ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνολογίες Αιχμής Στην Ψηφιακή Εγκληματολογία

Γεώργιος Καβαλιώτης

Α.Μ. : 19036

Επιβλέπων: Δημήτριος Καλλέργης, Λέκτορας Εφ.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνολογίες Αιχμής Στην Ψηφιακή Εγκληματολογία

Γεώργιος Καβαλιώτης

Α.Μ. : 19036

Τριμελής εξεταστική επιτροπή

1. **<u>Επιβλέπων καθηγητής</u>: Δημήτριος Καλλέργης,** Λέκτορας Εφ. Πανεπιστημίου Δυτικής Αττικής

   Digitally signed by Dimitrios Kallergis
   Date: 2023.07.11 00:43:54 +03'00'

2. **<u>Μέλος</u>: Βασίλειος Μάμαλης,** Καθηγητής Πανεπιστημίου Δυτικής Αττικής

   Vasileios Mamalis
   Digitally signed by Vasileios Mamalis
   Date: 2023.07.12 10:51:10 +03'00'

3. **<u>Μέλος</u>: Παναγιώτης Καρκαζής,** Αναπλ. Καθηγητής Πανεπιστημίου Δυτικής Αττικής

   Panagiotis Karkazis
   Digitally signed by Panagiotis Karkazis
   Date: 2023.07.11 10:55:16 +03'00'

Αθήνα, Μάρτιος 2023

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος, **Γεώργιος Καβαλιώτης του Δημητρίου**, με αριθμό μητρώου 19036, φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών Επιστήμης και Τεχνολογίας της Πληροφορικής και των Υπολογιστών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών (Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων) της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι 15-03-2023 και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή».

Ο Δηλών

Digitally signed by Dimitrios Kallergis
Date: 2023.07.11 00:44:12 +03'00'

Γεώργιος Καβαλιώτης

Περίληψη

Η παρούσα εργασία επικεντρώνεται στη μελέτη της σύγχρονης ψηφιακής εγκληματολογίας, όπως αυτή διεξάγεται στο περιβάλλον του Διαδικτύου των Αντικειμένων (IoT) και ιδιαίτερα στον τομέα των Συστημάτων Ευφυών Μεταφορών (ITS) και των έξυπνων οχημάτων. Η εργασία φιλοδοξεί να εκπονήσει μια συγκριτική μελέτη στις τεχνολογίες που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας. Ιδιαίτερη έμφαση δίνεται στο στάδιο της αναγνώρισης και συλλογής των εν δυνάμει αποδεικτικών στοιχείων από τις οντότητες του διαδικτύου των πραγμάτων (συσκευές IoT, Έξυπνα Οχήματα καθώς και νεφοϋπολογιστικές υποδομές και δίκτυα τηλεπικοινωνιών) καθώς και στη διατήρηση της ακεραιότητας των ψηφιακών τεκμηρίων, μέσω της αλυσίδας φύλαξης (Chain of Custody). Προκειμένου να συνοψιστούν και να συγκριθούν τα κριτήρια, τα οποία χρησιμοποιούν οι ερευνητές στο πεδίο της ψηφιακής εγκληματολογίας, είναι απαραίτητη η σύνθεση των αποτελεσμάτων, τα οποία προέρχονται από τις έρευνες που έχουν μέχρι τώρα πραγματοποιηθεί Για την εκπλήρωση του ερευνητικού σκοπού διεξήχθη συστηματική βιβλιογραφική ανασκόπηση και χρησιμοποιήθηκε η μέθοδος PRISMA. Η εργασία μεταξύ άλλων ανέδειξε ότι σήμερα μία πρόκληση συνιστά η ισχυροποίηση των κριτηρίων που αφορούν στην ασφάλεια, στην ιδιωτικότητα, στη διατήρηση των αποδεικτικών στοιχείων, καθώς αποτελούν πολύ σημαντικά χαρακτηριστικά των κατάλληλων πειστηρίων. Οι μέθοδοι που χρησιμοποιήθηκαν στις υπό μελέτη έρευνες θα μπορούσαν να επεκταθούν, να συνδυαστούν, να προσαρμοστούν σε κάθε περιστατικό ξεχωριστά, παρέχοντας στον ερευνητή πληθώρα κατάλληλων εργαλείων, ώστε να επιτελέσει το έργο του.

Λέξεις Κλειδιά: Συστηματική Βιβλιογραφική Ανασκόπηση, Τεχνολογίες Αιχμής, Ψηφιακή Εγκληματολογία.

Abstract

This paper focuses on modern digital forensics as it is conducted in the Internet of Things (IoT) environment, particularly in the field of Intelligent Transportation Systems (ITS) and innovative vehicles. The paper aspires to produce a comparative study of the technologies used in digital forensics. Particular emphasis is placed on the stage of identifying and collecting potential evidence from the entities of the Internet of Things (IoT devices, Smart Vehicles as well as cloud computing infrastructures and telecommunications networks) as well as on maintaining the integrity of digital evidence through the chain of custody (Chain of Custody). To summarize and compare the criteria used by researchers in the field of digital criminology, it is necessary to synthesize the results from the research that has been carried out so far. A systematic literature review used the PRISMA method to fulfil the research purpose. Among other things, the work highlighted that today a challenge is to strengthen the criteria related to security, privacy, and preservation of evidence, as they are essential characteristics of appropriate convictions. Furthermore, the methods used in the studies under study could be extended, combined, and adapted to each case, providing the researcher with the proper tools to carry out his mission.

Keywords: Systematic Literature Review, Cutting-edge Technologies, Digital Forensics.

Ευχαριστίες

Με την ολοκλήρωση της μεταπτυχιακής διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε όσους συνέβαλλαν στην εκπόνησή της.

Ευχαριστώ θερμά τον επιβλέποντα καθηγητή μου, κύριο Δημήτριο Καλλέργη, για την υποδειγματική βοήθεια, τη συνεχή καθοδήγησή του και την εμπιστοσύνη που μου έδειξε.

Θα ήθελα επίσης να ευχαριστήσω την οικογένειά μου, για την υπομονή τους, καθώς και την υποστήριξη τους, καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας Περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κατάλογος Συντομογραφιών

Πίνακας 1-ΚΑΤΑΛΟΓΟΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

IoT	Internet of Things
ITS	Intelligent Transportation Systems
IoE	Internet of Everything
Η/Υ	Ηλεκτρονικοί Υπολογιστές
IoV	Internet of Vehicles
DFaaS	Digital Forensics-as-a-Service
HPC	High Performance Computing
DRFWS	Digital Forensic Research Workshop
CART	Computer Analysis and Response Team CART
NIST	National Institute of Standards and Technology
P2P	Peer to Peer
VoIP	Voice over Internet Protocol

Κεφάλαιο 1

Εισαγωγή

1.1 Πρόλογος

Σήμερα γινόμαστε ολοένα και περισσότερο μάρτυρες ειδήσεων και γεγονότων που αφορούν γνωστοποίηση περιστατικών ψηφιακών επιθέσεων. Αυτές οι επιθέσεις λαμβάνουν χώρα σε ένα μεγάλο εύρος εφαρμογών και λειτουργιών, μιας και πλέον, λόγω της 4ης Βιομηχανικής Επανάστασης βρισκόμαστε στην εποχή του Διαδικτύου των Αντικειμένων (IoT) και οδεύουμε με ταχείς ρυθμούς στο Διαδίκτυο των Πάντων (IoE), [1]. Πλήθος δισεκατομμυρίων συσκευών είναι πλέον διασυνδεδεμένες στον ψηφιακό κόσμο και αυτό δημιουργεί σημαντικές προκλήσεις σε αρκετούς τομείς των σύγχρονων τεχνολογιών πληροφορικής και επικοινωνιών. Υπάρχουν προκλήσεις σε ζητήματα παροχής υπηρεσιών συνδεσιμότητας, αποθήκευσης δεδομένων, ασφάλειας, προστασίας της ιδιωτικότητας και πολλές άλλες, οι οποίες πηγάζουν από τη ραγδαία τεχνολογική ανάπτυξη.

Εκτός όμως από τα τεράστια οφέλη που προκύπτουν για την ανθρωπότητα από τη χρήση αυτών των επιτευγμάτων υπάρχει και η άλλη όψη του νομίσματος. Υπάρχει η κακόβουλη χρήση αυτών, η οποία οδηγεί στη διάπραξη αξιόποινων πράξεων. Εισήλθαν, λοιπόν στην καθημερινότητά μας, όροι όπως «ηλεκτρονικό έγκλημα», «έγκλημα στον κυβερνοχώρο», «κυβερνοασφάλεια» και «ψηφιακή εγκληματολογία». Η ψηφιακή εγκληματολογία είναι και ο χώρος στον οποίο εστιάζει η παρούσα εργασία, η οποία στοχεύει να αποτυπώσει τις ιδιαιτερότητες και τις προκλήσεις της συγκεκριμένης επιστημονικής περιοχής και να εξετάσει τις τεχνολογίες αιχμής που απαντώνται σε αυτήν ή/και προτείνονται για τη βελτίωση και τον εκσυγχρονισμό της.

Κατά κανόνα, η ψηφιακή εγκληματολογία συνδέεται με τη συλλογή ψηφιακών τεκμηρίων ή πειστηρίων τα οποία μπορούν να χρησιμοποιηθούν για να αποδείξουν ή να αποκλείσουν αστικές, διοικητικές και ποινικές κατηγορίες, κατά την εξέταση των αντίστοιχων υποθέσεων από το δικαστήριο, [2]. Ψηφιακό τεκμήριο μπορεί να είναι κάθε αντικείμενο που περιέχει ή διαβιβάζει ψηφιακά δεδομένα. Συνεπώς οι δυνατοί τύποι ψηφιακών τεκμηρίων περιλαμβάνουν ένα ευρύτατο φάσμα πηγών ψηφιακών δεδομένων, το οποίο εκτείνεται από το υλισμικό των τυπικών υπολογιστικών συστημάτων (Η/Υ, διακομιστές) και τις κινητές συσκευές (τηλέφωνα, wearables) με τα αφαιρούμενα αποθηκευτικά τους μέσα, έως το γιγαντιαίο πλήθος συσκευών και αισθητήρων του περιβάλλοντος IoT με τις υποδομές του υπολογιστικού νέφους και των τοπικών δικτύων τηλεπικοινωνιών που χρησιμοποιούνται για την υλοποίησή του.

Η ευμετάβλητη φύση των ψηφιακών τεκμηρίων, σε συνδυασμό με τον άυλο χαρακτήρα των δεδομένων που περιέχουν, επιβάλει τη χρήση κατάλληλων εργαλείων και την τήρηση συγκεκριμένων διαδικασιών κατά τη συλλογή, ανάλυση και την εν γένει διαχείρισή τους, μέσω της αλυσίδας φύλαξης (Chain of Custody), προκειμένου να εξασφαλιστεί η ακεραιότητά τους και η αποδοχή τους από το δικαστήριο (admissibility). Είναι συχνές οι περιπτώσεις που σημαντικά τεκμήρια εξαιρούνται από την εκδίκαση υπόθεσης λόγω αμφιβολιών ως προς την ακεραιότητα των δεδομένων τους ή ως προς την τήρηση των αυστηρών διαδικασιών μεταχείρισής τους. Οι τελευταίες προσδιορίζονται από το σχετικό θεσμικό πλαίσιο (διεθνές, ευρωπαϊκό και εθνικό) καθώς και από πληθώρα κατευθυντήριων οδηγιών και προτύπων που έχουν εκδοθεί από διάφορους φορείς και οργανισμούς, όπως το Συμβούλιο της Ευρώπης, το Εθνικό Συμβούλιο Αξιωματικών Αστυνομίας του Ηνωμένου Βασιλείου, το Εθνικό Ινστιτούτο Δικαιοσύνης των ΗΠΑ, η Επιστημονική Ομάδα Εργασίας για τα Ψηφιακά Πειστήρια των ΗΠΑ, [3].

Λόγω της μείζονος σημασίας που διαδραματίζει η εγγύηση της ακεραιότητας των ψηφιακών τεκμηρίων στη σύγχρονη ψηφιακή εγκληματολογία, η παρούσα εργασία επιδιώκει να εστιάσει στο κρίσιμο στάδιο της εγκληματολογικής έρευνας που άπτεται της συλλογής και διατήρησης ψηφιακών τεκμηρίων και δεδομένων, όπως αυτό διεξάγεται στο σύγχρονο περιβάλλον του Διαδικτύου των Αντικειμένων (IoT), καθώς επίσης και στο χώρο των Έξυπνων Οχημάτων.

Στο Διαδίκτυο των Αντικειμένων, (IoT) οποιοδήποτε αντικείμενο ή συσκευή μπορεί διασυνδεθεί και να ανταλλάξει πληροφορίες με άλλα αντικείμενα ή με άλλα έμβια όντα, [4]. Η διασύνδεση των συσκευών στο Διαδίκτυο έχει διανύσει τα τελευταία δέκα έτη μια εκθετική πορεία αύξησης. Εκτιμάται ότι σήμερα ο συνολικός αριθμός των συσκευών IoT ανέρχεται σε 50 δις, καθιστώντας την αναλογία σε περίπου 7 συσκευές ανά άτομο, [5], ενώ υπολογίζεται ότι θα ανέλθει σε περίπου 75 δις, έως το τέλος του 2025 (Department, 2021). Ενδεικτικά, αναφέρεται ότι στα μέσα του 2008 συνδέθηκαν στο διαδίκτυο περισσότερα αντικείμενα από ότι ανθρώπινοι χρήστες για πρώτη φορά στην ιστορία, [6].

Πολλές είναι οι εφαρμογές του Διαδικτύου των Αντικειμένων (IoT) και των Συστημάτων Ευφυών Μεταφορών (ITS) που αλλάζουν δραστικά την καθημερινότητα των ανθρώπων σε παγκόσμιο επίπεδο: γεωργία, ευφυή ηλεκτρικά δίκτυα, φορητές συσκευές (wearables), έξυπνη ιατρική, Συστήματα Ευφυών Μεταφορών (ITS) και εφοδιαστικής αλυσίδας, Έξυπνα Οχήματα και άλλες. Η παρούσα εργασία επιχειρεί να επικεντρωθεί στους τομείς του Διαδικτύου των Αντικειμένων (IoT) καθώς και στον τομέα των έξυπνων ή διασυνδεδεμένων οχημάτων που αποτελούν πολύ ενδιαφέρουσες και εξελισσόμενες περιοχές με πληθώρα εφαρμογών, [7]. Στον έξυπνο ιστό των μεταφορών, που εξελίσσεται ταχύτατα σε σήμα κατατεθέν των έξυπνων πόλεων του μέλλοντος, οχήματα, σηματοδότες, δρόμοι και πεζοί μπορούν να επικοινωνούν και να αλληλεπιδρούν μεταξύ

τους σε πραγματικό χρόνο. Βασικές τεχνολογίες που συνθέτουν το οικοσύστημα του διαδικτύου των οχημάτων (Internet of Vehicles / IoV) είναι το σύνολο των πρωτόκολλων επικοινωνίας που αποδίδονται με τον όρο «όχημα προς οποιαδήποτε οντότητα (V2X)», [8] και επιτρέπουν την ανταλλαγή δεδομένων μεταξύ οχήματος και άλλων οχημάτων, πεζών, υποδομών, δικτύων, τα συστήματα ψυχαγωγίας που διαθέτουν τα Έξυπνα Οχήματα καθώς και τα σύγχρονα συστήματα τηλεματικής. Παρά τα αναρίθμητα πλεονεκτήματα των έξυπνων οχημάτων σε όρους οδικής ασφάλειας, διαχείρισης της κυκλοφορίας και οδηγικής εμπειρίας, οι τεχνολογικές ευκολίες που ενσωματώνουν θέτουν νέες προκλήσεις στον τομέα της ψηφιακής εγκληματολογίας.

Οι κυριότερες προκλήσεις που καλούνται να αντιμετωπίσουν οι διωκτικές αρχές κατά τον εντοπισμό, τη συλλογή και τη διαχείριση των παραγόμενων δεδομένων από IoT οντότητες και Έξυπνα Οχήματα μπορούν να ταξινομηθούν στις ακόλουθες γενικές κατηγορίες:

(α) δικονομικές προκλήσεις με κυρίαρχες τη διασφάλιση της αξιοπιστίας και της ακεραιότητας των ψηφιακών πειστηρίων και της αλυσίδας φύλαξής τους, [9[, [10].
(β) ελλείψεις τυποποίησης (standardization) των σχετικών διαδικασιών και μεθόδων, [11],
(γ) τεχνικές προκλήσεις που περιλαμβάνουν την υιοθέτηση της προσέγγισης του προληπτικού σχεδιασμού ή εγκληματολογικής ετοιμότητας του περιβάλλοντος IoT (IoT Digital Forensic Readiness) και την ανάπτυξη κατάλληλων εργαλείων (IoT forensic tools) για την επίλυση προβλημάτων σχετικά με αντί-εγκληματολογικές πρακτικές (anti-forensic techniques), κρυπτογράφηση (data encryption) και μεγάλο όγκο δεδομένων (Big IoT data) καθώς και για την προστασία του οικοσυστήματος IoT έναντι παραβιάσεων που μπορεί να οδηγήσουν σε καταστροφή ή αλλοίωση των ψηφιακών πειστηρίων (κυβερνοασφάλεια/ IoT intrusion detection), [12], [13], [14].

Πολλές επιστημονικές μελέτες έχουν πραγματευτεί το ζήτημα της εγκληματολογίας στο οικοσύστημα του διαδικτύου των πραγμάτων ή ειδικότερα των οχημάτων και έχουν αναδείξει την ανάγκη ανάπτυξης και εφαρμογής ενός πλαισίου ψηφιακής εγκληματολογικής έρευνας προσαρμοσμένου στις απαιτήσεις και ιδιαιτερότητες του περιβάλλοντος αυτού. Οι σημαντικότερες από τις μελέτες αυτές, αναφέρονται στη βιβλιογραφική επισκόπηση και προτείνουν την αξιοποίηση σύγχρονων τεχνολογιών αιχμής για τη διαχείριση των ψηφιακών τεκμηρίων και την παραγωγή αποδεικτικών δεδομένων. Από τις προτεινόμενες τεχνολογίες αιχμής στη διεθνή βιβλιογραφία, το Blockchain σχεδόν μονοπωλεί το ενδιαφέρον των ερευνητών για την ανάπτυξη εφαρμογών ηλεκτρονικής αλυσίδας φύλαξης πειστηρίων (Digital Chain of Custody) ή μηχανισμών καταγραφής (logs) των αλληλεπιδράσεων μεταξύ των IoT οντοτήτων για την παραγωγή και την αποθήκευση ψηφιακών δεδομένων που μπορεί να είναι χρήσιμα στην έρευνα κλασικών εγκλημάτων (π.χ. κλοπή ή

ανθρωποκτονία) ή τροχαίων ατυχημάτων καθώς και για τον εντοπισμό και τη διερεύνηση κυβερνοεπιθέσεων στο IoT περιβάλλον.

Εκτός από το Blockchain άλλες τεχνολογίες αιχμής που προτείνονται σε κάποιες μελέτες για τη διαχείριση των δεδομένων είναι: η ψηφιακή εγκληματολογία -ως- υπηρεσία (Digital Forensics-as-a-Service /DFaaS), η υπολογιστική υψηλής απόδοσης και η παράλληλη επεξεργασία (High Performance Computing /HPC and Parallel Processing) και η Τεχνητή Νοημοσύνη (Artificial Intelligence), σε συνδυασμό με τη μάθηση σε βάθος (Deep Learning). Ωστόσο, στις περισσότερες περιπτώσεις η αναφορά σε αυτές τις τεχνολογίες είναι επιγραμματική και οι σχετικές προτάσεις αφορούν πιθανά πεδία μελλοντικής έρευνας.

1.2 Σκοπός και Αντικείμενο Μελέτης

Η παρούσα εργασία επικεντρώνεται στη μελέτη της σύγχρονης ψηφιακής εγκληματολογίας, όπως αυτή διεξάγεται στο περιβάλλον του Διαδικτύου των Αντικειμένων (IoT) και ιδιαίτερα στον τομέα των Συστημάτων Ευφυών Μεταφορών (ITS) και των έξυπνων οχημάτων. Η εργασία φιλοδοξεί να εκπονήσει μια συγκριτική μελέτη στις τεχνολογίες που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας [15].

Ειδικότερα διερευνώνται τα μοντέλα και οι μέθοδοι που εφαρμόζονται στη σύγχρονη ψηφιακή εγκληματολογία, τα εργαλεία και οι τεχνικές που αξιοποιούνται στη σχετική διεθνή πρακτική, οι ανάγκες και τα προβλήματα που αναδύονται σε αυτόν τον τομέα από την αδιάκοπη κούρσα της τεχνολογικής προόδου και οι τεχνολογικές καινοτομίες που μπορούν να συνεισφέρουν στην αντιμετώπισή τους.

Ιδιαίτερη έμφαση δίνεται στο στάδιο της αναγνώρισης και συλλογής των εν δυνάμει αποδεικτικών στοιχείων από τις οντότητες του διαδικτύου των πραγμάτων (συσκευές IoT, Έξυπνα Οχήματα καθώς και νεφοϋπολογιστικές υποδομές και δίκτυα τηλεπικοινωνιών) καθώς και στη διατήρηση της ακεραιότητας των ψηφιακών τεκμηρίων, μέσω της αλυσίδας φύλαξης (Chain of Custody).

Παράλληλα, συνοψίζονται οι νέες τάσεις που αναπτύσσονται στον τομέα του προληπτικού σχεδιασμού ή της εγκληματολογικής ετοιμότητας (IoT Digital Forensic Readiness) του διαδικτύου των πραγμάτων και των έξυπνων οχημάτων.

Τέλος επιχειρείται η συγκριτική επισκόπηση των μοντέλων και εφαρμογών που προτείνονται από τη διεθνή βιβλιογραφία αναφορικά με τα προεκτεθέντα ζητήματα.

Οι βασικές έννοιες γύρω από τις οποίες αναπτύσσεται η εργασία είναι οι παρακάτω.

- Διαδίκτυο των Αντικειμένων (IoT)
- Συστήματα Ευφυών Μεταφορών (ITS) και Έξυπνα Οχήματα.

1.3 Μεθοδολογική Προσέγγιση

Ως μεθοδολογία έρευνας επιλέχθηκε η συστηματική βιβλιογραφική ανασκόπηση κατά την οποία θα αξιοποιηθεί το μοντέλο PRISMA. Σε αυτό το πλαίσιο τέθηκαν κάποια κριτήρια επιλογής των άρθρων στα οποία θα στηριχθεί η συστηματική βιβλιογραφική ανασκόπηση για την συγκριτική μελέτη στις τεχνολογίες που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας.

Σκοπός της συγκριτικής αξιολόγησης είναι να εντοπιστούν τα κριτήρια που θέτουν οι επιλεγμένες έρευνες που μπορούν να εφαρμοστούν στη σύγκριση των διαφόρων τεχνολογιών που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας. Η εστίαση είναι πάντα στο Διαδίκτυο των Αντικειμένων (IoT) και στα συστήματα ευφυών μεταφορών. Απώτερος στόχος της συστηματικής ανασκόπησης είναι να γίνει σύγκριση των κριτηρίων.

Τα αποτελέσματα της έρευνας θα οργανωθούν σε πίνακες με βάση τα κριτήρια (π.χ. επίτευξη στόχων ασφαλείας (security analysis), που σχετίζονται ενδεικτικά με εμπιστευτικότητα και απόρρητο, ταυτοποίηση (authentication), αξιοπιστία, ακεραιότητα, δυνατότητα αποδοχής από το δικαστήριο, διαθεσιμότητα, ικανότητα επαλήθευσης, ανθεκτικότητα έναντι παραβίασης). Με βάση τα σχετικά άρθρα θα επιλεχθούν 6-7 κριτήρια προς εστίαση.

Κεφάλαιο 2

Η Ψηφιακή Εγκληματολογία

2.1 Εννοιολογικές Αποσαφηνίσεις

Η εγκληματολογία (Forensics), είναι η επιστήμη η οποία μελετά συστηματικά το έγκλημα και αναπτύσσει μεθόδους για την πρόληψη των εγκλημάτων ή και την καταστολή τους. Πρόκειται για ένα επιστημονικό κλάδο, στον οποίο χρησιμοποιούνται οι μέθοδοι και τα πορίσματα από άλλους επιστημονικούς κλάδους, όπως ο κλάδος της Κοινωνιολογίας, της Ψυχολογίας, της Ψυχιατρικής, της Ανθρωπολογίας, της Στατιστικής, της Νομικής, της Βιολογίας. Συνεπώς, οι ειδικοί επιστήμονες που ασχολούνται με τον κλάδο της εγκληματολογίας είναι δυνατό να προέρχονται από τους κλάδους, που προαναφέρθηκαν και με αυτό τον τρόπο να συνεισφέρουν με τις επιστημονικές γνώσεις τους, παρέχοντας στους εγκληματολόγους πειστήρια, προκειμένου να φέρουν εις πέρας το έργο τους, δηλαδή να επιτύχουν τη διαλεύκανση ενός εγκλήματος, [16].

Ένας από τους τομείς της εγκληματολογίας είναι η ψηφιακή εγκληματολογία, στην οποία τα πειστήρια του εγκλήματος δεν είναι γενετικό υλικό ή στοιχεία που μπορεί να οδηγήσουν στην εξιχνίαση ενός εγκλήματος, αλλά πρόκειται για ηλεκτρονικά ίχνη. Τα ηλεκτρονικά εγκλήματα, τα οποία διερευνά η ψηφιακή εγκληματολογία είναι η διαδικτυακή απάτη, η διαδικτυακή πειρατεία και η κλοπή, η διαδικτυακή τρομοκρατία και πορνογραφία [17]. Το ψηφιακό έγκλημα συχνά αναφέρεται και ως έγκλημα στον κυβερνοχώρο και περιλαμβάνει τα εγκλήματα που για να πραγματοποιηθούν απαιτείται η χρήση ηλεκτρονικών υπολογιστών και τεχνολογικών μέσων.

Η ψηφιακή εγκληματολογία, προκειμένου να πραγματοποιηθεί ο στόχος, ο οποίος είναι η εξιχνίαση του ψηφιακού εγκλήματος, χρησιμοποιεί διάφορες μεθόδους ώστε να ανακτηθούν οι πληροφορίες που χάθηκαν και να αναλυθούν ψηφιακά πειστήρια. Τα ψηφιακά πειστήρια, σύμφωνα με τους Carrier και Spafford, [18], αποτελούν εκείνες τις πληροφορίες, οι οποίες είναι δυνατόν να επιβεβαιώσουν ή να διαψεύσουν την εκτίμηση του ερευνητή για την επίλυση του ψηφιακού εγκλήματος και συνδέονται άμεσα με τις ψηφιακές συσκευές, μέσω των οποίων λαμβάνονται κάθε είδους δεδομένα. Τα ψηφιακά πειστήρια αποτελούν ευαίσθητα στη χρήση δεδομένα, οπότε είναι επιβεβλημένος ο κατάλληλος και προσεκτικός χειρισμός του ερευνητή, προκειμένου να μην αλλοιωθούν ή καταστραφούν [19].

Σύμφωνα με τον Palmer [20] η ψηφιακή εγκληματολογία είναι η επιστήμη που χρησιμοποιεί επιστημονικές και αποδεδειγμένες μεθόδους με σκοπό να διατηρηθούν, να περισυλλεγούν, να επικυρωθούν, να αναγνωριστούν, να αναλυθούν, να ερμηνευτούν, να καταγραφούν και να παρουσιαστούν όλα τα ψηφιακά τεκμήρια, βάσει των οποίων δύναται να ανακατασκευαστεί ή να

αναπαρασταθεί ένα ψηφιακό έγκλημα, αλλά και να προληφθούν κακόβουλες και άνευ εξουσιοδότησης ενέργειες. Για πρώτη φορά ο όρος της ψηφιακής εγκληματολογίας χρησιμοποιήθηκε κατά τη διάρκεια του Digital Forensic Research Workshop (DRFWS) στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ), το 2001, με σκοπό να συμπεριληφθούν με αυτή την έννοια όλα τα ψηφιακά μέσα που δύνανται να αποθηκεύσουν δεδομένα, όπως για παράδειγμα τα κινητά τηλέφωνα και τα δίκτυα. Στη σημερινή εποχή στους τρόπους αποθήκευσης δεδομένων ανήκουν όλα αυτά, τα οποία αποτελούν το Διαδίκτυο των Αντικειμένων (IoT), όπως wearables, έξυπνα κινητά και ρολόγια, έξυπνα σπίτια και αυτοκίνητα.

Δεδομένης της αλματώδους εξέλιξης της τεχνολογίας και τη χρήση των ηλεκτρονικών υπολογιστών, των ψηφιακών συσκευών και των δικτύων, η ανάκτηση των ψηφιακών δεδομένων, τα οποία μπορούν να χρησιμοποιηθούν ώστε να εντοπιστούν οι κακόβουλες ενέργειες, υλοποιείται από την ψηφιακή εγκληματολογία. Προκειμένου μάλιστα τα αποδεικτικά στοιχεία να γίνονται αποδεκτά από το δικαστήριο, θα πρέπει να ακολουθούνται πάγιες και έγκυρες διαδικασίες, οι οποίες να κάνουν χρήση των βασικών αρχών της τεχνολογίας.

Λόγω του εκτεταμένου αντικειμένου της, η ψηφιακή εγκληματολογία διακρίνεται στην εγκληματολογία δικτύων, εγκληματολογία υπολογιστών, εγκληματολογία βάσεων δεδομένων και την εγκληματολογία στο Διαδίκτυο των Αντικειμένων (IoT). Η εγκληματολογία δικτύων αποσκοπεί στην απόδειξη του τρόπου με τον οποίο έγινε μια παραβίαση. Η εγκληματολογία υπολογιστών αφορά τη διερεύνηση αποδεικτικών στοιχείων, τα οποία προέρχονται από σκληρούς δίσκους, συσκευές USB, CD, DVD, με σκοπό την εμπεριστατωμένη παρουσίαση των αποδεικτικών στοιχείων στο δικαστήριο. Η εγκληματολογία βάσεων δεδομένων εφαρμόζει τεχνικές για τη συλλογή αποδεικτικών στοιχείων σε βάσεις δεδομένων, [21]

Η εγκληματολογία στο Διαδίκτυο των Αντικειμένων (IoT), αποτελεί νέο σχετικά κλάδο της ψηφιακής εγκληματολογίας, ο οποίος έχει ως αντικείμενο το Διαδίκτυο των Αντικειμένων (IoT), με σκοπό να εντοπιστούν και να εξαχθούν τα ψηφιακά πειστήρια από διάφορες πηγές, όπως είναι το εσωτερικό δίκτυο, το Cloud, μνήμη RAM, ο επεξεργαστής, ο αποθηκευτικός χώρος, η δυνατότητα να καταγραφούν μηνύματα και επικοινωνίες και άλλα. Τα ψηφιακά πειστήρια θα πρέπει να αναζητηθούν και να εξαχθούν με νόμιμο τρόπο, ώστε να μπορούν να χρησιμοποιηθούν στο δικαστήριο. Η ψηφιακή εγκληματολογία εξετάζει τις τεχνολογίες και τις συσκευές του Διαδικτύου των Αντικειμένων (IoT), οι οποίες πλέον περιλαμβάνουν εκτός από κινητά τηλέφωνα, τα GPS, έξυπνες οικιακές συσκευές, έξυπνα τηλέφωνα, έξυπνες πόλεις, [22].

Αναφορικά με την ψηφιακή εγκληματολογία στο Διαδίκτυο των Αντικειμένων (IoT), οι πηγές των πειστηρίων είναι δυνατό να προέρχονται από συστήματα παρακολούθησης ασθενών, ιατρικών συσκευών, συστήματα που τοποθετούνται σε μέσα μεταφοράς, ξεφεύγοντας από τα συνήθη μέσα διερεύνησης, τα οποία είναι οι υπολογιστές, τα smartphones και άλλα, [23].

2.2 Ιστορική αναδρομή

Η ψηφιακή εγκληματολογία ξεκινά με την ομάδα Computer Analysis and Response Team (CART), την οποία δημιούργησε το 1984 το FBI, με σκοπό να ασχοληθεί με τα ψηφιακά πειστήρια. Σύμφωνα με τους Zareen et al, [24], το NortonDiskEdit αποτέλεσε ένα από τα πιο σημαντικά και αποτελεσματικά εργαλεία εκείνης της εποχής. Από τη στιγμή που δημιουργήθηκαν τα λειτουργικά συστήματα με γραφικό περιβάλλον το 1990, δημιουργήθηκαν εργαλεία της ψηφιακής εγκληματολογίας, τα οποία υιοθέτησαν το γραφικό περιβάλλον, ένα εκ των οποίων ήταν το Encase. Κατά την πρώτη δεκαετία του εικοστού πρώτου αιώνα η χρήση των Windows διευρύνθηκε και σταδιακά αποτέλεσαν το βασικό λειτουργικό σύστημα, σε υπολογιστές οικιακούς αλλά και εταιρικούς. Η υιοθέτηση ενός κοινού λειτουργικού συστήματος διευκόλυνε κατά πολύ τις διαδικασίες της ψηφιακής εγκληματολογίας, [25].

Η σταδιακή τεχνολογική ανάπτυξη προκάλεσε την αύξηση των παράνομων ενεργειών, οι οποίες αφορούσαν τη διακίνηση ύποπτου υλικού, αλλά και την απόσπαση δεδομένων από τους λογαριασμούς των χρηστών των τεχνολογικών μέσων. Σήμερα, η αλματώδης ανάπτυξη των ψηφιακών τεχνολογιών, θέτει την ψηφιακή εγκληματολογία στο επίκεντρο των εξελίξεων και στη διαχείριση των πιο δύσκολων για λύση ψηφιακών εγκλημάτων, [26].

Η θέσπιση νόμων, βάσει των οποίων πραγματοποιείται η ανεύρεση και η ανάλυση των ψηφιακών πειστηρίων έχει ως σκοπό να πληρούνται για τις ψηφιακές αποδείξεις οι κατάλληλες προϋποθέσεις, ώστε να έχουν άμεση σχέση με το έγκλημα, να μη δύναται να αμφισβητηθούν, η αναζήτησή τους να γίνεται επιστημονικά και να μπορούν να επικυρωθούν. Επιπλέον, είναι ιδιαίτερα σημαντική η απαίτηση της σωστής χρήσης των ψηφιακών πειστηρίων, όταν αυτά εντοπιστούν, καθώς είναι ουσιώδες να μην ανοιχτούν, [27], καθώς ανακύπτει και το ζήτημα της διατήρησης του απορρήτου και της διασφάλισης των προσωπικών δεδομένων. Με την κατάρτιση του χάρτη θεμελιωδών δικαιωμάτων κατοχυρώθηκε η προστασία των προσωπικών δεδομένων, ως θεμελιώδες δικαίωμα, ενώ συγχρόνως στον κανονισμό προστασίας δεδομένων συμπεριλήφθηκαν δικαιώματα των ανθρώπων σχετικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων.

2.3 Μέθοδοι Ψηφιακής Εγκληματολογίας

Για την επιστήμη της ψηφιακής εγκληματολογίας, όπως και για κάθε επιστημονικό κλάδο, αναπτύχθηκαν διάφορα μοντέλα εργασίας και διαδικασιών, τα οποία αποσκοπούσαν στη συνέπεια και την τυποποίηση των διαδικασιών, [28]. Τα μοντέλα αυτά, στο σύνολό τους καθόρισαν τα απαραίτητα στάδια, τα οποία θα πρέπει να ακολουθεί η διαδικασία της διερεύνησης. Τα στάδια τα οποία ακολουθεί μια έρευνα ψηφιακής εγκληματολογίας είναι:

Α) Συλλογή Δεδομένων (Data Collection): Σε αυτό το στάδιο, ο ερευνητής πρέπει να αναγνωρίσει τις πηγές, οι οποίες μπορεί να του χρησιμεύσουν στην απόκτηση των δεδομένων. Συνήθεις πηγές δεδομένων είναι οι υπολογιστές (επιτραπέζιοι ή φορητοί), διάφοροι εξυπηρετητές και ιδιαιτέρως τα δίκτυα. Οι ψηφιακές συσκευές που εντοπίζονται βοηθούν τον ερευνητή στην προσέγγιση του σκληρού δίσκου του συστήματος, αλλά και των θυρών USB, μέσω των οποίων θα λάβει τις πληροφορίες που αναζητά. Τα μέσα εξωτερικής αποθήκευσης, όπως οι οπτικοί δίσκοι, τα USB sticks, οι κάρτες μνήμης αποτελούν επίσης πιθανές πηγές δεδομένων για τον ερευνητή. Εκτός από τους ηλεκτρονικούς υπολογιστές ψηφιακά πειστήρια για ένα έγκλημα μπορούν να αναζητηθούν σε κινητά τηλέφωνα, ψηφιακές κάμερες, αυτοκίνητα τελευταίας τεχνολογίας, και άλλα πολλά, τα οποία αποτελούν το Διαδίκτυο των Αντικειμένων (IoT), [29].

Β) Εξέταση (Examination): Στο στάδιο της εξέτασης των ευρημάτων της έρευνας, ο ερευνητής αξιολογεί τα στοιχεία, τα οποία έχει συλλέξει και καταβάλλει προσπάθεια να εξάγει τις πληροφορίες που περιλαμβάνουν, [24]. Δεδομένου του μεγάλου όγκου των δεδομένων, απαιτείται να γίνει αναζήτηση ώστε να ανακτηθούν τα απαραίτητα για την έρευνα στοιχεία, τα οποία εντοπίζονται με διάφορους τρόπους, όπως η χρήση λέξεων-κλειδιών ή φράσεων, ακόμα και με κατάλληλο φιλτράρισμα.

Γ) Ανάλυση (Analysis): Στο στάδιο της ανάλυσης ο ερευνητής θα πρέπει να αναλύσει τα στοιχεία που περιέχονται στα αρχεία που έχει ανακαλύψει, και να εντοπίσει τα πειστήρια, τα οποία θα επιβεβαιώσουν μια υπόθεση για το ψηφιακό έγκλημα ή θα την απορρίψουν. Είναι πολύ σημαντικό να εξασφαλίζεται η εγκυρότητα των αποδεικτικών στοιχείων σε κάθε στάδιο της έρευνας, οπότε ο ερευνητής οφείλει να τα επαληθεύει και να τα διατηρεί στην κατάσταση που τα βρήκε. Επιπλέον, στο στάδιο της ανάλυσης είναι εφικτή, με κατάλληλα μέσα, η ανάκτηση δεδομένων, τα οποία έχουν διαγραφεί, και είναι δυνατόν να ανακατασκευαστούν.

Δ) Αναφορά (Reporting): Στο τέταρτο και τελευταίο στάδιο της έρευνας, ο ερευνητής θα πρέπει να συντάξει την αναφορά των συμπερασμάτων του, η οποία είναι η αναφορά του πορίσματός του. Πρόκειται για έγγραφο, στο οποίο τα συμπεράσματα του ερευνητή θα πρέπει να είναι κατάλληλα διατυπωμένα, ώστε αυτά να γίνονται άμεσα αντιληπτά, χωρίς εξειδικευμένους όρους, ενώ συγχρόνως θα πρέπει να περιλαμβάνονται αναλυτικές πληροφορίες για τη συλλογή και εγκυρότητα των δεδομένων, καθώς και των ερευνητικών εργαλείων που χρησιμοποιήθηκαν. Οι αναφορές των ερευνητών ψηφιακής εγκληματολογίας είναι συνήθως γραπτές ενώ υπάρχουν περιπτώσεις κατά τις οποίες ο ερευνητής καλείται να καταθέσει στο δικαστήριο προφορικά τα συμπεράσματά του, [30].

2.4 Εργαλεία Ψηφιακής Εγκληματολογίας

Τα εργαλεία της ψηφιακής εγκληματολογίας αποτελούν σημαντική βοήθημα για την ερευνητική διαδικασία, [31]. Η επιλογή του εκάστοτε εργαλείου αποτελεί ατομική επιλογή του ειδικού, ο οποίος χειρίζεται ένα έγκλημα, δεδομένου ότι υπάρχει πληθώρα εργαλείων ψηφιακής εγκληματολογίας [32]. Στην ιστοσελίδα του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST), [33] υπάρχει μια βάση με τα περισσότερα εργαλεία ψηφιακής εγκληματολογίας που βρίσκονται διαθέσιμα στο εμπόριο και τα οποία έχουν κατηγοριοποιηθεί σύμφωνα με τις λειτουργίες τους. Τέτοια εργαλεία είναι:

- Οι υπηρεσίες Cloud (Cloud services).#Η υπηρεσίες αυτές πραγματοποιούν την αποθήκευση αρχείων στο διαδίκτυο. Το το Hotmail, το Yahoo Mail είναι υπηρεσίες cloud και επιτρέπουν στο χρήστη να εκμεταλλεύεται τον αποθηκευτικό χώρο και την υπολογιστική ισχύ ενός απομακρυσμένου server, μέσω της σύνδεσης στο Internet.

Εικόνα 1-Υπηρεσίες Cloud. Πηγή:https://pcsecurity.gr/ti-einai-to-cloud-storage

- Λήψη και ανάλυση μνήμης (Memory capture and analysis). Καταγράφοντας τη μνήμη μιας παραβιασμένης συσκευής, μπορεί να εκτελεστεί άμεσα κάποια ανάλυση ώστε να εντοπιστούν πιθανά κακόβουλα προγράμματα και να εντοπιστούν άλλες παραβιασμένες συσκευές.

- Εγκληματολογία βάσης δεδομένων (Database forensics). Η ανάπτυξη βάσεων δεδομένων και η χρήση τους στο Διαδίκτυο, κάνει επιτακτική τη χρήση εργαλείων της Ψηφιακής Εγκληματολογίας, προκειμένου να διασφαλιστεί το απόρρητο της βάσης δεδομένων

- Απόκτηση, ανάλυση και διαλογή φορητών συσκευών (Mobile device acquisition, analysis & triage). Η ευρεία χρήση smartphones, tablets και άλλων συσκευών τηλεφώνου, επιβάλει σε πολλές εκ των περιπτώσεων ψηφιακού εγκλήματος την ιατροδικαστική εξέταση των τηλεφώνων που χρησιμοποιήθηκαν από τους εμπλεκόμενους με το εν λόγω έγκλημα.

- Ανάκτηση διαγραμμένων αρχείων (Deleted file recovery). Σε πολλές περιπτώσεις ψηφιακών εγκλημάτων, οι δράστες προβαίνουν σε διαγραφή των δεδομένων και των στοιχείων, τα οποία θα μπορούσαν να τους ενοχοποιήσουν. Σκοπός των εργαλείων ανάκτησης των

διαγραμμένων αρχείων είναι η χρήση αυτών από τον ερευνητή του εγκλήματος και έχουν αναπτυχθεί για το σκοπό αυτό πληθώρα τέτοιων εργαλείων. Ενδεικτικά αναφέρεται η ύπαρξη εργαλείων της Microsoft για την ανάκτηση διαγραμμένων αρχείων.

- Ανάλυση P2P (P2P analysis). Τα αναλυτικά στοιχεία της διαδικασίας πληρωμής (Procure to pay) αναφέρονται στα αναλυτικά δεδομένα που συλλέγονται κατά τη διάρκεια της διαδικασίας αρχής γενομένης από τον εντοπισμό της ανάγκης για προμήθειες, έως τις εγκρίσεις τιμολογίων και τελικά τις πληρωμές σε προμηθευτές. Τα αναλυτικά στοιχεία P2P χρησιμοποιούνται από τις επιχειρήσεις για τον εντοπισμό αναποτελεσματικών διαδικασιών, κινδύνων και άλλων πληροφοριών.

- Απεικόνιση δίσκου (Disk imaging). Η απεικόνιση δίσκου δημιουργεί αντίγραφα ασφαλείας του σκληρού και τοποθετεί τα δεδομένα σε ένα συμπιεσμένο αρχείο, το οποίο στη συνέχεια δύναται να αποθηκευτεί σε συσκευές αποθήκευσης ή στο Cloud. Η απεικόνιση δίσκου επιτρέπει στους ερευνητές ψηφιακών εγκλημάτων να ανακτήσουν όλα τα δεδομένα που υπήρχαν σε έναν υπολογιστή κατά τη δημιουργία της εικόνας.

- Ανάκτηση κωδικού (Password recovery). Τα εργαλεία ανάκτησης κωδικών προσφέρονται από τις περισσότερες εταιρίες, όπως οι Microsoft, Google και διάφορες ιστοσελίδες, όπως η NirSoft Web και άλλες. Με την ανάκτηση των κωδικών μπορούν οι ερευνητές των ψηφιακών εγκλημάτων να ανατρέξουν σε πολύτιμα στοιχεία από τους προσωπικούς λογαριασμούς των χρηστών.
- Εγκληματολογία Drone (Drone forensics). Η εγκληματολογία των drones είναι ένας όρος που αναφέρεται στην εγκληματολογική επεξεργασία, εξέταση και ανάλυση μη επανδρωμένων εναέριων οχημάτων (UAV).

- Απομακρυσμένες δυνατότητες, Απομακρυσμένη εγκληματολογία (Remote capabilities, Remote forensics). Ο όρος Remote Forensics (η και Network Forensics ή Online Forensics από ορισμένες εταιρείες) καλύπτει μια ευρεία ποικιλία εγκληματολογικών προσεγγίσεων, αλλά χρησιμοποιείται κυρίως για να αναφερθεί στην εξ αποστάσεως εκτέλεση ψηφιακών εγκληματολογικών ερευνών σε ένα εταιρικό περιβάλλον. Είναι η συλλογή, η εξέταση και η αναφορά ψηφιακών στοιχείων από έναν συνδεδεμένο, λειτουργικό υπολογιστή σε ένα δίκτυο.

- Ανάλυση email (Email parsing). Ο αναλυτής email είναι ένας τύπος εφαρμογής λογισμικού που χρησιμοποιείται για την εξαγωγή δεδομένων από εισερχόμενα email, δεδομένα κειμένου από την επικεφαλίδα και το σώμα του email, από συνημμένα αρχεία email όπως έγγραφα PDF, αρχεία CSV και αρχεία MS Office.

- Μέσα κοινωνικής δικτύωσης (Social media). Υπάρχουν εργαλεία έρευνας μέσων κοινωνικής δικτύωσης που μπορούν να μειώσουν σημαντικά το χρόνο εργασίας και να αυτοματοποιήσουν τη συλλογή αποδεικτικών στοιχείων. Με αυτά τα εργαλεία ο ερευνητής μπορεί να επεκτείνει τη διαδικτυακή έρευνα και να συλλέξει πολύτιμα στοιχεία προτού διαγραφούν.

- File Carving. Πρόκειται για τη διαδικασία επανασυναρμολόγησης αρχείων από έναν υπολογιστή που έχει καταστραφεί.

- Software write block. Ένα λογισμικό αποκλεισμού εγγραφής χρησιμοποιείται σε εγκληματολογικές έρευνες για να σταματήσει την εγγραφή νέων δεδομένων στην εν λόγω μονάδα δίσκου. Αυτό είναι σημαντικό λόγω των απαιτήσεων φύλαξης και αποδεικτικών στοιχείων.

- Forensics Boot Environment. Ο σκοπός του εγκληματολογικού δίσκου εκκίνησης είναι να εκκινήσει τον υπολογιστή και να φορτώσει ένα λειτουργικό σύστημα με τρόπο ώστε να μην αλλάξουν τα αποδεικτικά μέσα.

- Steganalysis. Πρόκειται για τη μελέτη της ανίχνευσης μηνυμάτων που κρύβονται χρησιμοποιώντας στεγανογραφία. Αυτό είναι ανάλογο με την κρυπτοανάλυση που εφαρμόζεται στην κρυπτογραφία.

- Forensics tool suite. Τα Digital Forensic Tools είναι πλήρεις σουίτες εφαρμογών λογισμικού που βοηθούν στη διατήρηση, τον εντοπισμό, την εξαγωγή και την τεκμηρίωση στοιχείων υπολογιστή με νόμιμες διαδικασίες. Αυτά τα εργαλεία βοηθούν να γίνει η ψηφιακή εγκληματολογική διαδικασία απλή και εύκολη.

- String search. Μια συμβολοσειρά αναζήτησης είναι ένας συνδυασμός λέξεων-κλειδιών, συμβόλων περικοπής και τελεστών Boolean, τα οποία εισάγονται στο πλαίσιο αναζήτησης μιας βάσης δεδομένων βιβλιοθήκης ή μιας μηχανής αναζήτησης.

- GPS forensics. Πρόκειται για τον εντοπισμό της θέσης ενός αντικειμένου ή ατόμου μέσω συσκευών GPS, η οποία προϋποθέτει τη χρήση κατάλληλων δορυφορικών συστημάτων.

- Video analytics. Η ανάλυση βίντεο μπορεί να επεξεργαστεί τα σήματα των οικιακών και δημοσίων καμερών για να ανιχνεύσει σε πραγματικό ή μετέπειτα χρόνο εάν ένα άτομο έχει διαπράξει κάποιο είδος εγκλήματος, ακόμα και να εντοπίσει το σημείο στο οποίο βρισκόταν κάποια ορισμένη στιγμή. πέσει.

- Hardware write block. Πρόκειται για μια εγκατεστημένη συσκευή που εκτελεί λογισμικό εσωτερικά και μπλοκάρει τη δυνατότητα εγγραφής του υπολογιστή στη συσκευή που είναι συνδεδεμένη στο πρόγραμμα αποκλεισμού εγγραφής.

- VoIP forensics. Το Voice over Internet Protocol (VoIP) είναι μια κυρίαρχη τεχνολογία που επιτρέπει στους χρήστες να πραγματοποιούν τηλεφωνικές κλήσεις μέσω Διαδικτύου και αντικαθιστά την παραδοσιακή τηλεφωνία. Έχουν αναπτυχθεί τεχνικές ώστε να συλλεχθούν και να αναλυθούν τα ψηφιακά στοιχεία που σχετίζονται με δραστηριότητες VoIP.

- Hash analysis. Ο κατακερματισμός είναι μια τεχνική προγραμματισμού στην οποία μια σειρά χαρακτήρων μετατρέπεται σε μια μικρότερη τιμή σταθερού μεγέθους, γνωστή και ως τιμή κατακερματισμού. Υπάρχουν πολλοί διαφορετικοί τύποι αλγορίθμων κατακερματισμού όπως RipeMD, Tiger, αλλά ο πιο κοινός τύπος κατακερματισμού που χρησιμοποιείται για ελέγχους ακεραιότητας αρχείων είναι οι MD5, SHA-2 και CRC32.

- Web browser forensics. Το Browser Forensics συμβάλει στην κατανόηση του τρόπου με τον οποίο διεξήχθη μια επίθεση σε ένα σύστημα, βοηθώντας στην εύρεση της πηγής κακόβουλων προγραμμάτων και λογισμικών κατασκοπείας, κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου και ιστοτόπων ηλεκτρονικού ψαρέματος και άλλα.

- Image analysis. Το λογισμικό ανάλυσης εικόνας, γνωστό και ως αναγνώριση εικόνας ή όραση υπολογιστή, επεξεργάζεται εικόνες για να εξάγει λεπτομέρειες χρησιμοποιώντας τεχνητή

νοημοσύνη. Πρόκειται για σημαντικό εργαλείο στη διάθεση των ερευνητών κάθε είδους εγκλήματος, συμπεριλαμβανομένων και των ψηφιακών εγκλημάτων.

- WiFi forensics. Τα εργαλεία αυτά αποσκοπούν στη συλλογή δεδομένων σε ένα περιβάλλον ασύρματης κυκλοφορίας, την ανάλυσή τους και τη δημιουργία έγκυρων αποδεικτικών στοιχείων που είναι αποδεκτά σε δικαστήριο.

- Infotainment & vehicle forensics. Πρόκειται για ένα ιατροδικαστικό εργαλείο Συστήματος Ευφυών Οχημάτων (ITS) που συλλέγει δεδομένα χρηστών από οχήματα και επιτρέπει στους ιατροδικαστές και τους ερευνητές να τα αναλύσουν άμεσα.

- Windows registry analysis. Τα εργαλεία για την ανάλυση του μητρώου επικεντρώνονται στον εντοπισμό ανεπιθύμητων εφαρμογών ή μη εξουσιοδοτημένης πρόσβασης στο μηχάνημα σε σχέση με τη δραστηριότητα του χρήστη, μέσω της σύνδεσης VNC για πιθανές ενδείξεις παράνομων δραστηριοτήτων.

- Instant Messenger. Η τεχνολογία άμεσων μηνυμάτων (IM) είναι ένας τύπος διαδικτυακής συνομιλίας που επιτρέπει τη μετάδοση κειμένου σε πραγματικό χρόνο μέσω του Διαδικτύου ή άλλου δικτύου υπολογιστών. Τα διαθέσιμα εργαλεία για τον ερευνητή ψηφιακής εγκληματολογίας επιτρέπουν την πρόσβαση στις συνομιλίες και στην αποκάλυψη χρήσιμων για το σκοπό της έρευνας πληροφοριών. Προϋπόθεση και σε αυτή την περίπτωση είναι να ακολουθηθεί η νόμιμη προβλεπόμενη διαδικασία.

- Media sensitization/ drive re-use. Πρόκειται για τη διαδικασία αφαίρεσης δεδομένων από μέσα αποθήκευσης, έτσι ώστε να υπάρχει βεβαιότητα ότι τα δεδομένα ενδέχεται να μην ανακτηθούν και να ανακατασκευαστούν εύκολα.

2.5 Τεχνολογία Cloud και Ψηφιακή Εγκληματολογία

Μια από τις τεχνολογίες αιχμής για την παροχή υπηρεσιών που αφορούν τους υπολογιστές είναι η τεχνολογία Cloud. Με τον όρο Cloud Computing, εννοείται το σύνολο των υπολογιστικών στοιχείων, τα οποία παρέχονται εξ αποστάσεως, κάνοντας χρήση δικτύου, το οποίο είναι συνήθως το internet. Οι παρεχόμενες υπηρεσίες περιλαμβάνουν πλατφόρμες ανάπτυξης εφαρμογών, εργαλεία για το σκοπό αυτό, έτοιμες εφαρμογές και φυσικά υπολογιστικούς πόρους, [34].

Οι υπηρεσίες που παρέχονται μέσω του Cloud δίνουν λύσεις που είναι σύγχρονες και πολύ ελκυστικές, τόσο για τις δυνατότητες που προσφέρουν, όσο και για τις τιμές τους. Αρκετές από τις μεγάλες εταιρείες όπως είναι η Microsoft, η Google, η Amazon, η Apple έχουν επεκτείνει τη δράση τους στις υπηρεσίες Cloud ενώ υπάρχουν και εταιρείες, όπως το Dropbox, η οποία έχει αναδειχθεί ακριβώς για αυτού του είδους την υπηρεσία**,** [35].

Τα ερωτήματα, τα οποία εγείρονται, τόσο σε προσωπικό επίπεδο, όσο και σε εταιρικό, επιχειρηματικό, κυβερνητικό, σχετίζονται με την ασφάλεια και τον βαθμό προστασίας των δεδομένων που παρέχουν αυτές οι υπηρεσίες. Δεδομένου του υφιστάμενου ανταγωνισμού, οι εταιρείες παροχής υπηρεσιών Cloud έχουν αναβαθμίσει τα επίπεδα ασφάλειας σ' αυτό τον τομέα. Τα προβλήματα δημιουργούνται περισσότερο, όταν οι χρήστες των εν λόγω υπηρεσιών δεν δίνουν την πρέπουσα προσοχή, [36].

Οι χρήστες των υπηρεσιών Cloud Computing, ιδιαιτέρως σε κοινόχρηστους υπολογιστές θα πρέπει να είναι πολύ προσεκτικοί στη χρήση των τοπικών εφαρμογών, διότι σε κοινόχρηστους υπολογιστές, η εγκατάσταση τέτοιων εφαρμογών μπορεί να αποτελέσει κενό ασφαλείας. Επιπλέον, απαιτείται η διαβαθμισμένη πρόσβαση ανάλογα με την σημασία των αρχείων, αλλά και προσεκτική ανάγνωση των όρων αποδοχής υπηρεσιών, καθώς μπορεί να αποκαλυφθούν στοιχεία που αφορούν τα προσωπικά δεδομένα του χρήστη, [37]. Συγκεκριμένα, στους όρους κάποιων εταιρειών, όπως η Amazon, η Google και το Dropbox, αναφέρεται το δικαίωμα πρόσβασης της εταιρείας στα αρχεία των χρηστών όταν υπάρχει υπόνοια για αξιόποινες ενέργειες. Τέλος, αυτό που προέχει κατά τη χρήση των υπηρεσιών που παρέχονται μέσω του Cloud, είναι η προσεκτική διαχείριση κωδικών, η χρήση εφαρμογών κρυπτογράφησης για αρχεία υψηλής διαβάθμισης, η προσοχή στην επικοινωνία μέσω email, η χρήση anti-spam φίλτρων και άλλες ενέργειες που προστατεύουν το χρήστη.

Τα εγκλήματα που σχετίζονται με τις υπηρεσίες της τεχνολογίας Cloud, αποτελούν ουσιαστικά ψηφιακά εγκλήματα και μπορεί να είναι εγκλήματα μέσω των οποίων η παρεχόμενη υπηρεσία γίνεται στόχος, είτε εργαλείο, είτε αποθηκευτικό μέσο:

- Το Cloud μπορεί να γίνει στόχος εγκληματιών για τα δεδομένα, τα οποία έχει αποθηκευμένα.

- Επιπλέον, το Cloud Storage θα μπορούσε να αποτελέσει αποθηκευτικό χώρο για παράνομες και εγκληματικές πράξεις.

- Οι υπηρεσίες του Cloud θα μπορούσαν να αποτελέσουν εργαλείο για κάποιον που θέλει να παρέμβει στη λειτουργία κάποιας εταιρείας και στην παρεμβολή του λογισμικού της, [38].

Οι ερευνητές ψηφιακής εγκληματολογίας αντιμετωπίζουν αρκετά προβλήματα στην πρόσβαση στο Cloud, δεδομένου του γεγονότος ότι θα πρέπει να ξεπεραστούν τα νομικής φύσεως ζητήματα, τα οποία είναι πιθανό να ανακύπτουν, αλλά και του γεγονότος ότι τα ψηφιακά πειστήρια μπορεί να σε διάφορα data centers και μάλιστα σε διαφορετικές χώρες. Επιπλέον, ακόμα και με την ανεύρεση των επιθυμητών αποδεικτικών στοιχείων μέσα από το Cloud, πολλές φορές είναι δύσκολη η συσχέτιση ενός φυσικού προσώπου, όπως θα συνέβαινε στην περίπτωση που από τον ηλεκτρονικό υπολογιστή ενός ατόμου προέκυπταν τα πειστήρια. Αυτό συμβαίνει διότι υπάρχουν αρκετά ανώνυμα δίκτυα, οπότε το γεγονός αυτό δύναται να αποτελέσει εμπόδιο για την έρευνα, [39].

Κεφάλαιο 3

Διαδίκτυο των Αντικειμένων

3.1 Εννοιολογικές αποσαφηνίσεις

Το Διαδίκτυο, το οποίο ξεκίνησε ως ένα μικρό διασυνδεδεμένο δίκτυο μικρότερου αριθμού υπολογιστών, έχει πλέον μετατραπεί σε ένα μεγάλο δίκτυο που περιέχει δισεκατομμύρια διασυνδεδεμένους υπολογιστές, οι οποίοι μοιράζονται και αποθηκεύουν πληροφορίες. Ο όρος IoT σημαίνει Internet of Things, στα ελληνικά Διαδίκτυο των Αντικειμένων (IoT), και μπορούμε να περιγράψουμε ένα σύστημα IoT ως ένα σύστημα ή ένα δίκτυο επικοινωνίας αντικειμένων (έξυπνων συσκευών), τα οποία ανταλλάσσουν δεδομένα, μέσω της ενσωμάτωσης ηλεκτρονικών μέσων, λογισμικού, αισθητήρων και συνδεσιμότητας σε δίκτυο [40].

Η εξέλιξη της τεχνολογίας με τη μεγάλη συνδεσιμότητα των εφαρμογών στο Διαδίκτυο, έχει οδηγήσει στην ανάπτυξη του Διαδικτύου των Αντικειμένων (IoT), το οποίο θα μπορούσε να θεωρηθεί ως ένα πρότυπο σύστημα, εντός του οποίου πραγματοποιείται η ενσωμάτωση δικτυακών και υπολογιστικών δυνατοτήτων σε κάθε αντικείμενο. Για να υλοποιηθεί αυτό οι συσκευές του Διαδικτύου των Αντικειμένων (IoT), είναι εξοπλισμένες με αισθητήρες, επεξεργαστές και δέκτες, οι οποίοι είναι και αυτά συσκευές που διευκολύνουν την επικοινωνία με το περιβάλλον. Στόχος είναι να συλλεχθούν πληροφορίες, οι οποίες θα αποθηκευτούν από τη συσκευή, αλλά και θα γίνει επεξεργασία τους ώστε να παραχθούν επιμέρους χρήσιμες πληροφορίες [41].

Την ορολογία IoT (Διαδίκτυο των Αντικειμένων ή Πραγμάτων, όπως μεταφράζεται και χρησιμοποιείται επίσης), χρησιμοποίησε πρώτος το 1999 ο Kevin Ashton, αναφερόμενος σε ένα σύστημα, εντός του οποίου τα αντικείμενα θα είχαν τη δυνατότητα να συνδεθούν με το Διαδίκτυο μέσω αισθητήρων με τη βοήθεια ραδιοσυχνοτήτων [42]. Στην πραγματικότητα το Διαδίκτυο των Αντικειμένων (IoT) βασίζεται σε ένα σύστημα υπολογιστών, το οποίο αλληλεπιδρά με μηχανικά ή ψηφιακά μηχανήματα, ενώ παράλληλα μπορεί να μεταφέρει δεδομένα μέσω του διαδικτύου, είτε αλληλεπιδρώντας με κάποιο χρήστη, είτε και χωρίς να υφίσταται αυτή η αλληλεπίδραση. Ιδιαίτερα σημαντική είναι η παρατήρηση ότι τα αντικείμενα που συμμετέχουν στην ανταλλαγή των πληροφοριών του Διαδικτύου των Αντικειμένων (IoT), δεν χρειάζονται για να λειτουργήσουν ή να επιτελέσουν το σκοπό τους την παρέμβαση του ανθρώπινου παράγοντα, αλλά ενεργούν αυτόνομα, κάνοντας χρήση των πληροφοριών που συλλέγουν [43].

Το Διαδίκτυο των Αντικειμένων (IoT) αποτελείται από πληθώρα συσκευών, όπως κινητά, κάμερες, όργανα, καθώς και οτιδήποτε έχει την ικανότητα να ενσωματώσει κυκλώματα, αισθητήρες και λογισμικό, ενώ συγχρόνως να μπορεί να συνδεθεί στο Διαδίκτυο, με σκοπό τη συλλογή και τη διασπορά των πληροφοριών. Οι δυνατότητες του Διαδικτύου των Αντικειμένων (IoT), έχουν ως αποτέλεσμα τη χρησιμότητά του στην καθημερινή ζωή των ανθρώπων, καθώς η χρήση του μπορεί να αυτοματοποιήσει πολλές από τις καθημερινές μας ενέργειες και δραστηριότητες (ηλεκτρικές συσκευές, αυτοκίνητα, εμπόριο, παραγωγική διαδικασία, τομέας υγείας, εμπόριο [41]. Η αυτοματοποίηση των καθημερινών δραστηριοτήτων του σπιτιού, ο αυτοματισμός στη βιομηχανία και την ιατρική τεχνολογία, η διαχείριση της κυκλοφορίας, και ο έξυπνος τρόπος χρήσης της ενέργειας αποτελούν ορισμένες από τις εφαρμογές του Διαδικτύου των Αντικειμένων (IoT), οι οποίες έχουν ήδη βελτιώσει τη ζωή των ανθρώπων και αναμένεται να την απλοποιήσουν περισσότερο.

Το Διαδίκτυο των Αντικειμένων (IoT) αναδεικνύεται με ταχείς ρυθμούς ως η νέα τάση, η οποία αντικαθιστά άλλες τεχνολογίες, γεγονός που ωθεί τους ερευνητές να το θεωρούν ως το μέλλον του Διαδικτύου. Καθώς η συνδεσιμότητα με τον Παγκόσμιο Ιστό γίνεται πολύ πιο εύκολη, το κόστος σύνδεσης μειώνεται συνεχώς, με αποτέλεσμα κάθε χρήστης να μπορεί να ανταπεξέλθει οικονομικά στις νέες τεχνολογικές απαιτήσεις. Το Διαδίκτυο των Αντικειμένων (IoT), με τα συστήματα και τις εφαρμογές που παρέχει, κάνοντας χρήση διαφόρων ειδών αισθητήρων και συσκευών συνδεδεμένων με το Internet, γίνεται εύχρηστο και μετατρέπεται ως κάτι το κοινό. Το γεγονός αυτό, καθιστά επιτακτική την ανάγκη να επιλυθούν τα ζητήματα που έχουν προκύψει, τα οποία σχετίζονται με την ασφάλεια των πληροφοριών, την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα [44].

3.2 Χαρακτηριστικά του Διαδικτύου των Αντικειμένων

Οι Patel et al, [43] επισήμαναν τα βασικά χαρακτηριστικά των συσκευών του Διαδικτύου των Αντικειμένων (IoT), ως ακολούθως:

- Διασυνδεσιμότητα: Όλες οι συσκευές, όλα τα αντικείμενα του Διαδικτύου των Αντικειμένων (IoT), μπορούν να συνδεθούν με την παγκόσμια υποδομή επικοινωνίας, ώστε να ανταλλάσσουν δεδομένα και να λαμβάνουν τις πρόσφατες ενημερώσεις.

- Υπηρεσίες σχετιζόμενες με τα αντικείμενα: Οι υπηρεσίες που παρέχονται μέσω των συσκευών του Διαδικτύου των Αντικειμένων (IoT), ακολουθούν συγκεκριμένα πρότυπα ασφαλείας και λειτουργούν κάτω από συγκεκριμένους περιορισμούς, όπως για παράδειγμα η προστασία των προσωπικών δεδομένων. Επιπρόσθετα, λαμβάνεται υπόψη η συνοχή

μεταξύ των αντικειμένων που υφίστανται πραγματικά και αυτών της εικονικής πραγματικότητας.

- Ετερογένεια: Οι συσκευές του Διαδικτύου των Αντικειμένων (IoT) έχουν διαφορετική δομή και λειτουργία, δεδομένου ότι κάνουν χρήση διαφορετικών δικτύων, πλατφορμών και υλικών. Παρόλα αυτά μπορούν να επικοινωνούν μεταξύ τους και να ανταλλάσσουν πληροφορίες.

- Δυναμικές αλλαγές: Οι συσκευές του Διαδικτύου των Αντικειμένων (IoT) έχουν ως βασικό τους χαρακτηριστικό την ευμετάβλητη λειτουργική τους κατάσταση και την ευκολία με την οποία συνδέονται και αποσυνδέονται με το δίκτυο και τις λοιπές συσκευές. Επιπρόσθετα, προστίθενται συσκευές, αφαιρούνται κάποιες άλλες, πρόκειται δηλαδή για ένα περιβάλλον, το οποίο αλλάζει διαρκώς.

- Τεράστια Κλίμακα Χρηστών: Το πλήθος των συσκευών που είναι συνδεδεμένες στο Διαδίκτυο των Αντικειμένων (IoT) είναι πολύ μεγάλο. Οι συσκευές αυτές θα πρέπει να μπορούν να επικοινωνήσουν μεταξύ τους και να ανταλλάξουν πληροφορίες, οπότε ο τρόπος διαχείρισης του συστήματος διαδραματίζει σημαντικό ρόλο.

- Ασφάλεια: Ο ασφαλής σχεδιασμός των δεδομένων, των δικτύων και των συσκευών διασφαλίζει τα ευαίσθητα προσωπικά δεδομένα του χρήστη, ενώ συγχρόνως αποτελεί και χαρακτηριστικό το οποίο προσελκύει τους πιθανούς χρήστες. Η ασφάλεια των συσκευών παρέχει στο χρήστη την εμπιστοσύνη ότι οι διακινούμενες πληροφορίες είναι ασφαλείς.

- Συνδεσιμότητα: Η συνδεσιμότητα συνδέεται με την προσβασιμότητα αλλά και με τη συμβατότητα ενός δικτύου. Η προσβασιμότητα αφορά τη σύνδεση της συσκευής σε ένα δίκτυο, ενώ η συμβατότητα αφορά τη δυνατότητα της συσκευής να ανταλλάσσει πληροφορίες με το δίκτυο.

3.3 Ασφάλεια του Διαδικτύου των Αντικειμένων

Η ασφάλεια στη διακίνηση και ανταλλαγή πληροφοριών στο Διαδίκτυο των Αντικειμένων (IoT) αποτελεί μείζον ζήτημα, το οποίο πολλές φορές δημιουργεί εμπόδια στην ανάπτυξη των εφαρμογών. Είναι προφανές, ότι η χρήση των συσκευών του Διαδικτύου των Αντικειμένων θα πρέπει να γίνεται κάτω από κατάλληλες συνθήκες, οι οποίες θα παρέχουν την ασφάλεια στο χρήστη και την προστασία του από άλλους χρήστες και κακόβουλο λογισμικό [47].

Ο αυξανόμενος ανταγωνισμός και λόγω αυτού, η ραγδαία τεχνολογική εξέλιξη των συσκευών που σχετίζονται με το Διαδίκτυο των Αντικειμένων (IoT), πολλές φορές προβλήματα ασφαλείας, είτε εξαιτίας της αδιαφορίας των κατασκευαστών, είτε λόγω της μειωμένης αίσθησης του κινδύνου που εγκυμονεί σε αυτές τις περιπτώσεις [48]. Καθώς οι χρήστες και οι συσκευές αυξάνονται, αυξάνεται και το πλήθος των χρηστών, οι οποίοι κακόβουλα επεμβαίνουν και παραβιάζουν προσωπικά δεδομένα, κυβερνητικά ή στρατιωτικά συστήματα, βάσεις δεδομένων επιχειρήσεων και πολλά άλλα.

Σύμφωνα με τον Thilakarathne, [44], υπάρχουν διάφορες επιθέσεις που μπορεί να δεχτεί το Διαδίκτυο των Αντικειμένων (IoT), αναφορικά με τα στρώματά του:

- Επίθεση στο Στρώμα Αντίληψης: Αυτό το στρώμα είναι το χαμηλότερο στρώμα της αρχιτεκτονικής του Διαδικτύου των Αντικειμένων (IoT) και ονομάζεται επίσης στρώμα Συσκευών. Κύριος στόχος αυτού του στρώματος είναι η συλλογή όλων κάθε είδους πληροφορίας από συσκευές ανίχνευσης και η αποστολή τους στο στρώμα πύλης. Οι απειλές που προκύπτουν σε αυτό το στρώμα είναι α) επίθεση άρνησης υπηρεσίας, με την οποία οι επιτιθέμενοι έχουν τη δυνατότητα να σταματήσουν τη χρήση της υπηρεσίας και να εμποδίσουν άλλους χρήστες να λαμβάνουν την υπηρεσία αυτή, β) Δυσλειτουργία του λογισμικού, με αντικατάσταση εξαρτημάτων των κομβικών σημείων, γ) Εισαγωγή παραποιημένου κόμβου μεταξύ των υπολοίπων κόμβων του συστήματος, προκειμένου να αποκτήσει ο εισβολέας πρόσβαση και έλεγχο όλου του συστήματος, δ) Επίθεση ωμής βίας, με την οποία σε αντίθεση με τις επιθέσεις που εστιάζουν σε αδυναμίες και κενά ασφαλείας του λογισμικού, ο επιτιθέμενος προσπαθεί να αποκτήσει πρόσβαση και έλεγχο του συστήματος, επαναλαμβάνοντας πολλές φορές κωδικούς και ονόματα [44]

- Επίθεση στο στρώμα πύλης εισόδου: Το δεύτερο στρώμα της αρχιτεκτονικής έχει ως κύριο σκοπό να παρέχει αξιόπιστη επικοινωνία μεταξύ του στρώματος Αντίληψης και του στρώματος Cloud. Οι απειλές κατά του στρώματος πύλης διακρίνονται σε α) επίθεση άρνησης υπηρεσίας, δεδομένου ότι σε αυτό το στρώμα παρέχεται η συνδεσιμότητα με το δίκτυο, β)

Επίθεση παραβίασης συνεδρίας, κατά την οποία οι εισβολείς παραβιάζοντας τη συνεδρία αποκτούν πρόσβαση στο δίκτυο, γ) Επιθέσεις εκ του μέσου, κατά τις οποίες ο εισβολέας μπορεί να διασταυρώσει το κανάλι επικοινωνίας, μεταξύ δύο κόμβων και να αποκτήσει διαβαθμισμένες πληροφορίες.

- Επίθεση στο στρώμα Cloud: Αυτό το στρώμα είναι το ανώτατο επίπεδο στην αρχιτεκτονική του Διαδικτύου των Αντικειμένων (IoT) και υπεύθυνο για την παροχή της υπηρεσίας στους χρήστες, οι οποίοι μπορούν να χειρίζονται και να παρακολουθούν τις συσκευές τους. Οι απειλές κατά του στρώματος Cloud μπορεί να είναι: α) ασφάλεια δεδομένων, β) Επιθέσεις στρώματος εφαρμογών και λογισμικού, γ) Επίθεση σε εικονικές μηχανές του Διαδικτύου των Αντικειμένων (IoT), γεγονός που μπορεί να θέσει σε κίνδυνο τη λειτουργία όλου του συστήματος.

Οι Conti et al. [49] ανέδειξαν τα ζητήματα ασφαλείας και απορρήτου για το Διαδίκτυο των Αντικειμένων (IoT) ως ακολούθως:

- Ζητήματα ταυτοποίησης: Είναι ιδιαίτερα σημαντικό να επαληθευτούν οι πληροφορίες που διαδίδονται και μεταφέρονται μέσω του Διαδικτύου των Αντικειμένων (IoT), να ταυτοποιηθεί η προέλευση αλλά και η διαδρομή τους. Η αναγνώριση των συσκευών είναι επίσης πολύ σημαντική. Για τους σκοπούς της ταυτοποίησης μπορούν να κατασκευαστούν κλειδιά και να δοθούν στους χρήστες [50].

- Ζητήματα εξουσιοδότησης και ελέγχου πρόσβασης: Τα δικαιώματα πρόσβασης καθορίζονται από την εξουσιοδότηση που παρέχεται σε κάθε χρήστη. Για την πρόσβαση πραγματοποιείται έλεγχος πρόσβασης αυτών που έχουν λάβει την εξουσιοδότηση. Το πλήθος των εξουσιοδοτήσεων διαφέρει από συσκευή σε συσκευή και σε κάθε κόμβο του Διαδικτύου των Αντικειμένων (IoT), με αποτέλεσμα να αναζητείται η βέλτιστη ανάπτυξη και διαχείριση των εξουσιοδοτήσεων [44].

- Ζητήματα ιδιωτικότητας: Τα ευαίσθητα προσωπικά δεδομένα, τα οποία διακινούνται μέσω του Διαδικτύου των Αντικειμένων (IoT) αποτελούν μείζον θέμα για αυτούς που ασχολούνται με ζητήματα ασφαλείας αλλά και τους χρήστες. Δεν είναι λίγες οι περιπτώσεις, κατά τις οποίες οι συσκευές συλλέγουν και μεταδίδουν πληροφορίες που αφορούν το χρήστη, χωρίς να έχει δώσει τη συγκατάθεσή του και δίχως να έχει ενημερωθεί για αυτό. Πρόκειται για την παραβίαση του δικαιώματος για διασφάλιση των προσωπικών δεδομένων, γεγονός το οποίο αποτελεί ένα ιδιαίτερα ευαίσθητο θέμα, καθώς αφορά χρήστες κάθε ηλικίας,

συμπεριλαμβανομένων και των παιδιών, τα οποία για εκπαιδευτικούς λόγους εξοικειώνονται και έρχονται σε επαφή με το Διαδίκτυο και το Διαδίκτυο των Αντικειμένων (IoT) από πολύ μικρή ηλικία. Τα ευαίσθητα προσωπικά δεδομένα των χρηστών, συνήθως συνεχίζουν να είναι αποθηκευμένα στις συσκευές, και αυτό σημαίνει ότι σε βάθος χρόνου είναι πολύ σημαντικό να εντοπιστούν και να αποτραπεί η πρόσβαση σε αυτά σε κάθε κακόβουλο χρήστη [47] .

- Ζητήματα Αρχιτεκτονικής Ασφαλείας: Προκειμένου να επιλυθούν τα ζητήματα ασφαλείας, είναι απαραίτητο να αναπτυχθεί μια αρχιτεκτονική του Διαδικτύου των Αντικειμένων (IoT), η οποία θα αντιμετωπίζει τα θέματα ασφαλείας αλλά και όλες τις δυσκολίες που είναι δυνατό να εμφανιστούν [49].

3.4 Εφαρμογές του Διαδικτύου των Αντικειμένων

Το Διαδίκτυο των Αντικειμένων (IoT) αποτελεί πλέον αναπόσπαστο τμήμα της ανθρώπινης ζωής, καθώς βρίσκει εφαρμογή στην καθημερινότητα του ανθρώπου, στον επαγγελματικό και τον ιατρικό τομέα, στη λειτουργία δημοσίων και ιδιωτικών επιχειρήσεων, σε συστήματα διαχείρισης ενεργειακών πόρων και τόσα άλλα.

- Οι έξυπνες πόλεις: σε μια έξυπνη πόλη είναι εφικτή η παρακολούθηση της σεισμικής δραστηριότητας και της δομικής κατάστασης των κτηρίων και όλων των υποδομών. Επιπλέον, υπάρχει έξυπνος φωτισμός, ο οποίος μπορεί να προσαρμοστεί με τις μεταβολές των καιρικών συνθηκών και την εποχή. Υπάρχει δυνατότητα ψηφιακής διαχείρισης των συστημάτων πυρασφάλειας και επιτυγχάνεται η ασφάλεια των πολιτών και της δημόσιας και ιδιωτικής ζωής μέσω συστημάτων καταγραφικών καμερών [51].

- Τα έξυπνα σπίτια: η καθημερινότητα με τις δραστηριότητες και τις δουλειές του σπιτιού μπορεί να απλοποιηθεί με τις έξυπνες συσκευές, οι οποίες μπορούν να συνδεθούν στο διαδίκτυο. Οι συσκευές αυτές έχουν αισθητήρες, οι οποίοι λαμβάνουν πληροφορίες από το περιβάλλον του σπιτιού και αυτόνομα προβαίνουν σε κάποιες ενέργειες, με αποτέλεσμα να μπορεί κανείς να ελέγχει τις οικιακές συσκευές, να παρακολουθεί με κάμερες το χώρο του σπιτιού και άλλα [52].

- Έξυπνα αυτοκίνητα: πρόκειται για αυτοκίνητα με έξυπνη τεχνολογία, τα οποία είναι αυτόνομα και λειτουργούν ρομποτικά. Τα έξυπνα αυτοκίνητα έχουν τη δυνατότητα ανίχνευσης του περιβάλλοντος και συνδυάζοντας διάφορους αισθητήρες μπορούν να κινούνται με ασφάλεια, εντοπίζοντας την κατάλληλη πορεία με ελάχιστη συμμετοχή των

οδηγών. Ο οδηγός του έξυπνου αυτοκινήτου μπορεί να το ξεκλειδώσει απομακρυσμένα, να βρει οδικούς χάρτες, να γνωρίζει την κίνηση που θα συναντήσει και να βρει τη βέλτιστη διαδρομή. Τα έξυπνα αυτοκίνητα διαθέτουν σύστημα υποβοήθησης οδήγησης, σύστημα βοήθειας φρεναρίσματος, σύστημα αυτόματου παρκαρίσματος. Σύστημα μηχανικού ελέγχου και αυτορρύθμισης σε αναρτήσεις και άλλα μέρη του οχήματος, σύστημα ηλεκτρονικής σύνδεσης με το Διαδίκτυο και τους δορυφόρους για ενημέρωση της κίνησης και για χάρτες [53].

- Σύστημα Ευφυών Μεταφορών (ITS): Πρόκειται για συστήματα, τα οποία παρέχουν παρακολούθηση του δικτύου μεταφοράς με σκοπό τον έλεγχο και τη σωστή λειτουργία του. Για τη λειτουργία των Συστημάτων Ευφυών Μεταφορών (ITS) υπάρχουν ενσωματωμένα GPS, αναγνώστες RFID και άλλα χαρακτηριστικά [54].

- Έξυπνη ενέργεια: Η διαχείριση της ενέργειας τόσο σε οικιακό επίπεδο, όσο και σε επιχειρηματικό, βιομηχανικό και περιβαλλοντικό είναι απαραίτητη προκειμένου να χρησιμοποιηθούν με το βέλτιστο τρόπο τα ενεργειακά αποθέματα. Οι έξυπνες συσκευές διαχείρισης της ενέργειας μπορούν να αναλύσουν δεδομένα που λαμβάνουν από το περιβάλλον και να λειτουργήσουν υπό το πνεύμα της εξοικονόμησης ενέργειας. Οι θερμοστάτες για παράδειγμα ρυθμίζουν τη θερμοκρασία του χώρου λαμβάνοντας δεδομένα θερμοκρασίας, ενώ υπάρχει πλέον δυνατότητα ενεργοποίησης ενός κλιματιστικού απομακρυσμένα, ώστε ο χρήστης να βρει το σπίτι του στη θερμοκρασία που επιθυμεί [55].

- Έξυπνη υγεία: τα συστήματα παρακολούθησης των ασθενών και της κατάστασής τους τόσο στο περιβάλλον του σπιτιού, του νοσοκομείου, όσο και όταν αυτοί δραστηριοποιούνται, αποτελεί μεγάλο επίτευγμα και η τελειοποίηση ενός τέτοιου συστήματος υγείας αποτελεί ευσεβή πόθο. Πλέον στους ασθενείς μπορούν να τοποθετηθούν εξειδικευμένοι αισθητήρες που μετρούν τους καρδιακούς παλμούς, τη θερμοκρασία και άλλα και δίνουν τη δυνατότητα για άμεση διάγνωση [56].

3.5 Η Ψηφιακή Εγκληματολογία στο Διαδίκτυο των Αντικειμένων

Οι Hou et al. [57] απεικονίζουν το τοπίο της ψηφιακής εγκληματολογίας σε περιβάλλον IoT ως ένα τρισδιάστατο πλαίσιο που αποτελείται από χρονική, χωρική και τεχνική διάσταση. Η χρονική διάσταση αφορά τα διαδοχικά στάδια μιας τυπικής εγκληματολογικής έρευνας, που περιλαμβάνουν τη συλλογή, εξέταση, ανάλυση και παρουσίαση των ευρημάτων. Η χωρική διάσταση σχετίζεται με τον

εντοπισμό πιθανών πηγών αποδεικτικών στοιχείων, ενώ η τεχνική διάσταση στοχεύει στη διερεύνηση κατάλληλων τεχνικών και εργαλείων συλλογής, εξέτασης και ανάλυσης των δεδομένων.

Οι Kebande et al [58] αναφέρουν πως η ψηφιακή εγκληματολογική διαδικασία για τη συλλογή και την ανάλυση ψηφιακών στοιχείων στο περιβάλλον IoT είναι ανάγκη να διαχωριστεί σε τρία επιμέρους επίπεδα: αυτό της συσκευής, του δικτύου και του Cloud. Προτείνουν το " Digital Forensic Investigation Framework for Internet of Things (DFIF-IoT)", ένα μοντέλο ψηφιακής εγκληματολογικής έρευνας κατάλληλο για το περιβάλλον Διαδικτύου των Αντικειμένων (IoT), που είναι συμβατό με το διεθνές πρότυπο ISO/IEC 27043: 2015. Το "DFIF-IOT" συγκρίνεται με τρία υφιστάμενα μοντέλα που έχουν αξιοποιηθεί στον χώρο του IoT και συμπεραίνεται ότι η ενσωμάτωση του σε εργαλεία ψηφιακής εγκληματολογίας μπορεί να συνεισφέρει στην αποτελεσματική διεξαγωγή σχετικών ερευνών.

Οι Atlam et al. [21] επισημαίνουν την ανάγκη εισαγωγής της τεχνητής νοημοσύνης στην ψηφιακή εγκληματολογία σε περιβάλλον IoT, για την επίλυση των υφιστάμενων περιορισμών σε χρόνο και διαθεσιμότητα πόρων που ανακύπτουν κατά την επεξεργασία του τεράστιου αριθμού δεδομένων που συλλέγονται. Οι συγγραφείς συγκρίνουν την παραδοσιακή ψηφιακή εγκληματολογία με την ψηφιακή εγκληματολογία στο νέφος και στο Διαδίκτυο των Αντικειμένων (IoT) ως προς τον αριθμό των εμπλεκόμενων συσκευών, τους τύπους των δικτύων, τις πηγές αποδεικτικών στοιχείων, τα πρωτόκολλα επικοινωνίας κλπ. Παρουσιάζουν μία σύνοψη σχετικών ερευνητικών εργασιών, τις οποίες ταξινομούν με βάση το αντικείμενο στο οποίο επικεντρώνονται και την κύρια συνεισφορά τους στη συγκεκριμένη επιστημονική περιοχή. Αναφέρουν οκτώ εργαλεία που αξιοποιούνται στις σχετικές έρευνες και περιγράφουν τις σημαντικότερες προκλήσεις που διαπιστώνονται και τους προτεινόμενους τρόπους αντιμετώπισης.

Οι Nieto et al. [59] στη μελέτη τους εξετάζουν τις πτυχές της ψηφιακής εγκληματολογίας υπό το πρίσμα της προστασίας του απορρήτου των δεδομένων και τονίζουν τη σημαντικότητα της συγκεκριμένης προσέγγισης. Αναφέρουν την κείμενη διεθνή νομοθεσία σχετικά με την προστασία των προσωπικών δεδομένων, τις αρχές της ιδιωτικότητας και πως αυτές θα πρέπει να διέπουν όλα τα στάδια της ψηφιακής εγκληματολογικής έρευνας.

Οι ίδιοι μελετητές σε άλλη τους δημοσίευση [60] προτείνουν ένα νέο μοντέλο για την ψηφιακή εγκληματολογία στο IoT που ονομάζεται "Privacy-aware IoT-Forensic Model (PRoFIT)" και παρουσιάζουν ένα υποθετικό σενάριο εφαρμογής του. Το μοντέλο αυτό λαμβάνει υπόψη τις αρχές προστασίας του απορρήτου των δεδομένων ενσωματώνοντας τις βασικές απαιτήσεις του προτύπου ISO/ IEC 29100: 2011 καθ' όλη τη διάρκεια του κύκλου ζωής της έρευνας. Στη μελέτη επισημαίνεται η

σημασία της συνεργασίας μεταξύ των διαφορετικών συσκευών IoT που σχετίζονται με τη σκηνή ενός εγκλήματος για τον εντοπισμό και τη συλλογή πιθανών ψηφιακών πειστηρίων.

Οι Wu et al. [61] διερευνούν τα διαθέσιμα εργαλεία που χρησιμοποιούνται στα διάφορα είδη ψηφιακής εγκληματολογίας, περιλαμβανομένης αυτής του διαδικτύου των πραγμάτων. Αναλύοντας 800 άρθρα από το 2014 έως το 2019, εντοπίζουν 62 εργαλεία εκ των οποίων τα 33 είναι διαθέσιμα ενώ στη συντριπτική τους πλειοψηφία δεν έχουν συντηρηθεί μετά την ανάπτυξή τους. Προτείνεται η δημιουργία ενός κεντρικού αποθετηρίου δοκιμασμένων εργαλείων ψηφιακής εγκληματολογίας.

Οι Arshad et al. [11] εξετάζουν διάφορες λύσεις που έχουν προταθεί στη διεθνή βιβλιογραφία αναφορικά με την τεκμηρίωση της εγκυρότητας των ψηφιακών πειστηρίων. Ειδικότερα αναλύεται η χρήση των τεσσάρων κριτηρίων του Daubert Test για την πειραματική αξιολόγηση των χρησιμοποιούμενων τεχνικών και εργαλείων συλλογής και διαχείρισής τους. Οι συγγραφείς επισημαίνουν τη δυσκολία αποδοχής των ψηφιακών τεκμηρίων στο δικαστήριο, αναφέροντας πολλές περιπτώσεις δικαστικών υποθέσεων από τις ΗΠΑ.

Οι Stoyanova et al. [23] παρουσιάζουν μια σύνοψη των θεωρητικών μοντέλων ψηφιακής εγκληματολογίας που έχουν αναπτυχθεί τα τελευταία 25 χρόνια (1995-2019). Ιδιαίτερη έμφαση δίνεται στα μοντέλα που εφαρμόζουν τις αρχές προστασίας της ιδιωτικότητας στην εξαγωγή δεδομένων καθώς και σε αυτά που εξασφαλίζουν την ακεραιότητα των ψηφιακών πειστηρίων με χρήση αποκεντρωμένων συστημάτων βασισμένων στην τεχνολογία blockchain. Αναφέρονται οι σύγχρονες τεχνολογικές καινοτομίες που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας όπως η Forensics-as-a-Service και η τεχνητή νοημοσύνη σε συνδυασμό με τεχνικές μείωσης του όγκου των δεδομένων. Τέλος επισημαίνεται η ανάγκη υιοθέτησης στρατηγικών εγκληματολογικής ετοιμότητας και ανάπτυξης κοινώς αποδεκτών προτύπων.

Οι Al-Khateeb et al. [62] αναλύουν τα πλεονεκτήματα που παρουσιάζει η χρήση της τεχνολογίας blockchain στα σύγχρονα μοντέλα ψηφιακής εγκληματολογίας, με σημαντικότερο την ανάπτυξη εφαρμογών ηλεκτρονικής αλυσίδας φύλαξης ψηφιακών πειστηρίων η οποία συνεισφέρει στην αποδοχή τους από το δικαστήριο. Περιγράφουν την έννοια του ψηφιακού μάρτυρα που μπορούν να διαδραματίσουν οι οντότητες του IoT υπό συγκεκριμένες προϋποθέσεις οι οποίες αναφέρονται και παρουσιάζουν μία μελέτη περίπτωσης στον τομέα της «έξυπνης» ιατρικής.

Στη μελέτη τους οι Ryu et al. [63] προτείνουν ένα μοντέλο ψηφιακής εγκληματολογίας για περιβάλλοντα IoT βασισμένο στην τεχνολογία Blockchain. Στο προτεινόμενο μοντέλο όλες οι επικοινωνίες των συσκευών IoT αποθηκεύονται σε ένα κατανεμημένο καθολικό, εξασφαλίζοντας με αυτό τον τρόπο τη διαφάνεια και την ακεραιότητα στη διαδικασία της αλυσίδας φύλαξης των

αποδεικτικών στοιχείων. Το μοντέλο δοκιμάζεται σε προσομοίωση και επιβεβαιώνεται η πρακτική εφαρμογή του. Ωστόσο πρέπει να δοκιμαστεί σε περισσότερες συσκευές IoT, σε διαφορετικά σενάρια χρήσης και σε πραγματικές εγκληματολογικές έρευνες.

Οι Dasaklis et al. [64], επιχειρούν μια επισκόπηση και ταξινόμηση των διαθέσιμων πλαισίων ψηφιακής εγκληματολογίας που βασίζονται στην τεχνολογία blockchain και περιγράφουν τα κύρια χαρακτηριστικά τους. Αναλύουν τα πλεονεκτήματα και τις προκλήσεις που πηγάζουν από την ενσωμάτωση της τεχνολογίας blockchain στις σύγχρονες προσεγγίσεις ψηφιακής εγκληματολογίας που προτείνονται στη βιβλιογραφία (εξέταση 24 άρθρων). Τέλος εντοπίζουν τα υπάρχοντα κενά στην έρευνα και προτείνουν μελλοντικές ερευνητικές κατευθύνσεις.

Οι Ab Rahman et al. [65] στην εργασία τους επισημαίνουν την ανάγκη ανάπτυξης ενός πλαισίου προληπτικού εγκληματολογικού σχεδιασμού (forensic-by-design) των κυβερνοφυσικών συστημάτων στο νέφος, που θα διευκολύνει την ανίχνευση της πηγής ενός περιστατικού καθώς και τη διατήρηση και ανάλυση κρίσιμων αποδεικτικών δεδομένων, απλοποιώντας και επιταχύνοντας τη διεξαγωγή εγκληματολογικών ερευνών. Προτείνουν ένα μοντέλο εγκληματολογικής ετοιμότητας που είναι συμβατό με το πρότυπο ISO/IEC 27043:2015 και υποστηρίζει διαδικασίες εντοπισμού πιθανών πηγών αποδεικτικών στοιχείων, προληπτικής συλλογής και ανάλυσης τους, κατάλληλης αποθήκευσης και διαχείρισης τους με παράλληλη διατήρηση της αλυσίδας φύλαξης καθώς και ανίχνευσης περιστατικών. Τέλος παρουσιάζουν μια υποθετική μελέτη περίπτωσης με αντικείμενο το προληπτικό εγκληματολογικό σχεδιασμό ενός οχηματικού δικτύου (vanet).

Ο Theobald [66] αναφέρει την ανάγκη προσέγγισης στον σχεδιασμό των διασυνδεδεμένων αντικειμένων με τρόπο τέτοιο ώστε αυτά να είναι ασφαλή. Οι συσκευές IoT έχουν σχεδιαστεί για να συνδέονται στο Διαδίκτυο δίχως να δίνεται έμφαση στην ασφάλεια με αποτέλεσμα να τις καθιστά εξαιρετικά ευάλωτες σε επιθέσεις που μπορούν κυριολεκτικά να επηρεάσουν τις ζωές των ανθρώπων. Η λύση σε αυτό είναι η υιοθέτηση της ενσωμάτωσης της ασφάλειας από τον σχεδιασμό και την κατασκευή αυτών των συσκευών.

Κεφάλαιο 4

Συστήματα Ευφυών Μεταφορών

4.1 Εννοιολογικές αποσαφηνίσεις

Τα Συστήματα Ευφυών Μεταφορών (Intelligent Transport Systems, ITS) εφαρμόζονται στον τομέα των μεταφορών και συνδυάζουν τεχνολογίες πληροφόρησης και επικοινωνίας, που αποσκοπούν στην πιο ασφαλή κυκλοφορία, πιο οικονομική και πιο αποδοτική, συμβάλλοντας επιπλέον στην προστασία του περιβάλλοντος. Οι πληροφορίες με τα Συστήματα Ευφυών Μεταφορών (ITS) παρέχονται σε πραγματικό χρόνο στους οδηγούς, στους ταξιδιώτες, στους διαχειριστές της κυκλοφορίας, μέσω συσκευών ψηφιακής τεχνολογίας [67].

Σύμφωνα με τους Haydari et al, [68], με την αυξανόμενη αστικοποίηση και τις τελευταίες εξελίξεις στις αυτόνομες τεχνολογίες, οι μελέτες σχετικά με τα συστήματα μεταφορών ανέδειξαν τη χρήση ευφυών συστημάτων, τα οποία ορίζονται ως Συστήματα Ευφυών Μεταφορών (ITS). Η τεχνητή νοημοσύνη (AI) προσπαθεί να ελέγξει τα συστήματα με ελάχιστη ανθρώπινη παρέμβαση, με σκοπό να βρεθούν αποτελεσματικές λύσεις για τις μεταφορές του 21ου αιώνα. Ο κύριος στόχος του Συστήματος Ευφυών Μεταφορών (ITS) είναι να παρέχει ασφαλή, αποτελεσματικά και αξιόπιστα συστήματα μεταφοράς σε όσους συμμετέχουν στη διαδικασία μεταφοράς και μετακίνησης εντός της πόλης.

Οι Nelson, et al, [69] όρισαν τα Συστήματα Ευφυών Μεταφορών (ITS) ως μια εφαρμογή, μέσω της οποίας είναι εφικτή η διαχείριση της ψηφιακής πληροφορίας, για την αντιμετώπιση προβλημάτων κίνησης και μεταφορών. Οι Vahidi και Sayed [70] όρισαν τα Συστήματα Ευφυών Μεταφορών (ITS) , ως εκείνα τα συστήματα μεταφορών, τα οποία έχουν σχεδιαστεί για να συμβάλουν στη βελτίωση της μετακίνησης πάνω στη γη, με την αύξηση της κινητικότητας, την αναβάθμιση του επιπέδου ασφαλείας, τον περιορισμό της κατανάλωσης καυσίμων και την προστασία του περιβάλλοντος.

Μια έξυπνη πόλη είναι αυτή η οποία επωφελείται από τις εφαρμογές του Διαδικτύου των Αντικειμένων (IoT) [51], και παρέχει στους πολίτες της διευκολύνσεις στην καθημερινότητά τους. Η έξυπνη πόλη χαρακτηρίζεται από το προηγμένο σύστημα μεταφοράς της και τη δυνατότητα ενσωμάτωσης των ψηφιακών τεχνολογιών σε αυτό, ώστε να προαχθεί η ασφάλεια στους δρόμους, να διευκολύνονται οι μετακινήσεις και να προστατεύεται το περιβάλλον. Η τεχνολογία της ψηφιακής πληροφορίας έχει σταδιακά αλλάξει τα συστήματα μεταφορών, αναφορικά με την ύπαρξη και αυξανόμενη χρήση περισσότερων δρόμων και υποδομών, τη δυνατότητα λήψης πληροφοριών σε

πραγματικό χρόνο και την ύπαρξη διαφόρων ειδών αισθητήρων που αποσκοπούν στη λήψη πληροφοριών μεταξύ των χρηστών και των διαχειριστών του συστήματος, αλλά και των διαχειριστών σε σχέση με την κυκλοφορία.

Η χρηματοδότηση των Συστημάτων Ευφυών Μεταφορών (ITS) διαδραματίζει σημαντικότατο ρόλο για την ανάπτυξη και την εξέλιξή τους. Στις αναπτυγμένες χώρες και σε κάποιες αναπτυσσόμενες, όπου υπάρχουν διαθέσιμοι οι απαραίτητοι οικονομικοί πόροι, έχει σημειωθεί σημαντική πρόοδος σχετικά με την απόδοση των συστημάτων μεταφορών, έχει περιοριστεί η συμφόρηση της κυκλοφορίας, έχει προαχθεί και διασφαλιστεί η ασφάλεια των ταξιδιωτών και έχει διευκολυνθεί η μετακίνησή τους. Ιδιαίτερη είναι η συμβολή των έξυπνων κινητών με τις εφαρμογές που διαθέτουν, αλλά και η δυνατότητα σύνδεσης στο Διαδίκτυο, ανεξάρτητα της τοποθεσίας που βρίσκεται ο χρήστης, [71].

Τα μελλοντικά συστήματα μεταφορών αναμένεται να χαρακτηρίζονται από πλήρη αυτονομία όπως για παράδειγμα αυτόνομη διαχείριση κυκλοφορίας και αυτόνομη οδήγηση. Ακόμα και σήμερα, τα ημιαυτόνομα οχήματα καταλαμβάνουν τους δρόμους και το επίπεδο αυτονομίας είναι πιθανό να αυξηθεί στο εγγύς μέλλον. Υπάρχουν διάφοροι λόγοι για τους οποίους θέλουν οι αρχές την αυτονομία των Συστημάτων Ευφυών Μεταφορών (ITS), όπως είναι η εξοικονόμηση χρόνου για τους οδηγούς, η εξοικονόμηση ενέργειας για το περιβάλλον και την ασφάλεια για όλους τους συμμετέχοντες. Επιπλέον, μπορεί να επιτευχθεί η συντόμευση του χρόνου ταξιδιού μέσω συντονισμένης κυκλοφορίας και σύνδεσης των οχημάτων σε ένα αυτόματο και αυτόνομο σύστημα κυκλοφορίας. Όταν τα οχήματα παραμένουν για περισσότερο χρόνο στην κυκλοφορία, η κατανάλωση καυσίμου αυξάνεται, κάτι που έχει περιβαλλοντικές και οικονομικές επιπτώσεις. Ένας άλλος λόγος για τον οποίο γίνεται προσπάθεια να ελαχιστοποιηθεί η ανθρώπινη παρέμβαση είναι γιατί με αυτό τον τρόπο αναμένεται ότι θα μειωθούν τα τροχαία ατυχήματα και θα αυξηθεί η ποιότητα των μεταφορών [68].

Ο αυξανόμενος πληθυσμός στις αστικές περιοχές προκαλεί μεγάλο όγκο κυκλοφορίας, γεγονός που προκαλεί την αύξηση του ετήσιου κόστους συμφόρησης για τους οδηγούς [72]. Ως εκ τούτου, ο πιο αποτελεσματικός έλεγχος των φωτεινών σηματοδοτών παρουσιάζει μεγάλο ενδιαφέρον, καθώς αναμένεται να συμβάλει στην επίλυση του προβλήματος. Εκτός από τους φωτεινούς σηματοδότες, υπάρχουν πλέον και άλλα ηλεκτρονικά σήματα κυκλοφορίας, τα οποία μπορούν ανιχνεύσουν την κίνηση σε ένα κόμβο, τη σύγκρουση οχημάτων, την εκτός λωρίδας κίνηση ενός οχήματος και τόσα άλλα.

Τα συστήματα διαχείρισης κυκλοφορίας μας επιτρέπουν να λύσουμε ένα από τα πιο σημαντικά προβλήματα σήμερα, το οποίο είναι η κυκλοφοριακή συμφόρηση. Η χρήση νέων προσεγγίσεων από τον τομέα των Συστημάτων Ευφυών Μεταφορών (ITS) καθιστά δυνατή την ελαχιστοποίηση των

απωλειών και των ζημιών, προάγει το υψηλό επίπεδο κυκλοφοριακής ικανότητας και τη βέλτιστη χρήση των υπαρχόντων δρόμων και των υποδομών. Ταυτόχρονα επιτυγχάνεται η μείωση του χρόνου που ξοδεύεται όταν υπάρχει συμφόρηση του οδικού δικτύου και η βέλτιστη χρήση του υφιστάμενου οδικού δικτύου. Τέτοιες προσεγγίσεις περιλαμβάνουν τον έλεγχο της ταχύτητας, τη βελτιστοποίηση των τρόπων ελέγχου των φωτεινών σηματοδοτών, τους πίνακες πληροφοριών, τα διάφορα συστήματα ενημέρωσης των οδηγών και άλλα [73]. Όλα αυτά τα συστήματα μπορούν να λειτουργήσουν είτε μεμονωμένα είτε σε συνεργασία το ένα με το άλλο, με τα σύγχρονα κυκλοφοριακά προβλήματα να αποκαλύπτουν την ανάγκη συνδυασμού όλων των συστημάτων που επιτρέπουν να έχουν οι οδηγοί το επιθυμητό αποτέλεσμα με την υπάρχουσα υποδομή. Για την εφαρμογή τέτοιων προσεγγίσεων, είναι απαραίτητο να ληφθούν αξιόπιστες μετρήσεις των παραμέτρων κυκλοφορίας και να πραγματοποιηθεί η ανάπτυξη κατάλληλων αλγορίθμων για τη διαχείριση των ροών κυκλοφορίας. Η ανάπτυξη κατάλληλων συστημάτων στη σύγχρονη διαχείριση της κυκλοφορίας συνίσταται στην ευρεία χρήση καμερών. Από τις ληφθείσες εγγραφές βίντεο, μπορούν να βρεθούν αρκετές παράμετροι κυκλοφορίας, οι οποίες δύνανται να αξιολογηθούν χρησιμοποιώντας κάμερες εγγραφής φωτογραφιών και βίντεο, όπως η ένταση της κυκλοφορίας των οχημάτων, η απόσταση ασφαλείας μεταξύ των οχημάτων, ο τύπος του οχήματος, η ταχύτητα, οι πίνακες προορισμού και ούτω καθεξής [74].

Ο τομέας των Συστημάτων Ευφυών Μεταφορών (ITS), παρόλο που δεν αποτελεί ένα καινούριο και άγνωστο ερευνητικό περιβάλλον, λόγω της ραγδαίας εξέλιξης της ψηφιακής τεχνολογίας, αλλά και της πληθυσμιακής αύξησης των πόλεων, συνιστά ένα ευρύ ερευνητικό πεδίο, με πολλά νέα εργαλεία, υπηρεσίες και υποδομές, με άμεση επίδραση στην κοινωνία [75]. Τα Συστήματα Ευφυών Μεταφορών (ITS) βρίσκουν εφαρμογή σε όλα τα συστήματα μεταφορών, επίγεια (οδικά, σιδηροδρομικά), θαλάσσια και εναέρια στοχεύοντας να περιοριστεί το κόστος μετακίνησης, ο χρόνος μεταφοράς, να ενισχυθεί η ασφάλεια και να προστατευτεί το περιβάλλον από την περιττή χρήση των καυσίμων. Για το λόγο αυτό στις υπηρεσίες του συστήματος συγκαταλέγεται η παροχή πληροφοριών για το ταξίδι, τη συμφόρηση, τις εκπομπές αερίων ρύπων, τις καθυστερήσεις λόγω ατυχημάτων και πολλά άλλα.

Το γεγονός αυτό καθιστά απαραίτητο τον κατάλληλο και ορθό σχεδιασμό των συστημάτων μεταφορών, ανάλογα με τις απαιτήσεις που υπάρχουν, ανάλογα με τη λειτουργία και τις δυνατότητες των μέσων μαζικής μεταφοράς, ανάλογα με τις έκτακτες απαιτήσεις και ανάγκες που μπορεί να προκύψουν από μια ακραία κατάσταση (σεισμός, τσουνάμι, πλημμύρα). Επομένως, τα Συστήματα Ευφυών Μεταφορών (ITS) συνεισφέρουν στην ανάπτυξη στρατηγικών, οι οποίες αποσκοπούν στη δημιουργία μιας έξυπνης πόλης που θα είναι προετοιμασμένη για κάθε μεταβολή που μπορεί να

συναντήσει ο οδηγός, ο ταξιδιώτης, τα μέσα μαζικής μεταφοράς και όλοι ακόμα οι εμπλεκόμενοι στο σύστημα μεταφοράς [67].

4.2 Κατηγορίες Συστημάτων Ευφυών Μεταφορών

Τα Συστήματα Ευφυών Μεταφορών (ITS), ανάλογα με το σκοπό που επιτελούν μπορούν να κατηγοριοποιηθούν ως ακολούθως:

Α. Προηγμένα συστήματα πληροφόρησης ταξιδιωτών, (Advanced Travelers Information Systems, ATIS).

Τα συστήματα αυτά αντλούν τις πληροφορίες που παρέχονται από τα συστήματα διαχείρισης της κυκλοφορίας, με σκοπό την ενημέρωση των ταξιδιωτών σε πραγματικό χρόνο. Με αυτό τον τρόπο περιορίζεται η συμφόρηση στους δρόμους, η ρύπανση του περιβάλλοντος από τα αυτοκίνητα που είναι σε λειτουργία ενώ περιμένουν σε ουρές στους δρόμους, ενώ επιτυγχάνεται η βελτίωση της κυκλοφορίας. Τα συστήματα πληροφόρησης ταξιδιωτών επιτρέπουν στους ταξιδιώτες να επιλέξουν το μέσο που τους εξυπηρετεί καλύτερα και στους οδηγούς να έχουν εικόνα της βέλτιστης διαδρομής που μπορούν να ακολουθήσουν, προκειμένου να φτάσουν στον προορισμό τους [76].

Η λειτουργία των συστημάτων πληροφόρησης ταξιδιωτών μπορεί να ελέγχεται από σύστημα εντός του οχήματος ή μέσω φορητών συσκευών που έχουν πρόσβαση στο Διαδίκτυο. Ένα σύστημα εντός του οχήματος μπορεί να είναι ένας ψηφιακός χάρτης, ο οποίος να παρέχει πληροφορίες για τη θέση του οχήματος, την κίνηση στους γύρω δρόμους, τη βέλτιστη διαδρομή, ακόμα και ηχητικές οδηγίες πρόσβασης στον προορισμό. Οι φορητές συσκευές μπορούν να παρέχουν υπηρεσίες, όπως πληροφορίες για δρομολόγια των μεταφορικών μέσων, τοποθεσίες, βενζινάδικα, κίνηση στους δρόμους και άλλα.

Β. Προηγμένα συστήματα διαχείρισης κυκλοφορίας (Advanced Traffic Management Systems, ATMS).

Τα συστήματα διαχείρισης κυκλοφορίας αποσκοπούν στη βελτιστοποίηση της κυκλοφοριακής ροής, τη διασφάλιση μεγαλύτερης ασφάλειας για όσους βρίσκονται στο δρόμο και τη μείωση της ρύπανσης που προκαλούν τα οχήματα με κινητήρες εσωτερικής καύσης. Για το λόγο αυτό είναι εξοπλισμένα με συσκευές που ελέγχουν την κυκλοφορία, όπως κάμερες κυκλοφορίας, ανιχνευτές οχημάτων και ραντάρ, αισθητήρες, και άλλα, ώστε να είναι εφικτή η παρακολούθηση της κυκλοφορίας σε πραγματικό χρόνο [76].

Τα προηγμένα συστήματα διαχείρισης της κυκλοφορίας έχουν τη δυνατότητα να μετρήσουν και να καταγράψουν την υπερβολική ταχύτητα, την παραβίαση του κόκκινου σηματοδότη, να καθορίσουν

την κατηγορία του οχήματος και να εξασφαλίσουν τη σωστή χρήση των λωρίδων. Οι δυνατότητες συνεχώς επεκτείνονται, καθώς είναι πλέον δυνατό να λαμβάνονται πληροφορίες σχετικά με τη ροή της κυκλοφορίας, και να δίνονται άμεσα οδηγίες μέσω ψηφιακών μέσων, ώστε οι οδηγοί να αλλάξουν διαδρομής για την αποφυγή κυκλοφοριακής συμφόρησης. Επιπλέον είναι εφικτή η απαγόρευση διέλευσης για συγκεκριμένες κατηγορίες και τύπους οχημάτων σε δρόμους και περιοχές με συγκεκριμένα χαρακτηριστικά και κυκλοφοριακή ροή [77].

Τα συστήματα, τα οποία παρακολουθούν την κυκλοφορίας καταγράφουν τη ροή της κυκλοφορίας σε όλες τις λωρίδες και προς τις δύο κατευθύνσεις, με αισθητήρες IoT και κάμερες. Τα δεδομένα που λαμβάνονται μπορούν να χρησιμεύσουν για επί τόπου επεξεργασία ή συγκεντρώνονται σε μια κεντρική βάση δεδομένων για περεταίρω επεξεργασία, ανάλυση και λήψη αποφάσεων.

Γ. Προηγμένα συστήματα τηλε-διοδίων

Τα Συστήματα Ευφυών Μεταφορών (ITS) παρέχουν προηγμένες και ολοκληρωμένες λύσεις, καθώς μπορούν να συμβάλουν στην είσπραξη διοδίων σε συγκεκριμένους δρόμους ή τμήματα δρόμων, γνωστά ως αστικά διόδια [78]. Με αυτά είναι επίσης δυνατή η τιμολόγηση με κριτήριο την απόσταση που διανύθηκε μέσω συστημάτων τελών. Επιπρόσθετα, τα προηγμένα συστήματα τιμολόγησης σχετίζονται με την περιβαλλοντική προστασία.

Δ. Προηγμένα συστήματα δημοσίων μεταφορών (Advanced Public Transportation Systems, APTS).

Τα συστήματα αυτά κάνουν χρήση ψηφιακών τεχνολογιών, με σκοπό να βελτιωθεί η λειτουργία των μέσων μαζικής μεταφοράς, τα οποία εμφανίζουν υψηλά ποσοστά χρήσης από τους πολίτες, όπως είναι τα τρένα και τα λεωφορεία. Με αυτό τον τρόπο γίνεται εφικτή η ενημέρωση των πολιτών για τα δρομολόγια, το χρονοδιάγραμμα και την πορεία ενός μεταφορικού μέσου, τις πιθανές αλλαγές στα δρομολόγια, το κόστος των δρομολογίων, ακόμα και η τροποποίηση της λειτουργίας των φωτεινών σηματοδοτών, προκειμένου να ομαλοποιηθεί η κυκλοφοριακή ροή [79].

Ε. Προηγμένα συστήματα ελέγχου οχημάτων (Advanced Vehicle Control Systems, AVCS).

Τα συστήματα αυτά λειτουργούν με αισθητήρες, οι οποίοι τοποθετούνται εντός του οχήματος, με σκοπό να ενημερώσουν ή να προειδοποιήσουν τους οδηγούς, κάνοντας χρήσης οπτικοακουστικών μηνυμάτων. Αισθητήρες μπορεί επίσης να τοποθετηθούν στην άκρη των δρόμων, σε φυσικά ή τεχνητά εμπόδια, στα φανάρια, σε κτήρια και άλλα [80].

Επιπλέον, με τα συστήματα ελέγχου του οχήματος, τα οποία έχουν τη δυνατότητα συμμετοχής στην οδήγηση, είναι δυνατή η ενεργοποίηση διαφόρων συστημάτων του οχήματος, όπως το σύστημα

πέδησης, εξασφαλίζοντας με τον τρόπο αυτό μια πιο αποτελεσματική αντίδραση στην εμφάνιση οποιουδήποτε εμποδίου.

4.3 Τεχνολογία Συστημάτων Ευφυών Μεταφορών

Την τελευταία δεκαετία, η τεχνολογία αισθητήρων έχει γίνει πανταχού παρούσα και έχει προσελκύσει μεγάλη προσοχή. Οι αισθητήρες έχουν αναπτυχθεί σε πολλούς τομείς όπως η υγειονομική περίθαλψη η γεωργία, η δασοκομία, η παρακολούθηση οχημάτων και θαλάσσιων μεταφορών. Στις μεταφορές, η τεχνολογία αισθητήρων υποστηρίζει το σχεδιασμό και την ανάπτυξη ενός ευρέος φάσματος εφαρμογών για τον έλεγχο της κυκλοφορίας, την ασφάλεια και την ψυχαγωγία. Τα τελευταία έτη, για παράδειγμα στις Ηνωμένες Πολιτείες Αμερικής οι αισθητήρες και ενεργοποιητές, όπως ο αισθητήρας πίεσης ελαστικών και συστήματα ορατότητας οπισθοπορείας έχουν γίνει υποχρεωτικοί (λόγω ομοσπονδιακών κανονισμών στις Ηνωμένες Πολιτείες), [81], στην κατασκευή οχημάτων και στην εφαρμογή έξυπνων συστημάτων μεταφορών, με στόχο την παροχή υπηρεσιών για την αύξηση της ασφάλειας των οδηγών και την ικανοποίηση των επιβατών, τη βελτίωση της οδικής ασφάλειας γενικότερα και τη μείωση της κυκλοφοριακής συμφόρησης. Άλλοι αισθητήρες είναι προαιρετικά εγκατεστημένοι από τους κατασκευαστές για την παρακολούθηση της απόδοσης και της κατάστασης του οχήματος με στόχο την υψηλότερη απόδοση και την παροχή βοήθειας για τους οδηγούς. Επί του παρόντος, ο μέσος αριθμός αισθητήρων σε ένα όχημα είναι περίπου 60-100, αλλά καθώς τα οχήματα γίνονται πιο έξυπνα, ο αριθμός των αισθητήρων μπορεί να φτάσει έως και 200 αισθητήρες ανά όχημα [81].

Σύμφωνα με τον Fleming, [82], οι αισθητήρες μπορούν να ταξινομηθούν με βάση τη θέση τους στο όχημα σε τρεις κατηγορίες, α) αισθητήρες στο σύστημα μετάδοσης κίνησης, β) αισθητήρες στο πλαίσιο και γ) αισθητήρες στο αμάξωμα. Άλλες ερευνητικές μελέτες ταξινομούν τους αισθητήρες σε ένα όχημα με βάση τον τύπο της εφαρμογής που προορίζεται να υποστηρίξει ο αισθητήρας, οπότε υπάρχουν α) αισθητήρες για την ασφάλεια, β) αισθητήρες για διαγνωστικές λειτουργίες, γ) αισθητήρες για ευκολία και δ)αισθητήρες για παρακολούθηση του περιβάλλοντος [83]. Τις τέσσερις αυτές κατηγορίες αισθητήρων ο Guerrero-Ibáñez, [81], για να συμπεριλάβει δύο πρόσθετες κατηγορίες αισθητήρων, τους αισθητήρες για παρακολούθηση της οδήγησης και τους αισθητήρες για την παρακολούθηση κυκλοφορίας.

Οι λοιπές τεχνολογίες, οι οποίες συμβάλουν στη λειτουργία του Ευφυούς Συστήματος Μεταφοράς είναι:

- Οι δορυφόροι και το σύστημα Galileo

- Το Παγκόσμιο Σύστημα Πλοήγησης (Global Positioning System, GPS), το οποίο αποτελεί ένα παγκόσμιο σύστημα πλοήγησης για την εύρεση θέσης που αποτελείται από δορυφόρους μεγάλης εμβέλειας, καλύπτοντας τις επίγειες, τις θαλάσσιες και τις εναέριες μεταφορές.
- Οι χάρτες πραγματικού χρόνου που βρίσκει κανείς στο Διαδίκτυο, με πιο γνωστό παράδειγμα των χαρτών του Google maps
- Η ασύρματη τεχνολογία Bluetooth, η οποία είναι μια επικοινωνιακή τεχνολογία
- Η τεχνολογία 4G, 5G

και τόσες άλλες υπηρεσίες, οι οποίες μπορούν να συλλέξουν δεδομένα και να τα μεταβιβάσουν τόσο στους χρήστες τους όσο και στους διαχειριστές του Ευφυούς Συστήματος Μεταφορών [84].

4.4 Εφαρμογές Συστημάτων Ευφυών Μεταφορών

Τα Συστήματα Ευφυών Μεταφορών (ITS) βρίσκουν εφαρμογή σε όλες τις δραστηριότητες των πολιτών που περιλαμβάνουν κάθε είδους μετακίνηση. Λαμβάνοντας υπόψη ότι οι περισσότεροι άνθρωποι σήμερα επιλέγουν να εγκατασταθούν στις μεγαλουπόλεις, κρίνεται απαραίτητη η μετατροπή αυτών των πόλεων σε έξυπνες πόλεις, οι οποίες θα σχεδιαστούν στο πλαίσιο της βιωσιμότητας και της διευκόλυνσης της ζωής των πολιτών [67]. Το γεγονός αυτό, σε συνδυασμό με την αύξηση των εκπομπών αερίων ρύπων, αποδεικνύει ότι ο κατάλληλος σχεδιασμός του συστήματος μεταφορών και η διαχείριση της κυκλοφορίας, αναμένεται να δημιουργήσει ένα πιο καθαρό, ασφαλές σύστημα μεταφορών στις περιοχές των μεγάλων πόλεων.

Προϋπόθεση για να αναπτυχθεί το Ευφυές Σύστημα Μεταφορών, είναι να υπάρχει κατάλληλο και αναβαθμισμένο δίκτυο επικοινωνιών. Κάνοντας χρήση αυτού του δικτύου μπορούν να σχεδιαστούν οι στρατηγικές ελέγχου της κυκλοφορίας, ώστε οι υπεύθυνοι του συστήματος να μπορούν να διαχειριστούν διάφορες καταστάσεις, όπως η συμφόρηση της κυκλοφορίας, μια ακραία κατάσταση, να μπορούν να ενημερώνουν τους ταξιδιώτες για τα όρια ταχύτητας, για κάποιο ατύχημα, για την πιο σύντομη διαδρομή [69]. Αξιοσημείωτο είναι ότι τις πληροφορίες αυτές, μπορεί να τις λάβει κάθε πολίτης από το χώρο του σπιτιού του.

Οι ανάγκες των πολιτών που διαρκώς αυξάνονται καθιστούν απαραίτητη την εύρεση λύσεων, μέσα από τις τεχνολογίες των Συστημάτων Ευφυών Μεταφορών (ITS), γεγονός το οποίο αποτελεί τον ευσεβή πόθο της δημόσιας πολιτικής, του δημόσιου σχεδιασμού και της δημόσιας τάξης. Στην Ελλάδα η χρήση των τεχνολογιών Συστημάτων Ευφυών Μεταφορών (ITS) έχει αρχίσει με αργά αλλά σταθερά βήματα να ωριμάζει. Υπάρχουν αξιόλογες εταιρείες, οι οποίες έχουν την επιστημονική τεχνογνωσία για να παρέχουν αξιόπιστες τεχνολογικές λύσεις, οι οποίες αναμένεται σύντομα να εφαρμοστούν με

τον τρόπο, που εφαρμόζονται στις σύγχρονες ευρωπαϊκές πόλεις αρκετών αναπτυγμένων ευρωπαϊκών χωρών [76].

4.5 Η Ψηφιακή Εγκληματολογία στα Συστήματα Ευφυών Μεταφορών

Οι Cebe et al. [85] αναπτύσσουν το «Block4forensic», ένα μοντέλο εγκληματολογικής έρευνας για τη συλλογή δεδομένων από Έξυπνα Οχήματα βασισμένο σε ένα σύστημα blockchain εξουσιοδοτημένης πρόσβασης. Στόχος του μοντέλου είναι η επίλυση νομικών διενέξεων μεταξύ ασφαλιστικών εταιρειών, ιδιοκτητών ή οδηγών και κατασκευαστών καθώς και η αντικειμενική απόδειξη ελλαττωματικού οχήματος στην περίπτωση τροχαίου ατυχήματος. Το μοντέλο διαθέτει ένα ελαφρύ κατακερματισμένο καθολικό (fragmented ledger) για τους συμμετέχοντες στην εγκληματολογική έρευνα, στο οποίο αποθηκεύονται δεδομένα μόλις συμβεί ατύχημα. Για την προστασία του απορρήτου χρησιμοποιείται μία απλοποιημένη υποδομή δημόσιου κλειδιού προσαρμοσμένη σε δίκτυα οχημάτων (vehicular networks). Το προτεινόμενο μοντέλο, καλύπτει ζητήματα επιχειρησιακής ετοιμότητας και διαδικασιών ασφαλείας, έχει ελάχιστες απαιτήσεις σε πόρους αποθήκευσης και επεξεργασίας, διευκολύνει την αξιόπιστη και ιχνηλατήσιμη εξέταση, αλλά δεν βασίζεται σε κάποιο διεθνές πρότυπο ή άλλο εγκεκριμένο πλαίσιο.

Οι Hossain et al.[86] προτείνουν το «Trust-IoV», ένα εγκληματολογικό μοντέλο προσαρμοσμένο στην κατανεμημένη υποδομή του διαδικτύου των οχημάτων (Internet of Vehicles/IoV) το οποίο μπορεί να συλλέγει και να διατηρεί αξιόπιστα πειστήρια, παρέχοντας εγγυήσεις ασφαλούς προέλευσης και ακεραιότητας των αποθηκευμένων τεκμηρίων. Το προτεινόμενο μοντέλο αποτελείται από τα εξής δύο μέρη: 1.Forensics Gateway και 2.IoV-Forensic Service. Το πρώτο συλλέγει πληροφορίες από τις οντότητες του διαδικτύου των οχημάτων, όπως Έξυπνα Οχήματα, οδικές μονάδες (roadside units), έξυπνα τηλέφωνα και νεφοϋπολογιστικές υπηρεσίες και το δεύτερο τα αποθηκεύει. Η εμπιστευτικότητα και η ακεραιότητα των ψηφιακών τεκμηρίων εξασφαλίζεται μέσω ενός module ηλεκτρονικά υπογεγραμμένων πειστηρίων (Electronically Signed Evidence) που παρέχει πρόσβαση στο αποδεικτικό υλικό χρησιμοποιώντας διεπαφές προγραμματισμού εφαρμογών (APIs) μόνο για ανάγνωση. Τα αποτελέσματα της έρευνας δείχνουν ότι το Trust-IoV μπορεί να λειτουργήσει με ελάχιστη υπολογιστική επιβάρυνση.

Οι Feng et.al. [87] αναλύουν τις απειλές που αντιμετωπίζουν τα Έξυπνα Οχήματα στο περιβάλλον της έξυπνης πόλης, διερευνώντας μια ποικιλία κυβερνοεγκλημάτων σε αυτόνομα οχήματα και προτείνουν ένα μοντέλο για την εγκληματολογική εξέταση έξυπνων οχημάτων. Οι συγγραφείς χρησιμοποιούν ένα διαγνωστικό εργαλείο για τη σύνδεση ενός φορητού υπολογιστή με τη διαγνωστική διεπαφή των οχημάτων προκειμένου να αποκτήσουν πρόσβαση στα δεδομένα του

«εγκεφάλου» σε δύο διαφορετικά αυτοκίνητα. Η αποτελεσματικότητα του προτεινόμενου μοντέλου επιβεβαιώνεται από τα αποτελέσματα της έρευνας. Ωστόσο, το μοντέλο χρειάζεται να επαληθευτεί με τη χρήση κυκλοφοριακών δεδομένων που έχουν παραχθεί από Έξυπνα Οχήματα σε ένα πραγματικό σενάριο.

Οι Mansor et al. [88] περιγράφουν την υλοποίηση μίας εφαρμογής για κινητά τηλέφωνα που στοχεύει να δώσει στον οδηγό τον έλεγχο των παραμέτρων που συλλέγονται από τον ηλεκτρονικό καταγραφέα συμβάντων (Event Data Recorder/ EDR) του αυτοκινήτου του. Η εφαρμογή έχει τη δυνατότητα να συνδέεται στο εσωτερικό δίκτυο του αυτοκινήτου, μετά από ταυτοποίηση, και να συλλέγει δεδομένα συμβάντων λειτουργώντας σαν μηχανισμός παραγωγής αντιγράφου ασφαλείας (back up). Τα συλλεγόμενα δεδομένα μπορούν επίσης να αποθηκεύονται και στο υπολογιστικό νέφος. Κατά την εξέταση μιας υπόθεσης ο ερευνητής έχει την εναλλακτική επιλογή να ανακτήσει τα δεδομένα από τον χρήστη, το αυτοκίνητο ή το cloud, γεγονός που του επιτρέπει να διασταυρώσει τη συνέπεια τους, ενώ παράλληλα ο χρήστης γνωρίζει σε ποια δεδομένα έχει πρόσβαση ο ερευνητής.

Σε μια άλλη καινοτόμα προσέγγιση οι Le-Khac et al. [89], εστιάζουν στα ζητήματα ιδιωτικότητας που σχετίζονται με τα έξυπνα και αυτοκινούμενα οχήματα λαμβάνοντας υπόψη την πληθώρα ψηφιακών πληροφοριών που αποθηκεύουν, όπως πρόσφατοι προορισμοί και προτιμώμενες διαδρομές καθώς και προσωπικά δεδομένα (π.χ. λίστες επαφών, μηνύματα SMS, φωτογραφίες, βίντεο). Η εργασία συνοψίζει τις προκλήσεις που συνδέονται με την ψηφιακή εγκληματολογία στον τομέα των έξυπνων οχημάτων και παρουσιάζει μια μελέτη περίπτωσης πάνω στη διαδικασία εξαγωγής και ανάλυσης δεδομένων από ένα σύστημα ψυχαγωγίας σε ένα αυτοκίνητο μάρκας Volkswagen.

Κεφάλαιο 5

Μεθοδολογία

5.1 Σκοπός-ερευνητικά ερωτήματα

Η παρούσα εργασία αποσκοπεί στην ενδελεχή μελέτη του θεσμικού πλαισίου, των προτύπων και οδηγιών που διέπουν τη διεξαγωγή ψηφιακών εγκληματολογικών ερευνών, στη διερεύνηση της διεθνούς βιβλιογραφίας, η οποία αναδεικνύει τις ελλείψεις και αδυναμίες των εφαρμοζόμενων τεχνικών, προτείνοντας πιθανά μέτρα αντιμετώπισής τους, καθώς και στη συγκριτική επισκόπηση των προτεινόμενων λύσεων. Επιπλέον, επιχειρεί να προσδιορίσει, να αξιολογήσει και να συνθέσει τα αποτελέσματα προηγούμενων ερευνών για το θέμα των κριτηρίων, τα οποία χρησιμοποιούν οι ερευνητές ψηφιακής εγκληματολογίας. Σκοπός της συγκριτικής αξιολόγησης είναι να εντοπιστούν τα κριτήρια που θέτουν οι επιλεγμένες έρευνες, τα οποία μπορούν να εφαρμοστούν στη σύγκριση των διαφόρων τεχνολογιών που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας. Η εστίαση είναι πάντα στο Διαδίκτυο των Αντικειμένων (IoT) και στα Συστήματα Ευφυών Μεταφορών (ITS). Απώτερος στόχος της συστηματικής ανασκόπησης είναι να γίνει σύγκριση των κριτηρίων.

Για την επίτευξη του σκοπού της παρούσας μελέτης, με βάση τα παραπάνω, **τα ερευνητικά ερωτήματα** στα οποία θα εστιάσει η έρευνα διατυπώνονται ως ακολούθως:

1. Ποια κριτήρια χρησιμοποιούν οι ερευνητές στις μεθόδους ψηφιακής εγκληματολογίας στο Διαδίκτυο των Αντικειμένων (IoT) και στα Συστήματα Ευφυών Μεταφορών (ITS) (σύγκριση κριτηρίων);

2. Ποιες μέθοδοι προτείνονται για την αξιοποίηση αυτών των κριτηρίων;

3. Ποιο συμπέρασμα προκύπτει από τη σύγκριση των μεθόδων, τις οποίες χρησιμοποιούν οι ερευνητές ψηφιακής εγκληματολογίας, κατά την αξιοποίηση των τιθέμενων κριτηρίων;

Για την ανεύρεση πιθανών κριτηρίων, τα οποία μπορούν να εφαρμοστούν στη σύγκριση των διαφόρων τεχνολογιών που αξιοποιούνται στο πεδίο της ψηφιακής εγκληματολογίας, συγκεντρώθηκαν αρκετές δημοσιεύσεις άρθρων που πραγματεύονται συγκριτικές μελέτες ή κριτικές ανασκοπήσεις (reviews) πρόσφατα προτεινόμενων ψηφιακών εγκληματολογικών μοντέλων και

εντοπίστηκαν τα κριτήρια που χρησιμοποιούν [90], [91]. Διαπιστώθηκε ότι στη συντριπτική τους πλειοψηφία οι συγκριτικές μελέτες υιοθετούν ποιοτικά κριτήρια, όπως:

1. Επίτευξη στόχων ασφαλείας (security analysis), που σχετίζονται με
    - Ασφάλεια
    - Εμπιστευτικότητα
    - Απόρρητο/Ιδιωτικότητα
    - Ταυτοποίηση (authentication)
    - Αξιοπιστία
    - Ακεραιότητα
    - Αυθεντικότητα
    - Νομικώς αποδεκτά πειστήρια/Μη άρνηση
    - Διαθεσιμότητα
    - Ικανότητα επαλήθευσης
    - Διαφάνεια

2. Πλήθος σταδίων της ψηφιακής εγκληματολογικής έρευνας που αντιμετωπίζονται με επιτυχία (προετοιμασία, εξουσιοδότηση, αναγνώριση, συλλογή, διατήρηση, εξέταση, ανάλυση, ανακατασκευή, τεκμηρίωση, επισκόπηση, επικοινωνία, μεταφορά, παρουσίαση), [93], [94], [95].

3. Γενικά κριτήρια, όπως
    - Ευκολία χρήσης
    - Απαιτούμενος χρόνος
    - Αποκέντρωση
    - Διατήρηση ιστορικού
    - Πρόληψη

4. Τα τέσσερα κριτήρια του Daubert Test για την αξιολόγηση των νέων εναλλακτικών μεθόδων (frameworks) ψηφιακής εγκληματολογίας καθώς και των προτεινόμενων τεχνικών και εργαλείων παραγωγής και διατήρησης ψηφιακών πειστηρίων, [96].

Εντούτοις, τα συγκεκριμένα κριτήρια απαιτούν την πειραματική ή εμπειρική απόδειξη των εφαρμοζόμενων επιστημονικών μεθόδων και την εκτίμηση της συχνότητας σφάλματος αυτών (rate of errors), τα οποία είναι εξαιρετικά δύσκολο να επιτευχθούν στην περίπτωση της

ψηφιακής εγκληματολογίας, λόγω έλλειψης τυποποιημένων ομάδων δεδομένων (Standard Data Sets) για τη διεξαγωγή προσομοιώσεων και της πολυπλοκότητας που υπεισέρχεται στην εκτίμηση του σφάλματος [97-98].

Σε μικρότερο αριθμό ερευνών έχουν διεξαχθεί προσομοιώσεις των προτεινόμενων μοντέλων και παρουσιαστεί πειραματικά αποτελέσματα για την αξιολόγηση της απόδοσής τους. Στις περιπτώσεις αυτές έχουν χρησιμοποιηθεί ποσοτικά κριτήρια για την εξαγωγή σχετικών συμπερασμάτων όπως ο χρόνος επεξεργασίας, η κατανομή υπολογιστικών πόρων, η κατανάλωση ενέργειας και το λειτουργικό κόστος.

5.2 Μέθοδος

Προκειμένου να συνοψιστούν και να συγκριθούν τα κριτήρια, τα οποία χρησιμοποιούν οι ερευνητές στο πεδίο της ψηφιακής εγκληματολογίας, είναι απαραίτητη η σύνθεση των αποτελεσμάτων, τα οποία προέρχονται από τις έρευνες που έχουν μέχρι τώρα πραγματοποιηθεί [85], [87]. Για την εκπλήρωση του ερευνητικού σκοπού διεξήχθη συστηματική βιβλιογραφική ανασκόπηση και χρησιμοποιήθηκε η μέθοδος PRISMA [99].

- Αρχικά αναζητήθηκαν τα άρθρα με συγκεκριμένες λέξεις κλειδιά και με βάση τα κριτήρια επιλογής και αποκλεισμού που τέθηκαν, στις εξής βάσεις δεδομένων: Google Scholar, Semantic Scholar, Springer Link και Science Direct (ELSEVIER).

- Οι λέξεις κλειδιά, οι οποίες χρησιμοποιήθηκαν, είναι: digital forensics, digital forensics framework, Internet of Things, IoT, Intelligent Transport Systems, ITS, Principles of Digital Forensics. Δεδομένου του γεγονότος ότι τα αρχικά αποτελέσματα συμπεριλάμβαναν γενικά άρθρα, χρησιμοποιήθηκαν οι δυαδικοί τελεστές (Boolean operators) “OR”, “AND”, “NOT”, προκειμένου να επιτευχθούν όλοι οι συνδυασμοί των παραπάνω λέξεων κλειδιών, καθώς και άλλων λέξεων, ώστε να συμπεριληφθούν στα αποτελέσματα τα πιο συναφή με τα ερευνητικά ερωτήματα άρθρα.

- Για την αναζήτηση των άρθρων εφαρμόστηκαν όλα τα όρια που σχετίζονται με την αναζήτηση των άρθρων όπως χρονιά (2017-2022) και γλώσσα (Αγγλικά). Επιλέχθηκε μόνο η Αγγλική Γλώσσα γιατί οι δημοσιεύσεις στις εν λόγω βάσεις δεδομένων είναι στα Αγγλικά είτε σε άλλη ευρωπαϊκή γλώσσα. Συνεπώς, και οι Έλληνες συγγραφείς, οι οποίοι μπορεί να έχουν κάνει σχετική δημοσίευση, αυτή θα είχε μεταφραστεί στα Αγγλικά για να δημοσιευτεί σε κάποια από αυτές τις βάσεις δεδομένων.

- Η ταξινόμηση των άρθρων έγινε με βάση τη συνάφεια του θέματος του τίτλου και στη συνέχεια σε σχέση με τη χρονολογία δημοσίευσης. Επισημαίνεται ότι ένα μεγάλο πλήθος εγγραφών ήταν συστηματικές ανασκοπήσεις και μετα-αναλύσεις, οι οποίες και αποκλείστηκαν από τα επιλεγέντα άρθρα.

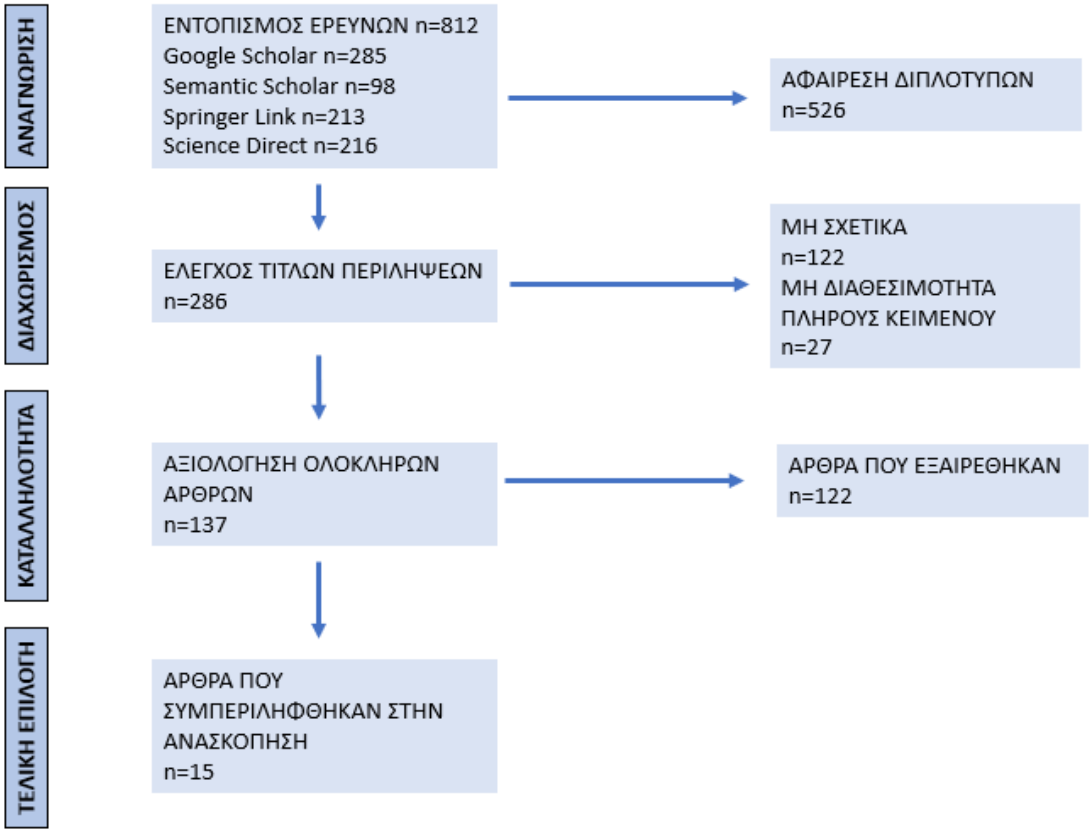
- Από την αναζήτηση προέκυψε ένας τελικός αριθμός εγγραφών (άρθρων) για κάθε βάση δεδομένων. Ο τελικός αριθμός εγγραφών περιλαμβάνει τον συνολικό αριθμό συνδυασμένων αποτελεσμάτων από όλες τις βάσεις δεδομένων (συμπεριλαμβανομένων των διπλότυπων). Τα συνολικά άρθρα και στις τρεις βάσεις δεδομένων ήταν n=812.

- Αποκλείστηκαν οι διπλές εγγραφές (άρθρα που υπάρχουν και στις τέσσερις βάσεις δεδομένων). Για να αποκλειστούν οι διπλές εγγραφές αναζητήθηκαν τα ονόματα συγγραφέων ανάμεσα στις λίστες των άρθρων και των τεσσάρων βάσεων δεδομένων, και πραγματοποιήθηκε σύγκριση όλων των αποτελεσμάτων. Τα διπλότυπα άρθρα, τα οποία εξαιρέθηκαν ήταν 526, οπότε οι μη διπλότυπες εγγραφές, οι οποίες παρέμειναν ήταν n=286.

- Στη συνέχεια στα άρθρα που επιλέχθηκαν πραγματοποιήθηκε έλεγχος με βάση τον τίτλο και την περίληψη, οπότε εξαιρέθηκαν 122 άρθρα, τα οποία ήταν εκτός των ερευνητικών ερωτημάτων της εργασίας. Συγχρόνως αποκλείστηκαν τα άρθρα, για τα οποία δεν υπάρχει πρόσβαση στο πλήρες κείμενο, οπότε εξαιρέθηκαν 27 άρθρα.

- Ακολούθως, στα 137 άρθρα πραγματοποιήθηκε πλήρης ανάγνωση. Τα άρθρα αυτά, τα οποία διαβάστηκαν και αξιολογήθηκαν για την καταλληλόλητά τους ως προς την σχέση τους με τα ερευνητικά ερωτήματα της έρευνας. Αφού ελέγχθηκαν όλα τα άρθρα στο στάδιο ελέγχου πλήρους κειμένου για καταλληλόλητα κάποια άρθρα αποκλείστηκαν λαμβάνοντας υπόψιν τα κριτήρια αποκλεισμού της έρευνας. Τα άρθρα που αποκλείστηκαν ήταν 122, οπότε τα άρθρα που συμμετείχαν στην βιβλιογραφική ανασκόπηση ήταν 15.

Μετά την ολοκλήρωση της παραπάνω διαδικασίας δημιουργήθηκε το διάγραμμα PRISMA.



Εικόνα 2-Διάγραμμα PRISMA

5.3 Κριτήρια επιλογής/αποκλεισμού άρθρων

Κριτήρια επιλογής άρθρων

Τα κριτήρια επιλογής των άρθρων που μελετήθηκαν για τη συστηματική βιβλιογραφική ανασκόπηση σχετικά με τις τεχνικές ψηφιακής εγκληματολογίας και τα κριτήρια, τα οποία χρησιμοποιούν οι ερευνητές είναι:

- Τα άρθρα, τα οποία επιλέχθηκαν για τη διεξαγωγή της έρευνας έπρεπε να είναι στην Αγγλική Γλώσσα.
- Επιλέχθηκαν άρθρα τα οποία είχαν δημοσιευτεί μεταξύ 2017-2022.
- Επιλέχθηκαν άρθρα, τα οποία αφορούσαν την Ψηφιακή Εγκληματολογία στο Διαδίκτυο των Αντικειμένων (IoT) και τα Συστήματα Ευφυών Μεταφορών (ITS).
- Τα επιλεχθέντα άρθρα έπρεπε να έχουν δημοσιευθεί σε παγκοσμίως αναγνωρισμένα επιστημονικά περιοδικά.
- Οι μελέτες έπρεπε να προτείνουν ένα μοντέλο Ψηφιακής Εγκληματολογίας

Κριτήρια αποκλεισμού άρθρων

Τα κριτήρια αποκλεισμού των άρθρων είναι:

- Αποκλείστηκαν οι ανασκοπήσεις, συμπεριλαμβανομένων των συστηματικών βιβλιογραφικών ανασκοπήσεων και οι μετα-αναλύσεις.
- Αποκλείστηκαν άρθρα, τα οποία βρέθηκε ότι αποτελούσαν βιβλιογραφική αναφορά σε πιο πρόσφατα άρθρα, με το ίδιο θέμα.
- Αποκλείστηκαν μελέτες, οι οποίες δεν είχαν κάποιο αποτέλεσμα ή κάποιο εύρημα που να δικαιολογεί την επιλογή τους.

5.4 Περιορισμοί

Στις περισσότερες εκ των περιπτώσεων, τα άρθρα που εντοπίζονται από τη συστηματική βιβλιογραφική ανασκόπηση, οδηγούν σε μελέτες με θετικά ευρήματα ή σε μελέτες που στο συμπέρασμά τους αποτυπώνουν την άποψη του συγγραφέα. Επομένως, οι μελέτες που οδηγούν σε θετικά ευρήματα είναι πιθανότερο να εμφανιστούν με τη συστηματική ανασκόπηση.

Επιπλέον, θα πρέπει να ληφθεί υπόψη η ετερογένεια των μελετών, η οποία οφείλεται και στην πληθώρα θεμάτων σχετιζόμενων με το Διαδίκτυο των Αντικειμένων (IoT) και τα Συστήματα Ευφυών Μεταφορών (ITS). Για να συγκριθούν οι μελέτες θα πρέπει να έχουν παρόμοιες μεθόδους, και να χρησιμοποιούν τεχνολογίες. Στην πραγματικότητα, ο συνδυασμός όλων αυτών των επιθυμητών χαρακτηριστικών των μελετών είναι ανύπαρκτος, δεδομένου του τρόπου διεξαγωγής των ερευνών και των πολυάριθμων επιστημονικών εργαλείων.

Τέλος, ένα άλλο πρόβλημα, το οποίο προκύπτει κατά την αναζήτηση των μελετών είναι ότι αρκετές φορές δεν είναι εφικτή η πρόσβαση στα άρθρα των μελετών, με αποτέλεσμα αυτές να αποκλείονται από την έρευνα.

Κεφάλαιο 6

Αποτελέσματα συστηματικής αποτίμησης

6.1 Πίνακας αποτελεσμάτων

Στην παρούσα βιβλιογραφική ανασκόπηση περιλαμβάνονται 15 έρευνες εκ των οποίων 12 έχουν πεδίο εφαρμογής το Διαδίκτυο των Αντικειμένων (IoT) και 3 τα Συστήματα Ευφυών Μεταφορών (ITS).

Στον Πίνακα 2 παρατίθενται τα 15 άρθρα τα οποία ελέγχθηκαν για τη συνάφειά τους με το θέμα της μελέτης και επιλέχθηκαν να συμπεριληφθούν στη συστηματική βιβλιογραφική ανασκόπηση. Τα άρθρα έχουν καταχωρηθεί ανά γραμμή του πίνακα και κατά αλφαβητική σειρά με κριτήριο το επώνυμο του συγγραφέα/ων. Επομένως, η πρώτη στήλη περιλαμβάνει τον πρώτο συγγραφέα του άρθρου και τη χρονολογία δημοσίευσης, η δεύτερη στήλη περιλαμβάνει τη χώρα προέλευσης του άρθρου, η τρίτη στήλη το σκοπό, η τέταρτη στήλη το πεδίο εφαρμογής, η πέμπτη στήλη το μοντέλο ψηφιακής εγκληματολογίας, η έκτη στήλη την τεχνολογία που χρησιμοποιήθηκε, η έβδομη στήλη τα κριτήρια και η τελευταία και όγδοη στήλη το αποτέλεσμα της έρευνας.

Πίνακας 2-ΑΡΘΡΑ ΒΙΒΛΙΟΓΡΑΦΙΚΗΣ ΑΝΑΣΚΟΠΗΣΗΣ

ΑΡΘΡΑ ΒΙΒΛΙΟΓΡΑΦΙΚΗΣ ΑΝΑΣΚΟΠΗΣΗΣ							
Συγγραφέας/ Χρονολογία	**Χώρα**	**Σκοπός**	**Πεδίο εφαρμογής**	**Μοντέλο Ψηφιακής Εγκληματολογίας**	**Τεχνολογία/ Εργαλείο**	**Κριτήρια**	**Αποτέλεσμα**
Agbedanu et al, 2021	Ιρλανδία	Διατήρηση των κατακερματισμένων τιμών των αρχείων καταγραφής που παράγονται στο IoT περιβάλλον ως αρχεία συναλλαγών	IoT	BLOF (Blockchain-based Forensic model for IoT)	Blockchain	Ικανότητα Επαλήθευσης Αποκέντρωση Ακεραιότητα Απόρρητο/Ιδιωτικότητα Αυθεντικότητα	Το BLOF συμβάλει στην επαλήθευση της αυθεντικότητας των αρχείων καταγραφής
Akhtar et al, 2022	Κίνα	Διασφάλιση της ασφάλειας και της ακεραιότητας των αποδεικτικών στοιχείων, αλλά και πρόληψη των απειλών	IoT	Blockchain and Hashing Algorithms	Blockchain XGBoost algorithm	Ακεραιότητα Ασφάλεια Πρόληψη	Το προτεινόμενο μοντέλο είναι αποτελεσματικό, καθώς ανιχνεύει και προβλέπει επιθέσεις σε πρώιμο στάδιο
Ali et al, 2022	Αίγυπτος	Διερεύνηση των αλγορίθμων κατακερματισμού της τεχνολογίας blockchain, για τη διατήρηση της ακεραιότητας των ψηφιακών στοιχείων (εικόνων)	IoT	Tracing Chain of Custody in Digital Image (Blockchain)	MRSH-v2 (Grey Hash), Blockchain Approximate Matching Peer to Peer (P2P)	Ακεραιότητα Αξιοπιστία	Η προτεινόμενη τεχνολογία συμβάλει στη διατήρηση της ακεραιότητας των αποδεικτικών στοιχείων και της αξιοπιστίας τους.
Cebe et al, 2018	ΗΠΑ	Διασφάλιση ιδιωτικότητας Με την εισαγωγή ενός πλαισίου διερεύνησης ιατροδικαστικών οχημάτων που	ITS	Block4Forensic	Blockchain Event data recorder (EDR)	Απόρρητο/Ιδιωτικότητα Ακεραιότητα Νομικώς αποδεκτά πειστήρια/Μη άρνηση	Το προτεινόμενο ιατροδικαστικό πλαίσιο επιτρέπει Αξιόπιστη ανάλυση, με ελάχιστο κόστος αποθήκευσης και επεξεργασίας.

		περιέχει όλα τα απαραίτητα δεδομένα για μια ολοκληρωμένη ιατροδικαστική έρευνα				Διατήρηση ιστορικού Αξιοπιστία Ανίχνευση Ολοκληρωμένη Εγκληματολογική Ανάλυση	
Feng et al, 2017	Ηνωμένο Βασίλειο	Διερεύνηση και ανάλυση απειλών σε έξυπνα Αυτόνομα Αυτοματοποιημένα Οχήματα	ITS AAV (Autonomous Automated Vehicle)	Integrated Digital Investigation Process model served for Smart City Automated Vehicles	CarScanner OBD (OnBoard Diagnostics) Auto Doctor diagnostic tools ICT (Information Communications Technology) Laboratory experiment example	Απόρρητο/Ιδιωτικότητα Ασφάλεια Ακεραιότητα Αξιοπιστία Διαφάνεια	Το νέο μοντέλο προβλέπει επιθέσεις τόσο από το φυσικό περιβάλλον, όσο και από τον κυβερνοχώρο. Η έρευνα έδειξε ότι τα αποδεικτικά στοιχεία από τα οχήματα μπορούν να εξαχθούν, να αποθηκευτούν και να παρουσιαστούν
Hossain et al, 2018	ΗΠΑ	Συλλογή αποδεικτικών στοιχείων και αποθήκευση αποδεικτικών στοιχείων με αξιόπιστο τρόπο	IoT	FIF (Forensic Investigation Framework)	Blockchain Public digital ledger	Διαθεσιμότητα αποδείξεων Ακεραιότητα Εμπιστευτικότητα Απόρρητο/Ιδιωτικότητα Νομικώς αποδεκτά πειστήρια/Μη άρνηση	Το FIF-IoT παρέχει ένα μηχανισμό απόκτησης αποδεικτικών στοιχείων από το καθολικό και διασφαλίζει την επαλήθευση και την ακεραιότητα των αποδεικτικών στοιχείων που αποκτήθηκαν
Kebande et al, 2018	Νότια Αφρική	Προτείνεται ένα ολοκληρωμένο, μη αμφισβητήσιμο πλαίσιο	IoT	IDFIF-IoT	Συνολικά 9 διαδικασίες Things (1), Device	Ασφάλεια Πρόληψη Απόρρητο/Ιδιωτικότητα	Το ολοκληρωμένο ψηφιακό πλαίσιο εγκληματολογικής έρευνας συμβάλει στην εκ των προτέρων ανίχνευση και αντιμετώπιση περιστατικών ασφαλείας στον κυβερνοχώρο

		εγκληματολογικών τεχνικών για την ανάλυση Δυναμικών Ψηφιακών Στοιχείων (PDE) από το οικοσύστημα που βασίζεται στο IoT			Connectivity and Communicating Networks (2), Readiness Process Groups (3), IoT Forensics (4), Digital Forensic Investigation (5), Concurrent Processes (6), IoT Management Platforms (7), IoT Policy (8) and IoT Standards and Protocols (9).	Συνδεσιμότητα αντικειμένων	
Le et al, 2018	Δημοκρατία Σιγκαπούρης	Προτείνεται ένα εξουσιοδοτημένο πλαίσιο εγκληματολογίας IoT που βασίζεται στην τεχνολογία blockchain για τη βελτίωση των κριτηρίων της ακεραιότητας,	IoT	BIFF (Blockchain-based IoT Forensics Framework)	Blockchain Merkle signature scheme	Αποκέντρωση Ακεραιότητα Απόρρητο/Ιδιωτικότητα Ασφάλεια Νομικώς αποδεκτά πειστήρια/Μη άρνηση	Το προτεινόμενο μοντέλο διασφαλίζει την ακεραιότητα των αποδεικτικών στοιχείων και την αποδοχή τους για νόμιμη χρήση

		αυθεντικότητας και μη άρνησης για τον τρόπο που συλλέχθηκαν τα αποδεικτικά στοιχεία.					
Musa et al, 2022	Ηνωμένο Βασίλειο	Προτείνεται α) μια μεθοδολογία ζωντανής παρακολούθησης για δίκτυα P2P και β) τυποποίηση του μοντέλου ADDIE ως επίσημο ψηφιακό ιατροδικαστικό μοντέλο	IoT	ADDIE Model	P2P network investigation United States Daubert Test FSR-G-218 FSR-G-201 SHA256	Ακρίβεια Ασφάλεια Ακεραιότητα Επαλήθευση Διατήρηση αλυσίδας φύλαξης	Το μοντέλο ADDIE, με την παρούσα προσέγγιση μπορεί να χρησιμοποιηθεί ως επίσημο ψηφιακό ιατροδικαστικό μοντέλο
Nieto et al, 2018	Ισπανία	Εφαρμόζεται η μεθοδολογία PROFIT για την προσέγγιση του ψηφιακού μάρτυρα με μια μεθοδολογία που επιτρέπει στους πολίτες να μοιράζονται τα δεδομένα τους με ορισμένες εγγυήσεις απορρήτου	IoT	PRoFIT	PRoFIT Privacy Manager (PPM) OMUD module	Ακεραιότητα Απόρρητο/Ιδιωτικότητα Διατήρηση αλυσίδας φύλαξης Τεκμηρίωση Ακρίβεια Διαφάνεια Νομικώς αποδεκτά πειστήρια/Μη άρνηση	Το προτεινόμενο μοντέλο παρέχει μια ισορροπία μεταξύ της ιδιωτικής ζωής και των αρχών της ψηφιακής εγκληματολογίας
Qatawneh et al, 2019	Ιορδανία	Προτείνεται ένα μοντέλο ψηφιακής εγκληματολογίας για τη διασφάλιση όλων των αρχών και κριτηρίων της συλλογής και επεξεργασίας των	IoT	DFIM	Data Provider Zone (DPZ) Ανάλυση 7 σημείων	Ασφάλεια, Απόρρητο/Ιδιωτικότητα Ακρίβεια, Απόδοση, Αυθεντικοποίηση Μείωση δεδομένων,	Το μοντέλο DFIM ικανοποιεί όλα τα κριτήρια εφαρμογής του ως ψηφιακό ιατροδικαστικό εργαλείο, καθώς εξασφαλίζει την τήρηση όλων των απαραίτητων αρχών.

		ψηφιακών δεδομένων				Νομικώς αποδεκτά πειστήρια/Μη άρνηση Διαφάνεια	
Sadineni et al, 2019	ΗΠΑ	Προτείνεται μια ολιστική προσέγγιση που δίνει έμφαση στην εγκληματολογική ετοιμότητα που μπορεί να εφαρμοστεί σε οποιονδήποτε τομέα του Διαδικτύου των πραγμάτων.	IoT	Holistic Forensic Model	Machine learning techniques fog/edge computing blockchain	Ασφάλεια Ακεραιότητα	Το μοντέλο, είναι προσαρμόσιμο και με δυνατότητα διαμόρφωσης ενώ υποστηρίζει διάφορες εφαρμογές IoT
Sathwara et al, 2018	Ρουμανία	Το προτεινόμενο πλαίσιο αναμένεται να συμβάλει στη συλλογή των αποδεικτικών στοιχείων, στον εντοπισμό του επιτιθέμενου και των προβλημάτων που δημιουργήθηκαν	IoT	Ecosystem for IoT forensic	Fingerprint collection SLA Inspection Log analysis Cache and memory analysis	Ασφάλεια Συνάφεια Ακεραιότητα Διατήρηση δεδομένων Νομικώς αποδεκτά πειστήρια/Μη άρνηση/Ακρίβεια Επίκαιρα στοιχεία	Το εγκληματολογικό οικοσύστημα βοηθά τους ερευνητές στη συλλογή και επεξεργασία πληροφοριών
Servida et al, 2019	Ελβετία	Μελέτη συσκευών IoT και σχετικών εφαρμογών smartphone, εξαγωγή και ανάλυση ψηφιακών ήχων, ανακάλυψη τρωτών σημείων σε πολλές συσκευές	IoT	DFRWS	Smartphone Application Analysis Open source forensic tools	Αξιοπιστία Απόρρητο/Ιδιωτικότητα Ασφάλεια Τρωτότητα Νομικώς αποδεκτά πειστήρια/Μη άρνηση	Εκτός από τα smartphones αποδεικτικά στοιχεία μπορούν να βρεθούν και στις συσκευές IoT. Η ανάλυση αυτών με τα κατάλληλα εργαλεία περιορίζει την τρωτότητά τους

Yoon et al, 2019	Κορέα	Προτείνεται ένα πλαίσιο διερεύνησης τροχαίων ατυχημάτων που αξιοποιεί τα ψηφιακά δεδομένα που δημιουργούνται από αισθητήρες και συσκευές που είναι εγκατεστημένοι σε ένα όχημα ακόμη και όταν το όχημα δεν έχει εγγραφή βίντεο ή εγγραφή οδήγησης	ITS	DID (Decentralized Identity)	Blockchain	Αξιοπιστία Ακεραιότητα Ασφάλεια	Το μοντέλο που προτείνεται εξασφαλίζει την ακεραιότητα της ψηφιακής ανάλυσης, ακόμα και όταν το όχημα δε διαθέτει κάποιο είδος εγγραφής

6.2 Κριτήρια μεθόδων ψηφιακής εγκληματολογίας

Στον Πίνακα 3 παρουσιάζονται τα κριτήρια, τα οποία χρησιμοποιούν οι ερευνητές στις μεθόδους ψηφιακής εγκληματολογίας στο Διαδίκτυο των Αντικειμένων (IoT) και στα Συστήματα Ευφυών Μεταφορών (ITS). Επισημαίνεται ότι έχουν καταχωρηθεί τα οκτώ (8) κριτήρια, που εμφανίζουν μεγαλύτερη συχνότητα στις υπό μελέτη έρευνες και έχουν κατανεμηθεί στον πίνακα κατά αύξουσα σειρά εμφάνισης στο σύνολο των δεκαπέντε άρθρων της βιβλιογραφικής ανασκόπησης:

Πίνακας 3-ΚΡΙΤΗΡΙΑ ΜΕΘΟΔΩΝ ΨΗΦΙΑΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ

ΚΡΙΤΗΡΙΑ	**ΠΛΗΘΟΣ ΕΡΕΥΝΩΝ**	**ΤΕΧΝΟΛΟΓΙΑ BLOCKCHAIN**
ΑΚΕΡΑΙΟΤΗΤΑ	12	9
ΑΣΦΑΛΕΙΑ	10	6
ΑΠΟΡΡΗΤΟ/ΙΔΙΩΤΙΚΟΤΗΤΑ	9	5
ΝΟΜΙΚΩΣ ΑΠΟΔΕΚΤΑ/ΜΗ ΑΡΝΗΣΗ	7	4
ΑΞΙΟΠΙΣΤΙΑ	5	4
ΔΙΑΤΗΡΗΣΗ	4	2
ΔΙΑΦΑΝΕΙΑ	3	1
ΑΚΡΙΒΕΙΑ	3	1

Σχεδόν όλες οι μελέτες που συμπεριλήφθηκαν στην παρούσα βιβλιογραφική ανασκόπηση έκριναν ως ιδιάζουσας σημασίας το κριτήριο της ακεραιότητας, το οποίο ξεκάθαρα μνημονεύουν οι δώδεκα από τις δεκαπέντε συμπεριληφθείσες έρευνες [9], [85], [86], [87], [100], [101], [102], [103], [104], [105], [106], [107]. Η ακεραιότητα των δεδομένων, είναι μια πολύ σημαντική παράμετρος, όταν ο ερευνητής συλλέγει τα πειστήρια, δεδομένου ότι όταν τα αποδεικτικά στοιχεία θεωρηθεί πως μπορεί να έχουν αλλοιωθεί ή μεταβληθεί, τότε εγκυμονεί ο κίνδυνος της μη αποδοχής τους στο δικαστήριο. Συνεπώς, τα προτεινόμενα μοντέλα ψηφιακής εγκληματολογίας παρέχουν τη δυνατότητα εξασφάλισης της ακεραιότητας των αποδεικτικών στοιχείων, προκειμένου να γίνουν αποδεκτά. Επιπλέον, τεχνολογίες όπως η Blockchain, ιδιαίτερα όταν συνδυάζονται με αλγορίθμους Hash, είναι δυνατό να παρέχουν εγγυήσεις για τη διασφάλιση της ακεραιότητας των αποδεικτικών στοιχείων.

Η ασφάλεια κατά την έρευνα στην ψηφιακή εγκληματολογία αποτελεί ένα επίσης σημαντικό κριτήριο, γεγονός που αποκαλύπτεται από τη συχνότητα, με την οποία εντοπίζεται το κριτήριο αυτό στις μελέτες που εξετάστηκαν. Οι δέκα από τις δεκαπέντε μελέτες εντοπίζουν το κριτήριο της ασφάλειας ως αναπόσπαστο κομμάτι της έρευνας και επισημαίνουν την ανάγκη για την ασφάλεια των δεδομένων από αλλαγές και αμφισβητήσεις [87], [101], [102], [103], [105], [106], [107], [108], [109], [110]. Η ανάγκη για ασφάλεια και προστασία των δεδομένων που παρέχουν οι υπηρεσίες Cloud, θεωρείται ότι έχει ικανοποιηθεί, δεδομένων των αναβαθμίσεων που έχουν κάνει αυτές οι υπηρεσίες για να επιβιώσουν από τον ανταγωνισμό. Τα μοντέλα ψηφιακής εγκληματολογίας εστιάζουν στη χρήση αυτών των αναβαθμισμένων υπηρεσιών, κάνοντας χρήση της τεχνολογίας Blockchain.

Επιπρόσθετα, η συλλογή των αποδεικτικών στοιχείων θα πρέπει να διενεργείται διαφυλάσσοντας την ιδιωτικότητα του ατόμου. Οι εννέα εκ των δεκαπέντε ερευνών τονίζουν τη σπουδαιότητα της διασφάλισης του απορρήτου και της ιδιωτικότητας των διερευνώμενων ατόμων, προκειμένου να μην απορριφθούν τα αποδεικτικά πειστήρια, κατά τη διάρκεια της ιατροδικαστικής διαδικασίας [85], [86], [87], [100], [102], [104], [108], [109], [110]. Τα προτεινόμενα μοντέλα καθορίζουν το βαθμό, στον οποίο μπορεί να προχωρήσει η έρευνα εις βάθος, και το σημείο εκείνο στο οποίο ο ερευνητής οφείλει να σταματήσει προκειμένου να μη διακινδυνεύσει τη μη αποδοχή των πειστηρίων από το δικαστήριο.

Η αποδοχή των αποδεικτικών στοιχείων στο δικαστήριο προϋποθέτει ότι αυτά πληρούν συγκεκριμένες προϋποθέσεις. Μια από αυτές είναι να είναι τα πειστήρια νομικώς αποδεκτά, δηλαδή, να μη μπορεί κανείς να αμφισβητήσει τη νομιμότητά τους, ώστε να μη γίνουν αποδεκτά για την έρευνα. Τα αποδεικτικά στοιχεία για να γίνουν αποδεκτά θα πρέπει να έχουν ληφθεί με τρόπο επιστημονικό, ο οποίος να έχει εκ των προτέρων γίνει αποδεκτός και να έχει προηγηθεί της συλλογής τους κάποια μορφή εξουσιοδότησης ή εντάλματος. Από τις δεκαπέντε έρευνες που συμπεριλαμβάνονται στην παρούσα βιβλιογραφική ανασκόπηση, οι επτά επισημαίνουν τη σπουδαιότητα αυτού του κριτηρίου και για αυτό το εντάσσουν σε αυτά, τα οποία πληροί το μοντέλο που προτείνουν [85], [86], [102], [104], [105], [106], [109], [110]. Ανεξαρτήτως μοντέλου και τεχνολογίας ψηφιακής εγκληματολογίας, το να είναι τα αποδεικτικά στοιχεία νομικώς αποδεκτά, διαδραματίζει σημαντικό ρόλο στην εξελικτική πορεία της έρευνας. Επιπρόσθετα, τα μοντέλα που βασίζονται στην τεχνολογία Blockchain, θεωρείται ότι πληρούν αυτό το κριτήριο, καθώς διασφαλίζουν ορισμένα άλλα κριτήρια, τα οποία προ απαιτούνται, όπως η ακεραιότητα, η αξιοπιστία, η διαφάνεια και άλλα.

Η αξιοπιστία των αποδεικτικών στοιχείων μαζί με τη διατήρησή τους στην αλυσίδα φύλαξης, θεωρούνται από πέντε και τέσσερις ερευνητές αντίστοιχα, ως εξίσου σημαντικά κριτήρια με τα

προαναφερθέντα. Για να είναι αξιόπιστα τα πειστήρια θα πρέπει να έχουν βρεθεί με νόμιμο και αποδεκτό τρόπο [9], [85], [87], [107] , [110]. Η αξιοπιστία βοηθά τον ερευνητή να βασιστεί στα πειστήρια για να στηρίξει το συμπέρασμά του για την έρευνα ή για να κοινοποιήσει κάποια υπόθεσή του, χωρίς να κινδυνεύει να θεωρηθεί ότι ενεργεί αντίθετα με το νόμο. Αναφορικά με τη διατήρηση των αποδεικτικών στοιχείων, οι ερευνητές τονίζουν τη σημασία της κατά την κατασκευή των μοντέλων, εφόσον η απώλεια των πειστηρίων ή η αλλοίωσή τους, ή η μεταβολή τους, μπορεί να οδηγήσει σε άλλα συμπεράσματα από αυτά που έχει αποκομίσει ο ερευνητής [85],[103], [104], [106].

Τέλος, τρεις εκ των μελετών που παρουσιάστηκαν σε αυτή την έρευνα, αναφέρουν ότι τα μοντέλα ψηφιακής εγκληματολογίας που προτείνουν πληρούν το κριτήριο της διαφάνειας [87], [104], [109] και άλλες τρεις το κριτήριο της ακρίβειας των αποδεικτικών στοιχείων [103], [104] [109].

Όπως γίνεται αντιληπτό, όλα τα παραπάνω κριτήρια, άλλα και πολλά ακόμα, τα οποία αναφέρουν οι ερευνητές, αποτελούν όχι μόνο την προϋπόθεση για να εξάγει ο ερευνητής τα συμπεράσματά του, αλλά είναι εξίσου σημαντικά προκειμένου να υποστηρίξει ο ερευνητής ψηφιακής εγκληματολογίας τη θέση του ενώπιον του ακροατηρίου στο δικαστήριο. Επομένως, η χρήση νέων τεχνολογιών και αλγορίθμων, αλλά και ο συνδυασμός διαφόρων διαδικασιών και πρωτοκόλλων για τη διερεύνηση ενός ψηφιακού εγκλήματος, είναι εξέχουσας σημασίας.

6.3 Μέθοδοι ψηφιακής εγκληματολογίας

Στην παρούσα βιβλιογραφική ανασκόπηση περιλαμβάνονται 15 έρευνες εκ των οποίων οι περισσότερες, προτείνουν ένα μοντέλο ψηφιακής εγκληματολογίας που βασίζεται στην τεχνολογία Blockchain. Συνοπτικά οι μέθοδοι που χρησιμοποιήθηκαν παρατίθενται στον Πίνακα 3:

Πίνακας 4-ΜΕΘΟΔΟΙ ΨΗΦΙΑΚΗΣ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑΣ

ΜΕΘΟΔΟΣ/ΤΕΧΝΟΛΟΓΙΑ	**ΒΑΣΙΚΑ ΚΡΙΤΗΡΙΑ**	**ΠΛΗΘΟΣ ΕΡΕΥΝΩΝ**
BLOCKCHAIN (συνολικά)	Ακεραιότητα Ασφάλεια Απόρρητο/Ιδιωτικότητα Νομικώς Αποδεκτά/Μη Άρνηση Αξιοπιστία	12
Συνδυασμός BLOCKCHAIN και Αλγορίθμων Hash	Ακεραιότητα Ασφάλεια Αξιοπιστία	4
Μοντέλα με Πολυάριθμες Διαδικασίες	Ασφάλεια Απόρρητο/Ιδιωτικότητα	3
Μοντέλα με ψηφιακά μέσα (π.χ. εικόνες, αισθητήρες)	Απόρρητο/Ιδιωτικότητα Ακεραιότητα Νομικώς αποδεκτά πειστήρια/ Μη Άρνηση Αξιοπιστία	2

Από τον Πίνακα 4 διαπιστώνεται ότι η τεχνολογία, η οποία χρησιμοποιείται με μεγαλύτερη συχνότητα από τους ερευνητές ψηφιακής εγκληματολογίας είναι η τεχνολογία Blockchain, γνωστή και ως τεχνολογία κατανεμημένης λογιστικής. Στην πραγματικότητα η τεχνολογία Blockchain είναι ένας κατανεμημένος λογιστικός κατάλογος, που μπορεί να είναι δημόσιος ή ιδιωτικός, στον οποίο συναλλαγές ή δεδομένα συνδέονται μεταξύ τους σε συνδεδεμένα μπλοκ δεδομένων, γεγονός που

διατηρεί τα πρακτικά σε όλους τους κατανεμημένους κόμβους [100]. Οι ερευνητές αναφέρουν ότι τα δεδομένα σε ένα Blockchain είναι εσωτερικά συνεπή, δηλαδή είναι δυνατό να διενεργηθούν έλεγχοι σε αυτά, και εάν τα δεδομένα και τα hashes δεν ταιριάζουν, τότε υπήρξε σίγουρα κάποια αλλαγή, η οποία τελικά δεν θα επιβεβαιωθεί από την αλυσίδα των μπλοκ προς όλους τους κόμβους ενημέρωσης.

Οι Agbedanu et al, [100], προτείνουν ένα μοντέλο, το οποίο βασίζεται σε τεχνολογία Blockchain, ώστε να διασφαλιστεί η επαληθευσιμότητα των αρχείων καταγραφής που παράγονται σε περιβάλλοντα Διαδικτύου των Αντικειμένων (IoT). Η κύρια ιδέα αυτού του μοντέλου είναι να εξασφαλίσει την αξιοπιστία και αυθεντικότητα των αρχείων καταγραφής που παράγονται από συσκευές Διαδικτύου των Αντικειμένων (IoT) κατά τη διάρκεια ιατροδικαστικών ερευνών. Το μοντέλο χρησιμοποιεί την αποκεντρωμένη προσέγγιση και την ιδιότητα του αμετάβλητου που εξασφαλίζει η τεχνολογία Blockchain για να διασφαλιστεί ότι τα αρχεία καταγραφής και άλλα αποδεικτικά στοιχεία που παράγονται σε περιβάλλοντα Διαδικτύου των Αντικειμένων (IoT) μπορούν να επαληθευτούν από εγκληματολογικούς φορείς, εστιάζοντας στην ακεραιότητα, την επαλήθευση και την αυθεντικότητα των αποδεικτικών στοιχείων, αλλά και στη διαφύλαξη αυτών κατά τη διάρκεια της αλυσίδας κράτησης.

Στην τεχνολογία Blockchain στηρίζουν το μοντέλο τους και οι Akhtar et al, [101], οι Ali et al,[9], οι Cebe et al, [85], οι Hossain et al, [86], οι Le et al, [102], οι Musa et al, [103], οι Sadineni et al, [105], οι Sathwara et al, [106], οι Servida et al, [110] και οι Yoon et al, [107]. Τα κριτήρια που θεωρούνται από τα πιο σημαντικά είναι η ακεραιότητα, η ασφάλεια και η αξιοπιστία των αποδεικτικών στοιχείων, χαρακτηριστικά τα οποία συμβάλουν στην αποδοχή τους από τις δικαστικές αρχές.

Οι Feng et al, [87], Kebande et al, [108] , Qatawneh et al, [109], προτείνουν μοντέλα με πολλαπλές διαδικασίες, και βασικά κριτήρια, εκτός των υπολοίπων, την ασφάλεια και το απόρρητο, ενώ στα μοντέλα, στα οποία γίνεται χρήση ψηφιακών μέσων , όπως εικόνες, αισθητήρες και άλλα, τα κριτήρια που επισημάνθηκαν ήταν το απόρρητο, η ακεραιότητα, τα νομικώς αποδεκτά πειστήρια και η αξιοπιστία [87], [109].

6.4 Σύγκριση μεθόδων και κριτηρίων ψηφιακής εγκληματολογίας

Σύμφωνα με τους Agbedanu et al, [100], το μοντέλο που προτείνουν, το οποίο βασίζεται στην τεχνολογία Blockchain, συμβάλει στην αποκέντρωση, εξασφαλίζοντας ότι τα αρχεία καταγραφής μπορούν να επαληθευτούν, ενώ ταυτόχρονα προσδιορίζει τη γνησιότητά τους. Με την τεχνολογία

Blockchain εντοπίζεται κάθε παραβίαση καθώς η ιδιότητα του αμετάβλητου του Blockchain λειτουργεί υπέρ της διασφάλισης της ακεραιότητας των καταγραφών που παράγονται στο περιβάλλον Διαδικτύου των Αντικειμένων (IoT). Οι ερευνητές εστιάζουν στο πλεονέκτημα της επαληθευσιμότητας, την οποία εξασφαλίζει το μοντέλο που προτείνουν, καθώς αυτό το πλεονέκτημα δίνει τη δυνατότητα στους εγκληματολογικούς φορείς να επαληθεύσουν τη γνησιότητα των αρχείων καταγραφής που παράγονται σε περιβάλλοντα Διαδικτύου των Αντικειμένων (IoT).

Οι Akhtar et al, [101], χρησιμοποιούν την τεχνολογία Blockchain για τη διασφάλιση της ακεραιότητας των ψηφιακών ιατροδικαστικών στοιχείων σε περιβάλλον Διαδικτύου των Αντικειμένων (IoT). Με το μοντέλο που προτείνουν στοχεύουν στην εξασφάλιση της ασφάλειας και της ακεραιότητας των αποδεικτικών στοιχείων, αλλά και την πρόληψη των απειλών. Το προτεινόμενο μοντέλο είναι αποτελεσματικό, καθώς ανιχνεύει και προβλέπει επιθέσεις σε πρώιμο στάδιο, ικανοποιώντας τα κριτήρια της ακεραιότητας, της ασφάλειας και της πρόληψης. Κάνει χρήση της τεχνολογίας Blockchain σε συνδυασμό με τον αλγόριθμο Hashing και μπορεί να ανιχνεύει και να προβλέπει επιθέσεις σε πρώιμο στάδιο (αλγόριθμος XGBoost).

Οι Ali et al, [9], διερευνούν τους αλγόριθμους κατακερματισμού της τεχνολογίας Blockchain, για τη διατήρηση της ακεραιότητας και της αξιοπιστίας των ψηφιακών στοιχείων (εικόνων) στο Διαδίκτυο των Αντικειμένων (IoT). Οι ερευνητές συνδυάζουν τις τεχνολογίες Gray Hash και Blockchain, προκειμένου να δημιουργήσουν μια διαδικασία για τον εντοπισμό της αλυσίδας φύλαξης στην ψηφιακή εικόνα. Στόχος τους είναι να προσδιορίσουν την αποτελεσματικότητα των αλγορίθμων ασαφούς κατακερματισμού στο εσωτερικό της τεχνολογίας Blockchain, σε αντίθεση με τους συμβατικούς κρυπτογραφικούς αλγόριθμους κατακερματισμού, ώστε να εξασφαλιστεί η διατήρηση της ακεραιότητας των ψηφιακών στοιχείων.

Οι Cebe et al, [85], αναπτύσσουν ένα μοντέλο ψηφιακής εγκληματολογίας βασισμένο στην τεχνολογία Blockchain (Block4Forensic Model), με σκοπό να διασφαλιστεί η ιδιωτικότητα, με την εισαγωγή ενός πλαισίου διερεύνησης οχημάτων, που περιέχει όλα τα απαραίτητα δεδομένα για μια ολοκληρωμένη ιατροδικαστική έρευνα. Το προτεινόμενο ιατροδικαστικό πλαίσιο επιτρέπει την αξιόπιστη ανάλυση, με ελάχιστο κόστος αποθήκευσης και επεξεργασίας και την παροχή ολοκληρωμένων ιατροδικαστικών υπηρεσιών για έρευνες ατυχημάτων. Το προτεινόμενο πλαίσιο είναι προσανατολισμένο στην αύξηση του επιπέδου εμπιστοσύνης μεταξύ των συμμετεχόντων στο δίκτυο.

Οι Hossain et al, [86], προτείνουν το μοντέλο FIF (Forensic Investigation Framework), στο Διαδίκτυο των Αντικειμένων, για τη συλλογή αποδεικτικών στοιχείων και την αποθήκευσή τους με αξιόπιστο

τρόπο. Το μοντέλο χρησιμοποιεί την τεχνολογία Blockchain και παρέχει ένα μηχανισμό απόκτησης αποδεικτικών στοιχείων από το καθολικό, διασφαλίζοντας την επαλήθευση και την ακεραιότητα των αποδεικτικών στοιχείων που αποκτήθηκαν.

Οι Kebande et al, [108], στη μελέτη τους πρότειναν ένα ολοκληρωμένο, το οποίο το χαρακτηρίζουν ως μη αμφισβητήσιμο, πλαίσιο εγκληματολογικών τεχνικών για την ανάλυση Δυναμικών Ψηφιακών Στοιχείων από το οικοσύστημα που βασίζεται στο Διαδίκτυο των Αντικειμένων (IoT), το οποίο περιλαμβάνει συνολικά εννέα διαδικασίες. Το ολοκληρωμένο ψηφιακό πλαίσιο εγκληματολογικής έρευνας συμβάλει στην εκ των προτέρων ανίχνευση και αντιμετώπιση περιστατικών ασφαλείας στον κυβερνοχώρο, ενώ η αποτελεσματικότητά του συνίσταται στην ποικιλία των διαδικασιών, των ελέγχων και των πιστοποιήσεων που παρέχει, ικανοποιώντας όλα τα επιθυμητά κριτήρια.

Οι Le et al, [102], προτείνουν ένα εξουσιοδοτημένο πλαίσιο εγκληματολογίας που βασίζεται στο Διαδίκτυο των Αντικειμένων (IoT), κάνοντας χρήση της τεχνολογίας Blockchain, για τη βελτίωση των κριτηρίων της ακεραιότητας, της αυθεντικότητας και μη άρνησης για τον τρόπο που συλλέχθηκαν τα αποδεικτικά στοιχεία. Απώτερος στόχος του μοντέλου είναι να εξασφαλιστεί η ακεραιότητα των αποδεικτικών στοιχείων και η αποδοχή τους για νόμιμη χρήση, εξαλείφοντας την πιθανότητα να γίνουν νομικά μη αποδεκτά.

Οι Musa et al, [103], εστίασαν σε μια μεθοδολογία παρακολούθησης σε πραγματικό χρόνο για δίκτυα P2P (Peer to Peer) και τυποποίησαν το μοντέλο ADDIE (Analysis, Design, Development, Implementation, and Evaluation) ως επίσημο ψηφιακό ιατροδικαστικό μοντέλο για το Διαδίκτυο των Αντικειμένων (IoT). Οι ερευνητές εστίασαν στη συνεχή μετάλλαξη των απειλών ασφαλείας που σχετίζονται με τη χρήση δικτύων P2P, οι οποίες προκύπτουν από τις εκτεταμένες και φαινομενικά ατελείωτες εφαρμογές των δικτύων αυτών και αποσκοπούν στην καθοδήγηση των ερευνητών με τα απαραίτητα βήματα και τις διαδικασίες κατά τη διάρκεια της έρευνας. Οι ερευνητές επισήμαναν την ευαισθησία της επίβλεψης σε ένα τυπικό δίκτυο P2P, την ανάγκη για τη διαφύλαξη και διατήρηση των αποδεικτικών στοιχείων με σκοπό την επαλήθευση και τη διασφάλιση της ακεραιότητας της μεθόδου έρευνας.

Οι Nieto et al, [104], εφάρμοσαν τη μεθοδολογία PROFIT για την προσέγγιση του ψηφιακού μάρτυρα, με μια μεθοδολογία που επιτρέπει στους πολίτες να μοιράζονται τα δεδομένα τους με ορισμένες εγγυήσεις απορρήτου, εξασφαλίζοντας με αυτό τον τρόπο μια ισορροπία μεταξύ της ιδιωτικής ζωής και των αρχών της ψηφιακής εγκληματολογίας. Η μεθοδολογία PROFIT αναζητά αρχικά τα δεδομένα από μη προσωπικές συσκευές και όταν αυτές οι συσκευές δε μπορούν να παράσχουν επαρκή

αποδεικτικά στοιχεία για να διευθετηθεί μια έρευνα, τότε αναζητούνται δεδομένα από προσωπικές συσκευές.

Οι Qatawneh et al, [109], προτείνουν ένα μοντέλο ψηφιακής εγκληματολογίας για τη διασφάλιση όλων των αρχών και κριτηρίων της συλλογής και επεξεργασίας των ψηφιακών δεδομένων σε περιβάλλον Διαδικτύου των Αντικειμένων (IoT). Το μοντέλο, DFIM, (Digital Forensics Investigation Model for IoT), περιλαμβάνει την ομαδοποίηση όλων των δεδομένων που συλλέγονται από κόμβους αισθητήρων σε ένα σύνολο ομάδων, όπου κάθε ομάδα περιέχει δεδομένα ή έγγραφα που σχετίζονται μεταξύ τους, ενώ προκειμένου να βελτιωθεί η διαδικασία διερεύνησης αποτελείται από επτά στάδια στα οποία λαμβάνει υπόψη ένα σύνολο αρχών όπως η ασφάλεια, το απόρρητο, η ακρίβεια, η απόδοση, η μείωση δεδομένων και η διαφάνεια.

Στη μελέτη τους οι Sadineni et al, [105], προτείνουν μια ολιστική προσέγγιση που δίνει έμφαση στην εγκληματολογική ετοιμότητα που μπορεί να εφαρμοστεί σε οποιονδήποτε τομέα του Διαδικτύου των πραγμάτων (IoT). Το μοντέλο, είναι προσαρμόσιμο και με δυνατότητα διαμόρφωσης ενώ υποστηρίζει διάφορες εφαρμογές Διαδικτύου των Αντικειμένων (IoT).

Οι Servida et al, [110], εστιάζουν στη μελέτη συσκευών στο Διαδίκτυο των Αντικειμένων (IoT) και σχετικών εφαρμογών smartphone, για την εξαγωγή και ανάλυση ψηφιακών ήχων, και την ανακάλυψη τρωτών σημείων σε πολλές συσκευές (IoT). Επισημαίνουν ότι η ανάλυση των αποδεικτικών στοιχείων με τα κατάλληλα εργαλεία περιορίζει την τρωτότητά τους, ενώ ταυτόχρονα μπορούν να αντιμετωπιστούν τα θέματα αποδοχής των αποδεικτικών στοιχείων που προέρχονται από συσκευές IoT στο δικαστήριο.

Αναφορικά με τις έρευνες που έχουν ως αντικείμενο τα Συστήματα Ευφυών Μεταφορών, οι Yoon et al, [107], πρότειναν ένα πλαίσιο διερεύνησης τροχαίων ατυχημάτων που αξιοποιεί τα ψηφιακά δεδομένα που δημιουργούνται από αισθητήρες και συσκευές, οι οποίοι είναι εγκατεστημένοι σε ένα όχημα ακόμη και όταν το όχημα δεν έχει εγγραφή βίντεο ή εγγραφή οδήγησης. Επισημαίνουν ότι οι πρόσφατες έρευνες τροχαίων ατυχημάτων αναλύουν τα βίντεο και τα αρχεία οδήγησης που έχουν εγκατασταθεί σε ένα όχημα για να τα χρησιμοποιήσουν ως σημαντικά στοιχεία για τον εντοπισμό της αιτίας του ατυχήματος. Όταν υπάρχει μόνο εγγραφή βίντεο ή μόνο εγγραφή οδήγησης ή δεν υπάρχει κανένα από τα δύο διαθέσιμα, υπάρχουν πολλές περιπτώσεις όπου η αιτία του ατυχήματος είναι αδιευκρίνιστη γιατί η έρευνα βασίζεται αποκλειστικά στις δηλώσεις του δράστη και του θύματος. Με τη μελέτη τους οι Yoon et al, [107], εφαρμόζουν ένα πλαίσιο διερεύνησης τροχαίων ατυχημάτων που αξιοποιεί τα ψηφιακά δεδομένα που δημιουργούνται από αισθητήρες και συσκευές που είναι εγκατεστημένοι σε ένα όχημα ακόμη και όταν το όχημα δεν έχει εγγραφή. Στην περίπτωση της

ανάλυσης βίντεο, μπορεί να υπάρχει δυσκολία στην ανάλυση, επειδή τα προγράμματα οδήγησης θα προκαλούσαν ζημιά στα δεδομένα ή η εγγραφή μπορεί να μην είχε γίνει σωστά, ή επειδή ο οδηγός αρνήθηκε να παράσχει τα δεδομένα. Η ανάλυση που προκαλείται από την ποιότητα εικόνας των πληροφοριών βίντεο μπορεί να ξεπεραστεί, χρησιμοποιώντας τις πληροφορίες που έχουν οι αισθητήρες, ενώ στο μέλλον στα οχήματα αυτόνομης οδήγησης, τα οποία εμπλέκονται σε ατυχήματα, δε θα μπορεί να αμφισβητηθεί, να πλαστογραφηθεί και να τροποποιηθεί το αποδεικτικό στοιχείο.

Οι Feng et al, [87], διερευνούν και αναλύουν τις ενδεχόμενες απειλές σε έξυπνα Αυτόνομα Αυτοματοποιημένα Οχήματα (ITS), με την πρόθεση να εξασφαλιστεί η ιδιωτικότητα, η ασφάλεια, η ακεραιότητα, η αξιοπιστία και η διαφάνεια. Το νέο μοντέλο προβλέπει επιθέσεις τόσο από το φυσικό περιβάλλον, όσο και από τον κυβερνοχώρο. Η έρευνα έδειξε ότι τα αποδεικτικά στοιχεία από τα οχήματα μπορούν να εξαχθούν, να αποθηκευτούν και να παρουσιαστούν από τους ερευνητές. Ωστόσο, επισημαίνεται ότι το χρονικό διάστημα κατά το οποίο τα οχήματα βρίσκονται μακριά από το σημείο του περιστατικού, είναι αρκετό για να αλλάξουν τα στοιχεία, γεγονός που δυσκολεύει την έρευνα όταν μάλιστα δεν υπάρχουν αυτόπτες μάρτυρες. Οι ερευνητές αναλύουν τις απειλές που αντιμετωπίζουν τα Έξυπνα Οχήματα στο περιβάλλον της έξυπνης πόλης, διερευνώντας μια ποικιλία κυβερνοεγκλημάτων σε αυτόνομα οχήματα και προτείνουν ένα μοντέλο για την εγκληματολογική εξέταση έξυπνων οχημάτων. Οι συγγραφείς χρησιμοποιούν ένα διαγνωστικό εργαλείο για τη σύνδεση ενός φορητού υπολογιστή με τη διαγνωστική διεπαφή των οχημάτων προκειμένου να αποκτήσουν πρόσβαση στα δεδομένα του «εγκεφάλου» σε δύο διαφορετικά αυτοκίνητα. Η αποτελεσματικότητα του προτεινόμενου μοντέλου επιβεβαιώνεται από τα αποτελέσματα της έρευνας. Ωστόσο, το μοντέλο χρειάζεται να επαληθευτεί με τη χρήση κυκλοφοριακών δεδομένων που έχουν παραχθεί από Έξυπνα Οχήματα σε ένα πραγματικό σενάριο.

Κεφάλαιο 7

Συμπεράσματα-Προτάσεις

Στη σύγχρονη εποχή, το Διαδίκτυο των Αντικειμένων (IoT) έχει γίνει αναπόσπαστο μέρος της ανθρώπινης ζωής. Είναι ενσωματωμένο σε τομείς όπως η υγειονομική περίθαλψη, η αυτοκινητοβιομηχανία, η γεωργία, η βιομηχανία και τα νοικοκυριά. Ωστόσο, όπως κάθε τεχνολογία υπολογιστών, η ασφάλεια αυτής της τεχνολογίας απασχολεί και προβληματίζει τους επιστήμονες. Με την εκθετική αύξηση του αριθμού των επιθέσεων στον κυβερνοχώρο, είναι σημαντικό να διερευνώνται τα εγκλήματα και οι δράστες να οδηγούνται στη δικαιοσύνη [100]. Λόγω της ετερογενούς φύσης του περιβάλλοντος Διαδικτύου των Αντικειμένων (IoT) σε συνδυασμό με την ενσωμάτωση του cloud και του επιπέδου δικτύου, η εγκληματολογική έρευνα σε περιβάλλον Διαδικτύου των Αντικειμένων (IoT), καθίσταται πολύ δύσκολη εργασία.

Η ψηφιακή εγκληματολογία είναι ένας κλάδος της εγκληματολογίας που ασχολείται με τη διερεύνηση ψηφιακών αποδεικτικών στοιχείων και συγκεκριμένα με τον εντοπισμό, την απόκτηση, την επεξεργασία, την ανάλυση και την αναφορά υλικού που έχει αποθηκευτεί σε ένα ηλεκτρονική μορφή. Όταν πρόκειται για την επιβολή του νόμου, οι έρευνες που βασίζονται στην ψηφιακή εγκληματολογία είναι απαραίτητες, διότι τα ψηφιακά αποδεικτικά στοιχεία είναι δυνατόν να εντοπιστούν σχεδόν σε όλες τις περιπτώσεις της παράνομης συμπεριφοράς. Επομένως είναι εφικτό να ανακαλυφθεί ποιες πληροφορίες έχουν ληφθεί και πώς έχουν ληφθεί [101].

Μία από τις δυσκολίες που πρέπει να αντιμετωπίσει η ψηφιακή εγκληματολογία είναι η απειλή για την ασφάλεια και την ακεραιότητα. Η ακεραιότητα και η ασφάλεια των μεθόδων της ψηφιακής εγκληματολογίας που βασίζεται στο Διαδίκτυο των Πραγμάτων (IoT), πρόσφατα αποτέλεσε αντικείμενο πολυάριθμων μελετών, με την εμπιστευτικότητα να είναι άλλο ένα πολύ σημαντικό ζήτημα που πρέπει να αντιμετωπίσουν οι ερευνητές [9], [85], [86], [87], [100], [101], [102], [103], [104], [105], [106], [107].

Επιπλέον, είναι εξαιρετικά δύσκολο για τους ενδιαφερόμενους να προσδιορίσουν την αυθεντικότητα των αποδεικτικών στοιχείων με τα οποία ασχολούνται, αφού στις περισσότερες περιπτώσεις εξαρτώνται από τους παρόχους υπηρεσιών για αυτά τα αποδεικτικά στοιχεία. Για να διασφαλιστεί ότι τα αρχεία καταγραφής είναι αυθεντικά και χωρίς παραποίηση οι περισσότερες μελέτες που συμπεριλήφθηκαν στην παρούσα βιβλιογραφική ανασκόπηση προτείνουν ιατροδικαστικά μοντέλα, τα οποία βασίζονται στην τεχνολογία Blockchain [102], [110]. Επιπλέον, η τεχνολογία αυτή

χρησιμοποιεί μια αποκεντρωμένη προσέγγιση για να διατηρεί τις κατακερματισμένες τιμές των αρχείων καταγραφής που παράγονται στο Διαδίκτυο των Αντικειμένων (IoT) ως αρχεία συναλλαγών.

Τα προτεινόμενα μοντέλα, τα οποία βασίζονται στην τεχνολογία Blockchain, δίνουν τη δυνατότητα σε κάθε ερευνητή του ψηφιακού εγκλήματος να μπορεί να επαληθεύσει την αυθεντικότητα των αρχείων καταγραφής με τα οποία εργάζεται [9], [85], [86], [100], [101], [102], [103], [105], [106], [107] και [110]. Με αυτό τον τρόπο εξασφαλίζεται η ορθή συμπερασματολογία της ιατροδικαστικής έρευνας, η οποία ανακαλύπτει τους ενόχους και δεν εγκλωβίζει άτομα που δε σχετίζονται με το έγκλημα.

Η προσαρμογή της ψηφιακής εγκληματολογίας στα νέα δεδομένα καθίσταται επιτακτική, λαμβάνοντας υπόψη τις αυξανόμενες απαιτήσεις του Διαδικτύου των Αντικειμένων (IoT), όπως τον όλο και μεγαλύτερο αριθμό συσκευών, τη μεγαλύτερη ετερογένεια των συσκευών που απαιτούν εξειδικευμένα εργαλεία ανάκτησης πληροφοριών, την ευρεία εφαρμογή ιδιόκτητων πρωτοκόλλων, τον τεράστιο όγκο και την ποικιλία δεδομένων που συλλέγονται, περιπλέκοντας τον προσδιορισμό των σχετικών δεδομένων, την ανάγκη για νέες μορφές αποθήκευσης ψηφιακών στοιχείων σε συσκευές IoT και την ύπαρξη πολυάριθμων συσκευών περιορισμένων πόρων [104].

Το έργο των ερευνητών ψηφιακής εγκληματολογίας διευκολύνεται από την ανάπτυξη των νέων μεθόδων και τεχνολογιών, αλλά συγχρόνως δυσχεραίνει, καθώς η ανάπτυξη της τεχνολογίας διευκολύνει και τις κακόβουλες ενέργειες. Ο συνδυασμός των υφιστάμενων μεθόδων και ιδιαίτερα αυτών που συνδυάζουν βελτιωμένους αλγόριθμους με τεχνολογίες όπως η Blockchain, θα εξασφαλίσει την ακεραιότητα και την αξιοπιστία των αποδεικτικών στοιχείων, τη διατήρησή τους ώστε να είναι δυνατό να χρησιμοποιηθούν, την ασφάλεια και τη διαφάνεια των πειστηρίων και του τρόπου που αναζητήθηκαν και βρέθηκαν, πληρώντας ταυτόχρονα το κριτήριο της ιδιωτικότητας, γεγονός που προάγει τη συνεργασία των τελικών χρηστών.

Επιπρόσθετα, υπάρχει ανάγκη για μια εις βάθος φυσική ανάλυση των συσκευών του Διαδικτύου των Αντικειμένων (IoT), συμπεριλαμβανομένων των τεχνικών που εφαρμόζεται σε κινητές συσκευές. Απαιτείται επιπλέον μελέτη των πιο κοινών συστημάτων οικιακής ασφάλειας, των έξυπνων βοηθών και των έξυπνων τειχών προστασίας. Ένας εγκληματίας μπορεί να χρησιμοποιήσει πληροφορίες που δημιουργούνται από συσκευές IoT για να καταδιώξει ένα θύμα ή να σχεδιάσει μια επίθεση, όπως η πρόσβαση σε κάμερες παρακολούθησης και άλλα συστήματα IoT σε ένα σπίτι όταν σχεδιάζει μια ληστεία (καθορισμός πότε οι ιδιοκτήτες δεν βρίσκονται στο σπίτι τους), και την κακή χρήση ή απενεργοποίηση συσκευών IoT για να αποτρέψει την εγγραφή γεγονότων που σχετίζονται με ένα έγκλημα. Επομένως, οι μελλοντικές έρευνες θα πρέπει εστιάσουν σε αυτά τα ψηφιακά εγκλήματα,

επεκτείνοντας τα αποτελέσματα των μελετών που αναλύθηκαν στην παρούσα βιβλιογραφική ανασκόπηση.

Πρόκληση επίσης αποτελεί ισχυροποίηση των κριτηρίων που αφορούν στην ασφάλεια, στην ιδιωτικότητα, στη διατήρηση των αποδεικτικών στοιχείων, καθώς αποτελούν πολύ σημαντικά χαρακτηριστικά των κατάλληλων πειστηρίων. Οι μέθοδοι που χρησιμοποιήθηκαν στις υπό μελέτη έρευνες θα μπορούσαν να επεκταθούν, να συνδυαστούν, να προσαρμοστούν σε κάθε περιστατικό ξεχωριστά, παρέχοντας στον ερευνητή πληθώρα κατάλληλων εργαλείων, ώστε να επιτελέσει το έργο του. Η προσκόμιση εκείνων των αποδεικτικών στοιχείων, τα οποία καταδεικνύουν την παράβαση και τον παραβάτη , ενώ συγχρόνως διασφαλίζουν τη νομιμότητά τους, αποτελεί το κυριότερο στόχο της έρευνας στην ψηφιακή εγκληματολογία.

Βιβλιογραφία

1. Tucker, Kristin, et al. "Internet industry: A perspective review through internet of things and internet of everything." International Management Review 14.2 (2018): 26.
2. Lewulis, Piotr. "Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law." Criminal Law Forum. Vol. 33. No. 1. Springer Netherlands, (2022): 39-6
3. Stoyka, Radina, et al. "Reliability assessment of digital forensic investigations in the Norwegian police." Forensic Science International: Digital Investigation 40 (2022): 301351.
4. Garofalaki, Zacharenia, et al. "Transport services within the IoT ecosystem using localisation parameters." 2016 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT). IEEE, (2016): 87-92
5. “IoT and the rise of the knowledge provider” – Jeff Apcar, BRKSPG-2009/ Cisco live, 6-9 March 2018, Melbourne, Australia
6. Statista: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions), https://www.statista.com/statistics/471264/iot-number-of-connecteddevices-worldwide
7. Dave, Evans. "The internet of things: How the next evolution of the internet is changing everything". CISCO white paper, 1(2011):1–11.
8. Vehicle-to-everything. (n.d.) In Wikipedia. Retrieved Ιανουάριος 22, 2021, from https://en.wikipedia.org/wiki/Vehicle-to-everything
9. Ali, Mohamed, et al. "A Procedure for Tracing Chain of Custody in Digital Image Forensics: A Paradigm Based on Grey Hash and Blockchain." Symmetry 14.2 (2022): 334.
10. Ahmad, Liza, et al. "Blockchain-based chain of custody: towards real-time tamper-proof evidence management." Proceedings of the 15th international conference on availability, reliability and security. 2020.
11. Arshad, Humaira, et al. "Digital forensics: review of issues in scientific validation of digital evidence." Journal of Information Processing Systems 14.2 (2018): 346-376.
12. Wilson-Wilde, Linzi. "The international development of forensic science standards—a review." Forensic Science International 288 (2018): 1-9.
13. Montasari, Reza, et al. "Next-generation digital forensics: Challenges and future paradigms." 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3). IEEE, 2019.
14. Horsman, Graeme. "Tool testing and reliability issues in the field of digital forensics." Digital Investigation 28 (2019): 163-175.

15. Tully, Gillian, et al. "Quality standards for digital forensics: Learning from experience in England & Wales." Forensic science international: digital investigation 32 (2020): 200905.
16. Solanke, Abiodun Abdullahi. "Digital Forensics AI: on Practicality, Optimality, and Interpretability of Digital Evidence Mining Techniques." (2022).
17. Bossler, Adam M., et al. "Introduction: new directions in cybercrime research." Journal of Crime and Justice 42.5 (2019): 495-499.
18. Carrier, B. et al. "An event-based digital forensic investigation framework". In Digital forensic research workshop, (2004): 11-13.
19. Pradillo, Juan Carlos Ortiz. "Fighting against cybercrime in Europe: the admissibility of remote searches in Spain." European Journal of Crime, Criminal Law and Criminal Justice 19.4 (2011): 363-395.
20. Palmer, G. "A road map for digital forensic research". In First Digital Forensic Research Workshop, Utica, New York. (2001).
21. Atlam, Hany F., et al. "Internet of things forensics: A review." Internet of Things 11 (2020): 100220.
22. Yaqoob, Ibrar, et al. "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges." Future Generation Computer Systems 92 (2019): 265-275.
23. Stoyanova, Maria, et al. "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues." IEEE Communications Surveys & Tutorials 22.2 (2020): 1191-1221.
24. Zareen, Muhammad Sharjeel, et al. "Digital forensics: Latest challenges and response." 2013 2nd National Conference on Information Assurance (NCIA). IEEE, 2013.
25. Pollitt, Mark. "A history of digital forensics." IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg, 2010.
26. Iqbal, Salman, et al. "Advancing automation in digital forensic investigations using machine learning forensics." Digital Forensic Science (2019).
27. Foley, John P. "Ethics in Internet." Journal of Interdisciplinary Studies 32.1/2 (2020): 179-192.
28. Latzo, Tobias, Ralph Palutke, and Felix Freiling. "A universal taxonomy and survey of forensic memory acquisition techniques." Digital Investigation 28 (2019): 56-69.
29. Al-Dhaqm, Arafat, et al. "A review of mobile forensic investigation process models." IEEE access 8 (2020): 173359-173375.
30. Page, Helen, et al. "A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?." Science & justice 59.1 (2019): 83-92.
31. Umar, Rusydi, Imam Riadi, and Guntur Maulana Zamroni. "Mobile forensic tools evaluation for digital crime investigation." Int. J. Adv. Sci. Eng. Inf. Technol 8.3 (2018): 949-955.

32. Horsman, Graeme. "Tool testing and reliability issues in the field of digital forensics." Digital Investigation 28 (2019): 163-175.
33. National Institute of Standards and Technology, (NIST) https://www.nist.gov/search?s=forensics+tools&index=all-meta-engine
34. Manral, Bharat, et al. "A systematic survey on cloud forensics challenges, solutions, and future directions." ACM Computing Surveys (CSUR) 52.6 (2019): 1-38.
35. Moudud-Ul-Huq, Syed, et al. "Role of cloud computing in global accounting information systems." The Bottom Line 33.3 (2020): 231-250.
36. Tayal, Riya. "Cloud Services: An Ultimate Tool for Business Process Execution or Not." 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). IEEE, 2021.
37. Oh, Kwangsung, et al. "Wiera: Policy-driven multi-tiered geo-distributed cloud storage system." IEEE Transactions on Parallel and Distributed Systems 31.2 (2019): 294-305.
38. Barron, Chimere, et al. "Cloud computing security case studies and research." Proceedings of the world congress on engineering. Vol. 2. No. 2. 2013.
39. Naresh, R. "The concept of Privacy and Standardization of Microservice Architectures in cloud computing." European Journal of Molecular & Clinical Medicine 7.2 (2020): 5349-5370.
40. Fagbemi, Damilare D., David M. Wheeler, and J. C. Wheeler. The IoT architect's guide to attainable security and privacy. CRC Press, 2019.
41. Abdul-Qawy, Antar Shaddad, et al. "The internet of things (iot): An overview." International Journal of Engineering Research and Applications 5.12 (2015): 71-82.
42. Ashton, Kevin. "That 'internet of things' thing." RFID journal 22.7 (2009): 97-114.
43. Patel, Keyur K., Sunil M. Patel, and P. Scholar. "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges." International journal of engineering science and computing 6.5 (2016).
44. Thilakarathne, Navod Neranjan. "Security and privacy issues in iot environment." International Journal of Engineering and Management Research 10 (2020).
45. Wu, Miao, et al. "Research on the architecture of Internet of Things." 2010 3rd international conference on advanced computer theory and engineering (ICACTE). Vol. 5. IEEE, 2010.
46. Ray, Partha Pratim. "A survey on Internet of Things architectures." Journal of King Saud University-Computer and Information Sciences 30.3 (2018): 291-319.
47. Chacko, Anil, and Thaier Hayajneh. "Security and privacy issues with IoT in healthcare." EAI Endorsed Transactions on Pervasive Health and Technology 4.14 (2018): e2-e2.

48. Ahmed, Ali Saadoon, and Sefer KURNAZ. "Internet of things: Security threats and proposed solutions." 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2022.
49. Conti, Mauro, et al. "Internet of Things security and forensics: Challenges and opportunities." Future Generation Computer Systems 78 (2018): 544-546.
50. Yang, Yuchen, et al. "A survey on security and privacy issues in Internet-of-Things." IEEE Internet of Things Journal 4.5 (2017): 1250-1258.
51. Javed, Abdul Rehman, et al. "Future smart cities requirements, emerging technologies, applications, challenges, and future aspects." Cities 129 (2022): 103794.
52. Dong, Bowei, et al. "Technology evolution from self-powered sensors to AIoT enabled smart homes." Nano Energy 79 (2021): 105414.
53. Atiqur, Rahman. "Automated smart car parking system for smart cities demand employs internet of things technology." Int J Inf & Commun Technol ISSN 2252.8776 (2021): 8776.
54. Gohar, Ali, and Gianfranco Nencioni. "The role of 5G technologies in a smart city: The case for intelligent transportation system." Sustainability 13.9 (2021): 5188.
55. Li, Joey, et al. "Methods and Applications for Artificial Intelligence, Big Data, Internet-of-Things, and Blockchain in Smart Energy Management." Energy and AI (2022): 100208.
56. Li, Wei, et al. "A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system." Mobile Networks and Applications 26.1 (2021): 234-252.
57. Hou, Jianwei, et al. "A survey on digital forensics in Internet of Things." IEEE Internet of Things Journal 7.1 (2019): 1-15.
58. Kebande, Victor R., and Indrakshi Ray. "A generic digital forensic investigation framework for internet of things (iot)." 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE (2016).
59. Nieto, Ana, et al. "Privacy-aware digital forensics." Security and Privacy for Big Data,Cloud Computing and Applications, 2019. NICS Lab. Publications, (2019): 157-195.
60. Nieto, Ana, et al. "A methodology for privacy-aware IoT-forensics." 2017 IEEE Trustcom/BigDataSE/ICESS. IEEE, (2017): 626-633.
61. Wu, Tina, et al. "Digital forensic tools: Recent advances and enhancing the status quo." Forensic Science International: Digital Investigation 34 (2020): 300999.
62. Al-Khateeb, Haider, et al. "Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger." Blockchain and Clinical Trial. Springer, Cham, (2019): 149-168.
63. Ryu, Jung Hyun, et al. "A blockchain-based decentralized efficient investigation framework for IoT digital forensics." The Journal of Supercomputing 75.8 (2019): 4372-4387.

64. Dasaklis, Thomas K. et al. "Sok: Blockchain solutions for forensics." Technology Development for Security Practitioners. Springer, Cham, (2021): 21-40.
65. Ab Rahman, Nurul Hidayah, et al. "Forensic-by-design framework for cyber-physical cloud systems." IEEE Cloud Computing 3.1 (2016): 50-59.
66. Theobald, M., "The Importance of Security by Design for IoT Devices." Retrieved 20201213 from https://www.redalertlabs.com/blog/the-importance-of-security-by-design-for-iot-devices
67. Meneguette, Rodolfo I., R. De Grande, and A. A. Loureiro. "Intelligent transport system in smart cities." Cham: Springer International Publishing (2018).
68. Haydari, Ammar, and Yasin Yilmaz. "Deep reinforcement learning for intelligent transportation systems: A survey." IEEE Transactions on Intelligent Transportation Systems (2020).
69. Nelson, John D., et al. "Intelligent transport systems solutions in transitional countries: the case of Korea." Transport reviews 21.1 (2001): 51-74.
70. Vahidi, Homayoun, and Tarek Sayed. "Using the Canadian ITS architecture for evaluating the safety benefits of intelligent transportation systems." Canadian Journal of Civil Engineering 30.6 (2003): 970-980.
71. Zemrane, Hamza, Youssef Baddi, and Abderrahim Hasbi. "Mobile adhoc networks for intelligent transportation system: Comparative analysis of the routing protocols." Procedia computer science 160 (2019): 758-765.
72. Ali, Kashif, et al. "Crowdits: Crowdsourcing in intelligent transportation systems." 2012 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2012.
73. Kushchenko, Lilia, Sergey Kushchenko, and Alexander Novikov. "A system for monitoring traffic parameters using intelligent transport systems." AIP Conference Proceedings. Vol. 2503. No. 1. AIP Publishing LLC, 2022.
74. Tokody, Dániel, et al. "Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city." Interdisciplinary Description of Complex Systems: INDECS 16.3-A (2018): 384-396.
75. Vourgidis, Ioannis, et al. "Use of smartphones for ensuring vulnerable road user safety through path prediction and early warning: An in-depth review of capabilities, limitations and their applications in cooperative intelligent transport systems." Sensors 20.4 (2020): 997.
76. Ali, Qazi Ejaz, et al. "Issues, challenges, and research opportunities in intelligent transport system for security and privacy." Applied Sciences 8.10 (2018): 1964.
77. Shahgholian, M., and D. Gharavian. "Advanced traffic management systems: an overview and a development strategy." arXiv preprint arXiv:1810.02530 (2018).

78. Ambika, M., et al. "Intelligent Framework for Number Plate Detection and Recognition in Toll Using Image Processing Techniques." Advances in Parallel Computing Technologies and Applications 40 (2021): 183.
79. Patel, Palak, Zunnun Narmawala, and Ankit Thakkar. "A survey on intelligent transportation system using internet of things." Emerging Research in Computing, Information, Communication and Applications (2019): 231-240.
80. Ben–Haim, R., G. Ben–Haim, and Y. Shiftan. "Penetration and impact of advanced car technologies." MOJ Civil Eng 4.4 (2018): 175-184.
81. Guerrero-Ibáñez, Juan, Sherali Zeadally, and Juan Contreras-Castillo. "Sensor technologies for intelligent transportation systems." Sensors 18.4 (2018): 1212.
82. William J. Fleming. "New Automotive Sensors—A Review." Ieee Sensors Journal, 8.11, (2008): 1530-437.
83. Abdelhamid, S., Hassanein, H.S., Takahara, G. "Vehicle as a Mobile Sensor. " Procedia Comput. Sci. 34, (2014): 286–295.
84. Nikitas, Alexandros, et al. "Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility era." Sustainability 12.7 (2020): 2789.
85. Cebe, Mumin, et al. "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles." IEEE communications magazine 56.10 (2018): 50-57.
86. Hossain, Md Mahmud, et al. "Trust-IoV: A trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV)", IEEE International Congress on Internet of Things, (2017): 25–32.
87. Feng, Xiaohua, et al. "A new digital forensics model of smart city automated vehicles", IEEE International Congress on Internet of Things (iThings) & IEEE Green Computing and Communications (GreenCom) & IEEE Cyber, Physical and Social Computing (CPSCom) & IEEE Smart Data (SmartData), IEEE, (2017): 274–279.
88. Mansor, Hafizah, et al. "Log your car: The non-invasive vehicle forensics." 2016 IEEE Trustcom/BigDataSE/ISPA. IEEE, (2016): 974–982.
89. Le-Khac, Nhien-An, et al. "Smart vehicle forensics: Challenges and case study." Future Generation Computer Systems 109 (2020): 500-510.
90. Ammar, Mahmoud, et al. "Internet of Things: A survey on the security of IoT frameworks." Journal of Information Security and Applications 38 (2018): 8-27.
91. Giverts, P., et al. "On the Criteria for Evaluating an Expert's Opinion and Forensic Methods by Participants in the Legal Proceedings." Theory and Practice of Forensic Science 17.1 (2022): 27-37.

92. Girish, N., et al. "A Review on Digital Video Forgery Detection Techniques in Cyber Forensics." Science, Technology and Development 3.6 (2019): 235-239.
93. Alabdulsalam, Saad, et al. "Internet of things forensics–challenges and a case study." IFIP International Conference on Digital Forensics. Springer, Cham, (2018) : 35-48
94. HaddadPajouh, Hamed, et al. "A deep recurrent neural network based approach for internet of things malware threat hunting." Future Generation Computer Systems 85 (2018): 88-96.
95. Hegarty, Robert, et al. "Digital Evidence Challenges in the Internet of Things." INC. (2014): p. 163-172.
96. Khan, Minhaj Ahmad, et al. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82 (2018): 395-411.
97. Sha, Kewei, et al. "On security challenges and open issues in Internet of Things." Future generation computer systems 83 (2018): 326-337.
98. Yaqoob, Ibrar, et al. "The rise of ransomware and emerging security challenges in the Internet of Things." Computer Networks 129 (2017): 444-458.
99. Yaqoob, Ibrar, et al. "The rise of ransomware and emerging security challenges in the Internet of Things." Computer Networks 129 (2017): 444-458.
100 Agbedanu, Promise, and Anca Delia Jurcut. "BLOFF: a blockchain-based forensic model in IoT." Research Anthology on Convergence of Blockchain, Internet of Things, and Security. IGI Global, 2023. 738-749.
101 Agbedanu, Promise, and Anca Delia Jurcut. "BLOFF: a blockchain-based forensic model in IoT." Research Anthology on Convergence of Blockchain, Internet of Things, and Security. IGI Global, 2023. 738-749.
102 Akhtar, Muhammad Shoaib, and Tao Feng. "Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment." EAI Endorsed Transactions on Creative Technologies 9.31 (2022): e2-e2.
103 Le, Duc-Phong, et al. "BIFF: A blockchain-based IoT forensics framework with identity privacy." TENCON 2018-2018 IEEE region 10 conference. IEEE, 2018.
104 Musa, Ahmad Sanda, Irfan-Ullah Awan, and Fatima Zahrah. "The Case for Validating ADDIE Model as a Digital Forensic Model for Peer-to-Peer Network Investigation." Information Systems Frontiers (2022): 1-17.
105 Nieto, Ana, Ruben Rios, and Javier Lopez. "IoT-forensics meets privacy: towards cooperative digital investigations." Sensors 18.2 (2018): 492.
106 Sadineni, Lakshminarayana, Emmanuel Pilli, and Ramesh Babu Battula. "A holistic forensic model for the internet of things." IFIP International Conference on Digital Forensics. Springer, Cham, 2019.

107 Sathwara, Snehal, Nitul Dutta, and Emil Pricop. "IoT Forensic A digital investigation framework for IoT systems." 2018 10th international conference on electronics, computers and artificial intelligence (ECAI). IEEE, 2018.

108 Yoon, Cheolhee, et al. "Study on did application methods for blockchain-based traffic forensic data." Applied Sciences 11.3 (2021): 1268.

109 Kebande, Victor R., et al. "Towards an integrated digital forensic investigation framework for an IoT-based ecosystem." 2018 IEEE International Conference on Smart Internet of Things (SmartIoT). IEEE, 2018.

110 Qatawneh, Mohammad, et al. "Dfim: A New digital forensics investigation model for internet of things." Journal of Theoretical and Applied Information Technology 97.24 (2019).

111 Servida, Francesco, and Eoghan Casey. "IoT forensic challenges and opportunities for digital traces." Digital Investigation 28 (2019): S22-S29.