ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

«Χρήση τεχνητής νοημοσύνης και της μηχανικής μάθησης στην εγκληματολογία»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Κυριακής - Μαρίας Σωματοπούλου

Επιβλέπων : Γεώργιος Στεργιόπουλος

Μέλη εξεταστικής επιτροπής: Γεώργιος Στεργιόπουλος

Σάμος, Ιούνιος 2024

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πρόλογος και ευχαριστίες

Ένα μεγάλο ταξίδι και μια μακρά πορεία έφτασαν σταδιακά στο τέλος τους. Για αυτόν τον λόγο, είμαι στην ευχάριστη θέση να παρουσιάσω αυτή τη διπλωματική εργασία, το αποτέλεσμα μιας εκτενούς περιόδου έρευνας και προσπάθειας. Η παρούσα διπλωματική εργασία συντάχθηκε κατά το ακαδημαϊκό έτος 2023-2024 στο πλαίσιο του Προπτυχιακού Προγράμματος Σπουδών του Τμήματος "Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων", το οποίο ανήκει στην Πολυτεχνική Σχολή του Πανεπιστημίου Αιγαίου. Το θέμα της εργασίας επικεντρώνεται στη χρήση της τεχνητής νοημοσύνης και της μηχανικής μάθησης στην εγκληματολογία.

Βρίσκομαι σε ένα σημαντικό σημείο της ακαδημαϊκής μου πορείας και αισθάνομαι την ανάγκη να εκφράσω την ευγνωμοσύνη μου σε όλους όσους με στήριξαν καθ' όλη τη διάρκεια αυτής της διαδρομής. Η ολοκλήρωση αυτής της διπλωματικής εργασίας δεν θα ήταν εφικτή χωρίς τη συμβολή και τη στήριξη κάποιων σημαντικών ανθρώπων.

Πρώτα απ’ όλα, θα ήθελα να εκφράσω τις ευχαριστίες μου στον κ. Γεώργιο Στεργιόπουλο, τον επιβλέποντα καθηγητή μου από το Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων. Η εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτήν την εργασία υπήρξε για μένα κινητήριος δύναμη και πηγή έμπνευσης. Η καθοδήγηση, η υποστήριξη και οι συμβουλές του σε όλη τη διάρκεια της έρευνάς μου, συνέβαλαν καθοριστικά στην επιτυχή ολοκλήρωση της διπλωματικής μου εργασίας.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου Χρήστο και Ματίνα, τον αδελφό μου Στέλιο, τους συμφοιτητές και φίλους μου καθώς και τον Κώστα, που μου στάθηκαν με ποικίλους τρόπους καθ’ όλη τη διάρκεια της ακαδημαϊκής μου πορείας.

Η υποστήριξη και η συμβολή των παραπάνω προσώπων υπήρξε καθοριστική και τους ευχαριστώ θερμά για όλα όσα μου προσέφεραν κατά τη διάρκεια της ακαδημαϊκής μου πορείας και της εκπόνησης αυτής της διπλωματικής εργασίας.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Ακρωνύμια

Ακρωνύμιο	***Πλήρης μορφή***
DF	Digital Forensics / Ψηφιακή εγληματολογία
DI	Digital Investigations / Ψηφιακές Ερευνες
AI	Artificial Intelligence / Τεχνητή Νοημοσύνη
ASP	Answer Set Programming / Προγραμματισμός Συνόλων Απαντήσεων
ML	Machine Learning / Μηχανική Μάθηση
DL	Deep Learning / Βαθιά Μάθηση
DSS	Decision Support Systems / Συστήματα Υποστήριξης Απόφασης
XAI	Explainable Artificial Intelligence / Εξηγήσιμη Τεχνητή Νοημοσύνη
CNN	Convolutional Neural Networks / Συνελικτικά Νευρωνικά Δίκτυα
SVM	Support Vector Machines / Μηχανές Υποστήριξης Διανυσμάτων
IoT	Internet of Things / Διαδίκτυο των Πραγμάτων
ICS	Industrial Control Systems / Συστήματα Ελέγχου Βιομηχανίας
P	Polynomial-time complexity / Πολυωνυμική Πολυπλοκότητα
NP	Non-deterministic Polynomial-time complexity / Πολυπλοκότητα Πολυωνυμικού Χρόνου Μη Καθορισμένη
DNS	Domain Name System / Σύστημα Ονομάτων Τομέα
HQL	Hive Query Language / Γλώσσα Ερωτήσεων Hive
IP	Internet Protocol / Πρωτόκολλο Διαδικτύου
DDoS	Distributed Denial of Service / Κατανεμημένη Άρνηση Υπηρεσίας
CC	Cybercrime / Κυβερνοέγκλημα
NN	Neural Network / Νευρωνικό Δίκτυο
MADIK	MultiAgent Digital Investigation toolKit / Εργαλειοθήκη ψηφιακής έρευνας MultiAgent
ISA	Intelligent Software Agent / Εφυής Πράκτορας Λογισμικού

VR	Virtual Reality / Εικονική Πραγματικότητα
DFI	Digital Forensic Investigation / Ψηφιακή Εγκληματολογική Έρευνα
DSS	Decision Support System / Σύστημα Υποστήριξης Αποφάσεων
NAT	Network Address Translation / Μετάφραση Διευθύνσεων Δικτύου
NIDS	Network Intrusion Detection System / Σύστημα Ανίχνευσης Εισβολών Δικτύου
ICMP	Internet Control Message Protocol / Πρωτόκολλο Μηνυμάτων Ελέγχου Διαδικτύου
TCP	Transmission Control Protocol / Πρωτόκολλο Ελέγχου Μετάδοσης
UDP	User Datagram Protocol / Πρωτόκολλο Διεπαφής Χρήστη
DLCF	Deep Learning Cyber Forensics / Εγκληματολογική έρευνα στον κυβερνοχώρο/
NLP	Natural Language Processing / Επεξεργασία Φυσικής Γλώσσας
DFT	Discrete Fourier Transform / Διακριτός Μετασχηματισμός Φουριέ
SNN	Spiking Neural Network / Νευρωνικό δίκτυο αιχμής

Περίληψη

Η ψηφιακή εγκληματολογία (DF) είναι κρίσιμης σημασίας λόγω της έξαρσης των εγκλημάτων στον υπολογιστή, δίνοντας έμφαση στη διατήρηση και ανάλυση των ψηφιακών αποδεικτικών στοιχείων. Η παρούσα μελέτη εξετάζει τη χρήση της τεχνητής νοημοσύνης (AI) και του προγραμματισμού απαντητικών συνόλων (ASP) για την αυτοματοποίηση της ανάλυσης αποδεικτικών στοιχείων, καθιστώντας τις πολύπλοκες έρευνες διαχειρίσιμες ως προβλήματα πολυωνυμικού χρόνου (P) ή μη ντετερμινιστικού πολυωνυμικού χρόνου (NP), εκφραζόμενα σε προγραμματισμού απαντητικών συνόλων (ASP). Τα εργαλεία τεχνητής νοημοσύνης (AI), συμπεριλαμβανομένων των νευρωνικών δικτύων, βελτιώνουν την εγκληματολογία δικτύων αναλύοντας αποτελεσματικά μεγάλους όγκους δεδομένων και βελτιώνοντας την ακρίβεια ανίχνευσης και ταξινόμησης. Η ανάλυση μεταδεδομένων αρχείων με βάση την τεχνητή νοημοσύνη (AI) βοηθά στην αποκάλυψη αποδεικτικών στοιχείων εγκληματικών δραστηριοτήτων.

Προηγμένες μέθοδοι όπως το MapReduce και εργαλεία ανοικτού κώδικα όπως το Hadoop, το Hive και το Mahout διευκολύνουν την αποτελεσματική ανάλυση μεγάλων δεδομένων στην ωηφιακή εγληματολογία (DF). Οι τεχνικές τεχνητής νοημοσύνης, συμπεριλαμβανομένης της βαθιάς μάθησης (DL) και των συστημάτων πολλαπλών πρακτόρων, απλοποιούν την ανάλυση δεδομένων, μειώνουν τον χρόνο επεξεργασίας και βελτιώνουν την ακρίβεια. Η επεξηγήσιμη τεχνητή νοημοσύνη, (XAI) και οι τεχνολογίες blockchain προσφέρουν διαφανή και ασφαλή ανάλυση, απαραίτητη για τη διατήρηση της ακεραιότητας των εγκληματολογικών ερευνών.

Οι μέθοδοι μάθησης χωρίς επίβλεψη, ιδίως για την ανίχνευση ransomware Android, επιδεικνύουν υψηλή ακρίβεια και αποτελεσματικότητα, αντιμετωπίζοντας την πρόκληση των άγνωστων απειλών. Οι εφαρμογές τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) καλύπτουν διάφορες πτυχές της ψηγιακής εγκληματολογίας (DF), από την ανάλυση της κίνησης δικτύου έως την εγκληματολογία ψηφιακών μέσων, ενισχύοντας σημαντικά την αποτελεσματικότητα και την αξιοπιστία των ερευνών. Η ενσωμάτωση της τεχνητής νοημοσύνης (AI) στην ψηφιακή εγληματολογία (DF) όχι μόνο βελτιώνει τις διεργασίες έρευνας, αλλά διασφαλίζει επίσης ότι τα αποδεικτικά στοιχεία είναι ισχυρά και αξιόπιστα για τις νομικές διαδικασίες.

Λέξεις Κλειδιά: *Ψηφιακή εγληματολογία (DF), Ψηφιακές έρευνες (DI), Τεχνητή Νοημοσύνη (AI), Προγραμματισμός απαντητικών συνόλων (ASP), Μηχανική Μάθηση (ML), Βαθιά Μάθηση (DL), Ανάλυση αποδεικτικών στοιχείων, Συστήματα υποστήριξης αποφάσεων (DSS), εγκληματολογία δικτύων, κυβερνοασφάλεια, νευρωνικά δίκτυα, ανάλυση αποδεικτικών στοιχείων, εγκληματολογία δικτύων, μεγάλα δεδομένα, blockchain, Επεξηγήσιμη τεχνητή νοημοσύνη (XAI), Android ransomware.*

Abstract

Digital forensics (DF) is of critical importance due to the rise of computer crime, with an emphasis on the preservation and analysis of digital evidence. This study examines the use of artificial intelligence (AI) and answer set programming (ASP) to automate evidence analysis, making complex investigations manageable as polynomial-time (P) or non-deterministic polynomial-time (NP) problems expressed in answer set programming (ASP). Artificial intelligence (AI) tools, including neural networks, improve network forensics by efficiently analyzing large volumes of data and improving detection and classification accuracy. AI-based analysis of file metadata helps to uncover evidence of criminal activities.

Advanced methods such as MapReduce and open source tools such as Hadoop, Hive and Mahout facilitate efficient big data analysis in deaf enlightenment (DF). Artificial intelligence techniques, including deep learning (DL) and multi-agent systems, simplify data analysis, reduce processing time and improve accuracy. Explanatory artificial intelligence, (XAI) and blockchain technologies offer transparent and secure analysis, essential for maintaining the integrity of forensic investigations.

Unsupervised learning methods, particularly for Android ransomware detection, demonstrate high accuracy and efficiency, addressing the challenge of unknown threats. Artificial intelligence (AI) and machine learning (ML) applications cover various aspects of digital forensics (DF), from network traffic analysis to digital media forensics, significantly enhancing the efficiency and reliability of investigations. The integration of artificial intelligence (AI) into digital forensics (DF) not only improves investigation processes, but also ensures that evidence is robust and reliable for legal proceedings.

Keywords: *Digital Forensics (DF), Digital Investigations (DI), Artificial Intelligence (AI), Answer Set Programming (ASP), Machine Learning (ML), Deep Learning (DL), Evidence Analysis, Decision Support Systems (DSS), Network Forensics, Cybersecurity, neural networks, evidence analysis, network forensics, big data, blockchain, XAI, Android ransomware.*

1

Εισαγωγή

1.1 Αξιοποίηση της τεχνητής νοημοσύνης και της μηχανικής μάθησης για ενισχυμένη ψηφιακή εγκληματολογία και έρευνες

1.1.1 Η έννοια της Ψηφιακής Εγκληματολογίας (DF)

Ο χώρος της Ψηφιακής Εγκληματολογίας (DF) και των Ψηφιακών Ερευνών (DI) ασχολείται με την ανάλυση στοιχείων για την παροχή αντικειμενικών δεδομένων και τη στήριξη του σχηματισμού υποθέσεων για νομική απόδειξη. Η ψηφιακή εγκληματολογία είναι η υπόθεση του ακριβούς εντοπισμού και της συλλογής ηλεκτρονικών πληροφοριών που είναι αποθηκευμένες σε ψηφιακές συσκευές, της διατήρησης και ανάλυσης των πληροφοριών και της υποβολής τους στο δικαστήριο ως αποδεικτικών στοιχείων. Ανάλογα με το αντικείμενο της ανάλυσης, η ψηφιακή εγκληματολογία περιλαμβάνει την εγκληματολογία δίσκων, την εγκληματολογία συστημάτων, την εγκληματολογία δικτύων, την εγκληματολογία του Διαδικτύου, την εγκληματολογία κινητών τηλεφώνων, την εγκληματολογία βάσεων δεδομένων και την εγκληματολογία κρυπτογράφησης.

Καθώς σε αυτή την ψηφιακή εποχή, το έγκλημα στον κυβερνοχώρο επεκτείνεται καθημερινά. Είναι απαραίτητο να ληφθούν κατάλληλα μέτρα από τις υπηρεσίες επιβολής του νόμου για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και εδώ έρχεται η ψηφιακή εγκληματολογία. Η ψηφιακή εγκληματολογία αναπτύχθηκε το 1984, όταν το FBI ξεκίνησε προγράμματα στα εργαστήριά του για τη διερεύνηση εγκλημάτων που γίνονταν με τη χρήση υπολογιστών[7] [9].

Με την πρόοδο και την ανάπτυξη της ψηφιακής εγκληματολογίας αναπτύχθηκαν διάφορα πρότυπα και ορισμοί και μοντέλα διερεύνησης της ψηφιακής εγκληματολογίας. Πολλά μοντέλα διερεύνησης ψηφιακής εγκληματολογίας έχουν κάποια κοινά στάδια, αλλά έχουν αναπτυχθεί για τη διερεύνηση διαφορετικών ξεχωριστών εγκλημάτων σε διαφορετικά σενάρια.

1.1.2 Η εξέλιξη της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης, και ο συνδυασμός της με την Ψηφιακή Εγληματολογία

Οι πρόσφατες εξελίξεις στην Τεχνητή Νοημοσύνη (AI) και, συγκεκριμένα, στον Προγραμματισμό Απαντητικών Συνόλων (ASP) υπόσχονται να αυτοματοποιήσουν την ανάλυση στοιχείων. Στην πραγματικότητα, ο Προγραμματισμός Απαντητικών Συνόλων (ASP), είναι ένα καθιερωμένο παράδειγμα Υπολογιστικής Λογικής (Είναι ένας όρος που περιγράφει την πρόοδο λήψης αποφάσεων που χρησιμοποιείται στον προγραμματισμό και τη συγγραφή αλγορίθμων) για την επίλυση προβλημάτων συνδυαστικής / βελτιστοποίησης / σχεδιασμού ξεκινώντας από μια δηλωτική προδιαγραφή τους και τους σχετικούς περιορισμούς τους. Οι λύσεις του συγκεκριμένου προβλήματος ή, καλύτερα, τα σενάρια που διέπουν τη διατύπωση του προβλήματος ASP μπορούν να βρεθούν διαθέσιμων μηχανών εξαγωγής συμπερασμάτων ανοικτές για το κοινό τους, που ονομάζονται «solvers», ή αλλιώς «λύτες».

Οι διατυπώσεις αυτού του προγραμματισμού, παράγουν όλα τα πιθανά σενάρια, τα οποία είναι συμβατά με τα δεδομένα και τους περιορισμούς μιας συγκεκριμένης περίπτωσης. Στη γενική περίπτωση, αυτό μπορεί να είναι πολύ χρήσιμο, καθώς ο ένας ανθρώπινος εμπειρογνώμονας μπορεί μερικές φορές να παραβλέψει κάποιες από τις πιθανότητες.

Επίσης, η ανάλυση δικτύου εξετάζει δεδομένα / πακέτα κίνησης σε ένα δίκτυο για τον εντοπισμό μη εξουσιοδοτημένων συνδέσεων και μεταφοράς δεδομένων, χρησιμοποιώντας την τεχνητή νοημοσύνη (AI) για να βελτιώσει την ακρίβεια ανάλυσης κυκλοφορίας. Η μηχανική μάθηση (ML) και η χρήση βαθιάς μάθησης (DL) συμβάλλουν στην ανάλυση δικτυακών δεδομένων, περιλαμβάνοντας συσκευές Διαδίκτυο των πραγμάτων (IoT), εγκληματολογία του νέφους (CC) και εγκληματολογία έξυπνων δικτύων (smart devices).

Η ανάλυση μεταδεδομένων αρχείων, ζωτική για την ανίχνευση δραστηριοτήτων χρηστών (Η οποία περιλαμβάνει την παρακολούθηση του τρόπου με τον οποίο οι χρήστες συμπεριφέρονται, συμμετέχουν και αλληλεπιδρούν μέσα στις διαδικτυακές εφαρμογές σας. Βοηθά τις εταιρείες να λαμβάνουν αποφάσεις βάσει δεδομένων με βάση τη συμπεριφορά των επισκεπτών εντός της εφαρμογής και του ιστότοπου.), επωφελείται από αλγόριθμους μηχανικής μάθησης (ML) για την επιτάχυνση των ερευνών. Ο ρόλος της τεχνητής νοημοσύνης (AI) στην Ψηφιακή Εγκληματολογία (DF) επεκτείνεται στην ανάλυση μεγάλων συνόλων δεδομένων, και με στην εύρεση πειστηρίων εφόσον γίνει μια επίθεση.

Έξυπνες συσκευές σε έξυπνες πόλεις (smart cities), AI ηχεία και φορητή τεχνολογία παρέχουν ζωτικά στοιχεία σε εγκληματολογικές έρευνες. Τεχνικές που βασίζονται στην τεχνητή νοημοσύνη (AI) βελτιώνουν την ταυτοποίηση παραποιημένων μέσων, αν και παραμένουν προκλήσεις λόγω της ποικιλίας των δεδομένων.

Τα μοντέλα τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML), περιλαμβανομένων των συνελικτικών νευρωνικών δίκτυων (CNNs), και νευρωνικών δικτύων (NN), ενισχύουν την Ψηφιακή Εγκληματολογία (DF) αυτοματοποιώντας την ταξινόμηση στοιχείων, και την ανάλυση συμπεριφοράς.

Πτυχές της εγληματολογίας που αξιοποιούν την τεχνολογία blockchain την ομαδοποίηση και την μη εποπτευόμενη μηχανική μάθηση (ML) προσφέρουν καινοτόμες προσεγγίσεις στην ανάλυση ψηφιακών στοιχείων, εξασφαλίζοντας ισχυρές και αποδοτικές έρευνες. Αυτές οι εξελίξεις υπογραμμίζουν την μετασχηματιστική δύναμη της τεχνητής νοημοσύνης (AI) στην Ψηφιακή Εγκληματολογία (DF), οδηγώντας σε πιο ακριβείς και κλιμακούμενες εγκληματολογικές μεθοδολογίες.

Οι γενικές προκλήσεις στον χώρο περιλαμβάνουν την πολυπλοκότητα και την ταχύτητα των σύγχρονων επιθέσεων, την πολυπλοκότητα των δεδομένων που απαιτούν ανάλυση και τις ηθικές και νομικές προεκτάσεις της χρήσης τεχνητής νοημοσύνης (AI). Η διπλωματική εργασία θα επικεντρωθεί στην αντιμετώπιση αυτών των προβλημάτων, αναζητώντας λύσεις που θα βελτιώσουν την αποδοτικότητα και την ακρίβεια των ψηφιακών ερευνών.

1.1.3 Επεξήγηση γενικών εννοιών

1.1.3.1 Artificial Intelligence (AI)

Δεν είναι εύκολο να περιγράψει κανείς την Τεχνητή Νοημοσύνη (AI), δεν υπάρχει καθιερωμένος ορισμός της Τεχνητής Νοημοσύνης. Οι περισσότερες από τις έννοιες που υπάρχουν τείνουν να περιγράφουν την Τεχνητή Νοημοσύνη με την έννοια της «δημιουργίας μιας διαδικασίας υπολογιστή που ενεργεί (αλλά τι είναι η νοημοσύνη;) ή «δημιουργία μιας διαδικασία υπολογιστή που μπορεί να μιμηθεί τις ανθρώπινες ενέργειες» (οι άνθρωποι πάντα ενεργούν έξυπνα, τι συμβαίνει αν μια μηχανή συνήθως αποδίδει καλύτερα από έναν άνθρωπο;). Ισχύουν πολλές έννοιες στη «λογική δράση» (αλλά τι είναι λογική;) ή «εκτέλεση εργασιών που είναι αδύνατο να κάνει μια μηχανή» (αυτό σημαίνει ότι αφού ένα πρόγραμμα τεχνητής νοημοσύνης έχει κατασκευαστεί για να εκτελέσει τη λειτουργία, δεν είναι πλέον Τεχνητή Νοημοσύνη;) τα οποία είναι παρομοίως μη χρήσιμα σε αυτή τη συζήτηση. Επομένως, για να απλοποιήσουμε την πρόκληση για την παρούσα εργασία, μια ρεαλιστική προσέγγιση είναι και η Τεχνητή Νοημοσύνη περιγράφεται ως «η δημιουργία ενός διαδικασία υπολογιστή που συμπεριφέρεται με τρόπο που ένας μέσος άνθρωπος θα θεωρούσε ευφυή». Πολλές από τις διάφορες μορφές της τεχνητής νοημοσύνης και των τεχνικών τεχνητής νοημοσύνης που μπορεί να ενδιαφέρουν τους ανθρώπους της ψηφιακής εγκληματολογίας, κοινότητα συζητούνται επίσης. [25]

1.1.3.2 Machine learning (ML)

Μηχανική μάθηση αποκαλούμε ένα υποσύνολο του τομέα της τεχνητής νοημοσύνης. Πρόκειται για μια επιστημονική επιστήμη που επικεντρώνεται στην ανάπτυξη υπολογιστικών μοντέλων και αλγορίθμων που μπορούν να εκτελούν συγκεκριμένες εργασίες χωρίς προγραμματισμό, όπως η εκπαίδευση συνόλων δεδομένων και δοκιμές, και είναι δυνατό να βοηθήσει σε έρευνες. [28]

1.1.3.3 IoT – smart devices

Το έξυπνο περιβάλλον περιλαμβάνει διάφορους τύπους έξυπνων συσκευών, αισθητήρων και υπολογιστών που είναι συνδεδεμένα στο διαδίκτυο και ενσωματωμένα σε πολυάριθμα αντικείμενα εντός αυτού του περιβάλλον. Τα έξυπνα περιβάλλοντα έχουν εξελιχθεί γρήγορα σε ένα δίκτυο διαδικτυακών συσκευών, γνωστά και ως συσκευές IoT . [27]

1.1.3.4 Cloud computing (CC)

Το υπολογιστικό νέφος βασίζεται στο TCP/IP (είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται το Διαδίκτυο αλλά και μεγάλο ποσοστό των εμπορικών δικτύων. Η ονομασία TCP/IP προέρχεται από τις συντομογραφίες των δυο κυριότερων πρωτοκόλλων της συλλογής: το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol) και το Πρωτόκολλο Διαδικτύου (Internet Protocol).) για υψηλή ανάπτυξη και ενσωμάτωση τεχνολογιών πληροφορικής, όπως οι γρήγορες μικροεπεξεργαστής, τεράστια μνήμη, δίκτυο υψηλής ταχύτητας και αξιόπιστη αρχιτεκτονική του συστήματος. Χωρίς την τυποποιημένη διασύνδεση πρωτόκολλα και ώριμες τεχνολογίες συγκέντρωσης κέντρων δεδομένων, το υπολογιστικό νέφος δεν θα γινόταν πραγματικότητα. [31]

1.1.3.5 Deep learning (DL)

Η βαθιά μάθηση (DL) είναι ένας κλάδος της μηχανικής μάθησης. Είναι ένας αλγόριθμος που προσπαθεί να χρησιμοποιήσει την υψηλού επιπέδου αφαίρεση των δεδομένων με τη χρήση πολλαπλών επιπέδων επεξεργασίας που αποτελούνται από σύνθετες δομές ή πολλαπλούς μη γραμμικούς μετασχηματισμούς. Στη μηχανική μάθηση, η βαθιά μάθηση είναι μια αλγόριθμος που βασίζεται στον χαρακτηρισμό των δεδομένων μάθησης. [32]

1.1.3.6 Convolutional Neural Networks (CNN)

Το Συνελικτικό Νευρωνικό Δίκτυο (CNN) είναι ένα προσέγγιση βαθιάς μάθησης που χρησιμοποιείται ευρέως για την επίλυση σύνθετων προβλημάτων. Ξεπερνά τους περιορισμούς των παραδοσιακών μηχανών μαθησιακών προσεγγίσεων. Το κίνητρο αυτής της μελέτης είναι να παράσχει τη γνώση και την κατανόηση διαφόρων πτυχών του CNN.

1.1.3.7 Neural Networks (NN)

Τα νευρωνικά δίκτυα, επίσης γνωστά ως τεχνητά νευρωνικά δίκτυα (ANN) ή τεχνητά παραγόμενα νευρωνικά δίκτυα (SNN), είναι ένα υποσύνολο της μηχανικής μάθησης που αποτελεί τη βάση των τεχνικών βαθιάς μάθησης. Το όνομα και η μορφή τους είναι εμπνευσμένα από τον ανθρώπινο εγκέφαλο και αναπαράγουν τον τρόπο με τον οποίο οι πραγματικοί νευρώνες επικοινωνούν μεταξύ τους. Τα τεχνητά νευρωνικά δίκτυα (ANN) είναι μαζικά παράλληλα συστήματα που αποτελούνται από έναν τεράστιο αριθμό διασυνδεδεμένων βασικών επεξεργαστών. Η παρούσα εργασία πραγματεύεται τα τεχνητά νευρωνικά δίκτυα και τους βασικούς τύπους τους. [33]

1.1.3.8 Blockchain

Το blockchain είναι ένα κατανεμημένο ηλεκτρονικό βιβλίο που διατηρεί πληροφορίες χωρίς αλλοίωση για μεγάλο χρονικό διάστημα. Συνδέεται με πολλαπλά διαφορετικά υπολογιστικά συστήματα. Το blockchain μπορεί να αποθηκεύει ευρετηριασμένες εγγραφές και να τις διασυνδέει με κοινόχρηστο τρόπο. Το blockchain είναι μια αποκεντρωμένη τεχνολογία διαχείρισης συναλλαγών και δεδομένων που αναπτύχθηκε πρώτα για το κρυπτονόμισμα Bitcoin. [22]

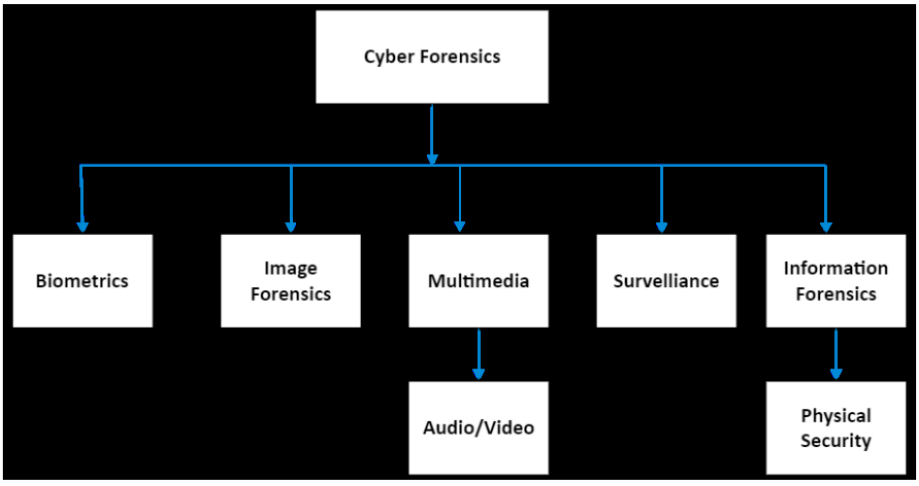
1.1.4 Κατηγορίες εφαρμογών ιατροδικαστικής στον κυβερνοχώρο

Η εγκληματολογία στον κυβερνοχώρο είναι ένα συνεχώς εξελισσόμενο επιστημονικό πεδίο με πολλούς επιμέρους κλάδους [9] όπως:

- ***Η εγκληματολογία υπολογιστών:*** Τα στοιχεία που βρίσκονται σε υπολογιστές και άλλα μέσα εντοπίζονται, διατηρούνται, συλλέγονται και αναλύονται για έρευνες και νομικές διαδικασίες. Προκειμένου να αποσαφηνιστεί η κατάσταση των ψηφιακών αντικειμένων σε πληροφοριακών συστημάτων και ηλεκτρονικών εγγράφων, χρησιμοποιεί στοιχεία του δικαίου και της επιστήμης των υπολογιστών για να εφαρμόσει διάφορες φάσεις της ψηφιακής εγκληματολογίας σε υπολογιστικούς πόρους .
- ***Εγκληματολογία δικτύων:*** Σε αυτόν τον τομέα, παρακολουθούνται, καταγράφονται, αποθηκεύονται και αναλύονται διάφορες δραστηριότητες δικτύου για την ανεύρεση της πηγής των επιθέσεων ασφαλείας, την ανίχνευση εισβολών, την ασυνήθιστη κυκλοφορία δικτύου και τις παραβιάσεις ασφαλείας. Το λογισμικό ανάλυσης εγκληματολογικών δεδομένων δικτύου μπορεί να υποστηρίξει πολλαπλές εργασίες, όπως η διερεύνηση της ασφάλειας του δικτύου, τον έλεγχο της ακεραιότητας των δεδομένων που προέρχονται από διάφορες πηγές, την πρόβλεψη πιθανών επιθέσεων, την κυκλοφορία του δικτύου ανάλυση, και καταγραφή διαφόρων τύπων ανάλυσης κίνησης βάσει εργαλείων χρήστη. Το τμήμα εγκληματολογίας δικτύου αντιμετωπίζει μια σειρά από ζητήματα, όπως προκλήσεις που σχετίζονται με τα δεδομένα και την κυκλοφορία, την ταχύτητα του δικτύου, τη χωρητικότητα αποθήκευσης, τα δεδομένα ακεραιότητα, την ιδιωτικότητα των δεδομένων και την εξαγωγή δεδομένων. Έχουν δημιουργηθεί διάφορα πλαίσια για την αντιμετώπιση αυτών των προβλημάτων όπως πλαίσια κατανεμημένων δικτύων, πλαίσιο δυναμικής εγκληματολογίας δικτύων, πλαίσιο με βάση τους μαλακούς υπολογιστές πλαίσια εγκληματολογίας δικτύου και πλαίσια εγκληματολογίας δικτύου με βάση τα γραφικά.
- ***Εγκληματολογία κινητών συσκευών:*** Είναι η μελέτη της απόκτησης και ανάλυσης αποδεικτικών στοιχείων από κινητά τηλέφωνα και κάρτες ταυτότητας συνδρομητή (κάρτες SIM). Τα έξυπνα κινητά τηλέφωνα διαθέτουν ποικίλα χαρακτηριστικά που επιτρέπουν στους χρήστες να εκτελούν σχεδόν οποιαδήποτε δραστηριότητα, όπως ηλεκτρονικές τραπεζικές συναλλαγές, κοινή χρήση φωτογραφιών, από ιδιωτική χρήση έως επαγγελματική. Προκειμένου να βοηθήσουν τον εγκληματολογικό ερευνητή να ταυτοποιήσει το πρόσωπο, να παρατηρήσει τις πρόσφατες δραστηριότητές του, τα smartphones προσφέρουν χρήσιμες πληροφορίες, όπως πρόσφατες συνομιλίες, αρχεία καταγραφής κλήσεων, στοιχεία τοποθεσίας και εικόνες.

- ***Εγκληματολογία ψηφιακών εικόνων:*** Ασχολείται με την επαλήθευση της αυθεντικότητας ψηφιακών φωτογραφικών εικόνων και ακεραιότητας. Χρησιμοποιώντας προηγμένες συσκευές, όπως τα smartphones ή οι ψηφιακές αντανακλαστικές κάμερες, ο καθένας μπορεί να καταγράψει ψηφιακές φωτογραφίες. Χρησιμοποιούνται εργαλεία επεξεργασίας φωτογραφιών για τη βελτίωσή τους και στη συνέχεια αναρτώνται σε ιστότοπους κοινωνικής δικτύωσης. Ωστόσο, αυτή η εξέλιξη της τεχνολογίας είναι δίκοπο μαχαίρι. Οι πλαστές εικόνες γίνονται όλο και πιο συχνές και μπορούμε σίγουρα να υποστηρίξουμε ότι το να βλέπεις δεν πιστεύεις πλέον, ειδικά με την χρήση τεχνικών όπως η τεχνητή νοημοσύνη (AI) και τα παραγωγικά αντιφατικά δίκτυα (GAN) που μπορούν να χρησιμοποιηθούν για τη διάδοση ψευδών ειδήσεων. Η εγκληματολογία ψηφιακών εικόνων ασχολείται με την εξαγωγή και την επαλήθευση των ακεραιότητας των μεταδεδομένων εικόνας.
- ***Εγκληματολογία πολυμέσων:*** Τα τελευταία τέσσερα χρόνια, η εγκληματολογία πολυμέσων έχει αποκτήσει μεγάλη σημασία στην έρευνες. Δύο κύριοι τομείς στους οποίους επικεντρώνεται η εγκληματολογία πολυμέσων είναι, πρώτον, η ταυτοποίηση της πηγής που αφορά την εύρεση των ψηφιακών συσκευών προέλευσης (φωτογραφικές μηχανές, κινητά τηλέφωνα και βιντεοκάμερες) με τη χρήση των πολυμέσων που δημιουργούν, και η ανίχνευση πλαστογραφίας που αποσκοπεί στον εντοπισμό σημείων παραποίησης με τον έλεγχο της νομιμότητας των ψηφιακών μέσων (κλιπ ήχου, βίντεο και εικόνων). Ελέγχει, μέσω της ανάλυσης και της αξιολόγησης, κατά πόσον ο ήχος και οι εγγραφές βίντεο είναι πρωτότυπες ή παραποιημένες.

Ας το δούμε και σε μια σχηματική απεικόνιση:



Εικόνα 1: Κατηγορίες Ψηφιακών Εγλημάτων

Το σχήμα παρουσιάζει τις κύριες κατηγορίες εφαρμογών της ψηφιακής εγκληματολογίας (DF), δηλαδή τις τεχνικές και τις μεθόδους που χρησιμοποιούνται για τη διερεύνηση ψηφιακών εγκλημάτων. Αυτές οι κατηγορίες περιλαμβάνουν τα βιομετρικά δεδομένα (Biometrics), που αναφέρονται στην αναγνώριση μέσω φυσικών χαρακτηριστικών, την εγκληματολογία εικόνας (Image Forensics), που εστιάζει στην ανάλυση και τον έλεγχο ψηφιακών εικόνων, και τα πολυμέσα (Multimedia), τα οποία περιλαμβάνουν την εξέταση ήχου και βίντεο (Audio/Video).

Επιπλέον, περιλαμβάνεται η παρακολούθηση (Surveillance), η οποία σχετίζεται με τη χρήση συστημάτων παρακολούθησης για τη συλλογή αποδεικτικών στοιχείων, και η εγκληματολογία πληροφοριών (Information Forensics), η οποία εξετάζει την προστασία και ανάλυση δεδομένων, καθώς και τη φυσική ασφάλεια (Physical Security), που ασχολείται με την προστασία φυσικών χώρων και εξοπλισμού.

1.2 Αντικείμενο διπλωματικής

Το θέμα της διπλωματικής εργασίας, «Χρήση Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης στην Εγκληματολογία», εστιάζει στη διερεύνηση και εφαρμογή τεχνολογιών τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) για την ενίσχυση και βελτίωση της διαδικασίας ψηφιακών ερευνών και ανάλυσης στοιχείων στον τομέα της εγκληματολογίας.

Η διπλωματική εργασία έχει ως κύριο στόχο την διερεύνηση και την αναζήτηση προηγμένων τεχνικών τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) για την ανάλυση δεδομένων στον τομέα της εγκληματολογίας. Πιο συγκεκριμένα, αποσκοπεί στην ανίχνευση αλγορίθμων και την ανάλυση εγκληματικών σεναρίων μέσω της χρήσης τεχνολογιών τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML).

Προβλήματα που θα λύσει:

1. **Ανάλυση μεγάλων όγκων δεδομένων:** Η επεξεργασία και ανάλυση μεγάλων δεδομένων από διάφορες πηγές ψηφιακών αποδεικτικών στοιχείων απαιτεί προηγμένες τεχνικές για την αυτοματοποίηση της διαδικασίας και την εξαγωγή συμπερασμάτων με υψηλή ακρίβεια.

   2. Ανάλυση αλγορίθμων εγκληματικής συμπεριφοράς: Η ανάλυση ενδεχόμενων εγκληματικών δραστηριοτήτων μέσω προηγμένων αλγορίθμων τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) απαιτεί την ανάπτυξη μοντέλων που να μπορούν να κατανοούν τις συνεκτικές αλληλεπιδράσεις στα δεδομένα και να αναγνωρίζουν ανωμαλίες στις συμπεριφορές.

Πώς σκοπεύει να τα λύσει:

1. **Μελέτη της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML) στην ψηφιακή εγκληματολογία:** Εξέταση του τρόπου με τον οποίο τα νευρωνικά δίκτυα και άλλα μοντέλα μηχανικής μάθησης (ML) μπορούν να αναγνωρίσουν μοτίβα και να κατανοήσουν τις αλληλεπιδράσεις στα δεδομένα, ώστε να επιτευχθεί καλύτερη ανάλυση και πρόβλεψη εγκληματικών συμπεριφορών και επιπτώσεών τους.
2. **Ανάπτυξη τεχνικών αναλυτικής εξόρυξης δεδομένων:** Μελέτη της χρήσης τεχνητής νοημοσύνης (AI) για την εξαγωγή κρίσιμων πληροφοριών από δεδομένα που έχουν συγκεντρωθεί από ψηφιακές ενέργειες, με στόχο την ανάλυση και την αναγνώριση αποκλίσεων και ανωμαλιών που μπορούν να υποδείξουν εγκληματική δραστηριότητα.

1.2.1 Εισαγωγή στην Ψηφιακή Εγκληματολογία και Έρευνες

Ο τομέας της ψηφιακής εγκληματολογίας ασχολείται με την ανάλυση ψηφιακών στοιχείων που συλλέγονται από ηλεκτρονικές συσκευές και δίκτυα, με σκοπό την παροχή αντικειμενικών δεδομένων και τη στήριξη του σχηματισμού υποθέσεων για νομική απόδειξη. Οι ψηφιακές έρευνες περιλαμβάνουν τον εντοπισμό, τη συλλογή, τη διατήρηση και την ανάλυση αυτών των στοιχείων, με στόχο την εξαγωγή χρήσιμων πληροφοριών που μπορούν να χρησιμοποιηθούν σε δικαστικές υποθέσεις ή σε έρευνες εγκλημάτων.

1.2.2 Ρόλος της Τεχνητής Νοημοσύνης και της Μηχανικής Μάθησης

Η τεχνητή νοημοσύνη και η μηχανική μάθηση έχουν αναδειχθεί ως κρίσιμα εργαλεία στην ψηφιακή εγκληματολογία. Αυτές οι τεχνολογίες προσφέρουν δυνατότητες για αυτοματοποίηση της ανάλυσης στοιχείων, βελτιώνοντας την ακρίβεια και την ταχύτητα των ερευνών.

- **Αυτόματη Ανάλυση Στοιχείων:** Χρήση Προγραμματισμού Συνόλων Απαντήσεων (ASP) για τη διαχείριση σύνθετων προβλημάτων βελτιστοποίησης, τη διατύπωση ερευνητικών υποθέσεων και το σχεδιασμό Συστημάτων Υποστήριξης Αποφάσεων (DSS).

- **Ανάλυση Μεταδεδομένων:** Επιτάχυνση των ερευνών μέσω αλγορίθμων μηχανικής μάθησης (ML) που αναλύουν μεταδεδομένα αρχείων για την ανίχνευση δραστηριοτήτων χρηστών.

- **Ενσωμάτωση σε Έξυπνες Συσκευές:** Χρήση τεχνητής νοημοσύνης (AI) σε έξυπνες συσκευές, AI ηχεία και φορητή τεχνολογία για την εξαγωγή ζωτικών στοιχείων σε εγκληματολογικές έρευνες.

- **Ταυτοποίηση Παραποιημένων Μέσων:** Βελτίωση των τεχνικών ταυτοποίησης παραποιημένων μέσων μέσω τεχνητής νοημοσύνης (AI), αντιμετωπίζοντας τις προκλήσεις που προκύπτουν από την ποικιλία των δεδομένων.

- **Ανάλυση Μεγάλων Δεδομένων:** Εφαρμογή προχωρημένων μεθόδων όπως το MapReduce και εργαλεία ανοικτού κώδικα όπως το Hadoop, το Hive και το Mahout για την αποτελεσματική ανάλυση μεγάλων δεδομένων στην Ψηφιακή Εγκληματολογία.

1.3 Κίνητρο

Υπάρχουν αρκετές δημοσιεύσεις που εξετάζουν τη χρήση τεχνητής νοημοσύνης και μηχανικής μάθησης στην εγκληματολογία. Το [1] εξετάζει τη συνδυασμένη χρήση της ψηφιακής έρευνας και της τεχνητής νοημοσύνης και προσφέρει νέες μεθόδους για την ανάλυση ψηφιακών εγκλημάτων. Με την εφαρμογή της τεχνητής νοημοσύνης (AI), η διαδικασία εντοπισμού και διερεύνησης εγκληματικών δραστηριοτήτων στο διαδίκτυο γίνεται πιο αποτελεσματική και ακριβής, βελτιώνοντας έτσι την κατανόηση και την ανάλυση αυτών των εγκλημάτων. Σε πιο συγκεκριμένο επίπεδο, το [2] εστιάζει στην εφαρμογή της τεχνητής νοημοσύνης (AI) στη δικτυακή ασφάλεια και την ανίχνευση εγκλημάτων, ενώ το [3] μελετά τη χρήση αλγορίθμων μηχανικής μάθησης στην ανάλυση μεταδεδομένων αρχείων στην ψηφιακή δικαστική.

Επιπλέον, το [5] αναλύει την εφαρμογή της μηχανικής μάθησης για την κατηγοριοποίηση επιθέσεων σε περιβάλλον νέφους δικτύων, ενώ το [13] εξετάζει τις πρακτικές και μεθοδολογίες ψηφιακής δικαστικής για τα οικοσυστήματα τεχνητής νοημοσύνης.

1.4 Συμβολή

Το πρώτο βήμα για την ανάπτυξη μιας ολοκληρωμένης προσέγγισης για την εφαρμογή της τεχνητής νοημοσύνης και της μηχανικής μάθησης στην εγκληματολογία είναι η χαρτογράφηση, ανάλυση και κατανόηση των σύγχρονων εγκληματικών προκλήσεων και των σημείων ευπάθειας σε αυτόν τον τομέα. Καθώς αντιμετωπίζουμε επιθέσεις και παραβάσεις στον τομέα της εγκληματολογίας, είναι ζωτικής σημασίας να αναλυθούν οι τεχνικές και οι μέθοδοι που χρησιμοποιούνται από τους εισβολείς, καθώς και να εξεταστούν οι κοινές τάσεις και παραδείγματα περιστατικών σε διάφορα επίπεδα ανάλυσης. Αφού προσδιοριστούν οι προκλήσεις και τα ευάλωτα σημεία, είναι σημαντικό να αξιολογηθεί η σοβαρότητα και η επίπτωση κάθε είδους επίθεσης, καθώς και να αναπτυχθούν μοντέλα μηχανικής μάθησης για την πρόβλεψη και την αντιμετώπιση μελλοντικών εγκληματικών ενεργειών.

Η εφαρμογή της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML) στην ψηφιακή εγκληματολογία έχει επιταχύνει σημαντικά την ανάλυση δεδομένων και την εξαγωγή αποδεικτικών στοιχείων μετά από μια επίθεση. Η χρήση αλγορίθμων μηχανικής μάθησης για την ανάλυση μεταδεδομένων αρχείων [3] αποδεικνύεται κρίσιμη για την εξαγωγή πειστηρίων από μεγάλα σύνολα δεδομένων, ενώ άλλες μελέτες προτείνουν πλαίσια για την ταξινόμηση επιθέσεων σε περιβάλλοντα νέφους χρησιμοποιώντας τεχνολογίες ML και ψηφιακής εγκληματολογίας [5]. Τεχνολογίες blockchain και επεξηγήσιμη τεχνητής νοημοσύνης (XAI) έχουν επίσης αναδειχθεί ως βασικά εργαλεία για τη διαφάνεια και την ακεραιότητα της ανάλυσης [19].

Η επεξηγήσιμη τεχνητή νοημοσύνη (XAI), είναι μια αναδυόμενη ερευνητική περιοχή που σχετίζεται με στη δημιουργία αλγορίθμων μηχανικής μάθησης (ML) από τους οποίους θα εξηγούνται τα αποτελέσματα και οι έξοδοι που παρέχονται.

Σημαντικές προσεγγίσεις για την ανάλυση δεδομένων IoT και κινητών συσκευών [6][12], σε συνδυασμό με την αξιοποίηση τεχνολογιών ανοικτού κώδικα, όπως το Hadoop, την Hive Query Language (HQL), το Mahout, την R, και το προγραμματιστικό μοντέλο της Google, που δουλεύει πάνω σε αυτά, το MapReduce [17], συμβάλλουν στην αποτελεσματική διαχείριση και ανάλυση μεγάλων δεδομένων στην ψηφιακή εγκληματολογία. Έτσι, η χρήση προηγμένων τεχνικών μηχανικής μάθησης προσφέρει σημαντική υποστήριξη στην ανάλυση πειστηρίων, εξασφαλίζοντας πιο ακριβή και αξιόπιστα αποτελέσματα, σύμφωνα με την επιστημονική έρευνα στον τομέα αυτό.

Το Hadoop, έχει δομή που βασίζεται στην κατανεμημένη συστάδα πολλαπλών κόμβων, που λειτουργούν συντονισμένα, αποθηκεύουν και επεξεργάζονται τα μεγάλα δεδομένα. Δηλαδή, η δομή ελέγχου του πλαισίου βασίζεται στην αρχιτεκτονική πελάτη-εξυπηρετητή (client-server).

Το μοντέλο MapReduce λειτουργεί με βάση την αρχιτεκτονική Hadoop για την κατανεμημένη επεξεργασία των μεγάλων δεδομένων στη συστάδα, στην οποία προγραμματίζεται με τη χρήση γλωσσών java ή python.

Η Hive, είναι μια γλώσσα ερωτημάτων που μοιάζει με SQL(Structured Query Language - Σχεδιάστηκε για τη διαχείριση δεδομένων,) και ονομάζεται HQL (Hive Query Language). Στην HQL, τα ερωτήματα μετατρέπονται σε κατανεμημένα σενάρια MapReduce που εργάζονται, παράλληλα για την υποβολή ερωτημάτων στις αποθήκες δεδομένων του συμπλέγματος Hadoop.

Το Apache Mahout είναι κλιμακούμενο εργαλείο μηχανικής μάθησης (ML) ανοικτού κώδικα που λειτουργεί με υποδομή Hadoop. Προκειμένου να αντιμετωπιστεί ο περιορισμός των 3 V των μεγάλων δεδομένων (Ο όγκος, η ποικιλία και η ταχύτητα έχουν γίνει ευρέως αποδεκτές ως οι βασικές προκλήσεις διαχείρισης δεδομένων που σχετίζονται με τα Μεγάλα Δεδομένα) με την υπάρχοντα εργαλεία μηχανικής μάθησης (ML), το Hadoop επέκτεινε τις δυνατότητες επεξεργασίας και αποθήκευσης για τη βελτιστοποίηση του κριτηρίου χρησιμοποιώντας παλαιότερα δεδομένα. Λόγω της εισαγωγής του mahout στον τομέα της μηχανικής μάθησης (ML), περιορίζεται σε λίγα μοντέλα που μπορεί να είναι καλά για έναν τύπο δεδομένων και όχι για άλλους.

Τέλος, η γλώσσα R που χρησιμοποιείται στο [17] είναι για τη σύγκριση και την επικύρωση του μοντέλου που επιλέχθηκε. Η R είναι μια διαγραμματικά (ιδιαίτερα γραφική) γλώσσα στατιστικών υπολογισμών. Μπορεί επίσης να διασυνδεθεί με άλλες γλώσσες και εργαλεία αποσφαλμάτωσης, καθιστώντας την αρκετά απλό και φιλικό προς τον χρήστη περιβάλλον εργασίας .

1.5 Σκοπός διπλωματικής εργασίας

Η διπλωματική εργασία στοχεύει στο να εξετάσει πώς η τεχνητή νοημοσύνη και η μηχανική μάθηση μπορούν να συμβάλουν στη βελτίωση της διαδικασίας ανάλυσης ψηφιακών πειστηρίων μετά από επιθέσεις. Τα βασικά προβλήματα που θα αντιμετωπιστούν είναι η δυσκολία στην ανάλυση μεγάλων και ετερογενών συνόλων δεδομένων, καθώς και η έλλειψη αποτελεσματικών εργαλείων για την εξαγωγή και κατηγοριοποίηση πειστηρίων που προκύπτουν από κυβερνοεπιθέσεις και άλλες εγκληματικές δραστηριότητες.

Η εργασία προτείνει τη χρήση προηγμένων αλγορίθμων μηχανικής μάθησης για την αυτόματη επεξεργασία δεδομένων και την κατηγοριοποίηση των αποδεικτικών στοιχείων που σχετίζονται με εγκληματικές ενέργειες. Η εφαρμογή των τεχνολογιών αυτών θα επιτρέψει την αποτελεσματική ανάλυση μεγάλου όγκου δεδομένων που συλλέγονται από συστήματα όπως IoT συσκευές και έξυπνα δίκτυα, με σκοπό την εξαγωγή των πιο σημαντικών πειστηρίων για την εγκληματολογική έρευνα.

Επιπλέον, η εργασία θα εστιάσει στη χρήση εξηγητικής τεχνητής νοημοσύνης (XAI) για την εξασφάλιση της διαφάνειας και της αξιοπιστίας των συμπερασμάτων που προκύπτουν από την ανάλυση, καθώς και στην χρήση διαφόρων εργαλειών και γλωσσων προγραμματισμού. Η ενσωμάτωση τεχνολογιών blockchain θα παρέχει επιπρόσθετη ασφάλεια στην καταγραφή και διαχείριση των πειστηρίων. Στόχος είναι να αναπτυχθεί ένα ενιαίο πλαίσιο που θα επιτρέπει στους ερευνητές να αναλύουν πιο αποδοτικά τα δεδομένα που συλλέγονται μετά από μια επίθεση και να εξάγουν τα πιο ουσιαστικά πειστήρια με ακρίβεια και αξιοπιστία.

1.6 Δομή της διπλωματικής

Η διπλωματική εργασία είναι δομημένη σε πέντε κύρια κεφάλαια, καθένα από τα οποία συμβάλλει στην ολοκληρωμένη παρουσίαση και ανάλυση του θέματος της "Χρήσης Τεχνητής Νοημοσύνης και Μηχανικής Μάθησης στην Εγκληματολογία".

Κεφάλαιο 1: Εισαγωγή

Στο πρώτο κεφάλαιο γίνεται μια γενική εισαγωγή στο αντικείμενο της διπλωματικής εργασίας. Περιλαμβάνει τη σημασία και το σκοπό της μελέτης, το πλαίσιο μέσα στο οποίο εντάσσεται, καθώς και μια σύνοψη των ερευνητικών στόχων και ερωτημάτων που θα απαντηθούν.

Κεφάλαιο 2: Μεθοδολογία Εργασίας

Στο τρίτο κεφάλαιο συζητούνται οι θεωρητικές βάσεις και τα μοντέλα που χρησιμοποιούνται για την ανάλυση των δεδομένων. Περιγράφονται οι μέθοδοι και οι αλγόριθμοι που εφαρμόζονται, καθώς και τα εργαλεία και τα λογισμικά που χρησιμοποιούνται. Επίσης, παρουσιάζεται η διαδικασία συλλογής και επεξεργασίας των δεδομένων.

Κεφάλαιο 3: Ανασκόπηση Βιβλιογραφίας

Αυτό το κεφάλαιο περιλαμβάνει μια ανασκόπηση της υπάρχουσας βιβλιογραφίας και των σχετικών ερευνών που έχουν γίνει στον τομέα της χρήσης της τεχνητής νοημοσύνης και της μηχανικής μάθησης στην εγκληματολογία. Παρουσιάζονται και συγκρίνονται διάφορες μεθοδολογίες και προσεγγίσεις.

Κεφάλαιο 4: Ανάλυση των Ομάδων που Συμπεριλαμβάνονται στην Εργασία

Αυτό το κεφάλαιο εστιάζει στην ανάλυση των δεδομένων και των αποτελεσμάτων που προέκυψαν από την εφαρμογή των τεχνικών και μεθόδων της μελέτης. Παρουσιάζονται οι ομάδες δεδομένων που χρησιμοποιήθηκαν, οι τεχνικές ανάλυσης και τα ευρήματα που προέκυψαν από την επεξεργασία των δεδομένων.

Κεφάλαιο 5: Σύνοψη και Ανάλυση

Στο πέμπτο κεφάλαιο παρουσιάζονται τα τελικά συμπεράσματα της διπλωματικής εργασίας. Γίνεται μια εκτενής ανάλυση των ευρημάτων, συζητούνται οι πιθανές ερμηνείες και προτείνονται βελτιώσεις και μελλοντικές έρευνες. Επιπλέον, αναφέρονται οι προκλήσεις που αντιμετωπίστηκαν και οι λύσεις που προτάθηκαν.

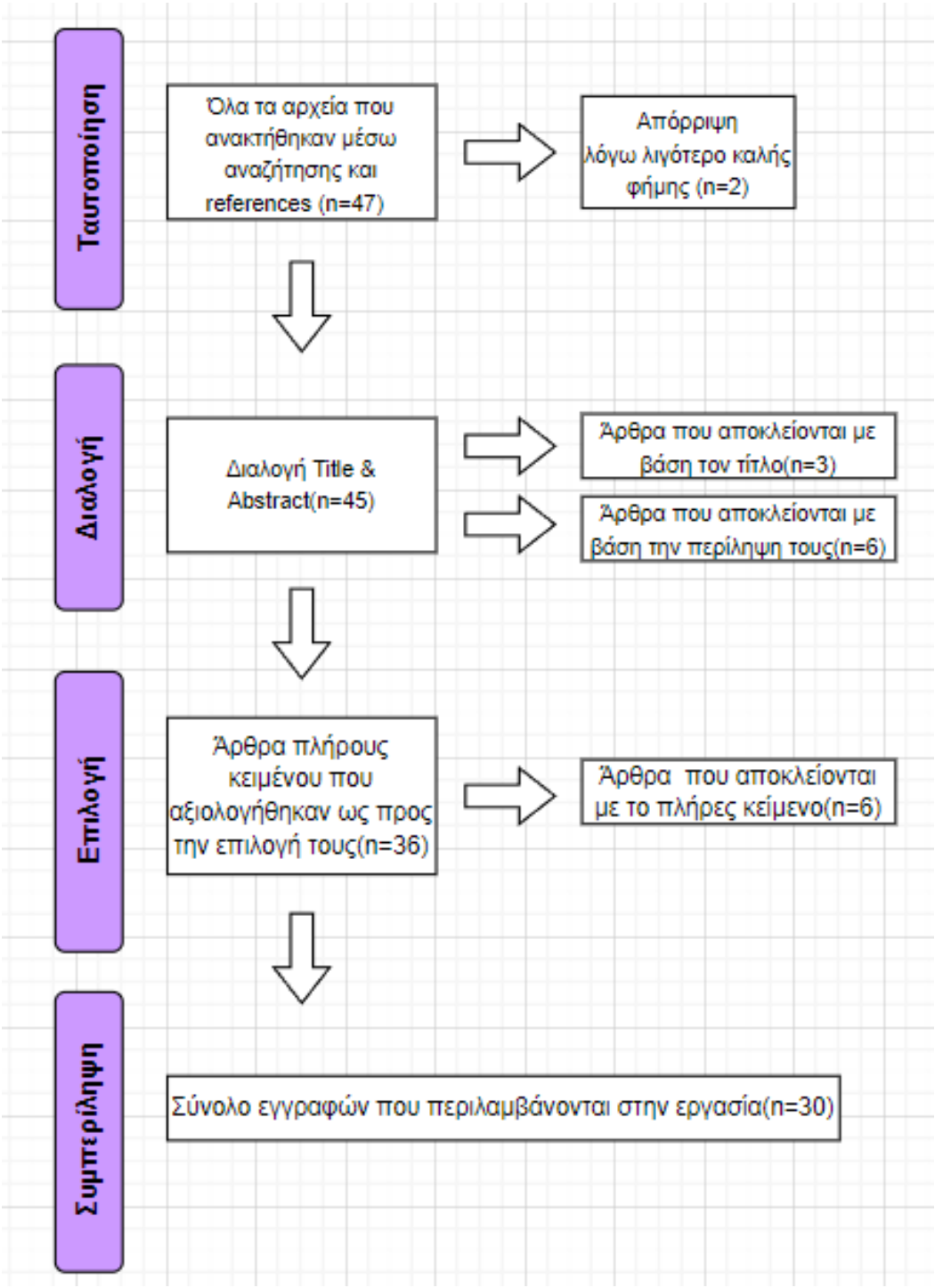
2

Μεθοδολογία εργασίας

Η μέθοδος που χρησιμοποιήθηκε για την ανάπτυξη αυτής της διπλωματικής εργασίας, περιλαμβάνει 4 βήματα: (1) Ανάπτυξη του πρωτοκόλλου και του πεδίου εφαρμογής της έρευνας, (2) Αναζήτηση και εντοπισμός επιλεγμένων μελετών με βάση (3) Διαλογή της βιβλιογραφίας με βάση την ποιότητα, και (4) Αναφορά (εξαγωγή πληροφοριών, σύνθεση και αναφορά των αποτελεσμάτων).

Στο Σχήμα 1 που φαίνεται παρακάτω, απεικονίζεται το συνολικό πλαίσιο της εργασίας και περιγράφει το πώς γίνεται κάθε προαναφερθέν βήμα. Η παρούσα προσέγγισή της διπλωματικής εργασίας είναι βασίζεται στη μεθοδολογία έρευνας που παρουσιάζεται στο [10] , [15] , [29] & [30].

Πρώτον, συγκέντρωσα όλα τα έγγραφα που εντόπισα τόσο από τον ερευνητικό χώρο, όσο και από την γκρίζα βιβλιογραφία (grey literature- εκθέσεις, δημοσιεύσεις εταιρειών κ.λπ.), τα οποία ήταν (47) στο σύνολό τους. Στη συνέχεια από όλα αυτά τα άρθρα, εξαιρέθηκαν τα αυτά που έχουν εκδοθεί από οίκους λιγότερο καλής φήμης (2). Ορισμένα άρθρα αποκλείστηκαν με βάση τον τίτλο (3), ενώ άλλα αποκλείστηκαν κατά την ανάγνωση την περίληψή τους (9) ή το πλήρες κείμενο (3). Πιο συνηθισμένο ζήτημα που αντιμετωπίστηκε ήταν η ανίχνευση πληροφοριών που είναι στενά συνδεδεμένες με την ψηφιακή εγληματολογία, και όχι σε ένα γενικό σύστημα. Η τελική συμπερίληψη αφορούσε 30 άρθρα, συν κάποια συμπληρωματικά άρθρα, τα οποία ήταν για την επεξήγηση κάποιων εννοιών.



Εικόνα 2: Επισκόπηση της μεθοδολογίας της εργασίας.

2.1 Κατηγορίες άρθρων

2.1.1 Γενική επισκόπιση

Οι **«Έρευνες» (Survey)** περιλαμβάνουν συστηματικές ανασκοπήσεις που συγκεντρώνουν και αναλύουν τα υπάρχοντα δεδομένα και τις τάσεις στον τομέα της μηχανικής μάθησης και τεχνητής νοημοσύνης στην ψηφιακή εγκληματολογία. Αυτές οι δημοσιεύσεις παρέχουν μια ευρεία εικόνα των υφιστάμενων τεχνικών και μεθόδων, καθιστώντας τες χρήσιμες για την κατανόηση του τρέχοντος ερευνητικού τοπίου και την αναγνώριση κενών στη βιβλιογραφία.

Τα **«Πολυμέσα» (Multimedia)** εξετάζουν την ασφάλεια και την προστασία των διάφορων τύπων πολυμέσων, όπως εικόνες και βίντεο, από επιθέσεις και παραβιάσεις, καθώς και την ανάλυση αυτών των δεδομένων για την ανίχνευση κακόβουλων δραστηριοτήτων. Οι έρευνες σε αυτόν τον τομέα επικεντρώνονται στις μεθόδους αναγνώρισης ανωμαλιών και την εφαρμογή της τεχνητής νοημοσύνης για την βελτίωση της ασφάλειας των πολυμέσων.

Οι **«Κινητές Συσκευές» (Mobile devices)** εστιάζουν στις προκλήσεις και τις λύσεις για την ασφάλεια και την ανάλυση δεδομένων από smartphones και tablets. Αυτές οι δημοσιεύσεις διερευνούν τις απειλές που αντιμετωπίζουν οι κινητές συσκευές, όπως η κακόβουλη λογισμική και οι επιθέσεις δικτύου, και προτείνουν μεθόδους ανίχνευσης και πρόληψης με τη χρήση τεχνικών μηχανικής μάθησης.

Οι **«Κυβερνοεπιθέσεις» (Cyberattacks)** αναλύουν τους διάφορους τύπους επιθέσεων, τις μεθόδους ανίχνευσης και την αντιμετώπισή τους. Οι δημοσιεύσεις αυτές περιλαμβάνουν έρευνες σχετικά με την ανίχνευση και την πρόληψη των επιθέσεων, καθώς και την ανάλυση των δεδομένων που σχετίζονται με αυτές, χρησιμοποιώντας τεχνητή νοημοσύνη και τεχνικές ανάλυσης δεδομένων για να βελτιώσουν την απόκριση και την ανθεκτικότητα στις κυβερνοεπιθέσεις.

Το **«Υπολογιστικό Νέφος» (Cloud)** διερευνά τις απειλές και τις λύσεις ασφάλειας για το cloud computing. Οι έρευνες αυτές εστιάζουν στην προστασία των δεδομένων και των εφαρμογών που φιλοξενούνται στο σύννεφο, χρησιμοποιώντας μηχανική μάθηση για την ανίχνευση ανωμαλιών και την πρόληψη παραβιάσεων ασφαλείας, καθώς και στην ανάλυση μεγάλων δεδομένων που παράγονται από τις υπηρεσίες cloud.

Οι **«Αλγόριθμοι» (Algorithms)** περιλαμβάνουν μελέτες που προτείνουν νέες ή βελτιωμένες μεθόδους κρυπτογράφησης και ανίχνευσης ανωμαλιών. Οι δημοσιεύσεις αυτές επικεντρώνονται στην ανάπτυξη αλγορίθμων μηχανικής μάθησης και τεχνητής νοημοσύνης που μπορούν να εφαρμοστούν στην ανάλυση δεδομένων για την ανίχνευση και την πρόληψη κακόβουλων δραστηριοτήτων.

Η **«Δικανική Ανάλυση Δικτύου» (Network Forensics)** εστιάζει στις τεχνικές και τα εργαλεία που χρησιμοποιούνται για την ανάλυση και την παρακολούθηση δικτύων με στόχο την ανίχνευση και την απόκριση σε κυβερνοεπιθέσεις. Αυτές οι δημοσιεύσεις αναλύουν τα δεδομένα δικτύου για να εντοπίσουν ίχνη επιθέσεων και να βοηθήσουν στη διενέργεια εγκληματολογικών ερευνών.

Η κατηγορία **«Botnet»** εξετάζει την ανίχνευση και την αντιμετώπιση αυτών των δικτύων κακόβουλου λογισμικού. Οι δημοσιεύσεις αυτές εστιάζουν στην αναγνώριση των μοτίβων επικοινωνίας των botnets και την εφαρμογή τεχνικών μηχανικής μάθησης για την ανάλυση και την αποτροπή της διάδοσής τους.

Οι **«Ανασκοπήσεις» (Review)** περιλαμβάνουν λεπτομερείς επισκοπήσεις της βιβλιογραφίας σε διάφορα θέματα μηχανικής μάθησης και τεχνητής νοημοσύνης στην ψηφιακή εγκληματολογία. Αυτές οι δημοσιεύσεις παρέχουν μια συνολική εικόνα των ερευνών και των προκλήσεων στον τομέα, επιτρέποντας την αναγνώριση των κύριων τάσεων και των μελλοντικών κατευθύνσεων έρευνας.

Το **«Διαδίκτυο των Πραγμάτων» (IoT)** εξετάζει τις προκλήσεις ασφάλειας που σχετίζονται με τις συνδεδεμένες συσκευές και την προστασία τους από επιθέσεις. Οι δημοσιεύσεις αυτές αναλύουν τα δεδομένα από τις συσκευές IoT για να εντοπίσουν ανωμαλίες και να εφαρμόσουν τεχνικές μηχανικής μάθησης για την πρόληψη και την απόκριση σε απειλές.

Οι **«Καταγραφές» (Logs)** και τα **«Εργαλεία» (Tools)** παρέχουν πληροφορίες για την παρακολούθηση και την ανάλυση συμβάντων ασφάλειας. Οι έρευνες αυτές επικεντρώνονται στη χρήση και την ανάπτυξη εργαλείων που αξιοποιούν την ανάλυση δεδομένων για την ανίχνευση και την αντιμετώπιση κακόβουλων δραστηριοτήτων.

Οι **«Πρακτικές» (Practice)** επικεντρώνονται σε συγκεκριμένες εφαρμογές και τεχνικές για την αποτροπή και την αντιμετώπιση κακόβουλων ενεργειών. Οι δημοσιεύσεις αυτές περιλαμβάνουν μελέτες περιπτώσεων και βέλτιστες πρακτικές που εφαρμόζουν μηχανική μάθηση και τεχνητή νοημοσύνη για την ενίσχυση της ασφάλειας και της ανάλυσης δεδομένων.

Τέλος, το **«ransomware»** είναι κακόβουλο λογισμικό που κρυπτογραφεί τα δεδομένα του θύματος και απαιτεί λύτρα για την αποκατάσταση της πρόσβασης. Διαδίδεται μέσω κακόβουλων email, μολυσμένων ιστότοπων και εκμετάλλευσης κενών ασφαλείας. Για προστασία, συνιστάται η τακτική δημιουργία αντιγράφων ασφαλείας, η ενημέρωση λογισμικού, η εκπαίδευση των χρηστών και η χρήση λογισμικού προστασίας από κακόβουλο λογισμικό.

2.2 Στόχοι και στρατηγική

Η εργασία αποσκοπεί στην ανάλυση των ευπαθειών και της κυβερνοασφάλειας που σχετίζονται με τη χρήση και εφαρμογή τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML), εστιάζοντας στην κατανόηση των υποκείμενων ζητημάτων μέσω της ανάλυσης δεδομένων και της ανακάλυψης αποδεικτικών στοιχείων. Στόχος είναι η αξιολόγηση της αποτελεσματικότητας των τεχνολογιών αυτών στη διαδικασία ανάλυσης δεδομένων, καθώς και η ανάπτυξη μιας ταξινόμησης ευπάθειας που θα υποστηρίξει την ανάλυση και την ανακάλυψη αποδεικτικών στοιχείων.

Η εργασία περιλαμβάνει μια εκτενή ανασκόπηση των διαθέσιμων ταξινομιών ευπάθειας και της επίδρασης των τεχνολογιών τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) στις στρατηγικές κυβερνοασφάλειας, εξετάζοντας πώς συμβάλλουν στην ανάλυση και εντοπισμό ευπαθειών, και αναλύει τα υποκείμενα ζητήματα που προκύπτουν από καταγεγραμμένες επιθέσεις. Επιπλέον, θα προταθούν στρατηγικές βελτίωσης για την ενίσχυση της ασφάλειας, εστιάζοντας στα κενά εφαρμογής και τις περιοχές που χρήζουν βελτίωσης, με σκοπό την

ανάπτυξη πιο αποτελεσματικών αμυντικών μέτρων και την αναβάθμιση της διαδικασίας ανάλυσης αποδεικτικών στοιχείων. Οι στόχοι μαζί με τα ερευνητικά ερωτήματα που τους υποστηρίζουν παρουσιάζονται στον πίνακα 2 που φαίνεται παρακάτω.

Ο πίνακας (Πίνακας 1) απεικονίζει την έρευνά μας στόχος, το σχετικό ερώτημα που τέθηκε για την επίτευξη του στόχου αυτού και τις σχετικές αναζητήσεις με λέξεις-κλειδιά που χρησιμοποιήθηκαν για τον εντοπισμό σχετικού υλικού. Οι αναζητήσεις λέξεων-κλειδιών βασίστηκαν αρχικά στον τίτλο ***TITLE*** κάθε άρθρου, και εξειδικεύτηκαν περαιτέρω με την αναζήτηση στο ***ABSTRACT*** κάθε δημοσίευσης που εντοπίστηκε.

Προκειμένου να έχουμε μια πιο πρόσφατη προσέγγιση, όλα τα άρθρα που θα συμπεριλάβω στην παρούσα εργασία, ξεκινούν με πιο παλιό το [18] με ημερομηνία δημοσίευσης 5 Μαΐου 2017, και με πιο πρόσφατο το [10] και το [14] με ημερομηνία δημοσίευσης τον Ιανουάριο 2024.

Οι μηχανές αναζήτησης που χρησιμοποιήθηκαν περιλάμβαναν τις Scopus, IEEE Xplore, Google και Google Scholar. Οι IEEE Xplore, Google Scholar και Scopus χρησιμοποιήθηκαν για την ανίχνευση επιστημονικής βιβλιογραφίας, ενώ η Google χρησιμοποιήθηκε για τον εντοπισμό διεθνών προτύπων, τεχνικών εκθέσεων, βέλτιστων πρακτικών του κλάδου και άρθρων σχετικά με επιθέσεις στον κυβερνοχώρο και σχετικά περιστατικά στη βιομηχανία.

Οι εκδοτικοί οίκοι και τα περιοδικά που έχουν δημοσιεύσει τα άρθρα που επιλέχθηκαν είναι οι εξής: Springer, IEEE, ICIITB, SciencePB, IRJET, Elsevier, MDPI, IJECE και Informatica. Ο Springer είναι ένας από τους μεγαλύτερους εκδοτικούς οίκους στον τομέα των επιστημών, της τεχνολογίας και της ιατρικής, ενώ ο IEEE(Institute of Electrical and Electronics Engineers) είναι κορυφαίος επαγγελματικός οργανισμός για την ηλεκτρολογία και την ηλεκτρονική, δημοσιεύοντας πλήθος επιστημονικών περιοδικών και προτύπων. Ο ICIITB(International Conference on Innovative Trends in Computer and Information Technology) εστιάζει στις καινοτόμες τάσεις στην πληροφορική και την τεχνολογία πληροφοριών, ενώ ο SciencePB καλύπτει διάφορα επιστημονικά πεδία μέσω περιοδικών και βιβλίων. Το IRJET(International Research Journal of Engineering and Technology) δημοσιεύει ερευνητικά άρθρα στον τομέα της μηχανικής και της τεχνολογίας, με έμφαση στις καινοτόμες έρευνες. Ο Elsevier είναι γνωστός για την εκτεταμένη γκάμα επιστημονικών, τεχνικών και ιατρικών περιοδικών και βιβλίων που δημοσιεύει, ενώ ο MDPI(Multidisciplinary Digital Publishing Institute) προωθεί την ανοικτή πρόσβαση στην επιστημονική γνώση μέσω πολυεπιστημονικών περιοδικών. Το IJECE(International Journal of Electrical and Computer Engineering) δημοσιεύει έρευνες στους τομείς της ηλεκτρολογίας και της πληροφορικής, και το Informatica εστιάζει στις πληροφορικές επιστήμες και την τεχνολογία, δημοσιεύοντας άρθρα που συμβάλλουν στην προώθηση της γνώσης και της έρευνας στον τομέα αυτό. Όλοι αυτοί οι εκδοτικοί οίκοι είναι αναγνωρισμένοι για την ποιότητα και την αξιοπιστία των δημοσιεύσεών τους, παρέχοντας έγκριτες πηγές πληροφοριών για ερευνητές και επαγγελματίες σε διάφορους επιστημονικούς και τεχνολογικούς τομείς.

Οι αναζητήσεις πραγματοποιήθηκαν με τη χρήση ποικιλίας λέξεων-κλειδιών και συνδυασμών τους, οι οποίες επανεξετάστηκαν και βελτιώθηκαν ανάλογα με τα αποτελέσματα που προέκυψαν. Η γκρίζα βιβλιογραφία (grey literature) και σχετικά άρθρα επιλέχθηκαν δειγματοληπτικά από ένα σύνολο 50+ αποτελεσμάτων από το Google. Επιπλέον, άρθρα εντοπίστηκαν μέσω των παραπομπών των βασικών άρθρων που προέκυψαν από τις αναζητήσεις.

Επιπρόσθετες παραπομπές εξήχθησαν επίσης από τον αλγόριθμο του Google Scholar, ο οποίος προτείνει σχετική βιβλιογραφία για κάθε αναζήτηση.

Πίνακας 1:Χαρακτηριστικά της μεθοδολογίας της έρευνας.

Στόχος	**Ερώτηση**	**Λέξεις-κλειδιά**	**Τύπος βιβλιογραφίας**
Χρήση μηχανικής μάθησης στην ψηφιακή εγληματολογία	Πως χρησιμοποιείται η μηχανική μάθηση στην ψηφιακή εγληματολογία;	TITLE («machine learning» Ή «ML» Ή «digital forensics» Ή «DF» Ή «machine learning in digital forensics» Ή «use of machine learning in digital forensics ») ABSTRACT («machine learning» Ή «digital science» Ή «cyber-crime» Ή «digital forensics»)	Research Grey literature
Χρήση τεχνητής νοημοσύνης στην ψηφιακή εγληματολογία	Πως χρησιμοποιείται η τεχνητή νοημοσύνη στην ψηφιακή εγληματολογία;	TITLE («artificial intelligence» Ή «AI» Ή «digital forensics» Ή «DF» Ή «artificial intelligence in digital forensics» Ή «use of artificial intelligence in digital forensics ») ABSTRACT («artificial intelligence» Ή «digital science» Ή «cyber-crime»)	Research Grey literature

Χρήση μηχανικής μάθησης στην ανάλυση των δεδομένων στην ψηφιακή εγληματολογία	Πως χρησιμοποιείται η μηχανική μάθηση στην ανάλυση των δεδομένων;	TITLE («machine learning» Ή «ML» Ή «digital forensics» Ή «DF» Ή «machine learning in digital forensics» Ή «algorithms»Ή «data analysis» Ή « machine learning in digital forensic analysis ») ABSTRACT («machine learning» Ή «digital science» Ή «cyber-crime» Ή «digital forensics» Ή «analysis»)	Research Grey literature
Χρήση τεχνητής νοημοσύνης στην ανάλυση των δεδομένων ψηφιακή εγληματολογία	Πως χρησιμοποιείται η τεχνητή νοημοσύνη στην ανάλυση των δεδομένων;	TITLE («artificial intelligence» Ή «AI» Ή «digital forensics» Ή «DF» Ή «artificial intelligence in digital forensics» Ή «algorithms»Ή «data analysis» Ή «use of artificial intelligence in digital forensics analysis ») ABSTRACT («artificial intelligence» Ή «digital science» Ή «cyber-crime» Ή «analysis»)	Research Grey literature
Ψηφιακή εγληματολογία	Που συναντάμε την ψηφιακή εγκληματολογία;	TITLE («big data analytics» Ή	Research Grey literature

		«dataset of photos and videos» Ή «file metadata» Ή «extraction» Ή «Network forensics» Ή « computing technics» Ή « IoT») ABSTRACT («photos and videos manipulation» Ή «deepfake» Ή «cloud» Ή «Logs» Ή «Multimedia» Ή «Ransomware»)	

2.3 Δημοσιεύσεις και grey literature

Τα ερωτήματα αναζήτησης οδήγησαν στη συγκέντρωση πλήθους δημοσιεύσεων και βιβλιογραφίας. Για να αξιολογηθεί η εγκυρότητα του περιεχομένου και να μειωθεί ο συνολικός όγκος των άρθρων, τέθηκαν ορισμένα κριτήρια συμπερίληψης και αποκλεισμού. Τα κριτήρια αποκλεισμού εφαρμόστηκαν πριν, κατά τη διάρκεια, και μετά τον έλεγχο τίτλων και περιλήψεων, με τελική αξιολόγηση κατά την ανάγνωση του πλήρους κειμένου.

Η διαδικασία επιλογής των άρθρων και δημοσιεύσεων πληρούσε τα ακόλουθα κριτήρια ένταξης: (α) συνάφεια του τίτλου, (β) αξιολόγηση της περίληψης και της εισαγωγής για χρήσιμο και σχετικό περιεχόμενο, και (γ) ανάγνωση του πλήρους κειμένου κάθε άρθρου και δημοσίευσης.

Τα κριτήρια αποκλεισμού περιλάμβαναν: (α) ερευνητικές εργασίες, κεφάλαια βιβλίων και επιστημονικά άρθρα χωρίς διαδικασίες αξιολόγησης από ομοτίμους, (β) άρθρα ή εργασίες από εκδοτικούς οίκους «κακής φήμης», (γ) άρθρα χωρίς περιλήψεις και εισαγωγή, (δ) άσχετες δημοσιεύσεις, και (ε) γενικά άρθρα χωρίς ειδικές περιγραφές.

Συναφείς έρευνες ήταν εάν: (i) αφορούσαν την ασφάλεια του ICS και είχαν παρόμοιο στόχο και πεδίο εφαρμογής ή (ii) σχετίζονταν άμεσα ή έμμεσα με την ασφάλεια στον κυβερνοχώρο του τομέα μας, δηλαδή του χώρου της ψηφιακής εγληματολογίας με την χρήση τεχνητών μέσων .

Οποιαδήποτε άρθρα ή δημοσιεύσεις πληρούσαν έναν από τους λόγους αποκλεισμού απορρίφθηκαν. Η ανάγνωση του πλήρους κειμένου ορισμένων άρθρων και εκθέσεων οδήγησε επίσης στον αποκλεισμό τους, καταγράφοντας τους λόγους αποκλεισμού τους. Ο πίνακας (Πίνακας 2) συνοψίζει τα παραπάνω.

Πίνακας 2: Κριτήρια συμπερίληψης και αποκλεισμού της εργασίας.

<table>
<tr><td>Κριτήρια ένταξης άρθρων</td><td colspan="2">Εργασίες και δημοσιεύσεις με αξιολόγηση από ομότιμους
Άρθρα και έρευνες από αξιόπιστους συγγραφείς
Δημοσιεύσεις από αναγνωρισμένους φορείς και οργανισμούς
Άρθρα σε διεθνώς αποδεκτούς εκδοτικούς οίκους και περιοδικά</td></tr>
<tr><td rowspan="3">Κριτήρια αποκλεισμού άρθρων</td><td rowspan="2">Πριν την ανάγνωση</td><td>~ Research papers, book chapters and scientific articles
~ Άρθρα από κακόφημους οίκους
~ Άρθρα που δεν έχουν περίληψη και εισαγωγή</td></tr>
<tr><td rowspan="2">~ Άσχετες δημοσιεύσεις</td></tr>
<tr><td>Κατά τη διάρκεια της ανάγνωσης της περίληψης και της εισαγωγής</td></tr>
<tr><td>Κατά την ανάγνωση του πλήρους κειμένου</td><td>~ Ειδησεογραφικά άρθρα και δημοσιεύσεις χωρίς παραπομπές
~ Οι συγγραφείς δεν είναι μέλη της σχετικής επιστημονικής ή βιομηχανικής κοινότητας
~ Γενικά άρθρα σχετικά με την ασφάλεια ή τις επιθέσεις στον κυβερνοχώρο χωρίς ειδικές περιγραφές</td></tr>
</table>

3

Ανασκόπηση της βιβλιογραφίας

3.1 Εισαγωγή

Υπάρχουν πολυάριθμες δημοσιεύσεις, τόσο στην ερευνητική όσο και στην γκρίζα βιβλιογραφία (grey literature), που εξετάζουν διάφορες πτυχές της χρήσης τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης (ML) στην εγκληματολογία.

Υπάρχει ένας μεγάλος όγκος ερευνητικών δημοσιεύσεων που εξετάζουν διάφορες πτυχές της ψηφιακής εγκληματολογίας και της ασφάλειας στον κυβερνοχώρο, ειδικά σε περιβάλλοντα που αφορούν κρίσιμες υποδομές και υπηρεσίες. Οι περισσότερες έρευνες επικεντρώνονται είτε στην αντιμετώπιση των κοινών απειλών και τρωτών σημείων που εμφανίζονται σε ποικίλους τύπους συστημάτων και τομέων [2], [17], [5], είτε εστιάζουν σε συγκεκριμένα περιβάλλοντα, όπως τα έξυπνα δίκτυα και οι IoT συσκευές [12], [28].

Το πεδίο της ψηφιακής εγκληματολογίας συνδυάζεται στενά με τις τεχνολογίες τεχνητής νοημοσύνης και μηχανικής μάθησης, με αρκετές μελέτες να προτείνουν πλαίσια που αναλύουν την αποτελεσματικότητα αυτών των τεχνολογιών για την εξαγωγή αποδεικτικών στοιχείων [18], [24], [20]. Επιπλέον, υπάρχουν δημοσιεύσεις που αναλύουν τα μεγάλα δεδομένα και τον ρόλο τους στην εγκληματολογική ανάλυση, ενώ άλλες επικεντρώνονται σε εξειδικευμένες προσεγγίσεις, όπως η εφαρμογή τεχνικών βαθιάς μάθησης σε συγκεκριμένους τομείς, όπως η ανάλυση δεδομένων από συσκευές κινητής τηλεφωνίας και cloud περιβάλλοντα [6], [23].

Σε αυτήν την ενότητα, παρουσιάζουμε συνοπτικά αυτούς τους τύπους ερευνών και επισημαίνουμε τις διαφορές τους ως προς το πεδίο εφαρμογής και τη συνεισφορά τους στην ψηφιακή εγκληματολογία (DF) και την ασφάλεια μετά από κυβερνοεπιθέσεις.

3.2 Ερευνητική βιβλιογραφία

Η ανάλυση των ψηφιακών μέσων και συγκεκριμένα των φωτογραφικών εικόνων, του ήχου και των βιντεοσκοπήσεις είναι πολύ σημαντική στην ψηφιακή εγκληματολογία. Υπάρχουν διάφορες μέθοδοι για την ψηφιακή εγκληματολογική ανάλυση. Επί του παρόντος, η βαθιά μάθηση (DL), κυρίως το συνελικτικό νευρωνικό δίκτυο (CNN) έχει αποδειχθεί πολύ ελπιδοφόρο στην ταξινόμηση ψηφιακών εικόνων και ήχου τεχνικές ανάλυσης.

Το [9] παρουσιάζει μια περιεκτική μελέτη των πρόσφατων έρευνας και των μεθόδων σε εγκληματολογικούς τομείς που βασίζονται στο συνελικτικό νευρωνικό δίκτυο (CNN), με σκοπό να καθοδηγήσει τους ερευνητές που εργάζονται σε αυτόν τον τομέα. Κατ' αρχάς, ορίστηκαν και εξηγήθηκαν κάποια πρώιμα μοντέλα της βαθιάς μάθησης (DL). Από τα διάφορα μοντέλα DL που υπήρχαν, έγινε εστίαση στο συνελικτικό νευρωνικό δίκτυο (CNN) και στη χρήση του σε τομείς της ψηφιακής εγκληματολογίας. Η ανασκόπηση δείχνει ότι το συνελικτικό νευρωνικό δίκτυο (CNN) έχει αποδείχθηκε καλή στους περισσότερους τομείς της εγκληματολογίας και εξακολουθεί να υπόσχεται να είναι καλύτερη. Ωστόσο, παρ'όλα τα θετικά των συνελικτικό νευρωνικό δίκτυο (CNN) διαπιστώνεται ότι τα βαθιά δίκτυα παρουσιάζουν ευπάθεια και είναι επιρρεπή σε επιθέσεις, επομένως υπάρχει ανάγκη για ένα πλαίσιο που θα ελέγχει την ανθεκτικότητα των εγκληματολογικών εργαλεία.

Το [14] εξετάζει τη χρήση της τεχνητής νοημοσύνης (AI) για την ανάλυση μεγάλων όγκων δεδομένων στον τομέα της κυβερνοασφάλειας. Χρησιμοποιώντας αλγόριθμους μηχανικής μάθησης και βαθιάς μάθησης, η τεχνητή νοημοσύνη (AI) αναλύει δεδομένα για την αναγνώριση μοτίβων και ανωμαλιών που σχετίζονται με κυβερνοαπειλές, όπως κακόβουλο λογισμικό, επιθέσεις δικτύου και ανωμαλίες στη ροή δεδομένων. Το έγγραφο εξετάζει επίσης τις προκλήσεις και τις ηθικές εκτιμήσεις που σχετίζονται με την τεχνητή νοημοσύνη (AI) στην κυβερνοασφάλεια και υπογραμμίζει τα δυνητικά οφέλη από την ενσωμάτωση των τεχνολογιών τεχνητής νοημοσύνης (AI) στα υφιστάμενα πλαίσια ασφάλειας.

Η μελέτη υπογραμμίζει την ανάγκη για υπεύθυνες πρακτικές τεχνητής νοημοσύνης (AI), συνεργασία μεταξύ ανθρώπων και μηχανών και συνεχή έρευ να για την αξιοποίηση του πλήρους δυναμικού της τεχνητής νοημοσύνης (AI) στην καταπολέμηση των απειλών στον κυβερνοχώρο. Υπογραμμίζει επίσης τις δυνατότητες της τεχνητής νοημοσύνης (AI) για την ενίσχυση των δυνατοτήτων κυβερνοασφάλειας, αναγνωρίζοντας παράλληλα τις προκλήσεις και τις εκτιμήσεις που πρέπει να αντιμετωπιστούν. Η ενότητα επαναλαμβάνει την ανάγκη για μια ισορροπημένη προσέγγιση που συνδυάζει την ανθρώπινη εμπειρογνωμοσύνη με τις τεχνολογίες τεχνητής νοημοσύνης (AI) για τη δημιουργία ισχυρών και προσαρμοστικών αμυνών κυβερνοασφάλειας.

Η έγκαιρη εξέταση μεγάλου όγκου δεδομένων για την αναζήτηση σημαντικών στοιχείων κατά τη διάρκεια ερευνών εγκλημάτων, είναι απαραίτητη για την επιτυχία των εγκληματολογικών εξετάσεων σε υπολογιστές. Οι περιορισμοί σε χρόνο και πόρους, τόσο υπολογιστικών και ανθρώπινων πόρων, έχουν αρνητικό αντίκτυπο στα αποτελέσματα που λαμβάνονται. Συνεπώς, η καλύτερη χρήση των διαθέσιμων πόρων είναι αναγκαία, πέραν των δυνατοτήτων των χρησιμοποιούμενων σήμερα εγκληματολογικών εργαλείων.

Το [18] περιγράφει τη χρήση της τεχνητής νοημοσύνης (AI) στην εγληματολογία των υπολογιστών μέσω της ανάπτυξης ενός συστήματος πολλαπλών πρακτόρων και της συλλογιστικής βάσει περιπτώσεων. Το σύστημα αυτό αποτελείται από εξειδικευμένους ευφυείς πράκτορες που ενεργούν με βάση τις γνώσεις των εμπειρογνωμόνων του τεχνικού τομέα. Στόχος τους είναι να αναλύουν και να συσχετίσουν τα δεδομένα που περιέχονται στα αποδεικτικά στοιχεία μιας έρευνας και με βάση την εμπειρογνωμοσύνη τους να παρουσιάσουν τους πιο ενδιαφέροντες αποδεικτικά στοιχεία στον ανθρώπινο εξεταστή, μειώνοντας έτσι τον όγκο των δεδομένων που πρέπει να αναλυθούν προσωπικά. Το χαρακτηριστικό συσχέτισης βοηθά στο να εντοπίζει συνδέσμους μεταξύ αποδεικτικών στοιχείων που μπορεί εύκολα να παραβλέψει ένας ανθρώπινος εμπειρογνώμονας, ειδικά λόγω του όγκου των δεδομένων. που εμπλέκονται. Το σύστημα αυτό δοκιμάστηκε με τη χρήση πραγματικών δεδομένων και τα αποτελέσματα ήταν πολύ θετικά σε σύγκριση με εκείνα που προέκυψαν από τον άνθρωπο εμπειρογνώμονα που εκτελεί την ίδια ανάλυση.

Μεταξύ άλλων, προτείνει μια εφυή εργαλειοθήκη όπως την αποκαλεί, και συγκεκριμένα ένα εργαλείο ονόματι «MultiAgent Digital Investigation toolKit (MADIK)», ένα σύστημα πολλαπλών πρακτόρων για την υποβοήθηση του εμπειρογνώμονα εγκληματολογίας υπολογιστών. Το σύστημα αποτελείται από ένα σύνολο εφυών πρακτόρων λογισμικού (ISA) που εκτελούν διαφορετικές αναλύσεις στα ψηφιακά αποδεικτικά στοιχεία που σχετίζονται με μια υπόθεση με κατανεμημένο τρόπο. Προκειμένου να αξιολογηθεί η αποδοτικότητα του εργαλείου MADIK, πραγματοποιήθηκαν δύο πειράματα χρησιμοποιώντας δεδομένα από πραγματικές έρευνες. Στο πρώτο παρατηρήθηκε μείωση των χρόνων εκτέλεσης των εξετάσεων Hash-SetAgent (πράκτορας που αποθηκεύει μοναδικά αντικείμενα χωρίς κάποια συγκεκριμένη σειρά) με την κατανομή της εργασίας του. Χρησιμοποιήθηκαν από ένας έως τέσσερις υπολογιστές με έναν έως οκτώ HashSetAgents σε κάθε μηχάνημα. Μοίρασαν το έργο της σύγκρισης των κατακερματισμών 500.000 αρχείων με ένα σύνολο κατακερματισμών 26.000 αρχείων.Τα αποτελέσματα ήταν θετικά με περίπου 10% του χρόνου να χάνεται λόγω της επιβάρυνσης της επικοινωνίας μεταξύ των πρακτόρων.

Το [19] επικεντρώνεται στη χρήση της εξηγήσιμης τεχνητής νοημοσύνης (XAI) για την ενίσχυση της ανάλυσης ψηφιακών αποδεικτικών στοιχείων. Επιδιώκει να διερευνήσει τις δυνατότητες της τεχνητής νοημοσύνης (AI) για την περαιτέρω ενίσχυση της ταξινόμησης και της ανάλυσης ψηφιακών εγκληματολογικών στοιχείων, χρησιμοποιώντας παραδείγματα της τρέχουσας κατάστασης της τέχνης ως σημείο εκκίνησης. Συζητάει τόσο πρακτικές και καινοτόμες ιδέες όσο και αμφιλεγόμενες σημεία για την αξιοποίηση της XAI για τη βελτίωση της αποτελεσματικότητας της ανάλυσης και την εξαγωγή εγκληματολογικά ορθών αποδεικτικών στοιχείων (επίσης γνωστών ως τεχνούργημα) που θα μπορούσαν να χρησιμοποιηθούν για να βοηθήσουν τις έρευνες και ενδεχομένως στο δικαστήριο.

Όπως προτάθηκε στην έρευνα, ένα από τα μελλοντικά πιθανά ερευνητικά προγράμματα είναι η διεξαγωγή μιας εμπειρικής μελέτης για την αξιολόγηση της αποτελεσματικότητας της XAI σε διάφορα στάδια των ερευνών Ψηφιακής Εγλήματολογίας (DF) σε ένα πραγματικό εργαστήριο. Με την εισαγωγή της τεχνητής νοημοσύνης (ή της XAI) στην Ψηφιακή Εγληματολογία (DF), πρέπει επίσης να ληφθεί υπόψη ο κίνδυνος που συνδέεται με την «αντίθετη» μηχανική μάθηση, όπου τα μοντέλα AI/XAI εκπαιδεύονται με τη χρήση αλλοιωμένων/μεροληπτικών δεδομένων. Με άλλα λόγια, πώς μπορούμε να γνωρίζουμε αν τα μοντέλα XAI που χρησιμοποιούνται στις έρευνες

είναι αξιόπιστα; Ως εκ τούτου, ένα επόμενο ερώτημα είναι κατά πόσον μπορούμε να αξιοποιήσουμε τέτοιες τεχνικές βασισμένες σε AI/XAI για να βοηθήσουμε την DF ερευνητές να εντοπίζουν και να εκμεταλλεύονται ευπάθειες στις υπολογιστικές συσκευές ή τα δίκτυα για να αποκτήσουν πρόσβαση σε αποδεικτικά στοιχεία.

Το [20] έχει ως στόχο να κατανοηθεί πώς μπορεί να χρησιμοποιηθεί η μηχανική μάθηση στο ψηφιακό έγκλημα και η εγκληματολογική της σημασία, δημιουργώντας ένα περιβάλλον για την εκπαίδευση τεχνητών νευρωνικών δικτύων και τη διερεύνηση καθώς και την ανάλυσή τους για την εύρεση αντικειμένων που μπορούν να φανούν χρήσιμα στην εγκληματολογική έρευνα. Η μελέτη εστιάζει στη δημιουργία και εκπαίδευση μοντέλων με TensorFlow για την ανάλυση ψηφιακών στοιχείων που είναι κρίσιμα για την ανάλυση εγκλημάτων. Το TensorFlow είναι ένα ανοιχτού κώδικα λογισμικό μηχανικής μάθησης που αναπτύχθηκε από την Google. Χρησιμοποιείται για τη δημιουργία και εκπαίδευση μοντέλων τεχνητής νοημοσύνης, με έμφαση στη βαθιά μάθηση (deep learning). Παρέχει εργαλεία για την κατασκευή νευρωνικών δικτύων και υποστηρίζει πλήρως διανεμημένες υπολογιστικές υποδομές. Ασχολείται κατά βάση με την υλοποίηση εκπαίδευσης και δοκιμής ενός chat bot σε περιβάλλον Linux Ubuntu 16.04 (έκδοση του Ubuntu, το 2016).

Η δημιουργία ενός νευρωνικού δικτύου με τη βοήθεια της μηχανικής μάθησης (ML) έχει γίνει καλύτερη με την εισαγωγή της βιβλιοθήκης μηχανικής μάθησης ανοικτού κώδικα TensorFlow της Google. Μετά την εύρεση των σχετικών τεχνουργημάτων κατά τη διερεύνηση των εικόνων αποδεικτικών στοιχείων, συμπερίνεται ότι ένα πρόγραμμα μηχανικής μάθησης που βασίζεται στην Tensorflow εκπαιδεύτηκε καθώς και εκτελέστηκε στο σύστημα. Αυτά τα ευρήματα μπορούν να χρησιμοποιηθούν ως αναφορά σε μελλοντικές περιπτώσεις για τον εντοπισμό ή την αναγνώριση της χρήσης βιβλιοθηκών μηχανικής μάθησης, αλγορίθμων, τεχνικών κ.λπ. Ωστόσο, πρέπει να γίνει ακόμη πολλή ερευνητική εργασία σε αυτόν τον τομέα. Η ορθή και βαθύτερη ανάλυση των πτητικών πληροφοριών θα ήταν ευεργετική, καθώς και η σε βάθος ανάλυση των νευρωνικών δικτύων θα μπορούσε να βοηθήσει στην εξοικείωση με τα προγράμματα μηχανικής μάθησης (ML) στο πλαίσιο της ψηφιακής εγκληματολογίας.

Το [22] προτείνει ένα πλαίσιο ανάλυσης δεδομένων ψηφιακής εγκληματολογίας για το Διαδίκτυο των Πραγμάτων (IoT), το οποίο χρησιμοποιεί τεχνητή νοημοσύνη και τεχνολογία blockchain. Το άρθρο προτείνει το πλαίσιο κοινού ελέγχου με τη βοήθεια blockchain (BSAF) για την ανάλυση ψηφιακών εγκληματολογικών δεδομένων στην πλατφόρμα του Διαδικτύου των Πραγμάτων (IoT). Το προτεινόμενο πλαίσιο σχεδιάστηκε για την ανίχνευση της πηγής/αιτίας των επιθέσεων απορρόφησης δεδομένων σε εικονικοποιημένους πόρους (VR - χρησιμοποιεί συχνά ακουστικά εικονικής πραγματικότητας ή περιβάλλοντα πολλαπλών προβολών, μερικές φορές σε συνδυασμό με φυσικά περιβάλλοντα ή σκηνικά, για τη δημιουργία εικόνων, ήχων και άλλων αισθήσεων που προσομοιώνουν τη φυσική παρουσία ενός χρήστη σε ένα εικονικό ή φανταστικό περιβάλλον). Το προτεινόμενο πλαίσιο υλοποιεί την τεχνολογία blockchain για τη διαχείριση των αρχείων καταγραφής και ελέγχου πρόσβασης.

Η ανάλυση των δεδομένων καταγραφής συναθροίζεται χρησιμοποιώντας μηχανική μάθηση λογικής παλινδρόμησης για τον εντοπισμό της κατάλληλης ανίχνευσης στο πρώτο επίπεδο με εύρος ανάλυσης 95% έως 96%. Στο δεύτερο επίπεδο, τα δεδομένα επαληθεύονται μέσω

διασταυρούμενης επικύρωσης για να επιβεβαιωθεί η αιτία της σάρωσης. Το προτεινόμενο πλαίσιο εντοπίζει πρώτα το αντίπαλο χρησιμοποιώντας αιτήσεις που αντιστοιχίζονται στον εικονικό πόρο και στη συνέχεια φιλτράρει την ανίχνευση για καλύτερη επαλήθευση με τη χρήση της πυκνότητας των συσκευών IoT. Το κοινό επίπεδο παρέχει βελτιωμένη αναλογία ανάλυσης 0,35-0,45 σε λιγότερο χρόνο και επιτυγχάνει λιγότερα ποσοστά συμβάντων σε διαδοχικές διαδικασίες πρόσβασης σε πόρους.

Το [26] έχει ως σκοπό να κάνει μια συστηματική ανασκόπηση της εφαρμογής αλγορίθμων μηχανικής μάθησης αναφορικά με την ασφάλεια στον κυβερνοχώρο και την εγκληματολογία στον κυβερνοχώρο, και για αυτό το λόγο, χρησιμοποιήθηκε η μέθοδος της συστηματικής έρευνας σχετικά με την πρόσφατη εφαρμογή αλγορίθμων μηχανικής μάθησης σε εγκληματολογία στον κυβερνοχώρο και την ασφάλεια στον κυβερνοχώρο με βάση τα ευρήματα αυτά παρατηρείται ότι η ασφάλεια στον κυβερνοχώρο βασίζεται στην εμπιστευτικότητα, την ακεραιότητα και την εγκυρότητα των δεδομένων, σημειώνεται επίσης ότι υπάρχουν δέκα βήματα για την ασφάλεια στον κυβερνοχώρο: ασφάλεια δικτύου, εκπαίδευση και ευαισθητοποίηση των χρηστών, πρόληψη κακόβουλου λογισμικού, έλεγχος αφαιρούμενων μέσων, ασφαλής διαμόρφωση, διαχείριση προνομίων χρηστών, διαχείριση περιστατικών, παρακολούθηση και εργασία στο σπίτι και την κινητή εργασία και ανοίγει δρόμους για περαιτέρω ερευνητικές κατευθύνσεις σχετικά με την εφαρμογή της βαθιάς μάθησης, της υπολογιστικής νοημοσύνης, και την εγκληματολογία στον κυβερνοχώρο.

Πρόσφατα, παρατηρήθηκε μια παγκόσμια τάση ότι υπάρχει ευρεία καθιέρωση σε όλους τους τομείς για την καθιέρωση έξυπνων περιβαλλόντων και αυτοματισμού. Τα έξυπνα περιβάλλοντα περιλαμβάνουν μια μεγάλη ποικιλία συσκευών Διαδικτύου των Πραγμάτων (IoT), οπότε πολλές προκλήσεις αντιμετωπίζουν συμβατικές ψηφιακές εγκληματολογικές έρευνες (DFI) σε τέτοια περιβάλλοντα. Αυτές οι προκλήσεις περιλαμβάνουν την ποικιλομορφία των δεδομένων, την κατανομή των δεδομένων και τεράστιες ποσότητες δεδομένων, οι οποίες υπερβαίνουν τις ανθρώπινες δυνατότητες των ερευνητών ψηφιακής εγκληματολογίας (DF) να αντιμετωπίσουν όλες αυτές τις προκλήσεις σε σύντομο χρονικό διάστημα.

Με την αυξανόμενη συχνότητα των ψηφιακών εγκλημάτων, απαιτούνται επειγόντως καλύτερες και πιο εξελιγμένες διαδικασίες συμβατικώς ψηφιακών εγκληματολογικών ερευνών (DFI), ιδίως σε τέτοια περιβάλλοντα. Δεδομένου ότι οι τεχνικές μηχανικής μάθησης (ML) μπορεί να είναι μια βιώσιμη επιλογή στις έξυπνες περιβάλλοντα, το [27] παρουσιάζει την ενσωμάτωση της μηχανικής μάθησης (ML) στη ψηφιακή εγληματολογία (DF), μέσω της ανασκόπησης των πιο πρόσφατων δημοσιεύσεων που αφορούν τις εφαρμογές της μηχανικής μάθησης (ML) στη ψηφιακή εγληματολογία (DF), ειδικά σε έξυπνα περιβάλλοντα. Επίσης την πιθανή περαιτέρω χρήση των τεχνικών της μηχανικής μάθησης (ML) στη ψηφιακή εγληματολογία (DF), σε έξυπνα περιβάλλοντα για τη μείωση των σκληρή εργασία των ανθρώπων.

3.3 Grey literature

Το [1] εξετάζει τη χρήση της τεχνητής νοημοσύνης για την ανάλυση αποδεικτικών στοιχείων στην ψηφιακή εγκληματολογία. Εστιάζει στη χρήση εργαλείων υπολογιστικής λογικής, όπως η Προγραμματισμός Συνόλων Απαντήσεων (ASP), για την αυτοματοποίηση της ανάλυσης δεδομένων και τη δημιουργία υποθέσεων. Η μελέτη δείχνει πώς σύνθετες ερευνητικές περιπτώσεις μπορούν να αναπαρασταθούν ως προβλήματα βελτιστοποίησης, τα οποία η ASP μπορεί να επιλύσει, βοηθώντας στη διαμόρφωση σαφών ερευνητικών υποθέσεων. Η εφαρμογή αυτής της μεθόδου υποστηρίζει την ανάπτυξη ενός Συστήματος Υποστήριξης Απόφασης (DSS) για τους ερευνητές, επιταχύνοντας την διαδικασία της ψηφιακής εγκληματολογίας.

Η πρόκληση της οποίας το παρόν άρθρο αποτελεί απλώς ένα πρώτο βήμα στοχεύει στη δημιουργία μιας υποδομής για την εφαρμογή της Τεχνητής Νοημοσύνης (AI) και της αυτοματοποιημένης συλλογιστικής στην ψηφιακή εγκληματολογία. Ειδικότερα, αφορά τη φάση της ανάλυσης αποδεικτικών στοιχείων που συλλέγονται από διάφορες ηλεκτρονικές συσκευές, με στόχο την ανακατασκευή γεγονότων και σεναρίων. Η έρευνα στοχεύει στην κατασκευή εργαλείων λογισμικού που συνδυάζουν τεχνικές από την αναπαράσταση γνώσης και τη συλλογιστική. Η εφαρμογή τέτοιων εργαλείων θα επιφέρει σημαντική ανακάλυψη στις διαδικασίες ανάλυσης αποδεικτικών στοιχείων. Η καθιέρωση των συστημάτων αυτών μπορεί να συμβάλει στην ταχύτερη και αξιόπιστη διεξαγωγή νομικών διαδικασιών. Η υπολογιστική λογική ως βάση εγγυάται τη διαφάνεια και επαληθευσιμότητα των αποτελεσμάτων. Ωστόσο, μια πρόκληση παραμένει η ενίσχυση της εμπιστοσύνης του κοινού σε τέτοια συστήματα, καθώς μπορεί να φαίνονται μη πειστικά ή απειλητικά.

Η εγκληματολογία δικτύων επικεντρώνεται στον εντοπισμό και τη διερεύνηση των εσωτερικών και εξωτερικών επιθέσεων δικτύου, και τη μη οργανωμένη διερεύνηση των δικτυακών συσκευών. Βρίσκεται στο σημείο τομής της ψηφιακής εγκληματολογίας, της αντιμετώπισης περιστατικών και της ασφάλειας δικτύων. Οι επιθέσεις δικτύου εκμεταλλεύονται ευπάθειες λογισμικού και υλικού και πρωτόκολλα επικοινωνίας. Το πεδίο εφαρμογής μιας δικτυακής εγκληματολογικής έρευνας μπορεί να κυμαίνεται από το σύνολο του Διαδικτύου έως την πορεία δικτύου μιας μεμονωμένης συσκευής. Τα εργαλεία ανάλυσης δικτύου (NAT - Η διαδικασία μετάφρασης μιας διεύθυνσης IP σε μια άλλη) βοηθούν τους επαγγελματίες της ασφάλειας και τις αρχές στη σύλληψη, ταυτοποίηση και την ανάλυσης της δικτυακής κίνησης. Ωστόσο, στις περισσότερες περιπτώσεις, ο όγκος των δεδομένων που πρέπει να αναλυθούν είναι τεράστιος και, παρά την ενσωματωμένη αυτοματοποίηση του NAT, η διερεύνηση της δικτυακής κίνησης, είναι συχνά μια επίπονη διαδικασία. Επιπλέον, σημαντικός χρόνος των εμπειρογνωμόνων χάνεται στη διερεύνηση μιας υψηλής συχνότητας ψευδώς θετικών ειδοποιήσεων από αυτοματοποιημένα συστήματα. Για την αντιμετώπιση αυτού του προβλήματος με παγκόσμιο αντίκτυπο, η τεχνητή προσεγγίσεις που βασίζονται στην ευφυΐα χρησιμοποιούνται όλο και περισσότερο για την αυτόματη ανίχνευση επιθέσεων και αύξηση της ακρίβειας ταξινόμησης των διαδρομών δικτύου.

Το [2] παρέχει μια ολοκληρωμένη επισκόπηση της κατάστασης της τεχνολογίας στην εγκληματολογία δικτύων και την εφαρμογή των συστημάτων εμπειρογνωμόνων, της μηχανικής

μάθησης, της βαθιάς μάθησης, και προσεγγίσεων συνόλου/υβριδικών προσεγγίσεων σε μια σειρά από τομείς εφαρμογών στον τομέα αυτό. Αυτές περιλαμβάνουν την παρακολούθηση δικτύου (NTA - εντοπίζει και αναλύει απειλές ασφάλειας και πιθανές επιχειρησιακές δυσκολίες, χρησιμοποιώντας τις επικοινωνίες δικτύου και τα σχετικά πρωτόκολλα.), συστήματα ανίχνευσης εισβολών (NIDS - είναι ένα μηχανισμός ανίχνευσης και πρόληψης που παρακολουθεί το δίκτυο κίνησης, για εχθρική και ύποπτη συμπεριφορά) , συσκευές Internet-of-Things (IoT forensics - είναι μια σχετικά νέα κατηγορία καταναλωτικών και βιομηχανικών ηλεκτρονικών), εγκληματολογία υπολογιστικού νέφους (cloud forensics - Μια έρευνα εγκληματολογίας νέφους περιγράφεται ως εξέταση του εγκλήματος στον κυβερνοχώρο που απαιτεί αποδεικτικά στοιχεία από οποιοδήποτε από τα πλατφόρμες ή υπηρεσίες υπολογιστικού νέφους), DNS tunneling (Η σήραγγα του συστήματος ονομάτων τομέα (DNS) είναι μια τεχνική επίθεσης που προσπαθεί να αποφύγει την ανίχνευση χρησιμοποιώντας αιτήσεις DNS και απαντήσεις για τη μετάδοση δεδομένων), έξυπνο δίκτυο (smart grid forensics - χρησιμοποιείται κυρίως για τον εντοπισμό ζητήματα ασφάλειας σε ένα έξυπνο σύστημα ηλεκτρικού δικτύου) και εγκληματολογία οχημάτων (vehicle forensics - Η συλλογή και ανάλυση ψηφιακών αποδεικτικών στοιχείων από αυτοκίνητα . αποτελεί μέρος της ψηφιακής εγκληματολογίας οχημάτων.). Ακόμα, αναλύει την αποδοτικότητα και την λειτουργία 10 dataset (Ένα σύνολο δεδομένων είναι μια δομημένη συλλογή δεδομένων που οργανώνονται και αποθηκεύονται μαζί για ανάλυση ή επεξεργασία. Τα δεδομένα εντός ενός συνόλου δεδομένων συνήθως σχετίζονται με κάποιο τρόπο και προέρχονται από μία μόνο πηγή ή προορίζονται για ένα μόνο έργο.), προκειμένου να δείξει πως αυτά αποδίδουν, ανάλογα με τον τομέα που εξετάζεται. Ωστόσο, αυτό που μας επισημαίνει, είναι ότι ο κύριος περιορισμός σε πολλούς από τους τομείς παραμένει η έλλειψη επαρκώς μεγάλων και καθαρών δεδομένων.

Τα μεταδεδομένα αρχείου αποτελούνται από τις διάφορες ιδιότητες του αρχείου, όπως το όνομα του αρχείου, το αρχείο μέγεθος, ημερομηνία πρόσβασης και τροποποιήσεων, ημερομηνία δημιουργίας και κωδικός κατακερματισμού των αρχείων. Προκειμένου να αναλυθεί οποιοδήποτε έγκλημα, είναι απαραίτητο να επικεντρωθούμε στα μεταδεδομένα αντί για τα δεδομένα του αρχείου. Η απλή απόκτηση των δεδομένων από τα αρχεία δεν αρκεί, είναι εξίσου σημαντικό να αναλύονται τα μεταδεδομένα τους, τα οποία μπορούν να κατευθύνουν ένα ψηφιακό εγκληματολογικό ερευνητή προς το ύποπτο σύστημα. Ανάλυση των μεταδεδομένων θα αποκαλύψει τα αποδεικτικά στοιχεία των εγκλημάτων που διαπράχθηκαν, τα οποία θα ήταν χρήσιμα στην περαιτέρω φάσεις της διαδικασίας έρευνας.

Το [3] επικεντρώνεται στην ανάλυση μεταδεδομένων αρχείων με την εφαρμογή αλγορίθμων μηχανικής μάθησης που θα είναι χρήσιμοι για την ψηφιακή ιατροδικαστική έρευνα. Από την εφαρμογή αυτών των αλγορίθμων αποδείχθηκε ότι τα μεταδεδομένα μπορούν επίσης να εφαρμοστούν σε αλγορίθμους μηχανικής μάθησης για την απόδειξη διαπραχθέντων εγκλημάτων. Μπορεί επίσης να είναι χρήσιμο για την επιλογή της σωστής κατεύθυνσης της έρευνας χωρίς σπατάλη πόρων στην λανθασμένη κατεύθυνση.

Η ψηφιακή εγκληματολογία (DF), ως κλάδος των εγκληματολογικών επιστημών, αντιμετωπίζει νέες προκλήσεις από την άποψη ότι τα ψηφιακά αποδεικτικά στοιχεία αυξάνονται και επεκτείνονται. Η ταχεία ανάπτυξη στους τομείς της επιστήμης των υπολογιστών και των πληροφοριών τεχνολογίας παρέχει καινοτόμες τεχνικές για τις ψηφιακές έρευνες.

Στο [4], ο σημαντικός ρόλος της μηχανικής μάθησης (ML) εξηγείται ως εφαρμογή της τεχνητής νοημοσύνης (AI) και πώς μπορεί να χρησιμοποιηθεί για την ανάλυση μεγάλων ποσοτήτω διαφορετικών συνόλων δεδομένων προκειμένου να αποκαλυφθεί τυχόν εγκληματική συμπεριφορά και πρόθεση μέσω της μάθησης από προηγούμενες και ιστορικές δραστηριότητες για την πρόβλεψη εγκληματικών συμπεριφορών στο μέλλον.

Στο [5], προτείνεται μια ταξινόμηση επιθέσεων στο Περιβάλλον Δικτύου του Νέφους (cloud) που βασίζεται στη μηχανική μάθηση (ML) με μια ψηφιακή εγκληματολογική διαδικασία. Ως εκ τούτου, ο αλγόριθμος σύντηξης που προτείνεται (ψηφιακή εγκληματολογία (DF) με βάση τη βαθιά μάθηση (ML)) λειτουργεί καλά ως ταξινομητής δεδομένων. Αντιμετωπίστηκαν προκλήσεις και απαιτήσεις της ψηφιακής εγκληματολογίας (DF) με μηχανική μάθηση (ML) στο cloud computing (CC). Λόγω των αυξημένων απειλών, τα τρέχοντα εργαλεία εγκληματολογίας δεν μπορούν να διεξάγουν πλήρη έρευνα στις υπηρεσίες νέφους. Η απόκτηση μεγάλου όγκου δεδομένων ως απόδειξη είναι δύσκολη στην ενσωμάτωση σε μια πλατφόρμα.

Προτάθηκαν νέες λύσεις για την ανάλυση «νεκρών»/»ζωντανών» εγκληματολογικών δεδομένων και αντιμετωπίστηκαν επιθέσεις όπως ICMP (Το ICMP (Internet Control Message Protocol) είναι ένα πρωτόκολλο που έχει ως αποστολή μηνυμάτων σφάλματος και άλλων καταστάσεων που απαιτούν ιδιαίτερη προσοχή. Μηνύματα/πακέτα ICMP αποστέλλονται εάν υπάρχει πρόβλημα στο επίπεδο IP και στο ανώτερο επίπεδο (TCP/UDP).), TCP Sync (είναι ένα από τα βασικά πρωτόκολλα του Διαδικτύου (IP), και είναι τόσο διαδεδομένο που ολόκληρη η σουίτα αποκαλείται συχνά TCP/IP), UDP (Το πρωτόκολλο δεδομένων χρήστη (UDP) είναι ένα από τα από τα βασικά μέλη της σουίτας πρωτοκόλλων του Διαδικτύου.). Επίσης, σχεδιάστηκε ταξινόμηση για τη μερική ανάλυση συστημάτων νέφους και τις προκλήσεις που αντιμετωπίζει ο ερευνητής στο περιβάλλον cloud.

Με την ταχεία ανάπτυξη του ασύρματου δικτύου και του έξυπνου κινητού εξοπλισμού, πολλοί παραβάτες του νόμου χρησιμοποιούν κινητές συσκευές για να καταστρέψουν και να κλέψουν σημαντικές πληροφορίες ιδιοκτησίας από άλλα πρόσωπα. Προκειμένου να καταπολεμηθεί η εγκληματική πράξη αποτελεσματικά, τα όργανα της δημόσιας ασφάλειας πρέπει να συλλέξουν τα αποδεικτικά στοιχεία από τα εργαλεία του εγκλήματος και να τα προσκομίσουν στο δικαστήριο. Με την ανάπτυξη της τεχνολογίας, ο υπάλληλοι επιβολής του νόμου συλλέγουν πολλές πληροφορίες από έναν έξυπνο φορητό εξοπλισμό, για χάρη του χειρισμού των τεράστιων ποσοτήτων δεδομένων.

Οπότε, το [6] προτείνει ένα πλαίσιο που συνδυάζει κατανεμημένες μεθόδους ομαδοποίησης για την ανάλυση συνόλων δεδομένων. Αυτό το μοντέλο θα διαχωρίσει τα δεδομένα σε μικρότερα κομμάτια και θα χρησιμοποιήσει τη μέθοδο ομαδοποίησης για την ανάλυση κάθε μικρότερου τμήματος σε διαφορετικές μηχανές, επιλύοντας έτσι το πρόβλημα του μεγάλου όγκου

δεδομένων. Ως αποτέλεσμα, η διεξαγωγή της εγκληματολογικής έρευνας θα είναι πιο αποτελεσματική.

Η τεχνητή νοημοσύνη (AI) επηρέασε τις τεχνικές πτυχές της έρευνας για τη δημιουργία αυτοματοποιημένων ευφυών συμπεριφορών που καλύπτουν διαφορετικούς τομείς, αλλά έδειξε αξιοσημείωτα αποτελέσματα όταν χρησιμοποιήθηκε στην εγκληματολογική τεχνολογία στον κυβερνοχώρο για την ανάλυση εγκλημάτων. Οι εμπειρογνώμονες της τεχνητής νοημοσύνης (AI) προειδοποίησαν για πιθανούς κινδύνους ασφαλείας που σχετίζονται με τους αλγορίθμους και τα δεδομένα εκπαίδευσης, καθώς η τεχνητή νοημοσύνη (AI) κληρονομεί υπολογιστικά χαρακτηριστικά που ασχολούνται με τις έξυπνες εφαρμογές που βασίζονται στο Διαδίκτυο των Πραγμάτων (IoT) και τις αυτόνομες μεταφορές και μπορεί να βρεθεί ευάλωτη σε ευπάθεια και απειλές.

Το [8] συζητά μοντέλα για την ανάλυση πληροφοριών που σχετίζονται με τρομοκράτες και την κατηγοριοποίηση κακόβουλων γεγονότων, καλύπτοντας τη βιβλιογραφική ανασκόπηση σχετικά με τους κινδύνους ασφάλειας και την εγκληματικότητα που σχετίζεται με την τεχνητή νοημοσύνη (AI), παρουσιάζοντας μια ταξινόμηση της εγκληματικής συμπεριφοράς και των υπογραφών που καλύπτουν εργαλεία και εγκληματικούς στόχους που χρησιμοποιούνται σε δόλιες δραστηριότητες χρησιμοποιώντας χαρακτηριστικά της τεχνητής νοημοσύνης (AI) με ψηφιακές εγκληματολογικές τεχνικές. Δείχθηκε επίσης πώς η τεχνητή νοημοσύνη (AI) μπορεί να ενισχύσει τα υπάρχοντα εγκλήματα και ότι θα μπορούσαν να εμφανιστούν νέοι τύποι εγκλημάτων που δεν έχουν εντοπιστεί προηγουμένως. Αυτή η μελέτη παρουσίασε μια συστηματική δομή για το έγκλημα με βάση την τεχνητή νοημοσύνη (AI) και τις στρατηγικές αντιμετώπισής του. Επιπλέον, προτάθηκε η εγκληματολογία τεχνητής νοημοσύνης (AI), μια μοναδική προσέγγιση για την καταπολέμηση των εγκλημάτων που σχετίζονται με την AI. Ανακαλύφθηκε επίσης ότι αρκετές έννοιες της Ψηφιακής Εγκληματολογίας (DF) δεν προτιμώνται ακόμη στην εγκληματολογία με βάση την τεχνητή νοημοσύνη (AI).

Το [10] αποσκοπεί στην ανακάλυψη της ικανότητας της μηχανικής μάθησης (ML) για την εξόρυξη εικονικών εγκληματολογικών στοιχείων. Συγκεκριμένα, επικεντρώνεται στην εξέταση μεθόδων με τις οποίες οι αλγόριθμοι μηχανικής μάθησης (ML) θα μπορούσαν να αξιοποιηθούν για την εύρεση και ανάλυση εικονικών αποδεικτικών στοιχείων, με στόχο τη μεγιστοποίηση της απόδοσης των ψηφιακών εγκληματολογικών ερευνών. Το πρώτο βήμα σε αυτή την έρευνα είναι η αξιοποίηση της τεχνογνωσίας των υφιστάμενων τεχνικών που χρησιμοποιούνται στην εξόρυξη εικονικών εγκληματολογικών αποδεικτικών στοιχείων. Αφού συζητηθούν τα εγγενή εμπόδια αυτών των στρατηγικών, το ενδιαφέρον μετατοπίζεται στην περιγραφή των ποικίλων διαδικασιών και αλγορίθμων μηχανικής μάθησης (ML) που έχουν εξελιχθεί τα τελευταία χρόνια και στον τρόπο με τον οποίο μπορούν να δώσουν ώθηση στις ψηφιακές έρευνες στον τομέα της ψηφιακής εγκληματολογίας.

Κυρίως, διάφορες προσεγγίσεις που βασίζονται στη μηχανική μάθηση (ML), όπως οι αλγόριθμοι ανάλυσης των ανωμαλιών, οι εποπτευόμενες μέθοδοι μάθησης, η μάθηση χωρίς επίβλεψη και οι αλγόριθμοι βαθιάς μάθησης. Μετά την επισκόπηση αυτών των προσεγγίσεων που βασίζονται στη μηχανική μάθηση (ML), αναλύονται οι πρωταρχικοί τομείς χρησιμότητας στους οποίους μπορούν να χρησιμοποιηθούν για την εξαγωγή ψηφιακών στοιχείων, όπως η αξιολόγηση

φωτογραφιών, η ανάλυση της κίνησης του δικτύου και η ανάλυση της συμπεριφοράς των χρηστών. Επίσης, συζητείται ένα παράδειγμα τρόπων με τους οποίους η μηχανική μάθηση (ML) μπορεί να χρησιμοποιηθεί για τον εντοπισμό και την ανάλυση δεδομένων από μια διαδικτυακή πλατφόρμα κοινωνικών μέσων για την εξεύρεση αποδεικτικών στοιχείων ενός ποινικού αδικήματος.

Το [11] αναφέρεται στη χρήση ψεύτικων ψηφιακών φωτογραφιών και βίντεο σε εγκλήματα όπως ransomware (κρυπτογραφεί αρχεία των χρηστών ή κλέβει / διαγράφει σημαντικές πληροφορίες και κατέχει το κλειδί αποκρυπτογράφησης μέχρι να καταβληθούν λύτρα από το θύμα, τα οποία είναι κυρίως σε bitcoins λόγω των μη ανιχνεύσιμων ιδιοτήτων τους), ψεύτικες ειδήσεις και ψηφιακές απαγωγές, όπου το αλλοιωμένο περιεχόμενο πολυμέσων παίζει βασικό ρόλο. Τα εργαλεία ψηφιακής εγκληματολογίας (DF) χρησιμοποιούνται ευρέως για την αυτόματη ταυτοποίηση ψηφιακών αποδεικτικών στοιχείων, αλλά η πολυπλοκότητα των εγκλημάτων απαιτεί σύγχρονες τεχνικές. Οι ερευνητές μηχανικής μάθησης (ML) καλούνται να βελτιώσουν την ανάλυση χειραγωγημένου περιεχομένου πολυμέσων, όμως η έλλειψη κατάλληλων συνόλων δεδομένων περιορίζει την ενσωμάτωση των μεθόδων αυτών στα εργαλεία εγκληματολογίας.

Στο άρθρο, παρουσιάζεται ένα ισορροπημένο σύνολο δεδομένων 40.588 φωτογραφιών και 12.400 καρέ βίντεο, που δοκιμάστηκαν με συνελικτικά νευρωνικά δίκτυα (CNN) και μηχανές μηχανημάτων υποστήριξης (SVM - είναι μια μέθοδος που βασίζεται σε πυρήνες μηχανικής μάθησης (ML) και έχει εφαρμοστεί με επιτυχία χρησιμοποιείται σε ένα ευρύ σύνολο προβλημάτων ταξινόμησης, και συγκεκριμένα σε αυτά που εφαρμόζονται σε δυαδική ταξινόμηση μεταξύ δύο διαφορετικών κλάσεων.). Τα CNN είχαν καλύτερη απόδοση με F1-score (είναι μια εναλλακτική μετρική αξιολόγησης της μηχανικής μάθησης (ML) που αξιολογεί την προβλεπτική ικανότητα ενός μοντέλου αναλύοντας την απόδοσή του ανά κλάση και όχι μια συνολική απόδοση όπως γίνεται με την ακρίβεια) 0,9968 για φωτογραφίες και 0,8415 για βίντεο. Διατίθεται επίσης κώδικας Python για επεξεργασία και εξαγωγή χαρακτηριστικών, μετατρέποντας δεδομένα σε συμβατά μορφότυπα για εργαλεία μηχανικής μάθησης (ML).

Πρόσφατα, οι έξυπνες πόλεις προσφέρουν διάφορες υπηρεσίες στους πολίτες μέσω της σύγκλισης των τεχνολογιών πληροφοριών, επικοινωνιών και βιομηχανιών, όπως οι μεταφορές, η υγειονομική περίθαλψη και τα αυτοκίνητα. Ως αποτέλεσμα, ο αριθμός των έξυπνων συσκευών που χρησιμοποιούν τεχνητή νοημοσύνη για την αποθήκευση προσωπικών πληροφοριών των χρηστών με στόχο την παροχή πιο αποτελεσματικών υπηρεσιών αυξάνεται. Αυτές οι συσκευές μπορούν να χρησιμοποιηθούν για την απόκτηση βασικών αποδεικτικών στοιχείων μέσω της ψηφιακής εγκληματολογίας, τα οποία μπορούν να χρησιμεύσουν και ως αποδεικτικά σε δικαστήριο.

Σύμφωνα με το [12], αποκτώνται και αναλύονται δεδομένα χρηστών που είναι αποθηκευμένα σε φορητές συσκευές, εφαρμόζοντας ένα πλαίσιο απόκτησης δεδομένων για έξυπνες συσκευές. Αυτή η μελέτη συμβάλλει στην απόκτηση κρίσιμων αποδεικτικών στοιχείων για ερευνητικούς σκοπούς. Οι συσκευές που χρησιμοποίθηκαν, ήταν μια Xiaomi συσκευή, μια Huawei και μια LG και κάποιες έξυπνες ζώνες, το Fitbit Charge 4 και το Mi Band 4. Στη συσκευή

Xiaomi, οι πληροφορίες της συσκευής, όπως το όνομα της συσκευής, τελευταίας φόρτισης/σύνδεσης, και η διεύθυνση MAC, καθώς και πληροφορίες εισόδου του χρήστη όπως ο καρδιακός ρυθμός και ο χρόνος άσκησης, μπορούσαν να αποκτηθούν. Στις συσκευές Huawei και LG επιβεβαιώθηκε ότι, παρόλο που η πρόσβαση στο εσωτερικό της συσκευής ήταν δυνατή με τη χρήση υπολογιστή, δεν ήταν δυνατή η λήψη ουσιαστικών δεδομένων και ότι τα δεδομένα μπορούσαν να ληφθούν με τη χρήση τεχνολογίας chip-off (είναι μια εγκληματολογική τεχνική που χρησιμοποιείται για την εξαγωγή δεδομένων απευθείας από ένα τσιπ μνήμης με τη φυσική αφαίρεσή του από την πλακέτα κυκλώματος μιας συσκευής.). Οι έξυπνες ζώνες όπως το Fitbit Charge 4 και το Mi Band 4 είναι πιο συμπαγή από τα έξυπνα ρολόγια και διαθέτουν λιγότερες λειτουργίες, καθιστώντας δύσκολη την εφαρμογή μιας λογικής/φυσικής εγκληματολογικής μεθόδου σε αυτά.

Διάφορες συσκευές Διαδίκτυο των Πραγμάτων (IoT), όπως τα ηχεία με τεχνητή νοημοσύνη (AI), κυκλοφορούν με διαφορετικές λειτουργίες για να βελτιώσουν την ευκολία χρήσης και την ποιότητα ζωής. Ένα οικοσύστημα ηχείων AI αποτελεί ένα σύστημα IoT βασισμένο στο cloud, το οποίο συνδέει ηχεία AI με άλλες συσκευές IoT. Στο άμεσο μέλλον, πολίτες σε πολλές χώρες θα ωφεληθούν στην καθημερινότητά τους από τη χρήση συσκευών εξοπλισμένων με AI στα σπίτια τους. Επειδή τα ηχεία AI είναι συνήθως συνεχώς ενεργά, μπορούν να χρησιμοποιηθούν για την παροχή ζωτικών αποδεικτικών στοιχείων στην ψηφιακή εγκληματολογία, αν και αυτό εγείρει ζητήματα προστασίας της ιδιωτικής ζωής. Ήδη, ηχεία AI έχουν παράσχει αποδεικτικά στοιχεία σε υποθέσεις δολοφονιών στις Ηνωμένες Πολιτείες και στο Μεξικό, ενώ κυκλοφορούν χωρίς σαφείς ρυθμιστικές κατευθυντήριες γραμμές.

Στο [13], προτείνονται πέντε μέθοδοι ψηφιακής εγκληματολογικής ανάλυσης για τέσσερα μοντέλα ηχείων AI από διαφορετικούς κατασκευαστές που κυκλοφόρησαν στη Δημοκρατία της Κορέας. Οι προτεινόμενες μέθοδοι εφαρμόστηκαν σε όλα τα μοντέλα και τα αποτελέσματα παρουσιάζονται στο παράρτημα. Επιπλέον, αναπτύχθηκε ένα εργαλείο εγκληματολογικής ανάλυσης για τη συλλογή του ιστορικού εντολών χρήστη για το NAVER Clova. Εξετάζοντας δεδομένα από κινητές συσκευές και ηχεία AI, βρέθηκαν και ανακτήθηκαν αποθηκευμένα και διαγραμμένα δεδομένα φωνής.

Η αύξηση των επιθέσεων στον κυβερνοχώρο επηρεάζει τις επιδόσεις των οργανισμών του βιομηχανικού τομέα, εκμεταλλευόμενοι τα τρωτά σημεία των δικτυωμένων μηχανών. Η αυξανόμενη ψηφιοποίηση και οι τεχνολογίες που υπάρχουν στο πλαίσιο της Βιομηχανίας 4.0 έχουν οδηγήσει σε αύξηση των επενδύσεων στην καινοτομία και την αυτοματοποίηση. Ωστόσο, υπάρχουν κίνδυνοι που συνδέονται με αυτόν τον ψηφιακό μετασχηματισμό, ιδίως όσον αφορά τον κυβερνοχώρο ασφάλεια. Οι στοχευμένες επιθέσεις στον κυβερνοχώρο αλλάζουν και βελτιώνουν συνεχώς τις στρατηγικές επίθεσής τους, με μια έμφαση στην εφαρμογή τεχνητής νοημοσύνης στη διαδικασία εκτέλεσης. Επιθέσεις στον κυβερνοχώρο που βασίζονται στην τεχνητή νοημοσύνη μπορούν να χρησιμοποιηθούν σε συνδυασμό με συμβατικές τεχνολογίες, δημιουργώντας εκθετική ζημία σε οργανισμούς της Βιομηχανίας 4.0. Η αυξανόμενη εξάρτηση από τη δικτυωμένη τεχνολογία πληροφοριών έχει αύξησε την επιφάνεια κυβερνοεπιθέσεων. Υπό αυτή την έννοια, οι μελέτες που αποσκοπούν στην κατανόηση των δράσεων των κυβερνο εγκληματιών του

κυβερνοχώρου, ώστε να αναπτυχθούν γνώσεις για μέτρα ασφάλειας στον κυβερνοχώρο, είναι απαραίτητες.

Το [15] παρουσιάζει μια συστηματική βιβλιογραφική έρευνα για τον εντοπισμό δημοσιεύσεων σχετικά με επιθέσεις στον κυβερνοχώρο που βασίζονται στην τεχνητή νοημοσύνη (AI) και την ανάλυσή τους για την εξαγωγή μέτρων ασφάλειας στον κυβερνοχώρο. Στόχος της παρούσας μελέτης είναι να αξιοποιήσει βιβλιογραφικής ανάλυσης για τη διερεύνηση των επιπτώσεων αυτής της νέας απειλής, με στόχο να παράσχει στην ερευνητική κοινότητα με γνώσεις για την ανάπτυξη άμυνας έναντι πιθανών μελλοντικών απειλών. Τα αποτελέσματα μπορούν να χρησιμοποιηθούν για την καθοδήγηση την ανάλυση των επιθέσεων στον κυβερνοχώρο που υποστηρίζονται από την τεχνητή νοημοσύνη (AI).

Η ψηφιακή εγκληματολογία (DF) αποδεικνύεται ένα επείγον και ένα επίκαιρο θέμα προς διερεύνηση με τη σημαντική αύξηση των υπολογιστών εγκλημάτων αυτές τις μέρες. Τυπικά, η ανάλυση DF αποσκοπεί στη διατήρηση όλων των συλλεχθέντα αποδεικτικά στοιχεία στην πιο αρχική τους κατάσταση, προσδιορίζοντας, συλλογή και αξιολόγηση των ψηφιακών δεδομένων για την ανακατασκευή παρελθόντων περιστατικών. Τα περισσότερα αποδεικτικά στοιχεία που σχετίζονται με το ψηφιακό έγκλημα διατηρούνται εντός τα αρχεία του συστήματος του υπολογιστή.

Το [16] άρθρο διερευνά και αξιολογεί τα εφαρμοσιμότητα των τεχνικών νευρωνικών δικτύων στην ανάλυση ψηφιακή εγκληματολογία (DF) από αναλύοντας πληροφορίες που σχετίζονται με το σύστημα αρχείων του υπολογιστή για να για να προσδιοριστεί εάν έχουν χειραγωγηθεί από ένα συγκεκριμένο πρόγραμμα εφαρμογής. Ένα σύνολο δεδομένων περιγράφεται ως ένα διάνυσμα χαρακτηριστικών που σχετίζονται με τις δραστηριότητες του συστήματος αρχείων κατά τη διάρκεια μιας συγκεκριμένης χρονικής στιγμής συλλέγεται και χρησιμοποιείται για τη δημιουργία ενός μοντέλου ταξινόμησης νευρωνικού δικτύου. Το πειραματικά αποτελέσματα δείχνουν καλά αποτελέσματα σε σχέση με διάφορα μέτρα εκτίμησης της απόδοσης.

Οι δεξιότητες των εγκληματολογικών αναλυτών διακυβεύονται για την επεξεργασία των αυξανόμενων δεδομένων από το Διαδίκτυο των Πραγμάτων (IoT) που βασίζονται σε πλατφόρμες περιβάλλοντος. Οι απτές πηγές έχουν συχνά τα όρια μεγέθους, αλλά αυτό είναι δεν ισχύει για την πηγή κίνησης επικοινωνίας. Ως εκ τούτου, αυξάνεται η δίψα για ένα αποτελεσματική συγκριτική αξιολόγηση για την ανάλυση μεγάλων δεδομένων. Οι διαθέσιμες λύσεις μέχρι σήμερα έχουν χρησιμοποιήσει ένα προσέγγιση με βάση τις ανωμαλίες ή έχουν προτείνει προσεγγίσεις που βασίζονται στην απόκλιση από ένα κανονικό μοτίβο.

Για την αντιμετώπιση τους κατασχεθέντων bytes, οι συγγραφείς έχουν προτείνει μια προσέγγιση για μεγάλα δεδομένων, με αποτελεσματική ευαισθησία και ακρίβεια. Το [17] έχει προτείνει ένα γενικευμένο εγκληματολογικό πλαίσιο που χρησιμοποιεί τον προγραμματισμό της Google μοντέλο, το MapReduce ως ραχοκοκαλιά για τη μετάφραση της κίνησης, την εξαγωγή και την ανάλυση των δυναμικών χαρακτηριστικών κίνησης. Για την προτεινόμενη τεχνική, οι συγγραφείς χρησιμοποίησαν ανοικτού κώδικα εργαλεία όπως το Hadoop, το Hive, το Mahout και το R. Εκτός του ότι είναι ανοικτού κώδικα, αυτά τα υποστηρίζουν επεκτασιμότητα και

παράλληλη επεξεργασία. Τέλος, οι εγκληματολογικές μετρήσεις επιδόσεων του μοντέλου δείχνουν την αποτελέσματα με ευαισθησία 99%.

Ο κόσμος βιώνει αυξημένες κυβερνοεπιθέσεις σε όλους τους τομείς της καθημερινής ζωής, καθιστώντας την καταπολέμηση των εγκλημάτων στον κυβερνοχώρο καθημερινό αγώνα για άτομα και οργανισμούς. Οι επαγγελματίες ασφαλείας και οι ερευνητές ψηφιακής εγκληματολογίας αναγκάζονται να αναλύουν μεγάλες και σύνθετες δεξαμενές δεδομένων (Big Data) για να βρουν ψηφιακά αποδεικτικά στοιχεία (PDE) που μπορούν να στηρίξουν δικαστικές διαδικασίες. Η διαδικασία περιπλέκεται από την ποικιλία και την πολυπλοκότητα των δεδομένων. Η βαθιά μάθηση (DL), ως υποσύνολο της Τεχνητής Νοημοσύνης (AI), προσφέρει υποσχόμενες λύσεις για την ενίσχυση της καταπολέμησης του κυβερνοεγκλήματος, παρά το γεγονός ότι δεν αποτελεί πανάκεια.

Στο [21] οι συγγραφείς συζήτησαν τις τεχνικές βαθιάς μάθησης (DL) στην εγκληματολογία στον κυβερνοχώρο. Οι συγγραφείς το παρουσίασαν αυτό χρησιμοποιώντας το πλαίσιο ψηφιακής εγκληματολογίας βαθιάς μάθησης (DLCF). Με τις τρέχουσες τάσεις της καινοτόμων τεχνολογιών, νέοι τρόποι και τεχνικές θα είναι πάντα για την αντιμετώπιση διαφορετικών περιστατικών. Επομένως, είναι σημαντικό να δημιουργηθούν πλαίσια με τη δυνατότητα να βοηθήσουν στις εγκληματολογικές έρευνες καθώς και την υποστήριξη της εγκληματολογικής κοινότητας. Η βαθιά μάθηση (DL) έχει χρησιμοποιείται σε πολλούς κλάδους, εξ ου και η ανάγκη ενσωμάτωσής της στην εγκληματολογία στον κυβερνοχώρο.

Οι επιθέσεις Ransomware δεν περιορίζονται μόνο σε προσωπικούς υπολογιστές, αλλά αυξάνονται ραγδαία για να στοχεύσουν σε έξυπνες κινητές συσκευές (smart-phones). Οι επιτιθέμενοι στοχεύουν σε έξυπνες κινητές συσκευές (smart-phones) για να κλέψουν τις προσωπικές πληροφορίες των χρηστών για νομισματικούς σκοπούς. Ωστόσο, το Android (είναι λειτουργικό σύστημα για συσκευές κινητής τηλεφωνίας το οποίο τρέχει τον πυρήνα του λειτουργικού Linux) είναι το πιο διαδεδομένο λειτουργικό σύστημα κινητών τηλεφώνων με το μεγαλύτερο μερίδιο αγοράς στον κόσμο, γεγονός που το καθιστά πρωταρχικό στόχο για τις επιθέσεις των εγκληματιών του κυβερνοχώρου.

Το [23] επισημαίνει ότι η ανίχνευση ransomware Android με επιβλεπόμενες τεχνικές μηχανικής μάθησης έχει περιορισμούς, όπως η εξάρτηση από προμηθευτές αντι-ιών για ετικέτες, ο κίνδυνος λανθασμένης ταξινόμησης και η δυσκολία ανίχνευσης άγνωστων ransomware σε πραγματικό χρόνο. Αυτή η εργασία διερευνά το Android ransomware μέσω αντίστροφης μηχανικής και εγκληματολογικής ανάλυσης για την εξαγωγή στατικών χαρακτηριστικών. Προτείνεται το πλαίσιο RansomDroid, το οποίο χρησιμοποιεί μη επιβλεπόμενη μηχανική μάθηση και Gaussian Mixture Model για την ανίχνευση απρόβλεπτου ransomware. Το RansomDroid ενσωματώνει επιλογή χαρακτηριστικών και μείωση διάστασης, επιτυγχάνοντας ακρίβεια 98,08% σε 44 ms.

Σήμερα, περισσότερο από ποτέ, οι δραστηριότητες ψηφιακής εγκληματολογίας εμπλέκονται σε κάθε ποινική, πολιτική ή στρατιωτική έρευνα και αποτελούν θεμελιώδες εργαλείο για την υποστήριξη της ασφάλειας στον κυβερνοχώρο. Οι ερευνητές χρησιμοποιούν μια ποικιλία τεχνικών και ιδιόκτητων εφαρμογών εγκληματολογίας λογισμικού για να εξετάσουν το αντίγραφο

των ψηφιακών συσκευών, αναζητώντας κρυμμένα, διαγραμμένα, κρυπτογραφημένα ή κατεστραμμένα αρχεία ή φακέλους. Οποιοδήποτε αποδεικτικό στοιχείο βρεθεί αναλύονται προσεκτικά και τεκμηριώνονται σε μια «έκθεση ευρημάτων» για την προετοιμασία νομικών διαδικασιών που που αφορούν την ανακάλυψη, τις καταθέσεις ή την πραγματική δικαστική διαμάχη. Ο στόχος είναι να ανακαλυφθούν και να αναλυθούν μοτίβα δόλιων δραστηριοτήτων.

Στο [24] προτείνεται μια νέα μεθοδολογία για την υποστήριξη των ερευνητών κατά τη διάρκεια της διαδικασία ανάλυσης, συσχετίζοντας στοιχεία που βρέθηκαν μέσω διαφορετικών εργαλείων εγκληματολογίας. Η μεθοδολογία υλοποιήθηκε μέσω ενός συστήματος που είναι σε θέση να προσθέτει σημασιολογικό ισχυρισμό στα δεδομένα που παράγονται από εργαλεία εγκληματολογίας κατά τη διάρκεια των διαδικασιών εξαγωγής. Αυτοί οι ισχυρισμοί επιτρέπουν την αποτελεσματικότερη πρόσβαση σε σχετικές πληροφορίες και βελτιωμένες δυνατότητες ανάκτησης και συλλογισμού. Η μεθοδολογία αυτή, είναι μια σημασιολογική μεθοδολογία που χρησιμοποιεί τεχνικές επεξεργασίας φυσικής γλώσσας (NLP- αυτές οι τεχνικές αποσκοπούν στην αυτόματη εξαγωγή δομημένων πληροφοριών από αδόμητα ή ημιδομημένα έγγραφα, γραμμένα σε φυσική γλώσσα) για την εξαγωγή και αναπαράσταση αδόμητης πληροφορίας σε τυποποιημένη μορφή. Επιλέχθηκε ο τομέας της εγκληματολογίας υπολογιστών, όπου απαιτείται εξαγωγή και ανάκτηση πληροφοριών, καθώς και συσχέτιση δεδομένων από διαφορετικές πηγές. Η σημασιολογική προσέγγιση διευκολύνει τη δημιουργία σχέσεων μεταξύ οντοτήτων στον τομέα αυτό και, μέσω των σύγχρονων μηχανισμών εξαγωγής συμπερασμάτων, επιτρέπει την άντληση σιωπηρής γνώσης από τις αποδείξεις.

Το [25] αποσκοπεί στην εξεύρεση βελτιωμένων και εκτεταμένων τρόπους ενίσχυσης, διεύρυνσης και ενίσχυσης των τεχνικών της εγκληματολογικής επιστήμης σε όλους τους κλάδους της με τη χρήση των σύγχρονων επιστημών και τεχνολογιών και χρησιμοποιώντας επίσης τις νέες, τελευταίες και επερχόμενες τεχνολογίες, όπως η Τεχνητή Νοημοσύνη (AI). Η τεχνητή νοημοσύνη (AI) έχει μια τεράστια ποικιλία εφαρμογών, με προκαταρκτική είναι η διερεύνηση της σκηνής εγκλήματος μέχρι την μέχρι την τελική απόφαση που εκδίδεται από το δικαστήριο, η τεχνητή νοημοσύνη (AI) παρουσιάζουν μεγάλες δυνατότητες στην ακρίβεια των αποτελεσμάτων.

Απ'όσο βλέπουμε, το άρθρο ασχολείται μόνο με δύο από τις διάφορες τεχνολογίες τεχνητής νοημοσύνης που μπορούν να εισαχθούν και υπάρχουν και άλλες τεκμηριωμένες και απροσδιόριστες λύσεις που μπορούν να ενσωματωθούν στον τομέα της Ιατροδικαστικής Επιστήμης. Η πλήρης εφαρμογή της Τεχνητής Νοημοσύνης στην Ιατροδικαστική είναι πολύ νωρίς για να γνωρίζουμε, διότι βρισκόμαστε στα αρχικά στάδια. Προς το παρόν, η Τεχνητή Νοημοσύνη χρησιμοποιείται στην 1) Αυτοματοποίηση της συγκεκριμένων ενοτήτων (π.χ. για την αναζήτηση του τύπου αρχείου) και 2) την καθοδήγηση εμπειρογνωμόνων για την ολοκλήρωση συγκεκριμένων εργασιών. Οι επιστήμονες έχουν πειραματιστεί σε συνδυασμό με άλλες τρέχουσα τεχνολογία και θα χρειαστεί αρκετός χρόνος για να μεταναστεύσουν πλήρως στην τεχνητή νοημοσύνη και θα χρειαστούν χρόνο για να δούμε ποιες εξελίξεις θα οδηγήσουν στη σύγχρονη κόσμο.

3.4 Research και grey literature

3.4.1 Research Papers (Ερευνητικά Άρθρα)

Είναι οι επιστημονικές δημοσιεύσεις που παρουσιάζουν πρωτότυπη έρευνα, πειράματα, αναλύσεις ή θεωρητικές μελέτες. Συνήθως δημοσιεύονται σε επιστημονικά περιοδικά και συνέδρια και έχουν περάσει από διαδικασία αξιολόγησης από ομότιμους (peer review). Αυτό σημαίνει ότι άλλοι ειδικοί στον τομέα εξετάζουν και επικυρώνουν την ποιότητα και την εγκυρότητα της έρευνας πριν αυτή δημοσιευτεί.

Οι ερευνητικές εργασίες είναι δομημένες με συγκεκριμένο τρόπο, περιλαμβάνοντας τίτλο, περίληψη, εισαγωγή, μεθοδολογία, αποτελέσματα, συζήτηση και βιβλιογραφία. Στόχος τους είναι να συμβάλλουν στη γνώση του επιστημονικού τομέα και να αναγνωριστούν από την ακαδημαϊκή κοινότητα. Η πρωτοτυπία και η αυστηρή επιστημονική μεθοδολογία είναι βασικά χαρακτηριστικά τους, καθιστώντας τα αξιόπιστες πηγές πληροφοριών.

3.4.2 Grey Literature (Γκρίζα Βιβλιογραφία)

Είναι τα έγγραφα και το υλικό που δεν εκδίδονται εμπορικά ή δεν διανέμονται ευρέως μέσω τυπικών καναλιών έκδοσης. Αυτά τα έγγραφα μπορεί να περιλαμβάνουν τεχνικές εκθέσεις από κυβερνητικούς οργανισμούς, ερευνητικά ινστιτούτα ή ιδιωτικούς οργανισμούς, διπλωματικές και διδακτορικές διατριβές, εκθέσεις συνεδρίων που δεν έχουν δημοσιευθεί σε επίσημα περιοδικά, λευκά βιβλία (white papers) που παρουσιάζουν την άποψη ή την πολιτική ενός οργανισμού για ένα συγκεκριμένο θέμα, εσωτερικές εκθέσεις για εσωτερική χρήση εντός οργανισμών ή εταιρειών, και δεδομένα και στατιστικές αναφορές.

Η γκρίζα βιβλιογραφία καλύπτει ένα ευρύ φάσμα θεμάτων και μορφών και μπορεί να είναι εξαιρετικά χρήσιμη, καθώς συχνά περιλαμβάνει πρωτογενείς πηγές και δεδομένα που δεν είναι διαθέσιμα αλλού. Ωστόσο, απαιτεί προσεκτική αξιολόγηση της ποιότητας και της αξιοπιστίας της, καθώς μπορεί να μην έχει περάσει από αυστηρή διαδικασία αξιολόγησης όπως τα ερευνητικά άρθρα.

3.4.3 Πίνακας κατηγοριοποίησης των άρθρων

Πίνακας 3: Κατηγοριοποίηση άρθρων και δημοσιεύσεων.

Paper	Research	Grey Literature
[1]		✓
[2]		✓
[3]		✓
[4]		✓
[5]		✓
[6]		✓
[8]		✓
[9]	✓	
[10]		✓
[11]		✓
[12]		✓
[13]		✓
[14]	✓	
[15]		✓
[16]		✓
[17]		✓
[18]	✓	
[19]	✓	
[20]	✓	
[21]		✓
[22]	✓	
[23]		✓
[24]		✓
[25]		✓
[26]	✓	
[27]	✓	
[28]	✓	

3.5 Σύγκριση με την παρούσα εργασία

Δεδομένων των επιλεγμένων papers και του περιεχομένου τους, η παρούσα εργασία προσφέρει μια εμπεριστατωμένη ανάλυση των επιπτώσεων κυβερνοεγκληματιών στην πραγματικότητα, σε αντίθεση με τις περισσότερες άλλες μελέτες που επικεντρώνονται απλώς στην καταγραφή των επιθέσεων ή στην ανάλυση τεχνικών επιθέσεων. Εδώ εξετάζονται τα πραγματικά αποτελέσματα και οι επιπτώσεις των κυβερνοεγκληματιών μέσα από συγκεκριμένες περιπτώσεις και αναλύσεις, παρέχοντας έτσι μια ποιοτική και ενδελεχή εκτίμηση των καταστάσεων.

Η μεθοδολογία που χρησιμοποιήθηκε στην παρούσα έρευνα είναι συγκρίσιμη με αυτήν που χρησιμοποιήθηκε στα papers [29] & [30]. Συγκεκριμένα, αναλύονται επιθέσεις πραγματικού κόσμου και σε περιβάλλον δοκιμών, ενώ δεν επικεντρώνονται ειδικά στον τομέα σας. Αυτό καθιστά την ανάλυση επιπτώσεων και τη συστηματική ανάλυση πιο εμπεριστατωμένες και χρήσιμες για τους φορείς εκμετάλλευσης.

Η παρούσα έρευνα διαφέρει σε ουσιαστικό βαθμό από τις παραπάνω αναφερθείσες μελέτες, καθώς προσφέρει μια συστηματική και ενδελεχή ανάλυση των επιπτώσεων και της αξιολόγησης σε πραγματικές επιθέσεις, που είναι άμεσα εφαρμόσιμη στην πραγματικότητα.

4

Ανάλυση group που συμπεριλαμβάνονται στην εργασία

4.1 Συγκεντρωτικός πίνακας για τις κατηγορίες των άρθρων

Ο παρακάτω πίνακας (Πίνακας 4) περιέχει κατηγοριοποιημένες πληροφορίες από διάφορες επιστημονικές δημοσιεύσεις, οργανωμένες με βάση τα κύρια θέματα που εξετάζουν. Οι κατηγορίες αυτές περιλαμβάνουν έρευνες (Survey), πολυμέσα (Multimedia), κινητές συσκευές (Mobile devices), κυβερνοεπιθέσεις (Cyberattacks), υπολογιστικό νέφος (Cloud), αλγόριθμους (Algorithms), δικανική ανάλυση δικτύου (Network Forensics), botnet, ανασκοπήσεις (Review), το Διαδίκτυο των Πραγμάτων (IoT), καταγραφές (Logs), εργαλεία (Tools), πρακτικές (Practice), και ransomware. Κάθε κατηγορία αντιπροσωπεύει ένα συγκεκριμένο πεδίο έρευνας στον τομέα της κυβερνοασφάλειας και των σχετικών τεχνολογιών, παρέχοντας μια οργανωμένη εικόνα των δημοσιευμένων εργασιών και των ερευνητικών τους θεμάτων. Όλες αυτές οι κατηγορίες που προαναφέρω, έχουν προκύψει είτε από τον τίτλο του κάθε paper, είτε από την ανάγνωση της περίληψης του άρθρου, είτε από την ανάγνωση του πλήρους κειμένου.

Πίνακας 1:Κατηγοριοποίση των papers.

Paper	Survey	Multimedia	Mobile devices	Cyberattacks	Cloud	Algorithms	Network Forensics	Botnet	Review
[1]						✓			
[2]	✓						✓	✓	
[3]						✓			
[4]						✓			
[5]					✓				
[6]			✓						
[8]				✓					
[9]									✓
[10]	✓								
[11]		✓							
[13]		✓							
[14]	✓								
[15]	✓			✓					
[19]						✓			
[21]				✓					
[23]			✓						
[26]						✓			
[28]									✓

Paper	IoT	Logs	Tools	Practice	Ransomware
[12]					
[16]		✓			
[17]	✓				
[18]			✓		
[20]				✓	
[22]		✓			
[23]					✓
[24]		✓			
[25]					
[27]	✓				

4.1.1 Ανάλυση με βάση τα άρθρα

4.1.1.1 Survey

Το [2] είναι survey paper επειδή συνοψίζει και αναλύει την υπάρχουσα βιβλιογραφία και τις σύγχρονες τεχνικές στον τομέα, προσφέροντας μια συστηματική επισκόπηση και εντοπίζοντας τις μελλοντικές ανάγκες έρευνας. Η καινοτομία έγκειται στην εισαγωγή νέων τεχνικών και μεθόδων για την ανίχνευση και διερεύνηση επιθέσεων δικτύου, βελτιώνοντας σημαντικά την ανάλυση δεδομένων δικτύου.

Το [10] είναι survey paper γιατί παρέχει μια ανασκόπηση της υπάρχουσας βιβλιογραφίας και των τρεχουσών τεχνικών, συγκρίνοντας και αντιπαραθέτοντας διάφορες προσεγγίσεις για να εντοπίσει κενά και να προτείνει βελτιώσεις. Το άρθρο αναδεικνύει τη σημασία της εφαρμογής μηχανικής μάθησης για τη βελτίωση της ανίχνευσης και ανάλυσης ψηφιακών αποδεικτικών στοιχείων.

Το [14] είναι survey paper γιατί συγκεντρώνει και αναλύει τις τρέχουσες μεθόδους και τεχνικές, παρέχοντας μια ολοκληρωμένη επισκόπηση της υπάρχουσας κατάστασης της τέχνης στον τομέα. Η καινοτομία έγκειται στην αναλυτική προσέγγιση της χρήσης τεχνητής νοημοσύνης για την ανίχνευση κυβερνοαπειλών, βελτιώνοντας την ασφάλεια των συστημάτων.

Το [15] survey paper διότι ανασκοπεί τη βιβλιογραφία, συγκεντρώνει υπάρχουσες μελέτες και αναλύει τα ευρήματα για να προσφέρει κατευθύνσεις για τη μελλοντική έρευνα. Το άρθρο συμβάλλει στην κατανόηση των κινδύνων και την ανάπτυξη λύσεων για την αντιμετώπιση των νέων απειλών στην εποχή της Βιομηχανίας 4.0.

4.1.1.2 Multimedia

Το άρθρο [11] κατατάσσεται στην κατηγορία των πολυμέσων λόγω της εστίασής της σε φωτογραφίες και βίντεο και της ανίχνευσης της χειραγώγησής τους με τη χρήση τεχνικών ML, υπογραμμίζοντας τη σημασία των ισχυρών εγκληματολογικών μεθόδων για την αυθεντικοποίηση ψηφιακών αρχείων που χρησιμοποιούνται σε διάφορα εγκλήματα στον κυβερνοχώρο.

4.1.1.3 Mobile devices

Το [6] εμπίπτει στην κατηγορία των κινητών συσκευών, επειδή ασχολείται ειδικά με ζητήματα που αφορούν την εγκληματολογική ανάλυση δεδομένων από smartphones και άλλο κινητό εξοπλισμό, αναδεικνύοντας τη σημασία των ισχυρών μεθοδολογιών για την αντιμετώπιση των πολύπλοκων ψηφιακών αποδεικτικών στοιχείων στο πλαίσιο των κινητών συσκευών.

Το [23] ανήκει στην κατηγορία των κινητών συσκευών, επειδή στοχεύει ειδικά στην εγκληματολογική ανάλυση ransomware σε smartphones Android, τονίζοντας την ανάγκη για προηγμένες και αξιόπιστες μεθόδους ανίχνευσης για την προστασία των κινητών χρηστών από απειλές στον κυβερνοχώρο.

4.1.1.4 Cyberattacks

Το [8] κατατάσσεται στην κατηγορία των cyberattacks επειδή ασχολείται με την ανίχνευση και την ανάλυση εγκληματικών δραστηριοτήτων στον σκοτεινό ιστό, χρησιμοποιώντας τεχνικές AI για την καταπολέμηση των απειλών στον κυβερνοχώρο.

Το [15] ανήκει στην κατηγορία των cyberattacks διότι εξετάζει τις τεχνικές και στρατηγικές που χρησιμοποιούν οι κυβερνοεγκληματίες για να εκτελέσουν επιθέσεις χρησιμοποιώντας τεχνητή νοημοσύνη, προσφέροντας γνώση για την αντιμετώπιση αυτών των επιθέσεων και την ενίσχυση της ασφάλειας στον βιομηχανικό τομέα.

Το [21] κατατάσσεται στην κατηγορία των cyberattacks λόγω της εστίασής του στην ανάλυση κυβερνοεπιθέσεων με τη χρήση τεχνικών βαθιάς μάθησης για τη βελτίωση της εγκληματολογικής ανάλυσης και την υποστήριξη των διαδικασιών λήψης αποφάσεων σε δικαστικές υποθέσεις που σχετίζονται με κυβερνοεγκλήματα.

4.1.1.5 Cloud

Το [13] εντάσσεται στην κατηγορία του νέφους λόγω της εστίασής της σε περιβάλλοντα δικτύων νέφους, της επεκτασιμότητας για την αντιμετώπιση σημαντικών όγκων κυκλοφορίας και της αποδοτικής αξιοποίησης εικονικών πόρων για την παρακολούθηση.

4.1.1.6 Algorithms

Το [1] ανήκει στην κατηγορία των αλγορίθμων επειδή χρησιμοποιεί τον Προγραμματισμό Συνόλων Απαντήσεων (ASP), μια αλγοριθμική μέθοδο που επιλύει προβλήματα μέσω υπολογιστικής λογικής. Ο ASP αυτοματοποιεί την ανάλυση αποδεικτικών στοιχείων στην ψηφιακή εγκληματολογία, μετατρέποντας σύνθετες ερευνητικές περιπτώσεις σε προβλήματα βελτιστοποίησης. Αυτή η αλγοριθμική προσέγγιση βοηθά στη δημιουργία υποθέσεων και στη διαμόρφωση σεναρίων, υποστηρίζοντας την ανάπτυξη συστημάτων υποστήριξης απόφασης (DSS). Ενισχύει την αποτελεσματικότητα και τη διαφάνεια στη διαδικασία ανάλυσης ψηφιακών δεδομένων.

Το [3] ανήκει στην κατηγορία των αλγορίθμων επειδή χρησιμοποιεί αλγορίθμους μηχανικής μάθησης (ML) για την ανάλυση μεταδεδομένων αρχείων στην ψηφιακή εγκληματολογία. Οι αλγόριθμοι αυτοί βοηθούν στην αποκάλυψη αποδεικτικών στοιχείων και καθοδηγούν την έρευνα προς τη σωστή κατεύθυνση. Μέσω της εφαρμογής τους, οι ερευνητές μπορούν να εντοπίσουν κρίσιμες πληροφορίες και να βελτιώσουν την ακρίβεια της έρευνας, χωρίς να σπαταλούν πόρους σε λανθασμένες υποθέσεις. Η αλγοριθμική προσέγγιση είναι κεντρική για την αποτελεσματικότητα αυτής της διαδικασίας.

Το [4] ανήκει στην κατηγορία των αλγορίθμων διότι εξετάζει τη χρήση της μηχανικής μάθησης (ML), η οποία βασίζεται σε αλγοριθμικές διαδικασίες για την ανάλυση μεγάλων ποσοτήτων δεδομένων στην ψηφιακή εγκληματολογία (DF). Οι αλγόριθμοι ML μαθαίνουν από

προηγούμενα δεδομένα για να προβλέπουν μελλοντικές εγκληματικές συμπεριφορές, ενισχύοντας έτσι την αποτελεσματικότητα των ψηφιακών ερευνών. Η χρήση τους επιτρέπει την αυτόματη αναγνώριση μοτίβων και την αποκάλυψη εγκληματικών προθέσεων σε μεγάλα και ετερογενή σύνολα δεδομένων.

Το [9] ανήκει στην κατηγορία των αλγορίθμων διότι εξετάζει τη χρήση της εξηγήσιμης τεχνητής νοημοσύνης (XAI) για την ανάλυση ψηφιακών αποδεικτικών στοιχείων. Η XAI βασίζεται σε αλγόριθμους AI για την ταξινόμηση, ανάλυση και ερμηνεία των δεδομένων, επιτρέποντας στους ερευνητές να κατανοούν και να εξηγούν τα αποτελέσματα των μοντέλων. Επιπλέον, θίγει τον κίνδυνο της "αντίθετης" μηχανικής μάθησης, η οποία περιλαμβάνει αλλοιωμένα δεδομένα που μπορούν να επηρεάσουν την αξιοπιστία των αλγορίθμων. Οι αλγόριθμοι αυτοί είναι κρίσιμοι για τη βελτίωση της ψηφιακής εγκληματολογίας και την αποφυγή σφαλμάτων.

Το [26] ανήκει στην κατηγορία των αλγορίθμων διότι εξετάζει την εφαρμογή αλγορίθμων μηχανικής μάθησης στην ασφάλεια και την εγκληματολογία στον κυβερνοχώρο. Οι αλγόριθμοι μηχανικής μάθησης είναι ζωτικής σημασίας για την ανίχνευση και πρόληψη κυβερνοεπιθέσεων, καθώς και για την ανάλυση ψηφιακών αποδεικτικών στοιχείων. Επίσης, το άρθρο διερευνά την εφαρμογή πιο εξελιγμένων αλγορίθμων, όπως της βαθιάς μάθησης και της υπολογιστικής νοημοσύνης, για τη βελτίωση της ασφάλειας στον κυβερνοχώρο, ανοίγοντας νέους δρόμους έρευνας.

Το [28] ανήκει στην κατηγορία των αλγορίθμων καθώς αναλύει την εφαρμογή αλγορίθμων μηχανικής μάθησης για τη βελτίωση της ψηφιακής εγκληματολογίας. Οι αλγόριθμοι αυτοί χρησιμοποιούνται για την ανάλυση και ερμηνεία ψηφιακών αποδεικτικών στοιχείων, διευκολύνοντας τις διαδικασίες συλλογής και ανάλυσης δεδομένων. Επιπλέον, η μελέτη συγκρίνει διάφορους αλγόριθμους με βάση τυποποιημένα κριτήρια, προσφέροντας έτσι μια αναλυτική προσέγγιση στη χρήση αλγορίθμων στη ψηφιακή εγκληματολογία, ενώ ταυτόχρονα επισημαίνει τους περιορισμούς τους.

4.1.1.7 Network Forensics

Το άρθρο [2] ανήκει στην κατηγορία των δικτυακών εγκληματολογικών ερευνών (network forensics) διότι επικεντρώνεται στην αναγνώριση και διερεύνηση επιθέσεων σε δίκτυα, την ανάλυση δικτυακής κίνησης και την αντιμετώπιση των προκλήσεων που σχετίζονται με τον τεράστιο όγκο των δεδομένων που πρέπει να αναλυθούν.

4.1.1.8 Botnet

Το [2] ανήκει στην κατηγορία των botnet, καθώς αντιμετωπίζει τις προκλήσεις της ανάλυσης μεγάλου όγκου δεδομένων δικτύου και την ανάγκη για ακριβή ανίχνευση επιθέσεων. Εξετάζει τη χρήση εργαλείων τεχνητής νοημοσύνης και μηχανικής μάθησης για την ανίχνευση και ταξινόμηση της δικτυακής κίνησης.

4.1.1.9 Review

Το [7] ανήκει στην κατηγορία των ανασκοπήσεων (review) καθώς παρουσιάζει μια ολοκληρωμένη μελέτη των τεχνικών και των αλγορίθμων μηχανικής μάθησης που χρησιμοποιούνται για την ανίχνευση και την ανάλυση επιθέσεων botnet. Η ανασκόπηση αυτή βοηθά τους ερευνητές να κατανοήσουν την τρέχουσα κατάσταση του πεδίου και να αναπτύξουν νέες μεθόδους για την αντιμετώπιση των επιθέσεων.

Το [9] ανήκει στην κατηγορία των ανασκοπήσεων (review) και επικεντρώνεται στη χρήση της βαθιάς μάθησης στις ψηφιακές εγκληματολογικές έρευνες.

Το [28] ανήκει στην κατηγορία των των ανασκοπήσεων (review), καθώς επικεντρώνεται στην ανασκόπηση της υπάρχουσας βιβλιογραφίας σχετικά με την εφαρμογή τεχνικών μηχανικής μάθησης (ML) στην ψηφιακή εγκληματολογία (DF), ειδικά σε έξυπνα περιβάλλοντα με συσκευές Διαδικτύου των Πραγμάτων (IoT).

4.1.1.10 IoT

Το [17] ανήκει στην κατηγορία του Διαδικτύου των Πραγμάτων (IoT) επειδή εστιάζει στην επεξεργασία δεδομένων που προέρχονται από πλατφόρμες περιβάλλοντος και συσκευές IoT. Αναφέρει την αυξανόμενη ποσότητα δεδομένων επικοινωνίας που δημιουργούνται από αυτές τις συσκευές και τονίζει την ανάγκη για αποτελεσματική ανάλυση μεγάλων δεδομένων. Οι προτεινόμενες τεχνικές, όπως το εγκληματολογικό πλαίσιο με το MapReduce, χρησιμοποιούνται για την εξαγωγή και ανάλυση χαρακτηριστικών κίνησης που σχετίζονται με το IoT. Το άρθρο συνδέει την εγκληματολογική ανάλυση με το IoT μέσω της ανάγκης διαχείρισης αυτών των αυξημένων δεδομένων.

Το [27] ανήκει στην κατηγορία του Διαδικτύου των Πραγμάτων (IoT) καθώς εστιάζει στις προκλήσεις που προκύπτουν από τη χρήση έξυπνων περιβαλλόντων, τα οποία βασίζονται σε συσκευές IoT. Αυτά τα περιβάλλοντα παράγουν τεράστιους όγκους κατανεμημένων και ποικιλόμορφων δεδομένων, που ξεπερνούν τις δυνατότητες των ερευνητών ψηφιακής εγκληματολογίας (DF) να τα διαχειριστούν με παραδοσιακές μεθόδους.

4.1.1.11 Logs

Το [16] ανήκει στην κατηγορία των logs λόγω της ανάλυσης που πραγματοποιεί σχετικά με τις δραστηριότητες του συστήματος αρχείων του υπολογιστή. Κατά την ανάλυση αυτή, το άρθρο χρησιμοποιεί ένα σύνολο δεδομένων το οποίο περιγράφει διάφορες δραστηριότητες των αρχείων σε συγκεκριμένα χρονικά διαστήματα. Σκοπός της ανάλυσης είναι η αναγνώριση τυχόν τροποποιήσεων που έχουν επιφέρει επιθέσεις ή παραβιάσεις της ακεραιότητας των αρχείων.

Το [22] ανήκει στην κατηγορία των αρχείων καταγραφής λόγω της εστίασής του στη διαχείριση και ανάλυση αρχείων καταγραφής πρόσβασης. Τα αρχεία καταγραφής διαδραματίζουν κρίσιμο ρόλο στην ψηφιακή εγκληματολογία και την ασφάλεια, ιδίως σε περιβάλλοντα IoT.

Το [24] συνδέεται με την κατηγορία των logs λόγω της ανάλυσης που πραγματοποιεί σε ψηφιακά δεδομένα που παράγονται από εργαλεία ψηφιακής εγκληματολογίας.

4.1.1.12 Tools

Το [18] ανήκει στην κατηγορία των εργαλείων στον τομέα της ψηφιακής εγκληματολογίας λόγω της προηγμένης τεχνολογικής λύσης που προτείνει για την ανάλυση και διερεύνηση ψηφιακών αποδείξεων κατά τη διάρκεια εγκληματικών ερευνών.

4.1.1.13 Practice

Το [20] ανήκει στην κατηγορία των πρακτικών καθώς περιγράφει την εφαρμογή και εκπαίδευση τεχνητών νευρωνικών δικτύων με τη χρήση της βιβλιοθήκης TensorFlow για την ανάλυση ψηφιακών στοιχείων. Η μελέτη επικεντρώνεται σε συγκεκριμένες τεχνικές πρακτικής χρήσης της μηχανικής μάθησης σε εγκληματολογικές έρευνες, όπως η εκπαίδευση μοντέλων και η ανάλυση αποδεικτικών στοιχείων. Επιπλέον, παρέχει παραδείγματα και αποτελέσματα που μπορούν να χρησιμοποιηθούν ως αναφορά για μελλοντικές έρευνες, δείχνοντας πώς αυτά τα εργαλεία εφαρμόζονται στην πράξη.

4.1.1.14 Ransomware

Το [23] ανήκει στην κατηγορία των ransomware επειδή μολύνει τη συσκευή του θύματος και απαιτεί λύτρα για την απελευθέρωση της συσκευής ή των δεδομένων. Εκμεταλλεύεται τα προσωπικά δεδομένα του χρήστη, τα μεταφέρει σε εξυπηρετητή ελέγχου, και εμφανίζει απειλητικά μηνύματα ζητώντας πληρωμή. Χρησιμοποιεί μηχανική μάθηση χωρίς επίβλεψη για την ανίχνευση ransomware σε πραγματικό χρόνο. Αυτή η προσέγγιση επιτρέπει την ανίχνευση άγνωστων δειγμάτων και την αντιμετώπιση νέων απειλών.

4.2 Άρθρα που ξεχωρίζουν γιατι εχουν κανει ουσιώδη δουλειά

Άρθρο [1]: Υπογραμμίζει την ανάγκη αποτελεσματικών ψηφιακών εγκληματολογικών εργαλείων για την αυτοματοποίηση της ταυτοποίησης ψηφιακών αποδεικτικών στοιχείων. Περιλαμβάνει τη χρήση του διακριτού μετασχηματισμού Fourier (DFT) για την εξαγωγή χαρακτηριστικών από αρχεία πολυμέσων και συγκρίνει μοντέλα βαθιάς μάθησης όπως τα Convolutional Neural Networks (CNN) και τα Support Vector Machines (SVM).

Άρθρο [4]: Επικεντρώνεται στη χρήση της βαθιάς μάθησης στις ψηφιακές εγκληματολογικές έρευνες. Εξετάζει τις μεθόδους ανάλυσης ψηφιακών αποδεικτικών στοιχείων, ειδικά με συνελικτικά νευρωνικά δίκτυα (CNN), και τονίζει τη σημασία της ανάλυσης ψηφιακών μέσων στις εγκληματολογικές έρευνες.

Άρθρο [2]: Περιγράφει τη διαδικασία προετοιμασίας συνόλου δεδομένων, εξαγωγής χαρακτηριστικών και δημιουργίας μοντέλου με επίβλεψη. Η τεχνική αυτή ενισχύει την ακεραιότητα των ψηφιακών αποδεικτικών στοιχείων και αποκαλύπτει αλλαγές σε βίντεο που έχουν υποστεί μετα-επεξεργασία, καθιστώντας τα κατάλληλα για νομικές διαδικασίες.

Άρθρο [5]: Παρέχει μεθόδους για προεπεξεργασία, εξαγωγή χαρακτηριστικών και μετατροπή του συνόλου δεδομένων για την ενσωμάτωση προηγμένων μεθόδων Μηχανικής Μάθησης (ML) σε εγκληματολογικά εργαλεία, ενισχύοντας την αποτελεσματικότητά τους σε πραγματικές εφαρμογές

Άρθρο [16]: Εφαρμόζει νευρωνικά δίκτυα για την ανάλυση και ταξινόμηση ψηφιακών δεδομένων από το σύστημα αρχείων ενός υπολογιστή. Οι βασικοί στόχοι περιλαμβάνουν την αναγνώριση απόπειρων παραβίασης της ακεραιότητας αρχείων και την ανίχνευση κακόβουλου λογισμικού.

Άρθρο [19]: Συζητά τη χρήση της μηχανικής μάθησης στην ψηφιακή εγκληματολογία, εστιάζοντας στην ανάπτυξη και εφαρμογή αλγορίθμων που δίνουν προτεραιότητα στη διαφάνεια και την εξηγήσιμότητα. Οι αλγόριθμοι Μηχανικής Μάθησης (ML) προσφέρουν λύσεις για την υπέρβαση της πολυπλοκότητας και τη διαχείριση μεγάλου όγκου δεδομένων.

Άρθρο [18]: Περιγράφει ένα πολύπλοκο σύστημα πολλαπλών πρακτόρων που αναλύει και συσχετίζει δεδομένα αποδείξεων, μειώνοντας τον όγκο των δεδομένων που απαιτούν ανθρώπινη επέμβαση. Η εφαρμογή της Τεχνητής Νοημοσύνης (AI) βελτιώνει την αποδοτικότητα και την ταχύτητα στην εξερεύνηση των δεδομένων.

4.3 Τάσεις που ξεχωρίζουν ανά ομάδα

4.3.1 Αντιμετώπιση του Μεγάλου Όγκου Δεδομένων στην Ψηφιακή Εγκληματολογία (DF)

Η πρώτη σημαντική τάση αφορά την αντιμετώπιση του τεράστιου όγκου δεδομένων που καλούνται να διαχειριστούν οι ψηφιακές εγκληματολογικές έρευνες. Η αύξηση των πηγών ψηφιακών δεδομένων, όπως το Διαδίκτυο των Πραγμάτων (IoT), τα κοινωνικά δίκτυα, και τα πολυμέσα, δημιουργεί μια νέα πραγματικότητα στην οποία τα παραδοσιακά εργαλεία ανάλυσης δεν μπορούν να ανταποκριθούν. Οι ερευνητές επικεντρώνονται στη βελτίωση των συστημάτων και των τεχνικών για τη διαχείριση και ανάλυση αυτών των δεδομένων με μεγαλύτερη αποδοτικότητα.

Ένα σημαντικό εργαλείο που ανταποκρίνεται σε αυτήν την ανάγκη είναι το MultiAgent Digital Investigation Toolkit (MADIK), το οποίο χρησιμοποιεί ευφυείς πράκτορες για τη διαχείριση μεγάλων ποσοτήτων δεδομένων και την αυτοματοποίηση της ταυτοποίησης των ψηφιακών αποδεικτικών στοιχείων. Η καινοτομία του MADIK είναι ότι επιτρέπει την κατανομή των εργασιών και τη μείωση του χρόνου που απαιτείται για την ανάλυση των δεδομένων. Αυτή η προσέγγιση μειώνει την ανθρώπινη παρέμβαση, βελτιώνοντας παράλληλα την ταχύτητα και την ακρίβεια της ανάλυσης. [18] [16]

4.3.1.1 Κύρια χαρακτηριστικά της τάσης

- ✓ Αυτοματοποίηση της ταυτοποίησης ψηφιακών αποδεικτικών στοιχείων.
- ✓ Ελαχιστοποίηση του χρόνου και των πόρων που απαιτούνται για την επεξεργασία μεγάλου όγκου δεδομένων.
- ✓ Χρήση ευφυών πρακτόρων που αναλαμβάνουν την κατανομή και τη διαχείριση των δεδομένων.
- ✓ Αυτό το εργαλείο δείχνει την κατεύθυνση της έρευνας προς την ανάπτυξη πιο ευέλικτων και ισχυρών τεχνολογιών για την ανάλυση δεδομένων, εστιάζοντας στη μείωση της ανθρώπινης επέμβασης και στην επιτάχυνση της εγκληματολογικής διαδικασίας.

4.3.1.2 Πρόβλημα

Η ραγδαία αύξηση του όγκου δεδομένων από διάφορες ψηφιακές συσκευές, όπως το Διαδίκτυο των Πραγμάτων (IoT), τα κοινωνικά δίκτυα, και τα πολυμέσα, δημιουργεί μεγάλες προκλήσεις στη διαχείριση και ανάλυση των ψηφιακών αποδεικτικών στοιχείων. Οι παραδοσιακές μέθοδοι ανάλυσης είναι χρονοβόρες και δεν μπορούν να ανταποκριθούν στην πολυπλοκότητα και το μέγεθος των δεδομένων.

4.3.1.3 Στόχοι

→ Αυτοματοποίηση της ταυτοποίησης των ψηφιακών αποδεικτικών στοιχείων για να επιταχυνθεί η διαδικασία ανάλυσης.

→ Μείωση του χρόνου και των πόρων που απαιτούνται για την ανάλυση μεγάλου όγκου δεδομένων.

4.3.1.4 Προτεινόμενες Λύσεις

MultiAgent Digital Investigation Toolkit (MADIK): Το MADIK είναι ένα εργαλείο όπως είπαμε και στην ενότητα 3.2, που χρησιμοποιεί ευφυείς πράκτορες για να επιτύχει την κατανομή των εργασιών ανάλυσης ψηφιακών δεδομένων, μειώνοντας την ανάγκη για ανθρώπινη παρέμβαση και επιταχύνοντας τη διαδικασία ανάλυσης. Οι πράκτορες αυτοί βελτιώνουν την αποδοτικότητα της ανάλυσης διαχειριζόμενοι τα δεδομένα αυτόνομα.

Εργαλεία Μεγάλης Κλίμακας Ανάλυσης Δεδομένων: Χρήση τεχνολογιών όπως το Hadoop και το MapReduce που επιτρέπουν την κατανεμημένη επεξεργασία δεδομένων σε πολλαπλές συσκευές και διακομιστές, διευκολύνοντας την επεξεργασία τεράστιων δεδομένων πιο αποδοτικά.

4.3.2 Εφαρμογή Τεχνικών Βαθιάς Μάθησης (DL) και Μηχανικής Μάθησης (ML)

Η εφαρμογή τεχνολογιών Βαθιάς Μάθησης (Deep Learning - DL) και Μηχανικής Μάθησης (Machine Learning - ML) είναι μια από τις πιο σημαντικές τάσεις στην ψηφιακή εγκληματολογία. Οι ερευνητές επικεντρώνονται στην αξιοποίηση αυτών των τεχνικών για την ανάλυση δεδομένων όπως εικόνες, βίντεο και ήχοι. Η βαθιά μάθηση προσφέρει τη δυνατότητα για εξαιρετικά ακριβή ανάλυση αυτών των δεδομένων, επιτρέποντας την αυτοματοποιημένη ανίχνευση και ταυτοποίηση παραβιάσεων της ακεραιότητας αρχείων.

Η ταχύτητα και η ακρίβεια αυτών των μεθόδων καθιστούν τη βαθιά μάθηση και τη μηχανική μάθηση ιδανικά εργαλεία για την επεξεργασία μεγάλων όγκων δεδομένων, ελαχιστοποιώντας την ανάγκη για ανθρώπινη παρέμβαση. Οι τεχνολογίες αυτές επιτρέπουν τη γρήγορη αναγνώριση παραβιάσεων και προβλημάτων στα δεδομένα, κάτι που είναι κρίσιμο για τις εγκληματολογικές έρευνες, όπου η ταχύτητα και η ακρίβεια είναι καίρια. [4] [5]

4.3.2.1 Κύρια χαρακτηριστικά της τάσης

- ✓ Αυτοματοποίηση της ανάλυσης εικόνων, βίντεο και ήχων.
- ✓ Βελτίωση της ταχύτητας και ακρίβειας στην αναγνώριση παραβιάσεων ακεραιότητας αρχείων.
- ✓ Ελαχιστοποίηση της ανθρώπινης παρέμβασης στις διαδικασίες ανάλυσης.
- ✓ Η εφαρμογή αυτών των τεχνικών ενισχύει τις εγκληματολογικές έρευνες, καθώς μειώνει τον χρόνο ανάλυσης, επιτρέποντας την ταχύτερη και πιο ακριβή απόδοση αποδεικτικών στοιχείων σε δικαστικές υποθέσεις.

4.3.2.2 Πρόβλημα

Οι επιθέσεις στον κυβερνοχώρο προκαλούν πολυπλοκότητα στην ανάλυση δεδομένων, καθώς τα δεδομένα από τέτοιες επιθέσεις είναι συχνά κατακερματισμένα και αμφισβητείται η ακεραιότητά τους. Επιπλέον, η συλλογή και η διατήρηση της αυθεντικότητας των αποδεικτικών στοιχείων αποτελούν σημαντικά προβλήματα που χρειάζονται αντιμετώπιση.

4.3.2.3 Στόχοι

→ Αναγνώριση παραβιάσεων ακεραιότητας των αρχείων και των δεδομένων που χρησιμοποιούνται ως αποδεικτικά στοιχεία.

→ Βελτίωση της ταχύτητας και της ακρίβειας στην ανάλυση ψηφιακών δεδομένων, ελαχιστοποιώντας την ανθρώπινη παρέμβαση.

4.3.2.4 Προτεινόμενες Λύσεις

Τεχνολογίες Blockchain: Το blockchain επιτρέπει τη διατήρηση της ακεραιότητας και της αυθεντικότητας των αποδεικτικών στοιχείων. Κάθε αλλαγή που γίνεται σε ένα αρχείο μπορεί να καταγραφεί, επιτρέποντας την ανίχνευση και την αδιάλειπτη παρακολούθηση των μεταβολών, προστατεύοντας έτσι τα αποδεικτικά στοιχεία από πιθανή παραποίηση.

Ανάλυση Μεταδεδομένων μέσω Τεχνητής Νοημοσύνης (AI) και Μηχανικής Μάθησης (ML): Οι τεχνικές Τεχνητής Νοημοσύνης (AI) και Μηχανικής Μάθησης (ML) χρησιμοποιούνται για την ανάλυση των μεταδεδομένων, τα οποία περιλαμβάνουν πληροφορίες για τη δημιουργία και τροποποίηση αρχείων. Η αυτόματη ανάλυση αυτών των μεταδεδομένων μπορεί να επιταχύνει την ανίχνευση αλλαγών και πιθανών παραβιάσεων.

Αυτόματη Ανάλυση Στοιχείων: Οι αλγόριθμοι Μηχανικής Μάθησης (ML) αναλαμβάνουν την αυτόματη ανάλυση μεγάλων συνόλων δεδομένων, αναζητώντας πρότυπα και ανωμαλίες χωρίς ανθρώπινη παρέμβαση, κάτι που βελτιώνει την ακρίβεια και την ταχύτητα των ερευνών.

4.3.3 Χρήση Τεχνητής Νοημοσύνης (AI) και Εργαλείων Υπολογιστικής Λογικής

Η Τεχνητή Νοημοσύνη (AI) και τα Εργαλεία Υπολογιστικής Λογικής αποτελούν κορυφαίες τεχνολογικές τάσεις για τη βελτίωση της αποδοτικότητας στις ψηφιακές εγκληματολογικές έρευνες. Η Τεχνητή Νοημοσύνη (AI) χρησιμοποιείται για την αναγνώριση μοτίβων και την αυτοματοποίηση της ανάλυσης πολύπλοκων δεδομένων. Η εφαρμογή αυτών των τεχνολογιών βελτιώνει την ταχύτητα και την ακρίβεια των ερευνών, επιτρέποντας την ανάλυση σύνθετων δεδομένων με μεγαλύτερη αποδοτικότητα.

Με την Τεχνητή Νοημοσύνη (AI) , οι εγκληματολογικές έρευνες αποκτούν εργαλεία που διευκολύνουν τη διαχείριση μεγάλου όγκου δεδομένων από πολλές διαφορετικές πηγές, όπως κινητές συσκευές, δίκτυα και πολυμέσα. Ταυτόχρονα, η υπολογιστική λογική επιτρέπει την αυτοματοποιημένη ανάλυση των δεδομένων αυτών, βοηθώντας στη βελτιστοποίηση των διαδικασιών και την πιο ταχεία ανάλυση. [19]

4.3.3.1 Κύρια χαρακτηριστικά της τάσης

- ✓ Αυτοματοποίηση της ανάλυσης πολύπλοκων υποθέσεων.
- ✓ Βελτίωση της αποδοτικότητας μέσω της χρήσης Τεχνητής Νοημοσύνης (AI) και υπολογιστικών εργαλείων για τη διαχείριση και ανάλυση μεγάλων δεδομένων.
- ✓ Ανάλυση δεδομένων από πολλαπλές πηγές, όπως Διαδίκτυο των Πραγμάτων (IoT), κινητές συσκευές και πολυμέσα.

4.3.3.2 Πρόβλημα

Η ανάλυση αποδεικτικών στοιχείων γίνεται όλο και πιο περίπλοκη λόγω της πολυμορφίας των δεδομένων που προέρχονται από πολλές και διαφορετικές πηγές, όπως κινητές συσκευές, Διαδίκτυο των Πραγμάτων (IoT) , πολυμέσα και δίκτυα. Η πολυπλοκότητα αυξάνεται επίσης από τη χρήση κρυπτογραφημένων επικοινωνιών, γεγονός που δυσχεραίνει τη συλλογή και ανάλυση των αποδεικτικών στοιχείων.

4.3.3.3 Στόχοι

- → Αυτοματοποίηση της ανάλυσης πολύπλοκων δεδομένων από πολλαπλές πηγές.
- → Βελτιστοποίηση σύνθετων ερευνών για τη διαχείριση της πολυπλοκότητας των δεδομένων, βελτιώνοντας την αποτελεσματικότητα και την ταχύτητα της ανάλυσης.

4.3.3.1 Προτεινόμενες Λύσεις

Ανάλυση Κρυπτογραφημένων Δεδομένων: Οι αλγόριθμοι Τεχνητής Νοημοσύνης (AI) και Μηχανικής Μάθησης (ML) μπορούν να αναλύσουν κρυπτογραφημένα δεδομένα, αποκρυπτογραφώντας πληροφορίες που είναι μεγάλης σημασίας για την έρευνα. Η δυνατότητα ανάλυσης κρυπτογραφημένων δεδομένων επιτρέπει τη γρήγορη και ακριβή ανάκτηση αποδεικτικών στοιχείων, διευκολύνοντας τη δικαστική αξιοποίηση τους.

Ενοποίηση Δεδομένων από Πολλαπλές Πηγές μέσω Τεχνητής Νοημοσύνης (AI): Η τεχνητή νοημοσύνη μπορεί να συνδέσει δεδομένα από διαφορετικές πηγές, όπως κινητές συσκευές, δίκτυα και πολυμέσα, ενοποιώντας την ανάλυσή τους σε ένα ενιαίο σύστημα. Αυτό επιτρέπει την ταχύτερη εξαγωγή συμπερασμάτων και την ανίχνευση κρίσιμων αποδεικτικών στοιχείων.

5

Σύνοψη/Ανάλυση

Κλείνοντας, παρούσα διπλωματική εργασία επικεντρώνεται στην εφαρμογή της Τεχνητής Νοημοσύνης (AI) και της Μηχανικής Μάθησης (ML) για την ενίσχυση των διαδικασιών της ψηφιακής εγκληματολογίας. Αναλύει πώς οι τεχνολογίες αυτές μπορούν να βελτιώσουν την ανάλυση και τη διατήρηση ψηφιακών αποδεικτικών στοιχείων, προσφέροντας αυξημένη ακρίβεια και αποδοτικότητα στις έρευνες. Ιδιαίτερη έμφαση δίνεται στην ανάλυση στοιχείων και τη συλλογή ή εντοπισμό στοιχείων σε μηχανήματα και συστήματα που έχουν πληγεί από κακόβουλες επιθέσεις, παρουσιάζοντας συγκεκριμένα παραδείγματα μέσα από τα paper.

Η σημασία της ψηφιακής εγκληματολογίας αυξάνεται λόγω της εξάπλωσης των εγκλημάτων μέσω υπολογιστών. Η ανάλυση των ψηφιακών αποδεικτικών στοιχείων είναι κρίσιμη για την υποστήριξη νομικών διαδικασιών. Σε αυτό το πλαίσιο, η AI και ML προσφέρουν εργαλεία για την αυτοματοποίηση της ανάλυσης αποδεικτικών στοιχείων, ενώ η χρήση νευρωνικών δικτύων και άλλων αλγορίθμων ML συμβάλλει στη βελτίωση της ανάλυσης και ταξινόμησης δεδομένων.

Προηγμένες τεχνικές, όπως το MapReduce, και εργαλεία ανοικτού κώδικα (Hadoop, Hive, Mahout), διευκολύνουν την ανάλυση μεγάλων δεδομένων. Το deep learning και τα συστήματα πολλαπλών πρακτόρων βοηθούν στη μείωση του χρόνου επεξεργασίας και στην αύξηση της ακρίβειας. Επιπλέον, η επεξηγήσιμη Τεχνητή Νοημοσύνη (XAI) και οι τεχνολογίες blockchain προσφέρουν διαφάνεια και ασφάλεια στην ανάλυση, απαραίτητα για τη διατήρηση της ακεραιότητας των ερευνών.

Η συνδυασμένη χρήση τεχνικών deep learning βελτιώνει την ανάλυση ανωμαλιών και την αποδοτικότητα των ερευνών δικτύου, ενισχύοντας τη διαχείριση δικτυακών δεδομένων και τις διαδικασίες ψηφιακής εγκληματολογίας.

Βιβλιογραφία

[1] S. Costantini, G. De Gasperis, and R. Olivieri, "Digital forensics and investigations meet artificial intelligence," *Annals of Mathematics and Artificial Intelligence*, vol. 86, no. 1–3, pp. 193–229, Apr. 2019, doi: https://doi.org/10.1007/s10472-019-09632-y.

[2] S. Rizvi, M. Scanlon, J. Mcgibney, and J. Sheppard, "Application of Artificial Intelligence to Network Forensics: Survey, Challenges and Future Directions," *IEEE Access*, vol. 10, pp. 110362–110384, 2022, doi: https://doi.org/10.1109/access.2022.3214506.

[3] E. P. Panchal, S. B. Yagnik, and B. K. Sharma, "Use of Machine Learning Algorithm on File Metadata for Digital Forensic Investigation Process," *Advances in Intelligent Systems and Computing*, pp. 401–408, Sep. 2018, doi: https://doi.org/10.1007/978-981-13-1165-9_37.

[4] A. Qadir and A. Varol, "The Role of Machine Learning in Digital Forensics," *IEEE Access*, pp 978-1-7281-6939-2/20, 2020.

[5] S. Sachdeva and A. Ali, "Machine learning with digital forensics for attack classification in cloud network environment," *International Journal of System Assurance Engineering and Management*, vol. 13, no. S1, pp. 156–165, Sep. 2021, doi: https://doi.org/10.1007/s13198-021-01323-4.

[6] L. Peng, X. Zhu, and P. Zhang, "A Framework for Mobile Forensics Based on Clustering of Big Data," *2021 IEEE 4th International Conference on Electronics Technology (ICET)*, May 2021, doi: https://doi.org/10.1109/icet51757.2021.9451014.

[7] N. Manzoor and M. Saleem, "ROLE OF MACHINE LEARNING TECHNIQUES IN DIGITAL FORENSIC INVESTIGATION OF BOTNET ATTACKS," 2021, doi: https://doi.org/10.34218/IJM.12.2.2021.057.

[8] R. Rawat, O. Oki, R. Chakrawarti, T. Adekunle, J. Lukose, and S. Ajagbe, "Autonomous Artificial Intelligence Systems for Fraud Detection and Forensics in Dark Web Environments," doi: https://doi.org/10.31449/inf.v47i9.4538.

[9] S. Ekhande, U. Patil, V. Kshama, and Kulhalli, "Review on effectiveness of deep learning approach in digital forensics," *International Journal of Electrical and Computer Engineering (IJECE*, vol. 12, no. 5, pp. 5481–5492, 2022, doi: https://doi.org/10.11591/ijece.v12i5.pp5481-5492.

[10] A. Awasthi, G. Khan, and M. Bargavi, "Application of Machine Learning to Extraction of Digital Forensics Evidence," *2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC)*, Jan. 2024, doi: https://doi.org/10.1109/icocwc60930.2024.10470725.

[11] S. Ferreira, M. Antunes, and M. E. Correia, "A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing," *Data*, vol. 6, no. 8, p. 87, Aug. 2021, doi: https://doi.org/10.3390/data6080087.

[12] S. Kim, W. Jo, J. Lee, and T. Shon, "AI-enabled device digital forensics for smart cities," *The Journal of Supercomputing*, vol. 78, no. 2, pp. 3029–3044, Jul. 2021, doi: https://doi.org/10.1007/s11227-021-03992-1.

[13] W. Jo *et al.*, "Digital Forensic Practices and Methodologies for AI Speaker Ecosystems," *Digital Investigation*, vol. 29, pp. S80–S93, Jul. 2019, doi: https://doi.org/10.1016/j.diin.2019.04.013.

[14] A. Abbas, "Artificial Intelligence in Cybersecurity: Enhancing Threat Detection and Response," Jan. 2024.

[15] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey," *Electronics*, vol. 12, no. 8, p. 1920, Apr. 2023, doi: https://doi.org/10.3390/electronics12081920.

[16] R. Mohammad, "A Neural Network based Digital Forensics Classification," IEEE Access, 978-1-5386-9120-5/18, 2018.

[17] G. S. Chhabra, V. P. Singh, and M. Singh, "Cyber forensics framework for big data analytics in IoT environment using machine learning," *Multimedia Tools and Applications*, vol. 79, no. 23–24, pp. 15881–15900, Jul. 2018, doi: https://doi.org/10.1007/s11042-018-6338-1.

[18] V. Ganesh and A. Professor, "International Journal of Advance Research in Computer Science and Management Studies Artificial Intelligence Applied to Computer Forensics," 2017.

[19] S. W. Hall, A. Sakzad, and K. R. Choo, "Explainable artificial intelligence for digital forensics," *WIREs Forensic Science*, vol. 4, no. 2, Jun. 2021, doi: https://doi.org/10.1002/wfs2.1434.

[20] P. Bhatt, "MACHINE LEARNING FORENSICS:A NEW BRANCH OF DIGITAL FORENSICS," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 8, pp. 217–222, Aug. 2017, doi: https://doi.org/10.26483/ijarcs.v8i8.4613.

[21] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," *Forensic Science International: Synergy*, vol. 1, pp. 61–67, 2019, doi: https://doi.org/10.1016/j.fsisyn.2019.03.006.

[22] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and C. E. Montenegro-Marin, "Internet of things forensic data analysis using machine learning to identify roots of data scavenging," *Future Generation Computer Systems*, vol. 115, pp. 756–768, Feb. 2021, doi: https://doi.org/10.1016/j.future.2020.10.001.

[23] S. Sharma, C. R. Krishna, and R. Kumar, "RansomDroid: Forensic analysis and detection of Android Ransomware using unsupervised machine learning technique," *Forensic Science International: Digital Investigation*, vol. 37, p. 301168, Jun. 2021, doi: https://doi.org/10.1016/j.fsidi.2021.301168.

[24] F. Amato, A. Castiglione, G. Cozzolino, and F. Narducci, "A semantic-based methodology for digital forensics analysis," *Journal of Parallel and Distributed Computing*, vol. 138, pp. 172–177, Apr. 2020, doi: https://doi.org/10.1016/j.jpdc.2019.12.017.

[25] S. Gupta, M. Sharma, and P. Johri, "ARTIFICIAL INTELLIGENCE IN FORENSIC SCIENCE," International Research Journal of Engineering and Technology (IRJET), pp. 7181-7184, May 2020.

[26] I. Goni, J. Mishion Gumpy, T. Umar Maigari, M. Muhammad, and A. Saidu, "Cybersecurity and Cyber Forensics: Machine Learning Approach," *Machine Learning Research*, vol. 5, no. 4, p. 46, 2020, doi: https://doi.org/10.11648/j.mlr.20200504.11.

[27] L. Tageldin and H. Venter, "Machine-Learning Forensics: State of the Art in the Use of Machine-Learning Techniques for Digital Forensic Investigations within Smart Environments," *Applied Sciences*, vol. 13, no. 18, p. 10169, Sep. 2023, doi: https://doi.org/10.3390/app131810169.

[28] Y. A. Balushi, H. Shaker, and B. Kumar, "The Use of Machine Learning in Digital Forensics: Review Paper," *Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022)*, pp. 96–113, 2023, doi: https://doi.org/10.2991/978-94-6463-110-4_9.

[29] Stergiopoulos, G., & Gritzalis, D. A. (2020). Cyber-Attacks on the Oil & Gas Sector: A Survey on Incident Assessment and Attack Patterns. In *IEEE Access* (Vol. 8). IEEE. https://doi.org/10.1109/ACCESS.2020.3007960

[30] R. Sharma, Diksha, A. R. Bhute, and B. K. Bastia, "Application of artificial intelligence and machine learning technology for the prediction of postmortem interval: A systematic review of preclinical and clinical studies," *Forensic Science International*, vol. 340, p. 111473, Nov. 2022, doi: https://doi.org/10.1016/j.forsciint.2022.111473.

[31] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The Characteristics of Cloud Computing," *2010 39th International Conference on Parallel Processing Workshops*, Sep. 2010, doi: https://doi.org/10.1109/icppw.2010.45.

[32] Z. Hao, "Deep learning review and discussion of its future development," *MATEC Web of Conferences*, vol. 277, p. 02035, 2019, doi: https://doi.org/10.1051/matecconf/201927702035.

[33] R. Qamar and B. Ali Zardari, "Artificial Neural Networks: An Overview," *Mesopotamian Journal of Computer Science*, pp. 130–139, Aug. 2023, doi: https://doi.org/10.58496/mjcsc/2023/015.