τροποποιηθούν είτε σκόπιμα, είτε ακόμα και από ατύχημα. Επίσης, υπάρχει η πιθανότητα εμφάνισης ακόμα και λάθους από τους ίδιους τους διαχειριστές που θα μπορούσαν να οδηγήσουν σε απώλεια δεδομένων, όπως είναι για παράδειγμα η επαναφορά λάθους αντιγράφων (backup). Έτσι, ένας επίδοξος επιτιθέμενος θα μπορούσε να αξιοποιήσει αυτά τα εξωτερικευμένα δεδομένα, καθώς έχει χαθεί ο έλεγχος πάνω τους.

Επιπλέον, τα συστήματα του fog και του cloud computing δεν έχουν να κάνουν μόνο με την ύπαρξη αποθηκευτικού χώρου. Υπάρχουν, επίσης, και ορισμένοι εξονυχιστικοί υπολογισμοί που απαιτούν επεξεργαστική ισχύ έτσι ώστε να φέρουν εις πέρας την εκάστοτε λειτουργίες. Κατά συνέπεια, οι χρήστες εξωτερικεύουν και τους υπολογισμούς. Από τη στιγμή που οι πάροχοι των cloud και fog δεν βρίσκονται μέσα στα όρια ασφάλειας, ενώ δεν είναι και διάφανοι απέναντι στους κατόχους των διεργασιών, δεν θα μπορεί να αποδειχθεί εάν η ακεραιότητα των υπολογισμών είναι ανέπαφη ή όχι. Μερικές φορές, οι πάροχοι συμπεριφέρονται με τέτοιο τρόπο ώστε κανείς να μην μπορεί να ανακαλύψει μια διαφοροποίηση των υπολογισμών, από την φυσιολογική εκτέλεση. Επίσης, επειδή οι πόροι έχουν αξία απέναντι στους παρόχους, αυτοί με τη σειρά τους δεν θα μπορούσαν να εκτελέσουν σωστά τις διεργασίες. Ακόμα και αν ο πάροχος θεωρείται περισσότερο ασφαλής, υπάρχουν πολλά θέματα που εγείρονται από το υποβόσκων σύστημά τους, όπως είναι ένας κακόβουλος κώδικας ή μια λανθασμένη ρύθμιση παραμέτρων.

4.2.3 Έλλειψη ασφάλειας στη διαχείριση δικτύου

Ένα σημαντικό σημείο αδυναμίας στο δίκτυο fog εμφανίζεται στη μη ασφαλή διαχείριση του δικτύου στο πίσω μέρος (backend). Για να μπορέσει να επιτευχθεί ένα ενιαίο λογικό υπόστρωμα, είναι απαραίτητο να επεκταθεί η διαχειριστική ικανότητα και πέρα από τα κέντρα δεδομένων. Συνήθως, τα cloud συμπεριλαμβάνουν διαφορετικά διαχειριστικά δίκτυα, ούτως ώστε να υποστηρίξουν την διοίκηση, τον έλεγχο και την παρακολούθηση του υλικού και των εικονικοποιημένων προγραμμάτων (Kanuparthi, A., Karri, R., and Addepalli, S, Hardware and embedded security in the context of internet of things, 2013). Τα παραπάνω δίκτυα βρίσκονται απομονωμένα από την κίνηση στο frond – end. Από την επέκταση της διαχείρισης έρχεται αναγκαστικά και η απώλεια αυτής της φυσικής απομόνωσης. Το γεγονός αυτό εκθέτει την διαχειριστική κίνηση σε ένα εύρος απειλών, με την ύπαρξη αρκετά μικρής ασφάλειας στο ενδιάμεσο.

Γνωρίζοντας, λοιπόν, αυτή την έλλειψη ασφάλειας, οι επιτιθέμενοι μπορούν να στοχεύσουν αυτά τα διαχειριστικά δίκτυα, με σκοπό να τα εκμεταλλευτούν. Μπορούν να χρησιμοποιήσουν ένα συνδυασμό από παραδοσιακές μεθόδους επίθεσης, καθώς και τεχνικές που σχεδιάστηκαν συγκεκριμένα για την πλατφόρμα του fog. Για παράδειγμα, εάν ένας επιτιθέμενος «σπάσει» ένα

κλειδί κρυπτογράφησης, είναι πιθανό να αλλάξει το περιεχόμενο των φορτίων των διαχειριστικών πακέτων. Αυτό θα φέρει ένα τεράστιο πλήγμα στην ακεραιότητα του συστήματος. Παράλληλα, δεδομένου ότι πολλές εικονοποιήσιμες πλατφόρμες βασίζονται σε απλοϊκές τεχνικές αυθεντικοποίησης, είναι πολύ πιθανό να εισαχθούν κακόβουλα δεδομένα μέσα στα κανάλια επικοινωνίας. Εάν αυτό επιτευχθεί, οι επιθέσεις αυτές θα αλλάξουν τελείως την συμπεριφορά του συστήματος fog, καθώς και την συνύπαρξη του με το cloud. Παραδείγματος χάριν, τα διάφορα cloud λαμβάνουν αποφάσεις, ως προς την κατανομή του φόρτου εργασιών, βάσει κάποιων δεδομένων τα οποία καταγράφονται από υπολογιστικούς κόμβους. Τα δεδομένα αυτά περιλαμβάνουν μετρήσεις απόδοσης του εξυπηρετητή, του φόρτου εργασίας καθώς και την διαθεσιμότητα των πόρων. Όμως, με την εισχώρηση κακόβουλων δεδομένων μέσα στα κανάλια των πακέτων, οι επιτιθέμενοι μπορούν να παρουσιάσουν πολλές ζώνες υποδομών ως μη διαθέσιμες.

4.2.4 Διαθεσιμότητα

Σε ό,τι αφορά τη διαθεσιμότητα, η αρχιτεκτονική του fog computing (αλλά και του cloud) εμφανίζει δύο αδύναμα σημεία. Το πρώτο σημείο αφορά στην εξάρτηση του από τις κατανεμημένες εικόνες. Γενικά, το εικονικοποιημένο περιβάλλον στα άκρα του δικτύου είναι πιθανό να ενοποιηθεί με το cloud, ούτως ώστε να υπάρχει ένα μοναδικό λογικό στρώμα το οποίο θα ενώνει τις δύο πλατφόρμες. Σε αυτή τη παραμετροποίηση, οι προγραμματιστικές λειτουργίες που εκτελούνται στους fog κόμβους είτε θα διατηρούνται στο cloud, είτε θα τοποθετούνται τοπικά. Και στις δύο περιπτώσεις, οι κόμβοι θα καταλήξουν να μεταδίδουν ψηφιοποιημένες εικόνες μέσα από δημόσια δίκτυα. Αυτό αντικατοπτρίζει την πρώτη κατηγορία αδυναμίας: την εξάρτηση σε κατανεμημένο πρόγραμμα.

Παράλληλα, η εικονικοποίηση δεν είναι ευαίσθητη μόνο στο θέμα της απώλειας πακέτων, αλλά και στο θέμα της καθυστέρησης. Ενδεχόμενες παρεμβολές, ακόμα και σε επίπεδο χιλιοστών του δευτερολέπτου, μπορούν να διακόψουν ή ακόμα και να αλλοιώσουν τα προγράμματα αναμετάδοσης, κάνοντας τις παρεχόμενες υπηρεσίες μη διαθέσιμες στους τελικούς χρήστες (Kaufman, L., Data security in the world of cloud computing, 2009*)*. Αντίστοιχα, επιθέσεις οι οποίες χαρακτηρίζονται ως απλοϊκές μπορούν να επιτύχουν τον σκοπό τους. Για παράδειγμα, στέλνοντας μια ομάδα από κακόβουλα πακέτα σε μια ενδιάμεση συσκευή δικτύου, μπορεί να προκαλέσει τόση καθυστέρηση που να ωθήσει ακόμα και σε επανεκκίνηση. Τέτοιου είδους επίθεση δεν είναι απαραίτητο να εκτυλίσσεται για μεγάλη χρονική περίοδο. Θα χρειαστεί να διατηρηθεί τόσο χρόνο, ούτως ώστε να «πυροδοτήσει» μια παρεμβολή. Έπειτα, απαιτείται να εκκινήσει ξανά μόνο όταν η στοχοποιημένη διαδικασία ξεκινά να ανακάμπτει. Τέλος, τέτοιες μικρές ομάδες κακόβουλων πακέτων μπορούν να αποφύγουν τον εντοπισμό ανωμαλιών στο δίκτυο, ενώ παράλληλα θα αρνούνται την παροχή υπηρεσιών στους τελικούς χρήστες.

Το δεύτερο σημείο αδυναμίας της πλατφόρμας αφορά την περιορισμένη χωρητικότητα των fog κόμβων. Σε σύγκριση με το cloud, οι κόμβοι αυτοί είναι πιθανό να κατακλειστούν από σχετικά μικρές επιθέσεις άρνησης υπηρεσίας (DOS) (Hong, K., Lillethun, D., Ramachandran, U., Ottenwalder, B., and Koldehofe, B., Mobile fog: a programming model for large-scale applications on the internet of things, 2013). Οι επιθέσεις αυτές μπορεί να βασίζονται είτε στις εφαρμογές είτε στα πακέτα, στοχεύοντας σε εξαντλητική μνήμη, επεξεργαστικές δυνατότητες, ή και κυρίαρχες δικτυακές διεπαφές. Παρ' όλο που η προσωρινή απώλεια ενός fog κόμβου δεν καθίσταται ως καταστροφική, μια γεωγραφικά σχεδιασμένη επίθεση μπορεί να επιφέρει πολύ σοβαρές επιπτώσεις. Για παράδειγμα, οι επίδοξοι επιτιθέμενοι μπορούν να στοχεύσουν μια σειρά από κόμβους στα άκρα του δικτύου, μέσω μιας συγκεκριμένης διαδρομής. Το γεγονός αυτό μπορεί να

προκαλέσει βλάβη στη λειτουργία οχημάτων που βασίζονται σε μεταδιδόμενο περιεχόμενο που αφορά την πλοήγηση ή ακόμα και τον αυτόνομο έλεγχο.

Επιπλέον, μια συντονισμένη σειρά από, μικρού επιπέδου, DOS επιθέσεις έχει την δυνατότητα να παρεμποδίσουν τα δίκτυα αισθητήρων, τα οποία υποστηρίζουν δημόσιες υποδομές. Παραδείγματος χάριν, με την αποδυνάμωση των fog κόμβων σε εργοστάσια παραγωγής ηλεκτρικής ενέργειας, σε εγκαταστάσεις διαχείρισης νερού, ή ακόμα και σε αεροδρόμια, μπορεί να προκληθεί μια αλυσίδα επιπτώσεων κατά μήκος μιας μεγάλης γεωγραφικής περιοχής. Παράλληλα, αναμένεται πως τα δίκτυα fog σε χώρους καταστημάτων, βιομηχανικά πάρκα, καθώς και επιχειρηματικές περιοχές θα στοχοποιηθούν, με σκοπό την υποκλοπή, κάτω από την απειλή των DOS επιθέσεων. Τέτοιες επιθέσεις θα είναι δύσκολο να εντοπιστούν και να διαχειριστούν, σε σύγκριση με προσπάθειες DOS επιθέσεων σε παραδοσιακές υποδομές. Τέλος, λόγω του ότι το fog είναι σχεδιασμένο για απευθείας συνδεσιμότητα με τους τελικούς χρήστες, δεν υπάρχουν τα κατάλληλα σημεία, έτσι ώστε να είναι πιθανή η παρακολούθηση των σχεδίων κίνησης.

4.3 Απειλές

Στη σημερινή εποχή, οι υπηρεσίες που προσφέρουν οι τεχνολογίες των fog και cloud computing αυξάνονται ολοένα και περισσότερο, με αποτέλεσμα να πρέπει να δίνεται μεγαλύτερη προσοχή στην αναγνώριση των πιθανών απειλών και προκλήσεων απέναντι στην ασφάλεια τους, με σκοπό την ομαλότερη λειτουργία τους. Η πρώτη μεγάλη πρόκληση αφορά το μέγεθος του δικτύου. Δυνητικά, εκατοντάδες ή χιλιάδες κόμβοι, οι οποίοι σχηματίζουν ένα δίκτυο IoT, χρησιμοποιούν τις υπηρεσίες του fog και του cloud, με στόχο να ξεπεράσουν τους περιορισμούς που αφορούν τους υπολογισμούς και τον αποθηκευτικό χώρο, καθώς και να βελτιώσουν την απόδοση. Από την στιγμή που όλες αυτές οι συσκευές δεν μπορούν να αυθεντικοποιηθούν από τους fog κόμβους, πιθανώς να μπορούν να βασιστούν σε έμπιστους εξωτερικούς συνεργάτες, όπως μια υπηρεσία πιστοποίησης, οι οποίοι εκδίδουν κάποιες μορφές διαπιστευτηρίων για να εξασφαλίσουν την ταυτοποίηση των συσκευών.

Παρ' όλα αυτά, η ύπαρξη αυτών των διαπιστευτηρίων επιτρέπουν μόνο στον κόμβο που εκτελεί εκείνη τη στιγμή την επεξεργασία να επαληθεύσει εάν το αίτημα έχει δημιουργηθεί από έναν έγκυρο κόμβο. Εν τούτοις, από την στιγμή που ένας τέτοιος συμβιβαστικός κόμβος αποτελεί ένα αποδεκτό κομμάτι του δικτύου, όλα τα παραπάνω αιτήματα θα μπορούν να εξεταστούν. Αντίθετα, το γεγονός του περιορισμού της συνδεσιμότητας στο δίκτυο ή το φιλτράρισμα των αιτημάτων που δημιουργούνται από τις συσκευές IoT αναιρεί, ως ένα βαθμό, το κίνητρο της ύπαρξης των fog κόμβων.

4.3.1 «Πονηρός» Κόμβος Fog (Rogue Fog Node)

Ένας «πονηρός» κόμβος fog είναι μια συσκευή fog ή ένα παράδειγμα fog που προσποιείται ότι είναι γνήσια και προσπαθεί να πείσει τους τελικούς χρήστες να συνδεθούν με αυτήν. Για παράδειγμα, σε μια εσωτερική επίθεση (insider attack), ένας διαχειριστής fog μπορεί να εξουσιοδοτείται για την διαχείριση των περιπτώσεων fog, αλλά μπορεί να «ενσαρκώνει» μια «πονηρή» κατάσταση παρά μια γνήσια. Η μέχρι τώρα μελέτη (Stojmenovic, I., Wen, S., The fog computing paradigm: Scenarios and security issues, 2014) έχει επιδείξει την εφαρμοσιμότητα της επίθεσης man-in-the-middle[12] στο fog computing, σύμφωνα με την οποία η πύλη του δικτύου μπορεί είτε να παραβιαστεί είτε να αντικατασταθεί από μια απομίμησή της. Εφόσον συνδεθεί, ο αντίπαλος μπορεί να χειραγωγεί τα εισερχόμενα και εξερχόμενα αιτήματα από το cloud ή τους τελικούς χρήστες, να συλλέξει ή να αλλοιώσει κρυφά τα δεδομένα χρηστών, καθώς και εύκολα να εξαπολύσει νέες επιθέσεις.

Η ύπαρξη ενός «πονηρού» fog κόμβου θα αποτελεί μια μεγάλη απειλή για την ασφάλεια και την ιδιωτικότητα των δεδομένων των χρηστών. Αυτό το πρόβλημα είναι δύσκολο να διευθετηθεί στο fog computing για διάφορους λόγους, όπως λόγου μια περίπλοκης κατάστασης εμπιστευτικότητας, που απαιτεί διαφορετικά σχέδια διαχείρισης της, αλλά και η δυναμική κατασκευή και διαγραφή μιας κατάστασης εικονικής μηχανής, που δυσκολεύει στο να κρατείται μια «μαύρη λίστα» για τους πονηρούς κόμβους. Ο Han (Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S., A measurement based

[12] Man-in-the-middle attack: Η επίθεση man-in-the-middle (Man-in-the-middle attack) είναι μια κοινή παραβίαση ασφάλειας. Ο επιτιθέμενος παρεμποδίζει τη νόμιμη επικοινωνία μεταξύ δύο μερών, τα οποία είναι φιλικά μεταξύ τους. Στη συνέχεια, ο κακόβουλος host ελέγχει τη ροή επικοινωνίας και μπορεί να αποσπάσει ή να αλλάξει πληροφορίες που στέλνονται από έναν από τους αρχικούς συμμετέχοντες.

rogue ap detection scheme, 2009) έχει προτείνει μια μέθοδο συστήματος μέτρησης, η οποία δίνει το δικαίωμα σε ένα πελάτη (client) να αποφεύγει σημεία διασύνδεσης με πονηρούς κόμβους (Access Point - AP). Η προσέγγιση τους αξιοποιεί τον χρόνο διαδρομής ανάμεσα σε τελικούς χρήστες και στον DNS εξυπηρετητή για την ανίχνευση πονηρών AP στην πλευρά του πελάτη.

4.3.2 Κατάχρηση των υπολογιστικών πόρων

Στο παρελθόν, οι hackers χρησιμοποιούσαν πολλούς υπολογιστές ή ένα botnet[13] για να παράγουν μια μεγάλη ποσότητα υπολογιστικής ισχύος, προκειμένου να διενεργήσουν ψηφιακές επιθέσεις σε υπολογιστικά συστήματα. Η διαδικασία αυτή είναι αρκετά περίπλοκη και μπορεί να χρειαστεί μέχρι και μήνες για να ολοκληρωθεί. Στις μέρες μας, μια ισχυρή υπολογιστική δομή, συμπεριλαμβανομένων των στοιχειών υλικού και λογισμικού, μπορεί εύκολα να δημιουργηθεί με τη χρήση μιας απλής διαδικασίας εγγραφής σε έναν πάροχο υπηρεσιών cloud και fog. Κατά συνέπεια, οι επίδοξοι επιτιθέμενοι, εκμεταλλευόμενοι αυτής της κυρίαρχης υπολογιστικής δύναμης των fog και cloud δικτύων, μπορούν να εξαπολύσουν επιθέσεις σε πολύ σύντομο χρονικό διάστημα. Για παράδειγμα, οι επιθέσεις «ωμής βίας» (brute – force attacks) και οι επιθέσεις άρνησης υπηρεσιών (Denial – Of - Service Attacks) μπορούν να προκληθούν μέσω της εκμετάλλευσης της ισχύος του fog computing.

Μια επίθεση «ωμής βίας» είναι μια τεχνική που χρησιμοποιείται για την εύρεση κωδικών ασφαλείας. Η επιτυχία αυτής της επίθεσης βασίζεται, σε πολύ μεγάλο βαθμό, σε συστήματα ισχυρών υπολογιστικών ικανοτήτων, καθώς απαιτείται η αποστολή χιλιάδων πιθανών κωδικών προς τον στοχοποιημένο λογαριασμό ενός χρήστη, μέχρις ότου να βρεθεί ο σωστός κωδικός πρόσβασης. Αναπόφευκτα, τα συστήματα του fog computing (όπως και του cloud) παρέχουν μια ενδεικτική πλατφόρμα για την εκτέλεση τέτοιου είδους επιθέσεων. Για παράδειγμα, ο Γερμανός ερευνητής Thomas Roth, παρουσίασε μια επίθεση brute-force στο συνέδριο Τεχνικής Ασφάλειας Black Hat (T. Roth, Breaking Encryptions Using GPU Accelerated Cloud Instances, 2011). Ο ερευνητής κατάφερε να «σπάσει» ένα δίκτυο, το οποίο ήταν προστατευμένο με WPA – PSK, ενοικιάζοντας έναν εξυπηρετητή από το EC2 της Amazon. Σε περίπου 20 λεπτά, ο ερευνητής εξαπέλυσε 400.000 κωδικούς το δευτερόλεπτο μέσα στο σύστημα, ενώ το κόστος της χρήσης της υπηρεσίας EC2 ανήλθε σε μόλις 28 λεπτά του ευρώ το λεπτό.

Αντίστοιχα, οι επιθέσεις άρνησης υπηρεσιών προσπαθούν να παρενοχλήσουν έναν εξυπηρετητή ή έναν πόρο του δικτύου με σκοπό να μετατρέψουν τους νόμιμους χρήστες σε χρήστες που να μην μπορούν να έχουν πρόσβαση στις υπηρεσίες των υπολογιστών. Οι επιθέσεις αυτές απαρτίζονται από διάφορες μορφές και στοχεύουν σε διαφορετικού είδους υπηρεσίες. Γενικά, μπορούν να κατηγοριοποιηθούν σε τρεις βασικούς τύπους: κατανάλωση αραιών, περιορισμένων ή μη – ανανεώσιμων πόρων, καταστροφή ή αλλαγή των παραμέτρων του συστήματος, καθώς και στην φυσική καταστροφή ή μετατροπή των δικτυακών δομικών στοιχείων (CERT Coordination Center, Denial of Service).

Ανάμεσα σε αυτούς τους τύπους, η «πλημμύρα» (flooding) αποτελεί τον συνηθέστερο τρόπο με τον οποίο οι επιτιθέμενοι «γκρεμίζουν» το σύστημα του θύματος, χρησιμοποιώντας μια τεράστια ποσότητα από ψευδή αιτήματα, με συνέπεια το μπλοκάρισμα των υπηρεσιών προς τους νόμιμους χρήστες. Όταν η μέθοδος της «πλημμύρας» εφαρμόζεται στις υπηρεσίες του fog και του cloud, δύο είναι τα είδη των επιθέσεων άρνησης υπηρεσιών που μπορούν να συμβούν στα υπολογιστικά

[13] Botnet: Ως botnet ορίζεται ένα δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως από τον λεγόμενο botmaster χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται bots ή και «ζόμπι».

συστήματα του fog και του cloud: η άμεση DoS και η έμμεση DoS επίθεση (M. Jensen, J. Schwenk, N. Gruschka, L. L. Iacono, On Technical Security Issues in Cloud Computing, 2009). Όταν ένας εξυπηρετητής cloud, ή ακόμα και ένας fog κόμβος, λαμβάνει έναν τεράστιο αριθμό από ψευδή αιτήματα, θα πρέπει να παρέχει περισσότερους υπολογιστικούς πόρους για να μπορεί να ανταπεξέλθει απέναντι σε αυτά τα αιτήματα. Τελικά, ο εξυπηρετητής εξαντλεί όλες του τις δυνατότητες, με συνέπεια την εφαρμογή μιας άμεσης DoS επίθεσης σε όλα τα αιτήματα που προέρχονται από τους νόμιμους χρήστες. Αντίστοιχα, η «πλημμύρα» μπορεί να προκαλέσει και πιθανή έμμεση επίθεση DoS στους άλλους εξυπηρετητές ή κόμβους στο ίδιο cloud, όταν αυτοί μοιράζονται τον φόρτο εργασίας του θύματος, με αποτέλεσμα την πλήρη απώλεια διαθεσιμότητας όλων των υπηρεσιών.

4.3.3 Παραβίαση Δεδομένων

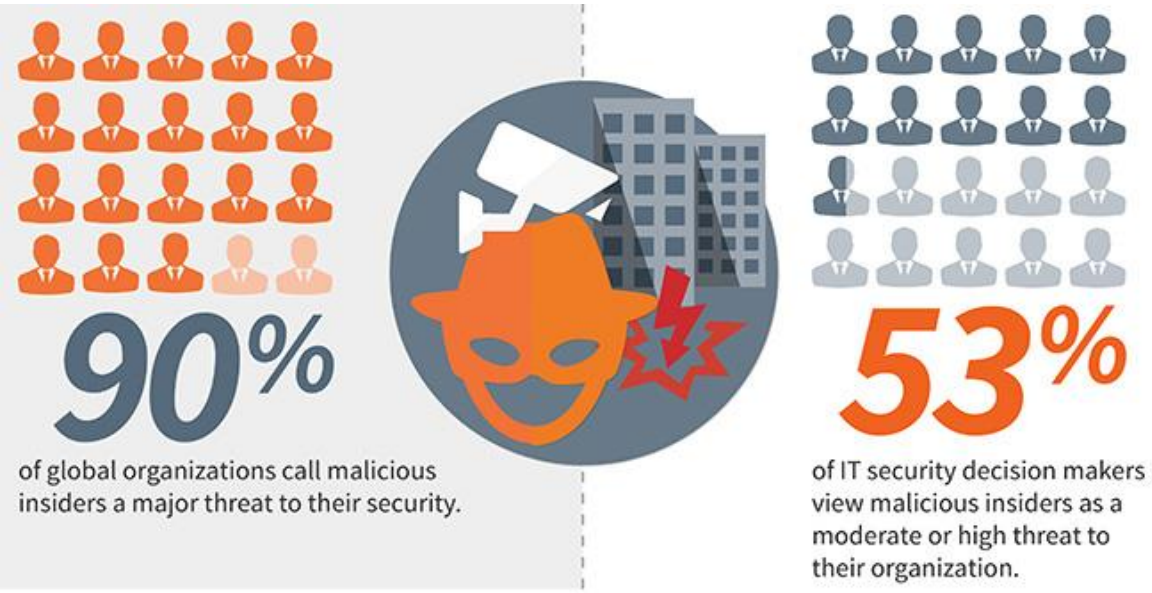
4.3.3.1 Κακόβουλος Πληροφοριοδότης (Malicious Insider)

Οι απειλές προς της ασφάλεια ενός οργανισμού μπορεί να προέρχονται είτε από εξωτερικούς παράγοντες, αλλά και από το εσωτερικό του ίδιου του οργανισμού. Σύμφωνα με την Έρευνα Παρακολούθησης Κυβερνο-ασφάλειας (Cybersecurity Watch Survey) του 2011, η οποία διενεργήθηκε σε 607 εταιρείες, κυβερνητικά στελέχη, επαγγελματίες και πελάτες, το 21% των κυβερνο – επιθέσεων προκλήθηκαν από εσωτερικούς συντελεστές. Επίσης, το 33% των ερωτηθέντων πιστεύουν πως οι εσωτερικές επιθέσεις είναι περισσότερο δαπανηρές και επιβλαβείς προς τους οργανισμούς (CERT Coordination Center, Cybersecurity Watch Survey, 2011).

Σύμφωνα με την έρευνα, οι πιο συχνές εσωτερικές επιθέσεις αφορούν την μη εξουσιοδοτημένη πρόσβαση και χρήση των εταιρικών πληροφοριών (63%), την ακούσια αποκάλυψη προσωπικών ή ευαίσθητων δεδομένων (57%), τους ιούς, τα «σκουλήκια» (worms) ή άλλου είδους κακόβουλων κωδικών (37%), καθώς και την υποκλοπή πνευματικής ιδιοκτησίας (32%).

Καθώς η μεταφορά των δεδομένων και των εφαρμογών σε περιβάλλοντα του fog και του cloud computing μπορεί να διευρύνει τις επιχειρηματικές δραστηριότητες, αντίθετα η κακόβουλη υπονόμευση των ευαίσθητων πληροφοριακών πόρων ενός οργανισμού μπορεί να θέσει σε κίνδυνο ολόκληρη τη λειτουργία του θύματος – οργανισμού. Ειδικότερα, υπάρχουν τρεις τύποι εσωτερικών επιθέσεων που σχετίζονται με τα περιβάλλοντα fog και cloud: ο «πονηρός» διαχειριστής (rogue administrator), τα μέλη που εκμεταλλεύονται τις αδυναμίες του fog και του cloud, καθώς και τα μέλη που χρησιμοποιούν αυτές τις πλατφόρμες για την διενέργεια κακόβουλων πρακτικών (CERT, Insider Threats Related to Cloud Computing, 2012).

Πιο συγκεκριμένα, ένας «πονηρός» διαχειριστής έχει το προνόμιο να υποκλέπτει μη προστατευμένα αρχεία, να εξαπολύει brute – force επιθέσεις απέναντι σε κωδικούς πρόσβασης, καθώς επίσης και να «κατεβάζει» τα δεδομένα των πελατών από τον οργανισμό. Παράλληλα, οι εσωτερικοί επιτιθέμενοι που εκμεταλλεύονται τις αδυναμίες του fog δικτύου, προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε απόρρητα δεδομένα του οργανισμού. Αυτό έχει ως πιθανό αποτέλεσμα να μπορούν να αποκτούν μεγάλα κέρδη από την πώληση των ευαίσθητων δεδομένων, ή ακόμα και να χρησιμοποιήσουν αυτές τις πληροφορίες για τις μελλοντικές τους επιχειρηματικές δραστηριότητες. Τέλος, οι επιτιθέμενοι που χρησιμοποιούν το fog και το cloud για τη διενέργεια κακόβουλων ενεργειών εξαπολύουν επιθέσεις απέναντι στη δομή του IT της δικής τους εταιρείας. Από τη στιγμή που οι επιτιθέμενοι γνωρίζουν τις λειτουργίες του τμήματος IT των δικών τους εταιρειών, οι επιθέσεις καθίστανται εξαιρετικά δύσκολες στο να ανιχνευθούν μέσω μιας εγκληματολογικής έρευνας.



Εικόνα 12 - Organizations still unprepared for malicious insiders (Source: Help Net Security – Mirko Zorz, Organizations still unprepared for malicious insiders)

4.3.3.2 Διαδικτυακή Κυβερνο – κλοπή (Online Cyber Theft)

Οι υπηρεσίες που προσφέρονται μέσω του fog computing, όπως και του cloud, παρέχουν στους χρήστες πανίσχυρες δυνατότητες επεξεργασίας και τεράστιες ποσότητες αποθηκευτικού χώρου. Λόγω του χαμηλού κόστους των παραπάνω υπηρεσιών, οι εταιρείες θα μπορούσαν να μεταφέρουν τις επιχειρηματικές τους δραστηριότητες στο cloud και το fog αντίστοιχα, έτσι ώστε να μην χρειαστεί να προμηθευτούν τους δικούς τους εξυπηρετητές για την αποθήκευση των πληροφοριών των πελατών τους ή τη διαχείριση της κίνησης από πελάτες και επισκέπτες. Για παράδειγμα, το Netflix μισθώνει υπολογιστικό χώρο από τις Διαδικτυακές Υπηρεσίες του Amazon (Amazon Web Services – AWS) για την παροχή συνδρομητικών υπηρεσιών για την παρακολούθηση τηλεοπτικών σειρών και ταινιών. Επίσης, το Dropbox προσφέρει υπηρεσίες αποθηκευτικού χώρου στο cloud, για την αποθήκευση δεδομένων μεγέθους terabyte.

Όπως γίνεται αντιληπτό, οι υπηρεσίες που βασίζονται στο νέφος και κατ' επέκταση στο fog, γίνονται όλο και μεγαλύτερο κομμάτι της καθημερινής ζωής. Ταυτόχρονα όμως, τα ευαίσθητα δεδομένα που αποθηκεύονται στους χώρους του cloud και του fog, γίνονται πολύ επιθυμητοί στόχοι για διαδικτυακή κυβερνο-κλοπή. Σύμφωνα με την ανάλυση των παραβιάσεων δεδομένων σε 209 παγκόσμιες εταιρείες το 2011, το 37% αυτών των παραβιάσεων περιλάμβαναν κακόβουλες επιθέσεις. Ο μέσος όρος κόστους κάθε παραβιασμένης εγγραφής ανήλθε στα 222$ (Symantec, Data Breach Trends & Stats,2012). Για παράδειγμα, το διαδικτυακό κατάστημα πώλησης Zappos (το οποίο ανήκει στο Amazon) ήταν ένα από τα θύματα τέτοιου είδους κλοπής. Κατά την επίθεση φαίνεται να παραβιάστηκαν περίπου 24 εκατομμύρια λογαριασμοί. Δυστυχώς, οι πληροφορίες αυτές περιλάμβαναν ονόματα, διευθύνσεις e-mail, διευθύνσεις χρέωσης και αποστολής, τηλεφωνικούς αριθμούς, τα τελευταία τέσσερα ψηφία των αριθμών πιστωτικών καρτών, καθώς και κρυπτογραφημένες εκδοχές των κωδικών ασφαλείας των λογαριασμών.

Η υποκλοπή δεδομένων που αποθηκεύονται στο cloud ή ακόμα και σε fog κόμβους, θα μπορούσε να πραγματοποιηθεί ακόμα και στα μέσα κοινωνικής δικτύωσης. Οι σελίδες κοινωνικές δικτύωσης, όπως είναι το Twitter, το Facebook και το Instagram, έχουν προσελκύσει τους ανθρώπους, οι οποίοι τα χρησιμοποιούν για να επικοινωνούν με φίλους. Παράλληλα, τα δίκτυα αυτά προσφέρουν μια

πλατφόρμα για την διαμοίραση προσωπικών πληροφοριών, όπως το γένος, το τηλέφωνο, την ημερομηνία γέννησης κτλ. Παρ΄ όλα αυτά, οι ευαίσθητες αυτές πληροφορίες μπορούν να γίνουν μέρος υποκλοπής, στην περίπτωση που οι επιτιθέμενοι εντοπίσουν τρόπους να παραβιάσουν το fog ή το cloud. Παραδείγματος χάριν, το LinkedIn, η μεγαλύτερη επαγγελματική σελίδα κοινωνικής δικτύωσης, με πάνω από 175 εκατομμύρια χρήστες, δήλωσε πως η βάση δεδομένων των κωδικών ασφαλείας παραβιάστηκε κατά τη διάρκεια μιας επίθεσης ασφαλείας (LinkedIn Blog, An Update on LinkedIn Member Passwords Compromised, 2012). Σύμφωνα με την αναφορά, περίπου 6,5 εκατομμύρια κωδικοί κλάπηκαν και «ανέβηκαν» σε ένα Ρωσικό διαδικτυακό forum, ενώ περισσότερο από 200.000 από αυτούς τους κωδικούς είχαν ήδη «σπάσει».

Οι διαδικτυακοί «κλέφτες» μπορούν, επίσης, να υποκλέψουν κωδικούς για να έχουν πρόσβαση σε λογαριασμούς χρηστών, με σκοπό να εξαπολύσουν επιθέσεις σε άλλους χρήστες. Το Dropbox έχει επιβεβαιώσει πως οι χρήστες του έπεσαν θύμα μιας επίθεσης spam (Dropbox, Yes, We Were Hacked, 2012). Ειδικότερα, τα ονόματα πρόσβασης και κωδικοί που είχαν κλαπεί από άλλες σελίδες χρησιμοποιήθηκαν για την είσοδο σε λογαριασμούς χρηστών του Dropbox. Επιπλέον, ένας από αυτούς τους κωδικούς χρησιμοποιήθηκε για την πρόσβαση σε λογαριασμό ενός υπαλλήλου του Dropbox, ο οποίος περιείχε τα έγγραφα ενός project με τις διευθύνσεις e-mail διαφόρων χρηστών. Κατά συνέπεια, ο επιτιθέμενος έστειλε spam e-mails, που είχαν ως θέμα τα διαδικτυακά καζίνο και τις στοιχηματικές εταιρείες, σε άλλους χρήστες.

Τέλος, οι επίδοξοι παραβάτες θα μπορούσαν να εκμεταλλευτούν ακόμα και την υπολογιστική ισχύ που προσφέρεται μέσω των υπηρεσιών του fog και του cloud για την εξαπόλυση επιθέσεων. Λόγου χάριν, η υπηρεσία νέφους EC2 της Amazon έχει χρησιμοποιηθεί για την παραβίαση προσωπικών πληροφοριών. Με την εγγραφή στην υπηρεσία, χρησιμοποιώντας ψεύτικα στοιχεία, οι επιτιθέμενοι ενοικίασαν έναν ψηφιακό εξυπηρετητή και εξαπέλυσαν επίθεση για την υποκλοπή δεδομένων από το PlayStation Network της Sony. Οι επιτιθέμενοι δεν εισήλθαν στους εξυπηρετητές της Amazon, αυτό όμως δεν τους απέτρεψε από το να παραβιάσουν περίπου 100 εκατομμύρια προσωπικούς λογαριασμούς αυτού του δικτύου.

4.3.4 Επιθέσεις ασφάλειας στο Fog (και Cloud)

Το περιβάλλον του fog computing είναι πιθανό να μπορεί να υπόκειται σε σοβαρές κακόβουλες επιθέσεις, κάτι το οποίο χωρίς τα κατάλληλα μέτρα ασφαλείας, μπορεί να υποβαθμίσει σε πολύ μεγάλο βαθμό τις ικανότητες του δικτύου. Οι υπάρχουσες στρατηγικές ασφάλειας για τους άλλους τύπους δικτύων δεν αποτελούν κατάλληλα μέσα για το περιβάλλον του fog computing, κυρίως λόγω του «ανοιχτού» χαρακτήρα του δικτύου. Στη συνέχεια της ενότητας θα αναλύσουμε ορισμένες από τις κυριότερες και πιο επικίνδυνες μορφές επιθέσεων απέναντι στα fog συστήματα και δίκτυα.

4.3.4.1 Malware Injection Attack

Οι εφαρμογές του διαδικτύου παρέχουν δυναμικές ιστοσελίδες στους χρήστες του, έτσι ώστε να μπορούν να έχουν πρόσβαση στους εξυπηρετητές των εφαρμογών, μέσω ενός περιηγητή (browser). Οι εφαρμογές αυτές μπορεί να είναι τόσο απλές όσο ένα σύστημα ηλεκτρονικής αλληλογραφίας, ή τόσο περίπλοκες όπως είναι ένα διαδικτυακό τραπεζικό σύστημα. Μέσα σε όλα αυτά, έρευνες έχουν δείξει πως οι εξυπηρετητές είναι ευάλωτοι απέναντι σε διαδικτυακές επιθέσεις (Symantec, Web Based Attacks, 2009). Σύμφωνα με την αναφορά της Symantec, ο αριθμός των διαδικτυακών επιθέσεων το 2018 αυξήθηκε κατά 56%, με πάνω από 1,3 εκατομμύρια μοναδικές νέες επιθέσεις κάθε μέρα, να μπλοκάρονται από την ίδια την Symantec (Symantec, Internet Security Threat

Report, 2019). Συγκεκριμένα, 1 στα 10 URL χαρακτηρίστηκαν ως κακόβουλα, από τα 1 στα 16 που ήταν το 2017.

Η επίθεση εκχώρησης κακόβουλου λογισμικού (Malware injection Attack) αποτελεί μια κατηγορία των διαδικτυακών επιθέσεων, με την οποία οι επιτιθέμενοι εκμεταλλεύονται τις αδυναμίες μιας διαδικτυακής εφαρμογής και ενσωματώνουν κακόβουλους κώδικες σε αυτή, με τους οποίους αλλάζει η σειρά της φυσιολογικής της εκτέλεσης. Όπως αυτές οι εφαρμογές, τα συστήματα cloud και fog είναι και αυτά ευάλωτα απέναντι σε τέτοιου είδους επιθέσεις. Πιο αναλυτικά, οι επιτιθέμενοι κατασκευάζουν μια κακόβουλη εφαρμογή, πρόγραμμα ή εικονική μηχανή και την εισχωρούν σε μοντέλα υπηρεσιών cloud και fog (όπως είναι το SaaS). Μόλις ολοκληρωθεί η εκχώρηση, το κακόβουλο μοντέλο εκτελείται ως ένα γνήσιο αντικείμενο το οποίο «τρέχει» μέσα στο fog. Έτσι, ο επιτιθέμενος μπορεί να κάνει το οτιδήποτε, από την παραποίηση των δεδομένων μέχρι και την υποκλοπή τους.

Ανάμεσα σε όλες τις malware injection επιθέσεις, η SQL injection και η Cross-Site scripting επίθεση αποτελούν τις πιο κοινές μορφές τους. Αρχικά, η SQL injection επίθεση στοχεύει σε βάσεις δεδομένων SQL και οι οποίες εκτελούν ευάλωτες εφαρμογές βάσεων δεδομένων. Οι επιτιθέμενοι εκμεταλλεύονται αυτές τις αδυναμίες, εισχωρώντας κακόβουλους κώδικες στους εξυπηρετητές, με σκοπό να παρακάμψουν την διαδικασία εισόδου (log in) και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε backend βάσεις δεδομένων. Εάν το επιτύχουν, οι επιτιθέμενοι θα έχουν την δυνατότητα να παραποιήσουν το περιεχόμενο των βάσεων δεδομένων, να ανακτήσουν απόρρητα δεδομένα, να εκτελέσουν (ασύρματα) εντολές προς το σύστημα, ή ακόμα και να αποκτήσουν τον έλεγχο του διαδικτυακού εξυπηρετητή για περισσότερες εγκληματικές ενέργειες. Ένα από τα πιο γνωστά θύματα μιας τέτοιας επίθεσης αποτέλεσε το PlayStation της εταιρείας Sony. Συγκεκριμένα, σύμφωνα με τον blog της Sophos, μια επίθεση SQL injection χρησιμοποιήθηκε επιτυχώς για την τοποθέτηση μη εξουσιοδοτημένου κώδικα σε 209 ιστοσελίδες, οι οποίες προωθούσαν δύο πολύ γνωστά βιντεοπαιχνίδια του PlayStation, το «SingStar Pop» και το «God Of War» (Sophos, Visitors to Sony PlayStation Website at Risk of Malware Infection, 2008*)*.

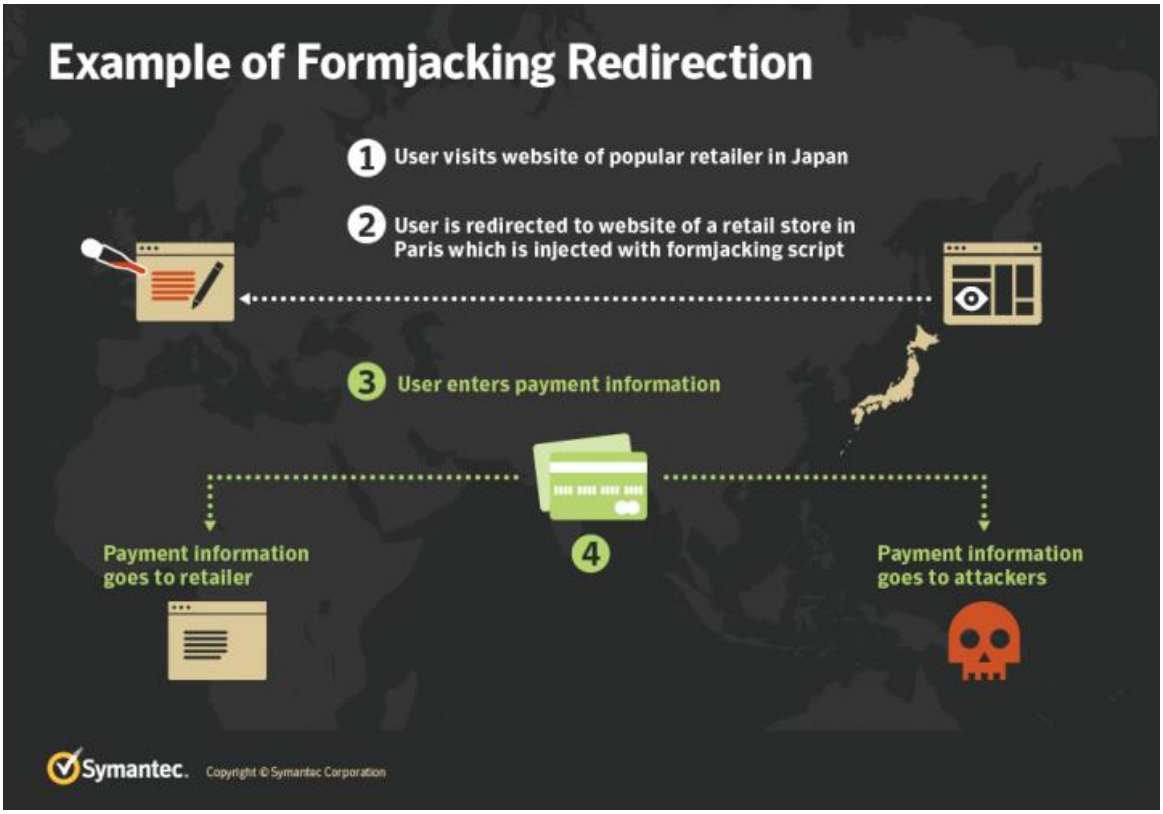
Επιπλέον, σύμφωνα με την FireHost ,η Cross-Site scripting (XSS) επίθεση συγκαταλέγεται ως μια από τις πιο κακόβουλες και επικίνδυνες επιθέσεις (FireHost, Web Application Attack Report For The Second Quarter of 2012, 2012). Οι επιτιθέμενοι εισχωρούν κακόβουλα script, όπως JavaScript, VBScript, ActiveX, HTML και Flash, μέσα σε μια ευάλωτη, δυναμική σελίδα για την εκτέλεση αυτών των script στον περιηγητή του θύματος. Έπειτα, η επίθεση θα οδηγήσει σε κακόβουλες ενέργειες (πχ. εκτέλεση κακόβουλου κώδικα στο σύστημα του θύματος και κλοπή των cookies που χρησιμοποιούνται για την αυθεντικοποίηση) που αφορούν στην πρόσβαση στον λογαριασμό του θύματος ή στην εξαπάτησή του ώστε να «κλικάρει» ένα κακόβουλο link. Παράλληλα, ερευνητές στην Γερμανία παρουσίασαν επιτυχώς μια XSS επίθεση απέναντι στη cloud πλατφόρμα AWS της Amazon (PCWorld, Researchers Demo Cloud Security Issue With Amazon AWS Attack, 2011*)*. Η ευπάθεια στο ηλεκτρονικό κατάστημα της Amazon επέτρεψε στους ερευνητές να καταλείψουν μια σύνοδο (session) του AWS, με αποτέλεσμα την πρόσβασή τους στα δεδομένα όλων των πελατών. Τα δεδομένα αυτά περιλάμβαναν δεδομένα αυθεντικοποίησης, ακόμα και κωδικούς ασφαλείας σε απλό κείμενο.

4.3.4.2 Formjacking Attack

Μια μορφή διαδικτυακής επίθεσης, η οποία βρίσκεται ολοένα και περισσότερο σε ανάπτυξη, λόγω και της αυξητικής τάσης της χρήσης των κρυπτονομισμάτων, είναι η επίθεση formjacking (MakeUseOf, What Is Formjacking and How Can You Avoid It?, 2019). Μια formjacking επίθεση είναι ο τρόπος ενός επιτιθέμενου να υποκλέψει τα τραπεζικά δεδομένα ενός χρήστη, απευθείας από μια ιστοσελίδα ηλεκτρονικού εμπορίου. Το γεγονός αυτό κάνει εύκολα αντιληπτό το ότι αποτελεί έναν μεγάλο κίνδυνο για τα συστήματα του fog computing, ειδικά από την σκοπιά της αποθήκευσης των προσωπικών, τραπεζικών δεδομένων των τελικών χρηστών.

Η formjacking επίθεση περιλαμβάνει την εισαγωγή κακόβουλου κώδικα σε μια ιστοσελίδα ενός παρόχου ηλεκτρονικού εμπορίου. Με τη σειρά του, ο κακόβουλος κώδικας υποκλέπτει τα δεδομένα πληρωμών, όπως για παράδειγμα τα στοιχεία της πιστωτικής κάρτας, ονόματα αλλά και άλλα είδη προσωπικών δεδομένων, τα οποία χρησιμοποιούνται κατά τη διάρκεια των ηλεκτρονικών αγορών. Τα κλεμμένα αυτά δεδομένα αποστέλλονται σε έναν εξυπηρετητή με σκοπό να επαναχρησιμοποιηθούν ή ακόμα και να πωληθούν, ενώ ο χρήστης – θύμα δεν γνωρίζει τίποτα για την υποκλοπή των δεδομένων του.

Για να γίνει αντιληπτό το πόσο έχει αναπτυχθεί μια τέτοιου είδους διαδικτυακή επίθεση, αρκεί να παρατηρήσουμε πως (σύμφωνα με το Internet Security Threat Report 2019 της Symantec) οι «formjackers» παραβίασαν 4.818 μοναδικές ιστοσελίδες μηνιαίως κατά το 2018. Κατά τη διάρκεια αυτής της χρονιάς, η Symantec μπλόκαρε πάνω από 3,7 εκατομμύρια προσπάθειες formjacking. Επιπλέον, πάνω από 1 εκατομμύριο από αυτές τις προσπάθειες έγιναν κατά τη διάρκεια των δύο τελευταίων μηνών του 2018, και συγκεκριμένα κατά τη διάρκεια του Σαββατοκύριακου της «Black Friday» τον Νοέμβριο και της Χριστουγεννιάτικης περιόδου του Δεκεμβρίου. Ένα χαρακτηριστικό παράδειγμα αυτής την επίθεσης έγινε κατά της ιστοσελίδας της British Airways στην Αγγλία (TechCrunch, British Airways customer data stolen in data breach, 2018). Ένας επίδοξος επιτιθέμενος χρησιμοποίησε μόλις 22 γραμμές κώδικα για να παραμετροποιήσει τα script που εκτελούνται στη ιστοσελίδα της αεροπορικής εταιρείας. Το αποτέλεσμα ήταν η επιτυχία του επιτιθέμενου να υποκλέψει 380.000 στοιχεία πιστωτικών καρτών, κερδίζοντας από αυτά περίπου 13 εκατομμύρια λίρες Αγγλίας.



Εικόνα 13 - Παράδειγμα Επίθεσης Formjacking (Source: Symantec – Formjacking: Targeting Popular Stores Near You)

Στις μέρες μας, είναι πρακτικά πολύ δύσκολο για τους ερευνητές ασφάλειας να προσδιορίσουν έναν μοναδικό επιτιθέμενο, όταν ο αριθμός των ιστοσελίδων που πέφτουν θύμα μιας τέτοιας μοναδικής επίθεσης είναι αρκετά μεγάλος. Όπως και με τα υπόλοιπα είδη κυβερνοεπιθέσεων, δεν υπάρχει μόνο ένας δράστης. Αντίθετα, η πλειοψηφία των επιθέσεων formjacking προέρχονται από τα επονομαζόμενα Magecart groups[14] (RiskIQ, Inside Magecart, 2019).

Ο ερευνητής Yonathan Klijnsma, ο οποίος ειδικεύεται στην περίπτωση αυτών των ομάδων, πρόσφατα κατηγοριοποίησε αυτές τις ομάδες σε 6 διαφορετικά γκρουπ, τα οποία χρησιμοποιούν το ίδιο ψευδώνυμο με σκοπό την αποφυγή του εντοπισμού τους. Αυτά τα διαφορετικά γκρουπ χαρακτηρίζονται από τους παρακάτω παράγοντες:

- **Group 1 & 2**: Επιτίθονται σε ένα μεγάλο εύρος στόχων, χρησιμοποιώντας αυτοματοποιημένα εργαλεία για την παραβίαση και την εκμετάλλευση.
- **Group 3**: Χαρακτηρίζονται από πολύ μεγάλο αριθμό στόχων, με τη χρήση μοναδικών εργαλείων κάθε φορά για την παραβίαση.
- **Group 4**: Μια από τις πιο εξελιγμένες ομάδες, η οποία αναμειγνύεται με τις ιστοσελίδες – θύματα χρησιμοποιώντας ένα πλήθος από εργαλεία «συσκότισης» (obfuscation tools).

[14] Ο όρος Magecart χρησιμοποιήθηκε για να περιγράψει τουλάχιστον εφτά διαφορετικές ομάδες που σχετίζονται με το κυβερνο – έγκλημα, και οι οποίες κατάφεραν να υποκλέψουν τα στοιχεία πληρωμών από πολύ μεγάλες ιστοσελίδες ηλεκτρονικών αγορών, όπως η British Airways και η Ticketmaster.

- **Group 5**: Στοχεύουν πάντα σε ενδιάμεσους παρόχους για την παραβίαση πολλαπλών στόχων. Χαρακτηριστικό παράδειγμα η επίθεση στην ιστοσελίδα Ticketmaster.
- **Group 6**: Χαρακτηρίζεται από επιλεκτική στοχοποίηση ιστοσελίδων και υπηρεσιών πολύ υψηλής αξίας, όπως για παράδειγμα της British Airways.

Όπως παρατηρούμε, οι ομάδες αυτές λειτουργούν στο «σκοτάδι», ενώ χρησιμοποιούν και διαφορετικές τεχνικές. Παράλληλα, οι ομάδες Magecart ανταγωνίζονται έτσι ώστε να δημιουργήσουν ένα αποτελεσματικό προϊόν υποκλοπής διαπιστευτηρίων. Οι στόχοι είναι διαφορετικοί, καθώς ορισμένες ομάδες στοχεύουν μόνο σε υψηλής αξίας θύματα. Το σίγουρο, όμως είναι, ότι όλες οι ομάδες προσπαθούν να πετύχουν το ίδιο αποτέλεσμα: την υποκλοπή στοιχείων με στόχο το προσωπικό κέρδος τους.

4.3.4.3 Wrapping Attack

Όταν ένας πελάτης αιτείται τις υπηρεσίες από έναν διαδικτυακό εξυπηρετητή (web server) μέσω ενός φυλλομετρητή, η υπηρεσία επικοινωνεί χρησιμοποιώντας μηνύματα πρωτοκόλλου πρόσβασης απλού αντικειμένου (Simple Object Access Protocol – SOAP), τα οποία μεταδίδονται διαμέσου ενός HTTP πρωτοκόλλου με τη μορφή XML (Extensive Markup Language). Για να επιτευχθεί η ακεραιότητα των δεδομένων και της ιδιωτικότητας των μεταδιδόμενων μηνυμάτων SOAP ανάμεσα σε πελάτη και εξυπηρετητή, εφαρμόζεται ένας μηχανισμός ασφαλείας που ονομάζεται WS – Security (Web Services Security). Ο μηχανισμός αυτός χρησιμοποιεί ψηφιακή υπογραφή για τα μηνύματα, καθώς και μια τεχνική κρυπτογράφησης για το περιεχόμενο των μηνυμάτων. Η πρακτική αυτή αυθεντικοποιεί τον πελάτη, ενώ παράλληλα ο εξυπηρετητής μπορεί να επιβεβαιώσει πως το μήνυμα δεν έχει παραποιηθεί κατά την μετάδοσή του.

Οι επιθέσεις wrapping («περιτυλίγματος)» χρησιμοποιούν ένα «περιτύλιγμα» υπογραφής XML για την εκμετάλλευση μιας αδυναμίας, όταν οι εξυπηρετητές επιβεβαιώνουν τις υπογεγραμμένες αιτήσεις (M. McIntosh and P. Austel, XML Signature Element Wrapping Attacks and Countermeasures, 2005). Η επίθεση πραγματοποιείται κατά τη διάρκεια της μετάφρασης των SOAP μηνυμάτων ανάμεσα σε έναν γνήσιο χρήστη και τον εξυπηρετητή. Με τη δημιουργία αντίγραφου του λογαριασμού του χρήστη και του κωδικού του κατά την περίοδο της σύνδεσης, ο επιτιθέμενος ενσωματώνει ένα ψεύτικο στοιχείο (το λεγόμενο «wrapper») μέσα στη δομή του μηνύματος, μεταφέρει το πραγματικό σώμα του μηνύματος κάτω από το «wrapper», αντικαθιστά το περιεχόμενο του μηνύματος με κακόβουλο κώδικα και τέλος στέλνει το μήνυμα στον εξυπηρετητή. Από τη στιγμή που το αρχικό «σώμα» του μηνύματος είναι γνήσιο, ο εξυπηρετητής θα εξαπατηθεί στο να εγκρίνει το μήνυμα, το οποίο στην πραγματικότητα έχει παραποιηθεί. Ως αποτέλεσμα, ο επιτιθέμενος αποκτά τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης σε προστατευόμενους πόρους, καθώς και να επεξεργάζεται τις επιθυμητές λειτουργίες.

Οι συγκεκριμένες επιθέσεις μπορούν να επιφέρουν πλήγμα ακόμα και στα συστήματα του fog και το cloud. Αυτό γίνεται λόγω του ότι οι τελικοί χρήστες αιτούνται τις υπηρεσίες των παροχών του fog και του cloud δια μέσου ενός φυλλομετρητή. Ένα παράδειγμα μιας τέτοιας ζημιάς, αποτελεί η παρατήρηση πως η υπηρεσία EC2 της Amazon ήταν ευάλωτη απέναντι σε τέτοιου είδους επιθέσεις (N. Gruschka and L. L. Iacono, Vulnerable Cloud: SOAP Message Security Validation Revisited, 2009). Η έρευνα έδειξε πως η υπηρεσία EC2 εμφάνισε μια αδυναμία στον μηχανισμό ασφάλειας των μηνυμάτων SOAP. Συγκεκριμένα, μια υπογεγραμμένη αίτηση SOAP, η οποία προήλθε από έναν γνήσιο χρήστη, μπορούσε να προσβληθεί και να παραποιηθεί. Ως αποτέλεσμα, οι επιτιθέμενοι μπορούσαν προβούν σε μη εξουσιοδοτημένες ενέργειες απέναντι στους λογαριασμούς των θυμάτων, μέσα στο ίδιο το cloud.

ΚΕΦΑΛΑΙΟ 5 - ΜΕΣΑ ΠΡΟΣΤΑΣΙΑΣ

Καθώς μελετήσαμε όλες τις πιθανές αδυναμίες ασφάλειας, αλλά και τις απειλές που διέπουν την ασφαλή λειτουργία του fog computing, καθίσταται απαραίτητο να καλύψουμε όλες τις πτυχές για την ορθή αντιμετώπιση αυτών των απειλών, με σκοπό την δημιουργία μιας αξιόπιστης, λειτουργικής και εμπιστευτικής πλατφόρμας του Fog computing.

Παρ' όλο που το fog computing παρέχει πολύ υψηλές δυνατότητες, καθώς και μεγάλο αριθμό εφαρμογών, αντιθέτως παρουσιάζεται μια έλλειψη στα μέσα προστασίας της ασφάλειας τα οποία είναι διαθέσιμα για τους προγραμματιστές και τους σχεδιαστές της fog πλατφόρμας. Ωστόσο, καθώς το cloud computing και οι υπόλοιπες παρόμοιες τεχνολογίες θυμίζουν τον μηχανισμό εργασίας του fog computing, μπορούν να παρέχουν μια βαθύτερη εικόνα των απειλών ασφαλείας τους, καθώς των αντίστοιχων μέσων προστασίας τους.

Σε αντίθεση με τα παραπάνω, και παρ' όλο που κάθε εφαρμογή του fog computing κατέχει διαφορετικές απαιτήσεις ασφάλειας, εφαρμογών και ευαισθησίας, οι επόμενες ενότητες παρέχουν ένα ευρύ φάσμα από αποδοτικές και εφαρμόσιμες πρακτικές λύσεις ασφάλειας. Παράλληλα, οι πρακτικές αυτές μπορούν να χρησιμοποιηθούν ως οι κατευθυντήριες πρακτικές για την ανάπτυξη των λογισμικών του fog computing, με τρόπο ώστε η ασφάλεια της πλατφόρμας να επιτυγχάνεται μέσα από αυτήν.

5.1 Αυθεντικοποίηση

Η αυθεντικοποίηση αποτελεί σημαντικό ζήτημα για την ασφάλεια του fog computing από την στιγμή που οι υπηρεσίες προσφέρονται σε τεράστιας κλίμακας τελικούς χρήστες από τους fog κόμβους. Ο Stojmenovic (Stojmenovic, I., Wen, S., The fog computing paradigm: Scenarios and security issues, 2014) θεωρεί την αυθεντικοποίηση σε διαφορετικά επίπεδα των fog κόμβων, ως το κυριότερο ζήτημα ασφάλειας στο fog computing. Η παραδοσιακή αυθεντικοποίηση που βασίζεται σε PKI δεν είναι αποδοτική και κατέχει φτωχή επεκτασιμότητα. Ο Balfanz (Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C., Talking to strangers: Authentication in ad-hoc wireless networks, 2002) έχει προτείνει μια φθηνή, ασφαλή και φιλική προς τον χρήστη λύση για το πρόβλημα αυθεντικοποίησης σε τοπικά, ειδικά ασύρματα δίκτυα, βασισμένη σε μια φυσική επαφή για αρχική αυθεντικοποίηση σε ένα κανάλι με περιορισμένη τοποθεσία.

Παρομοίως, το NFC[15] μπορεί επίσης να χρησιμοποιηθεί για την απλοποίηση της διαδικασίας της αυθεντικοποίησης στην περίπτωση του cloudlet. (Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H., Cloudlets authentication in nfc-based mobile computing, 2014). Καθώς γίνεται αντιληπτή η εμφάνιση της βιομετρικής αυθεντικοποίησης στο mobile computing και στο cloud computing, όπως η αυθεντικοποίηση μέσω δαχτυλικού αποτυπώματος, η αναγνώριση προσώπου,

[15] Η επικοινωνία κοντινού πεδίου (Near Field Communication, NFC) αποτελεί μια πρότυπη τεχνολογία συνδεσιμότητας, η οποία διαδίδεται και εξελίσσεται ραγδαία με κύριο σκοπό τη λύση αρκετών προβλημάτων, σύγχρονων αλλά και μελλοντικών. Είναι μια μικρής εμβέλειας ασύρματη τεχνολογία, η οποία λειτουργεί στη συχνότητα των 13,56 MHz και μεταφέρει δεδομένα με ρυθμό έως και 424 kbps και έχει γίνει γνωστή κυρίως μέσω της χρήσης της από τα κινητά τελευταίας γενιάς (smartphones). Η λειτουργία της βασίζεται στην επαφή ή στην προσέγγιση, σε απόσταση περίπου τεσσάρων με πέντε εκατοστών, της συσκευής που περιέχει το τσιπ NFC, σε κάποια άλλη συσκευή που περιλαμβάνει τον κατάλληλο αισθητήρα.

η αυθεντικοποίηση μέσω του αγγίγματος ή μέσω πληκτρολόγησης, θα μπορούσε να είναι ευεργετική η εφαρμογή της βιομετρικής αυθεντικοποίησης και στο fog computing.

5.2 Προστασία Ιδιωτικότητας

Η διαρροή προσωπικών πληροφοριών, όπως τα δεδομένα, η τοποθεσία κτλ., επιδέχονται μεγάλης προσοχής, όταν οι τελικοί χρήστες χρησιμοποιούν υπηρεσίες όπως το cloud computing, τα ασύρματα δίκτυα, το IoT κτλ. Τέτοιες προκλήσεις για την διατήρηση της ιδιωτικότητας εμφανίζονται και στο fog computing, καθώς οι κόμβοι βρίσκονται σε κοντινή απόσταση από τους τελικούς χρήστες και μπορούν να συλλέγουν περισσότερο ευαίσθητες πληροφορίες, σε σχέση με το απομακρυσμένο cloud που βρίσκεται στον πυρήνα του δικτύου. Οι προκλήσεις αυτές περιστρέφονται γύρω από ορισμένους βασικούς άξονες, όπως περιγράφονται παρακάτω.

Ιδιωτικότητα Δεδομένων. Στο δίκτυο fog, αλγόριθμοι διατήρησης της ιδιωτικότητας μπορούν να εκτελούνται ανάμεσα στο fog και το cloud, ενώ παράλληλα αυτοί οι αλγόριθμοι είναι συνήθως απαγορευτικοί ως προς τους πόρους στις τερματικές συσκευές. Επίσης, οι fog κόμβοι στα άκρα συνήθως συλλέγουν ευαίσθητα δεδομένα, που παράγονται από αισθητήρες και τερματικές συσκευές. Τεχνικές, όπως η ομομορφική κρυπτογραφία, μπορούν να εφαρμοσθούν για να επιτρέπουν την, ασφαλή ως προς την ιδιωτικότητα, συσσώρευση στις τοπικές εισόδους του δικτύου, χωρίς αποκρυπτογράφηση (Lu, R., et al.: Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications, 2012).

Ιδιωτικότητα Χρήσης. Ένα ακόμη ζήτημα ιδιωτικότητας αποτελεί το μοτίβο χρήσης, με το οποίο ένας fog πελάτης (fog client) αξιοποιεί τις fog υπηρεσίες. Για παράδειγμα, στο έξυπνο δίκτυο, η ανάγνωση του «έξυπνου» μετρητή μπορεί να αποκαλύψει πολλές πληροφορίες σχετικά με την οικία, όπως ποια είναι η ώρα που δεν υπάρχει άτομο στο σπίτι ή ποια ώρα λειτουργεί η τηλεόραση, τα οποία αναμφίβολα παραβιάζουν την ιδιωτικότητα του χρήστη. Παρ' όλο που έχουν προταθεί διάφοροι μηχανισμοί διατήρησης της ιδιωτικότητας στην «έξυπνη» καταμέτρηση [43,44], δεν μπορούν να εφαρμοσθούν απευθείας στο fog computing, λόγω της έλλειψης ενός έμπιστου εξωτερικού συνεργάτη (π.χ. ένας «έξυπνος» μετρητής στο «έξυπνο» δίκτυο) ή αντίστοιχη συσκευή, όπως μια μπαταρία στον fog κόμβο, ο οποίος μπορεί εύκολα να συλλέξει στατιστικά στοιχεία χρήσης από τους χρήστες. Μια πιθανή, αλλά απλοϊκή, λύση είναι ότι ο fog πελάτης δημιουργεί «εικονικές» εργασίες (dummy tasks) που τις αναθέτει σε πολλαπλούς κόμβους fog, αποκρύπτοντας τις πραγματικές εργασίες ανάμεσα στις εικονικές. Ωστόσο, η λύση αυτή θα αυξήσει το κόστος του fog πελάτη καθώς και την σπατάλη πόρων και ενέργειας. Αντίθετα, μια διαφορετική λύση θα ήταν ο σχεδιασμός ενός έξυπνου τρόπου διχοτόμησης της εφαρμογής, έτσι ώστε να διασφαλιστεί πως οι ανατιθέμενες χρήσεις πόρων δεν αποκαλύπτουν προσωπικές πληροφορίες.

Ιδιωτικότητα Τοποθεσίας. Στο fog computing, η ιδιωτικότητα της τοποθεσίας αναφέρεται κυρίως στην ιδιωτικότητα της τοποθεσίας των fog πελατών. Καθώς ένας fog πελάτης συνήθως αναθέτει τις εργασίες του στον κοντινότερο κόμβο fog, αυτός με την σειρά του, μπορεί να συμπεράνει πως ο πελάτης βρίσκεται κοντά του και μακριά από άλλους κόμβους. Επιπρόσθετα, εάν ένας πελάτης αξιοποιεί πολλαπλές υπηρεσίες του fog σε πολλές τοποθεσίες, μπορεί να αποκαλύψει την πορεία του προς του κόμβους, δεδομένου ότι οι κόμβοι συνεργάζονται μεταξύ τους. Όσο ένας τέτοιος πελάτης είναι δεσμευμένος με ένα άτομο ή ένα σημαντικό αντικείμενο, η ιδιωτικότητα της τοποθεσίας του ατόμου ή του αντικειμένου βρίσκονται σε κίνδυνο.

Εάν ένας fog πελάτης επιλέγει πάντα αυστηρά τον κοντινότερο σε αυτόν fog εξυπηρετητή, ο κόμβος μπορεί αναμφίβολα να γνωρίζει ότι ο πελάτης, που αξιοποιεί τους υπολογιστικούς πόρους, βρίσκεται κοντά. Ο μόνος τρόπος για την διαφύλαξη της ιδιωτικότητας της τοποθεσίας είναι μέσω της απόκρυψης της ταυτότητας, τέτοιας ώστε παρ' όλο που ο κόμβος γνωρίζει πως ένας fog

πελάτης βρίσκεται κοντά, δεν μπορεί να αναγνωρίσει τον πελάτη αυτόν. Στην πραγματικότητα, ένας fog πελάτης δεν επιλέγει απαραίτητα τον κοντινότερο κόμβο, αλλά επιλέγει κατά βούληση έναν κόμβο, τον οποίο μπορεί να φτάσει με βάση κάποια κριτήρια, όπως η καθυστέρηση, η φήμη, η ισορροπία φορτίου κτλ. Ωστόσο, μόλις ο fog πελάτης αξιοποιήσει υπολογιστικούς πόρους από πολλαπλούς κόμβους σε μια περιοχή, η τοποθεσία του μπορεί να συστηθεί σε ένα μικρό μέρος, από την στιγμή που αυτή πρέπει να βρίσκεται μέσα στην διασταύρωση των επιφανειών κάλυψης των πολλαπλών κόμβων.

5.3 Ασφαλής Αποθήκευση Δεδομένων

Στο fog computing, τα δεδομένα των χρηστών αναθέτονται σε εξωτερικούς συνεργάτες, ενώ ο έλεγχος των χρηστών πάνω στα δεδομένα παραδίδεται στους fog κόμβους, κάτι το οποίο αποφέρει παρόμοιους κινδύνους ασφαλείας, όπως συμβαίνει και στο cloud computing. Αρχικά, είναι δύσκολο να διασφαλιστεί η ακεραιότητα των δεδομένων, από την στιγμή που τα δεδομένα που αναθέτονται μπορούν να χαθούν ή να τροποποιηθούν εσφαλμένα. Δεύτερον, τα δεδομένα που «ανεβαίνουν» (uploaded) μπορούν να κακομεταχειριστούν από μη εξουσιοδοτημένες ομάδες για άλλους σκοπούς.

Για να αντιμετωπιστούν αυτές οι απειλές, έχει προταθεί ως λύση μια υπηρεσία αποθήκευσης ελεγχόμενων δεδομένων, στο ευρύτερο πλαίσιο του cloud computing, για την προστασία των δεδομένων. Τεχνικές, όπως η κρυπτογραφία ομομορφισμού ανιχνεύσιμη κρυπτογραφία συνδυάζονται για να παρέχουν ακεραιότητα, εμπιστευτικότητα και επαληθευσιμότητα για συστήματα αποθήκευσης cloud, έτσι ώστε μα επιτρέπουν στον πελάτη να ελέγχει τα δεδομένα του, που βρίσκονται αποθηκευμένα σε μη έμπιστους εξυπηρετητές. Επίσης, έχει προταθεί (Wang, C., Wang, Q., Ren, K., Lou, W, Privacy-preserving public auditing for data storage security in cloud computing, 2010) ένας δημόσιος έλεγχος δεδομένων, που διατηρεί την ιδιωτικότητα, για τα δεδομένα που βρίσκονται αποθηκευμένα στο cloud, ο οποίος βασίζεται σε έναν εξωτερικό ελεγκτή (TPA – third-party auditor), χρησιμοποιώντας ομομορφική πιστοποίηση γνησιότητας καθώς και μια τυχαία τεχνική «καμουφλάζ» για την προστασία της ιδιωτικότητας έναντι του TPA. Για να διασφαλιστεί η αξιοπιστία της αποθήκευσης δεδομένων, τα προγενέστερα συστήματα αποθήκευσης χρησιμοποιούν κώδικες διαγραφής κωδικοποίηση δικτύου για να μεταχειριστούν την ανίχνευση αλλοιωμένων δεδομένων και την αποκατάσταση τους, ενώ επίσης έχει προταθεί (Cao, N., Yu, S., Yang, Z., Lou, W., Hou, Y.T.: Lt codes-based secure and reliable cloud storage service, 2012) ένα σύστημα που χρησιμοποιεί κώδικα LT, το οποία παρέχει μικρότερο κόστος αποθήκευσης, αρκετά γρηγορότερη ανάκτηση δεδομένων και ισάξιο κόστος επικοινωνίας.

Στο fog computing, υπάρχουν νέες προκλήσεις στο σχεδιασμό ασφαλών συστημάτων αποθήκευσης, έτσι ώστε να επιτευχθεί χαμηλή καθυστέρηση, υποστήριξη δυναμικής λειτουργίας καθώς και να μεταχειριστεί σωστά η αλληλεπίδραση μεταξύ του cloud και του fog.

5.4 Ασφαλής και Ιδιωτικός Υπολογισμός Δεδομένων

Ένα επιπλέον σημαντικό ζήτημα στο fog computing είναι η επίτευξη και η διατήρηση των στοιχείων της ασφάλειας και της ιδιωτικότητας, σε ότι αφορά τους υπολογισμούς των δεδομένων που ανατίθενται στους fog κόμβους. Το ζήτημα αυτό μπορεί να περιγραφεί με βάση τους παρακάτω δύο κύριους άξονες:

Επαληθεύσιμη Υπολογιστική. Η επαληθεύσιμη υπολογιστική επιτρέπει μια υπολογιστική συσκευή να «ξεφορτώνεται» τον υπολογισμό μιας λειτουργίας σε άλλους, πιθανώς, μη έμπιστους εξυπηρετητές, ενώ παράλληλα διατηρεί επαληθεύσιμα αποτελέσματα. Οι άλλοι εξυπηρετητές αξιολογούν την λειτουργία και επιστρέφουν το αποτέλεσμα με την απόδειξη ότι ο υπολογισμός της λειτουργίας εκτελέστηκε σωστά. Στο fog computing, για να επιτευχθεί η εμπιστοσύνη στους υπολογισμούς που μεταφορτώνονται στους fog κόμβους, ο αντίστοιχος χρήστης θα πρέπει να είναι σε θέση να επαληθεύει την εγκυρότητα των υπολογισμών.

Στη συνέχεια, θα αναφερθούν κάποιες ήδη υπάρχουσες μέθοδοι για την επίτευξη επαληθεύσιμης υπολογιστικής. Αρχικά, έχει προταθεί (Gennaro, R., Gentry, C., Parno, B., Non-interactive variable computing: Out-sourcing computation to untrusted workers, 2010) ένα πρωτόκολλο επαληθεύσιμης υπολογιστικής που επιτρέπει στον εξυπηρετητή να επιστρέφει υπολογιστικής φύσης, μη διαδραστική απόδειξη, η οποία μπορεί να επαληθευθεί από τον πελάτη. Το πρωτόκολλο μπορεί να προσφέρει (χωρίς επιπλέον κόστος) εισερχόμενη και εξερχόμενη ιδιωτικότητα προς τον πελάτη, τέτοια που ο εξυπηρετητής δεν μαθαίνει καμία πληροφορία για τις εισαγωγές και τα αποτελέσματα. Παράλληλα, έχει κατασκευαστεί ένα σύστημα, ονόματι *Pinocchio*, μέσω του οποίου ο πελάτης μπορεί να επαληθεύει γενικούς υπολογισμούς που γίνονται από έναν εξυπηρετητή ενώ βασίζεται μόνο σε κρυπτογραφικές εικασίες (Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: Nearly practical verifiable computation, 2013). Με το Pinocchio, ο πελάτης δημιουργεί ένα δημόσιο κλειδί αξιολόγησης για την περιγραφή των υπολογισμών, ενώ στη συνέχεια ο εξυπηρετητής αξιολογεί τους υπολογισμούς και χρησιμοποιεί το κλειδί για να παράγει την απόδειξη της εγκυρότητας.

Αναζήτηση Δεδομένων. Για να προστατευθεί η ιδιωτικότητα των δεδομένων, τα ευαίσθητα δεδομένα των τελικών χρηστών πρέπει να κρυπτογραφούνται πριν την ανάθεση τους στον fog κόμβο, δυσκολεύοντας έτσι τις υπηρεσίες στην αποτελεσματική αξιοποίηση των δεδομένων. Μια από τις σημαντικότερες υπηρεσίες είναι η αναζήτηση «λέξης – κλειδί» (keyword search), όπως για παράδειγμα η αναζήτηση λέξης – κλειδί ανάμεσα σε κρυπτογραφημένα αρχεία δεδομένων. Για τον σκοπό αυτό, ερευνητές έχουν αναπτύξει διάφορα κρυπτογραφικά συστήματα αναζήτησης που επιτρέπουν στον χρήστη την ασφαλή αναζήτηση κρυπτογραφημένων δεδομένων μέσω λέξεων – κλειδιών, χωρίς να απαιτείται αποκρυπτογράφηση.

5.5 Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση των δεδομένων αποτελεί έναν ευρέως χρησιμοποιούμενο μηχανισμό για την προστασία της εμπιστευτικότητας των δεδομένων. Για να ξεπερασθεί το ζήτημα της υψηλής κατανομής πόρων για την κρυπτογράφηση, θα μπορούσαν να κρυπτογραφούνται μόνο τα καίριες και ευαίσθητες πληροφορίες, όπως είναι η ταυτότητα των χρηστών στα δίκτυα οχημάτων, τα δεδομένων των ασθενών στα υγειονομικά συστήματα κτλ. Για τα «αδρανή δεδομένα» (data at rest) μπορεί να χρησιμοποιηθεί ο αλγόριθμος AES με μέγεθος κλειδιού 256 bit, ενώ παράλληλα το πρωτόκολλα SSL (Secure Socket Layer) μπορεί να χρησιμοποιηθεί για την εγκαθίδρυση ασφαλών επικοινωνιών ανάμεσα σε εξυπηρετητές και πελάτες.

Επιπρόσθετα, θα πρέπει να πραγματοποιούνται έλεγχοι ακεραιότητας των αποδοτικών δεδομένων πριν και μετά την επικοινωνία, έτσι ώστε να επιβεβαιώνονται οι παραληφθείσες πληροφορίες, καθώς και οι αποστολείς τους. Το σημαντικό θέμα στην περίπτωση αυτή είναι να γίνει ξεκάθαρος ο διαχωρισμός των αρχειακών δεδομένων και των ευαίσθητων πληροφοριών. Η κρυπτογράφηση των αρχειακών δεδομένων, όπως είναι η δημόσια αναμετάδοση βίντεο (public video streaming) θα μειώσει την απόδοση του fog συστήματος, καθώς επίσης και θα επιφέρει αντίκτυπο στην απόδοση των συγγενών εφαρμογών. Για τον λόγο αυτό, καθίσταται απαραίτητο για τους σχεδιαστές ενός συστήματος fog να αξιολογούν επαρκώς την σημασία των δεδομένων καθώς και να ενσωματώνουν ασφαλιστικές δικλείδες όπου αυτό κρίνεται απαραίτητο.

5.6 Προστασία απέναντι σε επιθέσεις μνήμης (Cache attacks)

Τα συστήματα fog που χρησιμοποιούνται για την ενίσχυση της απόδοσης και της ενεργειακής κατανάλωσης άλλων εφαρμογών, χρησιμοποιώντας προηγμένες τεχνικές απόκρυψης μνήμης (advanced memory caching), μπορούν να διαταραχθούν μέσω των επιθέσεων πλευρικών καναλιών μνήμης (cache side channel attack), με αποτέλεσμα την έκθεση ευαίσθητων δεδομένων μέσω συνδεδεμένων συστημάτων. Η μνήμη αποθηκεύει δεδομένα τα οποία χρησιμοποιούνται συχνά και τα οποία μπορεί να περιέχουν προσωπικές πληροφορίες των χρηστών.

Οι πλατφόρμες fog που χρησιμοποιούνται για τους σκοπούς αυτούς θα μπορούν να περιλαμβάνουν κάποιες πρακτικές λύσεις, όπως την Newcache και την STEALTHMEM. Αυτές οι λύσεις αποτελούν εναλλακτικές, χαμηλού επιπέδου προσθήκες ενός συστήματος μνήμης κεντρικής ασφάλειας, το οποίο θα μπορεί να προστατεύει καλύτερα τα υπάρχοντα δεδομένα. Για τους νέους σχεδιασμούς μνήμης, λύσεις όπως η διαίρεση κλειδωμένης μνήμης (Partition Locked Cache) και η τυχαία μετάθεση μνήμης (Random Permutation Cache) μπορούν να ελαττώσουν τον κίνδυνο από επιθέσεις παρεμβολής μνήμης.

Επιπλέον, ο μηχανισμός για την αποφυγή παραμετροποιήσεων των έξυπνων, μετρήσιμων δεδομένων σε μια εξελιγμένη δομή μετρήσεων, θα μπορούσε να είναι η φύλαξη των δεδομένων που συλλέχθηκαν σε έναν fog κόμβο, για μια συγκεκριμένη διάρκεια πριν την απελευθέρωσή τους. Παρ’ όλο που αυτές οι πρακτικές λύσεις καθίστανται ακριβές και δύσκολες στον να εφαρμοσθούν, οι προγραμματιστές μιας πλατφόρμας του fog computing θα πρέπει να τις θεωρούν ως σημαντικές, καθώς είναι αναγκαίο να μην βασίζονται μόνο σε βασικές εφαρμογές που μπορεί να οδηγήσουν σε σημαντικές αδυναμίες ασφάλειας.

ΚΕΦΑΛΑΙΟ 6 - ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ: ΠΕΡΙΟΡΙΣΜΟΣ ΕΠΙΘΕΣΕΩΝ ΚΛΟΠΗΣ ΕΣΩΤΕΡΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Οι επιχειρήσεις, και ειδικά οι λεγόμενες «startups», επιλέγουν όλο και περισσότερο να εξωτερικεύουν τα δεδομένα και την επεξεργασία τους στο cloud. Το γεγονός αυτό από την μια υποστηρίζει καλύτερη υπολογιστική απόδοση, αλλά ταυτόχρονα ενδέχεται να εγκυμονεί περισσότερους κινδύνους, ένας από τους οποίους (και ίσως ο πιο σημαντικός) αποτελούν οι επιθέσεις υποκλοπής δεδομένων. Καθώς οι περισσότεροι χρήστες του cloud γνωρίζουν ήδη για αυτή την απειλή, δεν μπορούν να κάνουν τίποτα περισσότερο παρά να εμπιστευτούν την αυθεντικοποίηση του παρόχου των cloud υπηρεσιών, όσον αφορά στο θέμα της προστασίας των δεδομένων. Αντίθετα, η έλλειψη διαφάνειας στην αυθεντικοποίηση και στον κεντρικό έλεγχο του παρόχου επιδεινώνει όλο και περισσότερο την απειλή αυτή.

Ένα πολύ γνωστό παράδειγμα υποκλοπής δεδομένων αποτελεί το περιστατικό στο μέσο κοινωνικής δικτύωσης Twitter. Σύμφωνα με το περιστατικό, ένας μεγάλος αριθμός από εταιρικά αλλά και προσωπικά αρχεία του Twitter «φιλτραρίστηκαν» και στάλθηκαν στην τεχνολογική ιστοσελίδα «TechCrunch» (M. Arrington, In our inbox: Hundreds of confidential twitter documents, 2009), ενώ παράλληλα δόθηκε παράνομη πρόσβαση σε κάποιους λογαριασμούς χρηστών, μεταξύ των οποίων και του πρώην Προέδρου των Ηνωμένων Πολιτειών Barack Obama (P. Allen, Obama's Twitter password revealed after French hacker arrested for breaking into U.S. president's account, 2010). Συγκεκριμένα, ο επιτιθέμενος χρησιμοποίησε τον προσωπικό κωδικό ασφαλείας ενός διοικητικού υπαλλήλου, αποκτώντας πρόσβαση σε εταιρικά έγγραφα, τα οποία ήταν αποθηκευμένα στον δομή Google Docs της Google. Λόγω του περιστατικού, η ζημιά που προκλήθηκε τόσο στην ίδια την εταιρεία αλλά και στους χρήστες της ήταν τεράστια.

Λόγω της σημασίας και της επικινδυνότητας που διέπουν την συγκεκριμένη επίθεση, στο κεφάλαιο αυτό θα αναλύσουμε την πρόταση μιας ομάδας ερευνητών, για την ασφάλεια του cloud μέσω του fog computing, και συγκεκριμένα μέσω της χρήσης μιας τεχνολογίας πληροφοριών «αντιπερισπασμού» (decoy information technology). Οι ερευνητές χρησιμοποιούν αυτή την τεχνολογία για να εξαπολύσουν επιθέσεις «παραπληροφόρησης» (disinformation attacks) απέναντι σε κακόβουλους εσωτερικούς πληροφοριοδότες (malicious insiders), παρέχοντας έτσι την δυνατότητα της διάκρισης ανάμεσα στα πραγματικά, ευαίσθητα δεδομένα των πελατών και στα άχρηστα και ψεύτικα δεδομένα. Τέλος, στο κεφάλαιο αυτό θα αναφερθούμε σε δύο διαφορετικές χρήσεις του fog computing για την αποτροπή τέτοιου είδους επιθέσεων. Ο πρώτος τρόπος αφορά αξιοποίηση πληροφοριών «αντιπερισπασμού» μέσα στο cloud από τον χρήστη των υπηρεσιών του, ενώ ο δεύτερος τρόπος αφορά την αξιοποίηση των πληροφοριών σε προσωπικά προφίλ κοινωνικής δικτύωσης από τους ίδιους τους τελικούς χρήστες.

6.1 Βασική ιδέα

Κατά την σημερινή εποχή, πραγματοποιούνται ολοένα και περισσότερο δημιουργικές και αποδοτικές ψηφιακές επιθέσεις, οι οποίες μάλιστα δεν προβλέπονται από τους υπεύθυνους υλοποίησης των συστημάτων. Έτσι, δεν είναι αρκετή η κατασκευή ενός έμπιστου περιβάλλοντος των cloud και fog computing, καθώς αυτές οι επιθέσεις μπορούν να πραγματοποιηθούν ανά πάσα στιγμή, ενώ παράλληλα η ζημιά από τις πληροφορίες που χάνονται μπορεί να κριθεί ως ανεπανόρθωτη. Για τον λόγο αυτό, τα συστήματα θα πρέπει να είναι κατάλληλα προετοιμασμένα για τέτοια περιστατικά.

Η βασική ιδέα της μεθόδου που θα εξετάσουμε είναι η ελαχιστοποίηση της ζημιάς που προκαλείται από τα κλεμμένα δεδομένα, η οποία θα προέλθει από την μείωση της αξίας αυτών πληροφοριών προς τους επιτιθέμενους. Αυτό μπορεί να επιτευχθεί μέσω μιας «προληπτικής» επίθεσης παραπληροφόρησης (disinformation attack). Μπορούμε, λοιπόν, να θέσουμε πως οι ασφαλείας υπηρεσίες του cloud, και κατ' επέκταση του fog, μπορούν να εφαρμοσθούν δίνοντάς τους δύο επιπλέον χαρακτηριστικά ασφαλείας:

Σκιαγράφηση συμπεριφοράς χρήστη (User Behavior Profiling): Η σκιαγράφηση του προφίλ συμπεριφοράς αποτελεί μια αρκετά γνωστή τεχνική και η οποία μπορεί να εφαρμοσθεί στην περίπτωσή μας για να προβάρει το πώς, το πότε και πόσο συχνά ένας χρήστης έχει πρόσβαση στα δεδομένα του στο cloud. Έτσι, μια τέτοιου είδους «φυσιολογική» πρόσβαση μπορεί να ελέγχεται συνεχώς για να καθορίζεται το πότε επικρατεί μια ασυνήθιστη πρόσβαση στις προσωπικές πληροφορίες του χρήστη. Αυτή η μέθοδος ασφάλειας χρησιμοποιείται συχνά σε εφαρμογές εντοπισμού παραβάσεων. Επίσης, τα προφίλ που δημιουργούνται περιλαμβάνουν ογκομετρικές πληροφορίες, που σχετίζονται με το κάθε πότε και πόσα από τα δεδομένα αυτά «διαβάζονται» από τον χρήστη. Έτσι, αυτή η απλή λειτουργία μπορεί να βοηθήσει στον εντοπισμό μιας ασυνήθιστης πρόσβασης στο cloud, βασιζόμενη κυρίως στα δεδομένα τα οποία μεταφέρονται (M. Ben-Salem and S. J. Stolfo, Modeling user search-behavior for masquerade detection, 2011).

Αντιπερισπασμοί (Decoys): Οι πληροφορίες αντιπερισπασμού, όπως για παράδειγμα τα αρχεία αντιπερισπασμού, μπορούν να δημιουργηθούν «κατά παραγγελία» (on demand) και να εξυπηρετούν ως μέσο ανίχνευσης μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες, καθώς και να «δηλητηριάσουν» τα φιλτραρισμένες πληροφορίες των επιτιθέμενων. Επίσης, οι αντιπερισπασμοί θα μπερδέψουν τους επιτιθέμενους, κάνοντας τους να νομίζουν πως έχουν φιλτράρει χρήσιμες πληροφορίες, ενώ στην πραγματικότητα οι πληροφορίες αυτές θα είναι ψεύτικες.

Η τεχνολογία αυτή μπορεί να συνδυαστεί με την σκιαγράφηση της συμπεριφοράς, έτσι ώστε να ασφαλίσουν ακόμα περισσότερο τα δεδομένα των χρηστών στο fog και το cloud. Για παράδειγμα, κάθε φορά που θα παρατηρείται ασυνήθιστη πρόσβαση σε μια υπηρεσία, το cloud θα επιστρέφει αυτά τα δεδομένα αντιπερισπασμού και θα τα μεταδίδει με τέτοιο τρόπο, ούτως ώστε να εμφανίζονται ολοκληρωτικά ως φυσιολογικά και έγκυρα. Ο πραγματικός χρήστης, ο οποίος είναι ο ιδιοκτήτης αυτών των δεδομένων, θα μπορεί να αναγνωρίσει το πότε το cloud επιστρέφει αυτές τις πληροφορίες αντιπερισπασμού, ενώ έτσι θα μπορεί να τροποποιεί τις απαντήσεις του cloud με διάφορα μέσα, όπως για παράδειγμα με ερωτήσεις – προκλήσεις, για να ειδοποιεί το σύστημα ασφάλειας του cloud ότι έχει ανιχνεύσει ανακριβώς μια μη εξουσιοδοτημένη πρόσβαση.

Στην περίπτωση που μια πρόσβαση αναγνωριστεί σωστά ως μη εξουσιοδοτημένη, το σύστημα ασφαλείας θα μεταφέρει απεριόριστες ποσότητες από ψεύτικες πληροφορίες στον επιτιθέμενο. Με τον τρόπο αυτό το σύστημα ασφαλίζει τα πραγματικά δεδομένα του χρήστη από μια μη εξουσιοδοτημένη δημοσιοποίηση τους. Έτσι, οι αντιπερισπασμοί υποστηρίζουν δύο σκοπούς: την επιβεβαίωση για το πότε η πρόσβαση σε δεδομένα είναι εξουσιοδοτημένη, όταν ανιχνεύεται μια ασυνήθιστη πρόσβαση στα δεδομένα, ενώ παράλληλα μπερδεύει και τον επιτιθέμενο με ψεύτικες πληροφορίες.

Σύμφωνα με τα παραπάνω, οι ερευνητές διαπίστωσαν πως ο συνδυασμός των δύο παραπάνω χαρακτηριστικών θα παρέχουν πρωτοφανή επίπεδα ασφάλειας στο fog και κατ' επέκταση στο cloud computing. Η ιδέα αυτή εφαρμόστηκε για την ανίχνευση μη εξουσιοδοτημένης πρόσβασης από επιτιθέμενους, σε δεδομένα τα οποία ήταν αποθηκευμένα σε ένα τοπικό σύστημα αρχείων. Οι επιτιθέμενοι αυτοί παρίσταναν τους έγκυρους χρήστες μετά από την υποκλοπή των προσωπικών τους διαπιστευτηρίων. Τα αποτελέσματα αυτού του πειράματος έδειξαν πως ο συνδυασμός και των δυο τεχνικών μπορούν να επιφέρουν καλύτερα αποτελέσματα εντοπισμού, ενώ παράλληλα δείχνουν ότι αυτή η προσέγγιση μπορεί να δουλέψει σε ένα περιβάλλον του fog και του cloud computing, καθώς αυτά είναι προγραμματισμένα να είναι το ίδιο διαφανή προς τον τελικό χρήστη, όσο ένα τοπικό σύστημα αποθήκευσης αρχείων. Έτσι, στα επόμενα κεφάλαια θα αναφερθούμε σε κάποια από τα αποτελέσματα του πειράματος χρήσης των δύο τεχνικών για τον εντοπισμό αυτού του είδους επίθεσης.

6.2 Εφαρμογή των δύο τεχνολογιών

6.2.1 Σκιαγράφηση προφίλ συμπεριφοράς

Οι έγκυροι χρήστες ενός πληροφοριακού συστήματος είναι εξοικειωμένοι με το πού βρίσκονται τα αρχεία που είναι αποθηκευμένα στο σύστημα αυτό. Έτσι, η οποιαδήποτε αναζήτηση για συγκεκριμένα αρχεία είναι πολύ πιθανό να είναι στοχευμένη και ελαχιστοποιημένη. Αντίθετα, ένας «μεταμφιεσμένος» επιτιθέμενος, ο οποίο αποκτά παράνομη πρόσβαση στο σύστημα του θύματος, είναι απίθανο να είναι εξοικειωμένος με τη δομή και το περιεχόμενου αυτού του συστήματος. Έτσι, η αναζήτησή τους είναι πιθανό να χαρακτηρίζεται ως εκτενής και μη στοχευμένη.

Βασιζόμενοι σε αυτή την υπόθεση – κλειδί, οι ερευνητές σκιαγράφησαν το προφίλ της συμπεριφοράς των χρηστών, μέσω της ανάπτυξης ορισμένων μοντέλων χρηστών, τα οποία ήταν «εκπαιδευμένα» με τεχνική μοντελοποίησης μοναδικής ταξινόμησης (one-class modelling), τις επονομαζόμενες υποστηρικτικές διανυσματικές μηχανές μονής ταξινόμησης (one – class support vector machines). Η σημασία αυτής της μοντελοποίησης προέρχεται από την ικανότητα της κατασκευής ενός ταξινομητή χωρίς την απαίτηση για διαμοίραση δεδομένων από διαφορετικούς χρήστες. Με τον τρόπο αυτό διατηρείται η ιδιωτικότητα του χρήστη και των αντίστοιχων δεδομένων του.

Παράλληλα, οι ερευνητές παρακολουθούσαν για την εμφάνιση ασυνήθιστων συμπεριφορών αναζήτησης, οι οποίες παρουσίαζαν ορισμένες διαφοροποιήσεις σε σχέση με τις βασικές αναζητήσεις των χρηστών. Σύμφωνα με την υπόθεσή τους, αυτές οι διαφοροποιήσεις αποτελούν μια ένδειξη μιας πιθανής επίθεσης «μεταμφιεσμένων». Τα προηγούμενα πειράματά τους επιβεβαίωσαν την υπόθεσή τους, ενώ επίδειξαν πως θα μπορούσαν να ανιχνεύσουν αξιόπιστα όλες τις προσομοιωμένες επιθέσεις, χρησιμοποιώντας την συγκεκριμένη προσέγγιση, πετυχαίνοντας παράλληλα πολύ μικρό ποσοστό του δείκτη ψευδοθετικών (false positive) αποτελεσμάτων, της τάξεως του 1,12% (M. Ben-Salem and S. J. Stolfo, 2011).

6.2.2 Τεχνολογία αντιπερισπασμού

Όσον αφορά την τεχνολογία αντιπερισπασμού, οι ερευνητές τοποθέτησαν «παγίδες» στο εσωτερικό του συστήματος αποθήκευσης των αρχείων. Οι «παγίδες αυτές» είναι αρχεία αντιπερισπασμού τα οποία ελήφθησαν από μια υπολογιστική σελίδα του fog computing, μέσω της οποίας παρέχεται μια αυτοματοποιημένη υπηρεσία που προσφέρει διάφορους τύπους αρχείων αντιπερισπασμού, όπως καταστάσεις φορολογικής ενημερότητας, ιατρικά αρχεία, κινήσεις πιστωτικών καρτών κ.ά. (B. M. Bowen and S. Hershkop, Decoy Document Distributor, 2009). Τα αρχεία αυτά λαμβάνονται από τον γνήσιο χρήστη και τοποθετούνται σε πολύ ευδιάκριτες τοποθεσίες και οι οποίες δεν είναι πιθανό να προκαλέσουν την οποιαδήποτε παρεμβολή στις δραστηριότητες του γνήσιου χρήστη μέσα στο σύστημα.

Αντίθετα, ο επιτιθέμενος, ο οποίος δεν είναι οικείος με τον σύστημα αρχειοθέτησης και το περιεχόμενό του, είναι πιθανό να αποκτήσει πρόσβαση στα αρχεία αντιπερισπασμού, ειδικά αν βρίσκεται σε διαδικασία αναζήτησης ευαίσθητων δεδομένων, όπως είναι τα δεδομένα – «παγίδες» που τοποθετήθηκαν μέσα στα αρχεία αντιπερισπασμού. Κατά συνέπεια, η παρακολούθηση της πρόσβασης σε αυτά τα αρχεία θα πρέπει να σημάνει συναγερμό για ασυνήθιστες δραστηριότητες στο σύστημα. Παράλληλα, τα αρχεία αντιπερισπασμού φέρουν και έναν κατακερματισμένο κώδικα αυθεντικοποίησης μηνύματος[16] (HMAC – Hash Message Authentication Code), ο οποίος είναι κρυμμένος στο τμήμα της κεφαλίδας του εγγράφου. Ο HMAC τοποθετείται «πάνω» από το περιεχόμενο του αρχείου, χρησιμοποιώντας ένα μοναδικό κλειδί. Όταν ένα αρχείο αντιπερισπασμού φορτώνεται στην μνήμη, οι ερευνητές μπορούν να επιβεβαιώσουν εάν το αρχείο αυτό είναι αντιπερισπασμού, εκτελώντας ένα HMAC βασιζόμενο σε όλο το περιεχόμενο του εγγράφου. Τέλος, συγκρίνουν αυτόν τον HMAC με αυτόν που βρίσκεται στο εσωτερικό του αρχείου. Εάν οι δύο κώδικες ταιριάζουν, τότε συμπεραίνουν ότι το αρχείο αυτό αποτελεί ένα αρχείο αντιπερισπασμού και έτσι «ενεργοποιείται» ένας συναγερμός.

Κατ' επέκταση, τα πλεονεκτήματα της τοποθέτησης αντιπερισπασμών σε ένα σύστημα αρχειοθέτησης είναι τρία: 1) η ανίχνευση δραστηριότητας «μασκαρεμένου» επιτιθέμενου, 2) η σύγχυση του επιτιθέμενου και το αντίστοιχο κόστος που προκύπτει για τον διαχωρισμό των πραγματικών και των ψεύτικων πληροφοριών, και 3) το αποτέλεσμα της αποτροπής, το οποίο παρ' όλο που είναι δύσκολο να μετρηθεί, παίζει έναν πολύ σημαντικό ρόλο στην αποτροπή τέτοιου είδους απειλών, ειδικά από επιτιθέμενους που αποφεύγουν τον κίνδυνο.

6.2.3 Συνδυασμός των δύο τεχνικών

Η σύνδεση ανάμεσα στην ανίχνευση ασυνήθιστης συμπεριφοράς αναζήτησης με τα αρχεία αντιπερισπασμού ως παγίδες, θα πρέπει να παρέχουν πιο απτές αποδείξεις παράνομης δραστηριότητας, με αποτέλεσμα την βελτίωση της συνολικής ακρίβειας του ανιχνευτή. Οι ερευνητές υποθέτουν πως η ανίχνευση ασυνήθιστης συμπεριφοράς αναζήτησης, η οποία λαμβάνει χώρα πριν το άνοιγμα ενός αρχείου αντιπερισπασμού από έναν ανυποψίαστο χρήστη, θα υποστηρίξει την υποψία ότι ο συγκεκριμένος χρήστης στην πραγματικότητα υποδύεται έναν άλλον χρήστη – θύμα. Το σενάριο αυτό καλύπτει το μοντέλο απειλής της μη επιβεβαιωμένης πρόσβασης

[16] Στην κρυπτογραφία, ένας κωδικός HMAC είναι ένας ειδικού τύπου κώδικας αυθεντικοποίησης μηνύματος, ο οποίος περιλαμβάνει μια κρυπτογραφική συνάρτηση κατακερματισμού και ένα μυστικό κλειδί κρυπτογράφησης. Ο κώδικας αυτός μπορεί να χρησιμοποιηθεί για να επιβεβαιώνεται ταυτόχρονα η ακεραιότητα των δεδομένων και η αυθεντικότητα των μηνυμάτων.

σε δεδομένα του fog και κατ' επέκταση του cloud computing. Επιπλέον, ένα τυχαίο άνοιγμα ενός αρχείου αντιπερισπασμού από έναν γνήσιο χρήστη μπορεί να χαρακτηριστεί ως «ατύχημα», εάν η συμπεριφορά της αναζήτησης δεν καθίσταται ως αφύσικη.

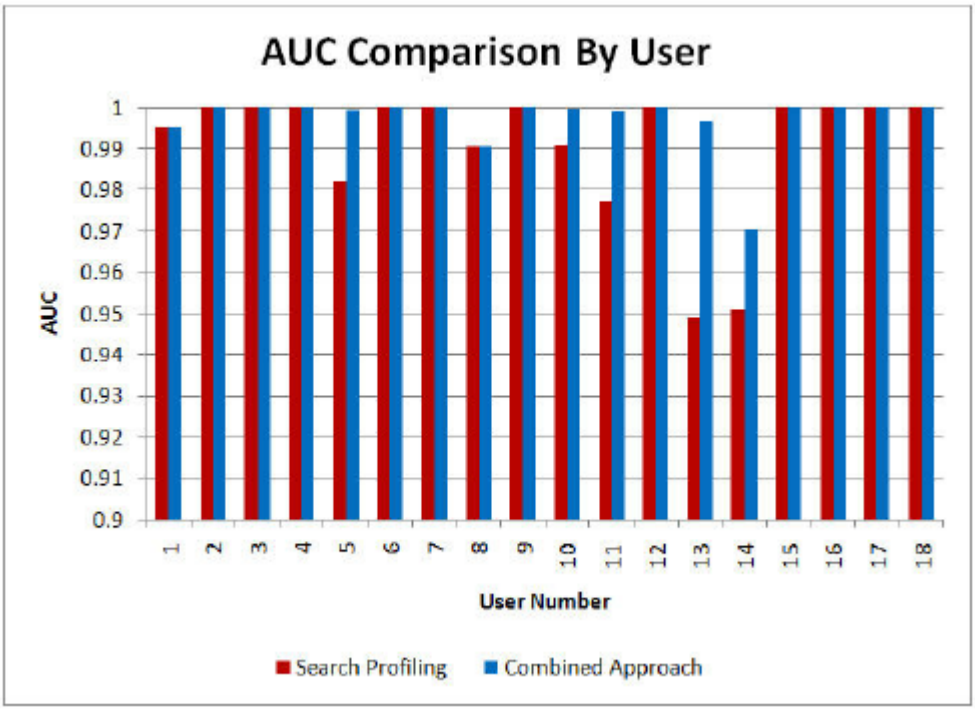
Για την εφαρμογή των δύο τεχνικών, οι ερευνητές χρησιμοποιήσαν τους αντιπερισπασμούς ως στοιχείο – κλειδί για την επιβεβαίωση των συναγερμών που εγέρθηκαν από τον αισθητήρα που παρακολουθεί την συμπεριφορά αναζήτησης και πρόσβασης του χρήστη. Στα πειράματά τους, οι ερευνητές δεν δημιούργησαν τους αντιπερισπασμούς κατ' αίτηση κατά τη διάρκεια της ανίχνευσης. Αντίθετα, προσπάθησαν να είναι σίγουροι ότι τα αρχεία αυτά ήταν αρκετά ευδιάκριτα προς τον επιτιθέμενο, ειδικά αν προσπαθούσε να υποκλέψει δεδομένα και πληροφορίες. Για να το πετύχουν αυτό, τα τοποθέτησαν σε πολύ εμφανείς τοποθεσίες ενώ τους έδωσαν και πολύ ελκυστικά ονόματα. Με την προσέγγιση αυτή, οι ερευνητές κατάφεραν να βελτιώσουν την ακρίβεια του ανιχνευτή τους. Παρ' όλο που δεν προχώρησαν στην ενέργεια αυτή, οι ερευνητές εκτιμούν πως η κατασκευή των αντιπερισπασμών κατ' αίτηση θα βελτίωνε ακόμα περισσότερο την ακρίβεια του ανιχνευτή. Όπως και να έχει, ο συνδυασμός των δύο τεχνικών, έχοντας παράλληλα τα αρχεία αντιπερισπασμού ως σημεία – κλειδιά για την ανίχνευση ασυνήθιστης συμπεριφοράς του χρήστη, μπορούν να μειώσουν σημαντικά τον δείκτη ψευδοθετικών (false positive) αποτελεσμάτων του ανιχνευτή.

6.3 Αποτελέσματα του πειράματος

Για να μπορέσουν να καταλήξουν στα αποτελέσματα του πειράματος, οι ερευνητές εκπαίδευσαν 18 ταξινομητές (classifiers)[17] με υπολογιστικά δεδομένα χρήσης από 18 φοιτητές της επιστήμης υπολογιστών και τα οποία συλλέχθηκαν μέσα σε μια περίοδο τεσσάρων ημερών. Οι ταξινομητές εκπαιδεύτηκαν με τη χρήση της ανίχνευσης αφύσικης συμπεριφοράς αναζήτησης που συζητήθηκε σε παλαιότερο άρθρο (M. Ben-Salem and S. J. Stolfo, 2011). Επίσης, εκπαιδεύτηκαν ακόμα 18 ταξινομητές που χρησιμοποιούσαν μια προσέγγιση ανίχνευσης που συνδυάζει την τεχνική της σκιαγράφησης της συμπεριφοράς του χρήστη με την παρακολούθηση της πρόσβασης σε αρχεία αντιπερισπασμού, τα οποία ήταν τοποθετημένα στο τοπικό σύστημα αρχειοθέτησης, όπως συζητήθηκε σε προηγούμενη ενότητα.

Στη συνέχεια, οι ερευνητές εξέτασαν τους παραπάνω ταξινομητές χρησιμοποιώντας προσομοιωμένα δεδομένα «μασκαρεμένων» επιτιθέμενων. Στην παρακάτω εικόνα παρουσιάζονται οι βαθμολογίες που πέτυχαν και οι δύο προσεγγίσεις ανίχνευσης που χρησιμοποιήθηκαν. Τα αποτελέσματα δείχνουν πως τα μοντέλα που χρησιμοποιούν την προσέγγιση του συνδυασμού των δύο τεχνικών ανίχνευσης πετυχαίνουν ίσα ή καλύτερα αποτελέσματα από αυτά της απλής σκιαγράφησης του προφίλ αναζητήσεων.

[17] Ένας classifier στην Μηχανική Μάθηση (Machine Learning) αξιοποιεί κάποια δεδομένα εκπαίδευσης για να γίνει κατανοητό πώς οι δοσμένες μεταβλητές σχετίζονται με την εκάστοτε κλάση. Για παράδειγμα, η ανίχνευση των spam emails από τους παρόχους υπηρεσιών email μπορεί να χαρακτηριστεί ως ένα πρόβλημα ταξινόμησης. Στην περίπτωση αυτή, τα ήδη γνωστά spam και non-spam email πρέπει να χρησιμοποιηθούν ως δεδομένα εκπαίδευσης. Όταν ο ταξινομητής εκπαιδευτεί επακριβώς, μπορεί να χρησιμοποιηθεί για να ανίχνευση ενός άγνωστου email.



Εικόνα 14 - Αποτελέσματα σύγκρισης του μοντέλου σκιαγράφησης και της συνδυαστικής προσέγγισης (Source: ResearchGate – Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud)

Σύμφωνα, λοιπόν, με την εφαρμογή του παραπάνω πειράματος, τα αποτελέσματα καταδεικνύουν πως τα προφίλ χρήσεις είναι αρκετά ακριβή για να χρησιμοποιηθούν στην ανίχνευση μη εξουσιοδοτημένης πρόσβασης στο fog και το cloud. Όταν ανιχνεύεται μια τέτοια πρόσβαση, το σύστημα μπορεί να παρουσιάζει στον χρήστη μια ερώτηση – πρόκληση ή ένα έγγραφο αντιπερισπασμού για να επιβεβαιώσει το εάν η πρόσβαση ήταν στην πραγματικότητα μη εξουσιοδοτημένη. Ο τρόπος αυτός είναι αρκετά παρόμοιος με τον τρόπο των ερευνητών, που χρησιμοποίησαν αντιπερισπασμούς σε ένα τοπικό αρχειακό σύστημα, για να επιβεβαιώσουν τους «συναγερμούς» που εγέρθηκαν από τον αντίστοιχο ανιχνευτή, ο οποίο με τη σειρά του παρακολουθεί την συμπεριφορά αναζήτησης αρχείων και πρόσβασης σε αυτά, του εκάστοτε χρήστη.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Archana L. A., Kavitha R. (2017), “A Study on Cloud and Fog Computing Security Issues and Solutions”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Issue 03, Volume 4.

Shanhe Yi, Zhengrui Qin, and Qun Li, “Security and Privacy Issues of Fog Computing: A Survey”, College of William and Mary.

Cisco (2015), *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are*, White Paper of CISCO.

Bernand Marr (2016), “What Is Fog Computing? And Why It Matters In Our Big Data And IoT World”, Forbes Site.

F. Bonomi, R. Milito, J. Zhu, and S. Addepalli (2012), “Fog computing and its role in the internet of things,” in workshop on Mobile cloud computing. ACM.

I. Stojmenovic (2014), “Fog computing: A cloud to the ground support for smart things and machine-to-machine networks,” in Telecommunication Networks and Applications Conference (ATNAC). IEEE.

K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, and M. Satyanarayanan (2014), “Towards wearable cognitive assistance”. In Mobisys. ACM.

Cao, Yu, et al. (2015) "FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation." Networking, Architecture and Storage (NAS), 2015 IEEE International Conference on. IEEE.

Cao, N., Yu, S., Yang, Z., Lou, W., Hou, Y.T. (2012): *Lt codes-based secure and reliable cloud storage service*. In: INFOCOM. IEEE.

Stantchev, Vladimir, et al. (2015) "Smart Items, Fog and Cloud Computing as Enablers of Servitization in Healthcare." Sensors & Transducers (1726-5479)185.2.

L. M. Vaquero and L. Rodero-Merino (2014) “Finding your way in the fog: Towards a comprehensive definition of fog computing”. ACM SIGCOMM Computer Communication Review.

Luan T. H, Cai L. X, Chen J. M, Shen X., Bai F (2011) VTube: towards the media rich city life with autonomous vehicular content distribution. Proceedings of the 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON’11), Jun 27−30, 2011, Salt Lake City, UT, USA. Piscataway, NJ, USA: IEEE, 2011: 359−367

Parno, B., Howell, J., Gentry, C., Raykova, M (2013).: *Pinocchio: Nearly practical verifiable computation*. In: Security and Privacy. IEEE.

Cisco, *IOx* [Online], Available: https://www.cisco.com/c/en/us/products/cloud-systems-management/iox/index.html

OSIsoft, PI System (2017), *From data to knowledge to transformation* [Online], Available: https://www.osisoft.com/pi-system/#tab1

Rockwell Software (2017), *FactoryTalk AssetCentre* [Online], Available: https://www.rockwellautomation.com/rockwellsoftware/products/factorytalk-assetcentre.page#overview

Cisco (2017) *Data in Motion: The Evolution of Data* [Online], Available: https://www.cisco.com/c/en/us/solutions/executive-perspectives/data-motion.html

Wikipedia (2017), *Representational state transfer* [Online], Available: https://en.wikipedia.org/wiki/Representational_state_transfer

LocalGrid (2017), *Accelerating IIoT, Industrial Internet of Things, Made Easy* [Online], Available: http://www.localgridtech.com/

Wikipedia (2017), *Machine to Machine* [Online], Available: https://en.wikipedia.org/wiki/Machine_to_machine

Wikipedia (2017), *Original Equipment Manufacturer* [Online], Available: https://el.wikipedia.org/wiki/Original_equipment_manufacturer

Cisco (2017), *Cisco has Completed the Acquisition of ParStream* [Online], Available: https://www.cisco.com/c/en/us/about/corporate-strategy-office/acquisitions/parstream.html

ADLINK (2017), *Vortex DDS* [Online], Available: http://www.prismtech.com/vortex

Wikipedia (2017), *MQTT (Message Queuing Telemetry Transport)* [Online], Available: https://en.wikipedia.org/wiki/MQTT

Wikipedia (2017), *Constrained Application Protocol* [Online], Available: https://en.wikipedia.org/wiki/Constrained_Application_Protocol

Josang, A., Ismail, R., Boyd, C. (2007), *A survey of trust and reputation systems for online service provision*. Decision support systems 43.

Damiani, E., et al. (2002) *A reputation-based approach for choosing reliable resources in peer-to-peer networks.* In: CCS. ACM

GlobalPlatform (2017), *GlobalPlatform made simple guide: Secure Element* [Online], Available: https://www.globalplatform.org/mediaguideSE.asp

Wikipedia (2017), *Trusted execution environment* [Online], Available: https://en.wikipedia.org/wiki/Trusted_execution_environment

Wikipedia (2017), *Trusted Platform Module* [Online], Available: https://en.wikipedia.org/wiki/Trusted_Platform_Module

Stojmenovic, I., Wen, S. (2014), *The fog computing paradigm: Scenarios and security issues*. In: FedCSIS. IEEE.

Wikipedia (2019), *NFC (Near Field Communication)* [Online], Available: https://el.wikipedia.org/wiki/NFC

Han, H., Sheng, B., Tan, C.C., Li, Q., Lu, S. (2009), *A measurement based rogue ap detection scheme*. In: INFOCOM. IEEE.

Balfanz, D., Smetters, D.K., Stewart, P., Wong, H.C. (2002), *Talking to strangers: Authentication in ad-hoc wireless networks*. In: NDSS

Bouzefrane, S., Mostefa, A.F.B., Houacine, F., Cagnon, H. (2014), *Cloudlets authentication in nfc-based mobile computing*. In: MobileCloud. IEEE

Tsugawa, M., et al., (2014), *Cloud computing security: What changes with software-defined networking?* In: Secure Cloud Computing. Springer

Shin, S., Gu, G. (2012), *Cloudwatcher: Network security monitoring using openflow in dynamic cloud networks*. In: ICNP. IEEE

McKeown, N., et al. (2008), *Openflow: enabling innovation in campus networks*. ACM SIGCOMM CCR 38.

Klaedtke, F., Karame, G.O., Bifulco, R., Cui, H. (2014), *Access control for sdn controllers*. In: HotSDN. vol. 14.

Yap, K.K., et al., (2011), *Separating authentication, access and accounting: A case study with openwifi*. Open Networking Foundation, Tech. Rep.

Wang, C., Wang, Q., Ren, K., Lou, W (2010), *Privacy-preserving public auditing for data storage security in cloud computing*. In: INFOCOM. IEEE.

Gennaro, R., Gentry, C., Parno, B (2010).: *Non-interactive variable computing: Out-sourcing computation to untrusted workers*. In: CRYPTO. Springer.

Lu, R., et al. (2012), *Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications*. TPDS 23.

Rial, A., Danezis, G. (2011), *Privacy-preserving smart metering*. In: Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. ACM.

McLaughlin, S., McDaniel, P., Aiello, W. (2011), *Protecting consumer privacy from electric load monitoring*. In: CCS. ACM.

A. Erbad (2012), *Real – time support for interactive multimedia applications*, Ph.D. dissertation, University of British Columbia, Canada.

J.K Zao, T.T. Gan, C.K. You, C.E. Chung, Y.T. Wang, S.J.R. Mendez, T. Mullen, C. Yu, C. Kothe, C.T. Hsiao, S.L. Chu, C.K. Shieh and T.P. Jung (2014), *Pervasive brain monitoring and data*

sharing based on multi-tier distributed computing and linked data technology, Frontiers in Human Neuroscience, vol.8, no. 370, pp. 1-16.

M. Friedli, L.K, Francesco Paganini, Rainer Kyburz (2016), *Energy Efficiency of the Internet of Things – Technology and Energy Assessment Report,* IEA 4E EDNA. p. 1-66.

Fatemeh Jalali, Safieh Khodadustan, Chrispin Gray, Kerry Hinton, Frank Suits (2017), *Greening IoT with Fog: A Survey,* IBM Research, University of Melbourne, Australia.

F. Jalali et al (2014), *Energy Consumption of Content Distribution from Nano Data Centers versus Centralized Data Centers,* SIGMETRICS Perform. Eval. Rev., 42(3), p. 49-54.

C. Gray κ. Ά (2015), *Power consumption of IoT access network technologies,* IEEE International Conference on Communication Workshop (ICCW).

Wikipedia (2018), *Passive Optical Network* [Online], Available: https://en.wikipedia.org/wiki/Passive_optical_network

F. Jalali κ. Ά (2016), *Fog Computing May Help to Save Energy in Cloud Computing,* IEEE Journal on Selected Areaw in Communication, 34(5): p. 1728-1739.

F. Jalali, A. Vishwanath, Julian de Hoog, F. Suits (2016)**,** *Interconnecting Fog computing and Microgrids for Greening IoT,* IEEE Innovative Smart Grid Technologies (ISGT) Asia, Melbourne .

R. Deng κ. Ά (2016), *Optimal Workload Allocation in Fog-Cloud Computing Towards Balanced Delay and Power Consumption,* IEEE Internet of Things Journal, PP (99): p.1-1.

S. Yi, C. Li and Q. Li (2015), *A Survey of Fog Computing: Concepts, Applications and Issues,* in Proceedings of the 2015 Workshop on Mobile Big Data, ACM: Hangzhou, China, p. 37-42.

Wikipedia (2016), *Εικονικοποίηση δικτυακών λειτουργιών* [Online], Available: https://el.wikipedia.org/wiki/%CE%95%CE%B9%CE%BA%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF%CF%80%CE%BF%CE%AF%CE%B7%CF%83%CE%B7_%CE%B4%CE%B9%CE%BA%CF%84%CF%85%CE%B1%CE%BA%CF%8E%CE%BD_%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B9%CF%8E%CE%BD

Wikipedia (2013), *Software-Defined Networking* [Online], Available: https://en.wikipedia.org/wiki/Software-defined_networking

IEEE, The Institute (2014), *Special Report: The Internet of Things*, [Online], Available: http://theinstitute.ieee.org/static/specialIreportItheIinternetIofIthings##

Wikipedia (2018), *RFID* [Online], Available: https://el.wikipedia.org/wiki/RFID

M. Satyanarayanan, P. Bahl, R. Caceres and N. Davies (2009), *The Case for VM-Based Cloudlets in Mobile Computing*, in *IEEE Pervasive Computing*, vol. 8, no. 4, pp. 14-23.

Willis, Dale & Dasgupta, Arkodeb & Banerjee, Suman. (2014), *ParaDrop: A multi-tenant platform to dynamically install third party services on wireless gateways*. MobiArch 2014 - Proceedings of the 9th ACM MobiCom Workshop on Mobility in the Evolving Internet Architecture.

Somorovsky, J., Heiderich, M., Jensen, M., Schwenk, J., Gruschka, N., and Iacono, L. (2011) *All your clouds are belonging to us: Security analysis of cloud management interfaces*, in Proceedings of the 3rd ACM Workshop on Cloud Computing (CCSW '11) Security Workshop: Chicago, Ill.

Kanuparthi, A., Karri, R., and Addepalli, S (2013), *Hardware and embedded security in the context of internet of things*, in Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles: Berlin, DE, pp. 61-64.

Kaufman, L (2009), *Data security in the world of cloud computing*, IEEE Security & Privacy (7:4), pp 61-64.

Hong, K., Lillethun, D., Ramachandran, U., Ottenwalder, B., and Koldehofe, B. (2013), *Mobile fog: a programming model for large-scale applications on the internet of things*, in *Proceedings of the second ACM SIGCOMM workshop on Mobile cloud computing (MCC '13)*, pp. 15-20.

M. A. Ferrag, L. Maglaras, and A. Ahmin (2016), *Privacy – preserving schemes for ad hoc social networks: A survey*, IEEE Commun. Surveys Tuts.

Y. Hong, W. M. Liu, L. Wang (2017), *Privacy preserving smart meter streaming against information leakages*, IEEE Trans. Inf. Forensics Security, vol.12 no. 9, pp. 2227 – 2241.

D. Koo, J. Hur (2017), *Privacy – preserving deduplication of encrypted data with dynamic ownership management in fog computing*, Future Generat. Comput. Syst.

Botnet (2011), *Τι εστί botnet; Είναι το PC μου ζόμπι;* [Online], Available: https://www.in.gr/2011/04/13/tech/future/ti-esti-botnet-einai-to-pc-moy-zompi/

T. Roth (2011), *Breaking Encryptions Using GPU Accelerated Cloud Instances*, Black Hat Technical Security Conference.

CERT Coordination Center, *Denial of Service* [Online], Available: http://www.packetstormsecurity.org/distributed/denial_of_service.htm

M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono (2009), *On Technical Security Issues in Cloud Computing*, IEEE International Conference in Cloud Computing, pp. 109-116, Bangalore.

CERT Coordination Center, Cybersecurity Watch Survey, Carnegie Mellon University (2011).

CERT (2012), *Insider Threats Related to Cloud Computing* [Online] Available: http://www.cert.org/

Symantec (2012**),** *Data Breach Trends & Stats* [Online], Available: http://www.indefenseofdata.com/data-breach-trends-stats

LinkedIn Blog (2012), *An Update on LinkedIn Member Passwords Compromised* [Online] Available: http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/

Dropbox (2012), *Yes, We Were Hacked* [Online] Available: http://gigaom.com/cloud/dropbox-yes-we-were-hacked/

Symantec (2009), *Web Based Attacks*, Symantec White Paper [Online] Available: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/web-based-attacks-09-en.pdf

Symantec (2019*), Internet Security Threat Report*, Vol. 24 [Online] Available: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

Sophos (2008), *Visitors to Sony PlayStation Website at Risk of Malware Infection* [Online] Available: http://www.sophos.com/en-us/press-office/press-releases/2008/07/playstation.aspx

FireHost (2012), *Web Application Attack Report For The Second Quarter of 2012*, [Online] Available: http://www.firehost.com/company/newsroom/web-application-attack-report-second-quarter-2012

PCWorld (2011), *Researchers Demo Cloud Security Issue With Amazon AWS Attack*, [Online] Available:http://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aws_attack/

MakeUseOf (2019), *What Is Formjacking and How Can You Avoid It?* [Online] Available: https://www.makeuseof.com/tag/what-is-formjacking/

TechCrunch (2018), *British Airways customer data stolen in data breach* [Online] Available: https://techcrunch.com/2018/09/06/british-airways-customer-data-stolen-in-data-breach/

RiskIQ (2019), *Inside Magecart* [Online] Available: https://www.riskiq.com/research/inside-magecart/

M. McIntosh and P. Austel (2005), *XML Signature Element Wrapping Attacks and Countermeasures*, 2005 workshop on Secure web services, ACM Press, New York, NY, pp. 20–27.

N. Gruschka and L. L. Iacono (2009), *Vulnerable Cloud: SOAP Message Security Validation Revisited*, IEEE International Conference on Web Services, Los Angeles.

M. Arrington (2009), *In our inbox: Hundreds of confidential twitter documents*, [Online] Available: http://techcrunch.com/2009/07/14/in-our-inbox-hundreds-of-confidential-twitter-documents/

P. Allen (2010), *Obama's Twitter password revealed after French hacker arrested for breaking into U.S. president's account* [Online] Available: http://www.dailymail.co.uk/news/article-1260488/Barack-Obamas-Twitter-password-revealed-French-hacker-arrested.html

M. Ben-Salem and S. J. Stolfo (2011), *Modeling user search-behavior for masquerade detection*, Proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection. Heidelberg: Springer, pp. 1–20.

B. M. Bowen and S. Hershkop (2009), *Decoy Document Distributor* [Online], Available: http://sneakers.cs.columbia.edu/ids/FOG/

Wikipedia (2019), *HMAC* [Online], Available: https://en.wikipedia.org/wiki/HMAC

Sidath Asiri (2018), *Machine Learning Classifiers*, [Online], Available: https://towardsdatascience.com/machine-learning-classifiers-a5cc4e1b0623