ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Βιβλιογραφική Έρευνα σε Digital Forensic Analysis σε Δίκτυα και Συστήματα IoT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ιωάννης Χ. Κίκιλας

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής ΕΜΠ

Αθήνα,Ιούλιος,2024

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Βιβλιογραφική Έρευνα σε Digital Forensic Analysis σε Δίκτυα και Συστήματα IoT

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ιωάννης Χ. Κίκιλας

Επιβλέπων: Δημήτριος Ασκούνης
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 15η Ιουλίου 2024.

.....	.....	.....
Δημήτριος Ασκούνης	Ιωάννης Ψαρράς	Ευάγγελος Μαρινάκης
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Επ. Καθηγητής ΕΜΠ

Αθήνα,Ιούλιος,2024

.....
Ιωάννης Χαράλαμπος Κίκιλας
Διπλωματούχος Ηλεκτρόλογος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Η παρούσα εργασία αναφέρεται στις digital forensics μεθόδους για τα δίκτυα IoT τα οποία συναντήθηκαν στη βιβλιογραφία. Το 2ο κεφάλαιο αναφέρεται στα διαφορα δίκτυα που υπάρχουν εγγενώς μέσα στον όρο IoT, οι προκλήσεις που αυτά προκαλούν στις Digital Forensics μεθόδους, ενώ ταυτόχρονα γίνεται μια πρώτη προσπάθεια κατηγοριοποίησης τους. Στο 3ο Κεφάλαιο παρουσιάζονται οι γενικότερες μεθοδολογίες IoT και Digital Forensics που συναντήθηκαν σε όλα τα paper.

Γίνεται μία ταξινόμηση όλων των IoT Forensics μεθόδων μαζί με μία σύντομη ανάλυση τους και παρουσιάζονται τα guidelines και τα βασικά frameworks. Στο 4ο κεφάλαιο αναφέρονται οι τεχνολογίες των CPS και Digital Twins, τα οποία αποτελούν το digital counterpart των τεχνολογιών και δικτύων IoT. Παρουσιάζονται έτσι διαφοροι τρόποι μέσω των οποίων οι συσκευές IoT μπορούν να φανούν στο δίκτυο και ποιες επιμέρους τεχνολογίες είναι απαραίτητες στη κατανόηση ώστε οι Digital Forensics analysts να μπορούν να αποκαλύψουν πληροφορία για δράστες.

Τέλος στο 5ο Κεφάλαιο παρουσιάζονται digital forensics μέθοδοι και εργαλεία που χρησιμοποιήθηκαν ήδη από ερευνητές για να αναλύσουν επακριβώς τα δίκτυα των IoT, όπως αυτά χωρίστηκαν από το 2ο κεφάλαιο. Τελικά κλείνουμε με μία σύντομη συζήτηση στο κεφάλαιο 6 και τον επίλογο στο κεφάλαιο 7.

Λέξεις – Κλειδιά

Digital Forensics, IoT (Internet of Things), CPS (Cyber-Physical Systems), Digital Twins, IoT Forensics Methods, 6G IoT, Smart Factory, Security in IoT, Wearables, XR/AR/VR (Extended Reality, Augmented Reality, Virtual Reality)

Abstract

This paper refers to the digital forensics methods for IoT networks that were encountered in the literature. The 2nd chapter refers to the different networks that exist inherently within the term IoT, the challenges that they cause to Digital Forensics methods, while at the same time a first attempt is made to categorize them. The 3rd chapter presents the general IoT and Digital Forensics methodologies that were encountered in all the papers.

A classification of all IoT Forensics methods is made along with a brief analysis of them and the guidelines and basic frameworks are presented. The 4th chapter refers to the technologies of CPS and Digital Twins, which are the digital counterpart of IoT technologies and networks. Different ways through which IoT devices can be seen on the network and also which individual technologies are necessary for understanding them are presented. Through these processes the Digital Forensics analysts can reveal information about perpetrators.

Finally, Chapter 5 presents digital forensics methods and tools that have already been used by researchers to accurately analyze IoT networks, presented from the classification presented from Chapter 2. Finally, we close with a brief discussion in Chapter 6 and the epilogue in Chapter 7.

Key words

Digital Forensics, IoT (Internet of Things), CPS (Cyber-Physical Systems), Digital Twins, IoT Forensics Methods, 6G IoT, Smart Factory, Security in IoT, Wearables, XR/AR/VR (Extended Reality, Augmented Reality, Virtual Reality)

Περιεχόμενα

1. Εισαγωγή

Η παρούσα εργασία αναφέρεται στις digital forensics μεθόδους για τα δίκτυα IoT τα οποία συναντήθηκαν στη βιβλιογραφία. Η Βιβλιογραφία αυτή βρέθηκε τροφοδώτοντας μία βάση από keywords σε διάφορες πλατφόρμες απο papers όπως το Scopus,IEEE Xplore,Google Scholar.Ορισμένα από αυτά τα keywords τροφοδοτήθηκαν και στο Google προκειμένου να μπορέσει να βρεθεί ορισμός και για αυτό στη βιβλιογραφία υπάρχουν και ιστοσελίδες. Τελικά κρατήθηκαν για τη δημιουργία αυτής της διπλωματικής εργασίας συνολικά 64 πηγές.

Εκτενώς ενδεικτικά κάποια από τα keywords που χρησιμοποιήθηκαν είναι «digital»,”forensics”,”IoT”,”CPS”,”Digital Twins”,”IoT Categorization”,”IoT forensics Methods”,”Satellite IoT”,”Smart Factory”,”Smart Home”,”Industry 4.0”,Industry 5.0”,Smart home forensics analysis”,Satellite IoT forensics analysis”, Smart City”,”Smart City forensic analysis”,”Wearables”,”Wearables forensics analysis”,”XR AR VR”,”XR VR AR forensic analysis”,”6G IoT”,”6G IoT forensic analysis”,”OWN forensic analysis”,”6G edge”,”6G edge forensic analysis”,”Smart Cars”,”Smart Cars forensics analysis”,”Drones”,”Drones forensics analysis”,”UAV”,”UAV forensic analysis”,”Vanet”,”Vanet forensic analysis”,”Smart office”,”Smart office forensic analysis”,””Industrial IoT”,”Industrial IoT forensic analysis”,”Smart healthcare”,”Smart healthcare forensic analysis”,”CPS Satellite IoT”,”CPS Smart home”,”CPS Wearables”,”CPS XR AR VR”,”CPS Smart Cars”,”CPS Drones”,”CPS Industrial IoT”,”CPS 6G edge”,”CPS Optical Wirelless Networks”,”CPS Smart healthcare”,”CPS Smart factory”,”Digital Twins Satellite IoT”,”Digital Twin Smart Home”,”Digital Twin Smart healthcare,”Digital Twin Wearables”,”Digital Twin XR AR VR”,”Digital Twin Smart office”,”Digital Twin 6G edge”,”Digital Twin Optical Wirelless Netoworks”,”Digital Twin Smart Car”,”Digital Twin Industrial IoT,”Digital Twin Drones”,”mURLLC”,”NOMA”,”RIS-IRS”,”mmWave”,”VLC”,”OWC”,”OCC 6G”,”FSO 6G”,”Li-Fi 6G”.

2. 5G and 6G IoT Networks

2.1 IoT Categorization

Θα ξεκινήσουμε τη παρούσα ενότητα προσπαθώντας να δώσουμε έναν ευρύ ορισμό του IoT(Internet of Things) και στη συνέχεια θα προσπαθήσουμε να παρουσιάσουμε μία γενικότερη κατηγοριοποίηση των συσκευών που την απαρτίζουν ώστε να έχουμε μία καλύτερη εικόνα του ευρύ και αναπτυσσόμενου αυτού πεδίου. Η κατηγοριοποίηση των συσκευών IoT είναι ενεργό προϊόν επιστημονικής ανάπτυξης οπότε καμία κατηγοριοποίηση των συσκευών αυτών, όπως και κανένας ορισμός κατά αντιστοιχία δεν μπορεί να είναι αρκετά σαφής για να καλύψει κάθε παρούσα και μελλοντική συσκευή IoT. Για όλους αυτούς τους λόγους η παρούσα ενότητα προσπαθεί να δώσει κατά βάση κάποια παραδείγματα προς το τέλος της, ώστε να έχουμε μία καλύτερη εικόνα αυτού του ευρύ πεδίου.

2.1.1 Ορισμός του IoT

Προσπαθώντας να μην αποκλείσουμε λοιπόν καμία συσκευή, ως μία συσκευή IoT μπορούμε να δώσουμε τον ακόλουθο ορισμό:

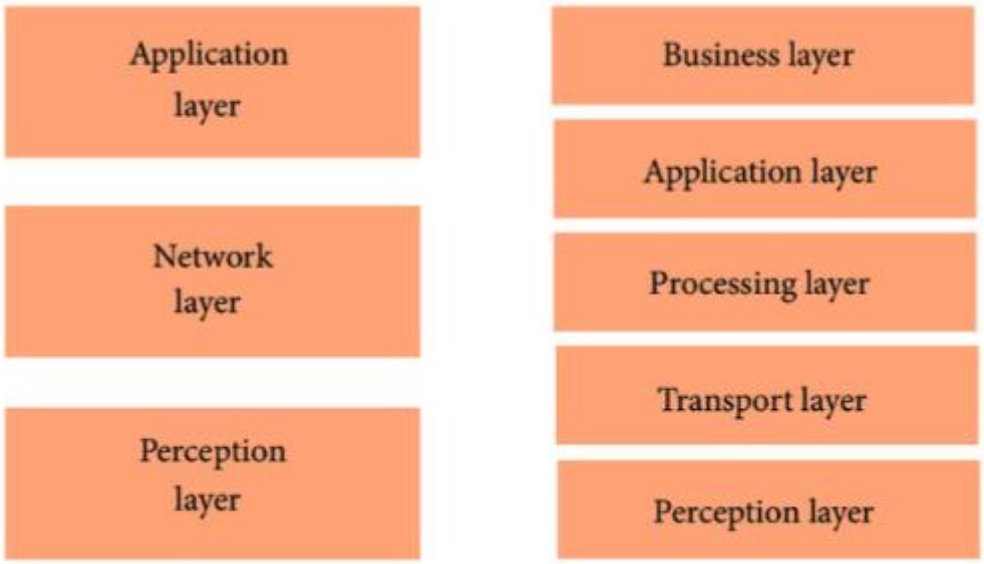
- ➔ **Οι συσκευές IoT είναι κομμάτια υλικού**, όπως αισθητήρες, ενεργοποιητές, gadgets, συσκευές ή μηχανήματα, που είναι προγραμματισμένα για συγκεκριμένες εφαρμογές και **μπορούν να μεταδώσουν δεδομένα μέσω του Διαδικτύου ή άλλων δικτύων**.[18]

Ήδη μπορεί να παρατηρήσει κανείς κάποια από τα προβλήματα που προκύπτουν από τέτοια είδη ορισμών. Ένα πολυσυζητημένο πρόβλημα είναι το ακόλουθο: Είναι δηλαδή οι κινητές συσκευές και οι υπολογιστές IoT ή όχι; Η απάντηση προφανώς εξαρτάται από τον ερευνητή και την περίσταση. Συνεχίζουμε παρόλα αυτά σε μία κατηγοριοποίηση των συσκευών IoT προκειμένου να έχουμε μία καλύτερη εικόνα της έκτασης του φάσματος τους, με τη σιωπηρή παραδοχή ότι οι υπολογιστές και οι κινητές συσκευές έχοντας υπερβολικά πολλές δυνατότητες σε σχέση με άλλες συσκευές που θα αναφέρουμε στη συνέχεια, είναι στη καλύτερη μία πολύ ειδική κατηγορία των συσκευών IoT και για αυτό το λόγο δεν θα μιλήσουμε για αυτές τις συσκευές σε αυτή την εργασία.

2.1.2 Σύντομη παρουσίαση κάποιων τρόπων κατηγοριοποίησης των IoT συσκευών

Μέσα από τη βιβλιογραφία [7], [8], [16], [18], [19], [20], [21] μπορεί να παρατηρήσει κανείς ότι είναι πολύ δύσκολο να βρεθεί και μία καλή ταξινόμηση των συσκευών IoT, καθώς κάθε ερευνητής εστιάζει σε διαφορετικά σημεία. Μπορούμε να κατηγοριοποιήσουμε δηλαδή τις συσκευές IoT με βάση:

❖ Την αρχιτεκτονική 3 ή 5 επιπέδων [19]:



Σχήμα 1: Η αρχιτεκτονική 3 ή 5 επιπέδων

Η πιο βασική αρχιτεκτονική είναι μια αρχιτεκτονική τριών επιπέδων όπως φαίνεται στο Σχήμα 1. Εισήχθη στα αρχικά στάδια της έρευνας σε αυτόν τον τομέα. Έχει τρία επίπεδα, δηλαδή, τα επίπεδα perception, network και application [19]:

- Το επίπεδο **perception** είναι το φυσικό στρώμα, το οποίο διαθέτει αισθητήρες για την ανίχνευση και τη συλλογή πληροφοριών για το περιβάλλον. Αισθάνεται κάποιες φυσικές παραμέτρους ή προσδιορίζει άλλα έξυπνα αντικείμενα στο περιβάλλον. [19]
- Το επίπεδο **network** είναι υπεύθυνο για τη σύνδεση με άλλα έξυπνα πράγματα, συσκευές δικτύου και διακομιστές. Τα χαρακτηριστικά του χρησιμοποιούνται επίσης για τη μετάδοση και την επεξεργασία δεδομένων αισθητήρων. [19]
- Το επίπεδο **application** είναι υπεύθυνο για την παροχή συγκεκριμένων υπηρεσιών εφαρμογής στον χρήστη. Ορίζει διάφορες εφαρμογές στις οποίες μπορεί να αναπτυχθεί το Internet of Things, για παράδειγμα, έξυπνα σπίτια, έξυπνες πόλεις και έξυπνη υγεία. [19]

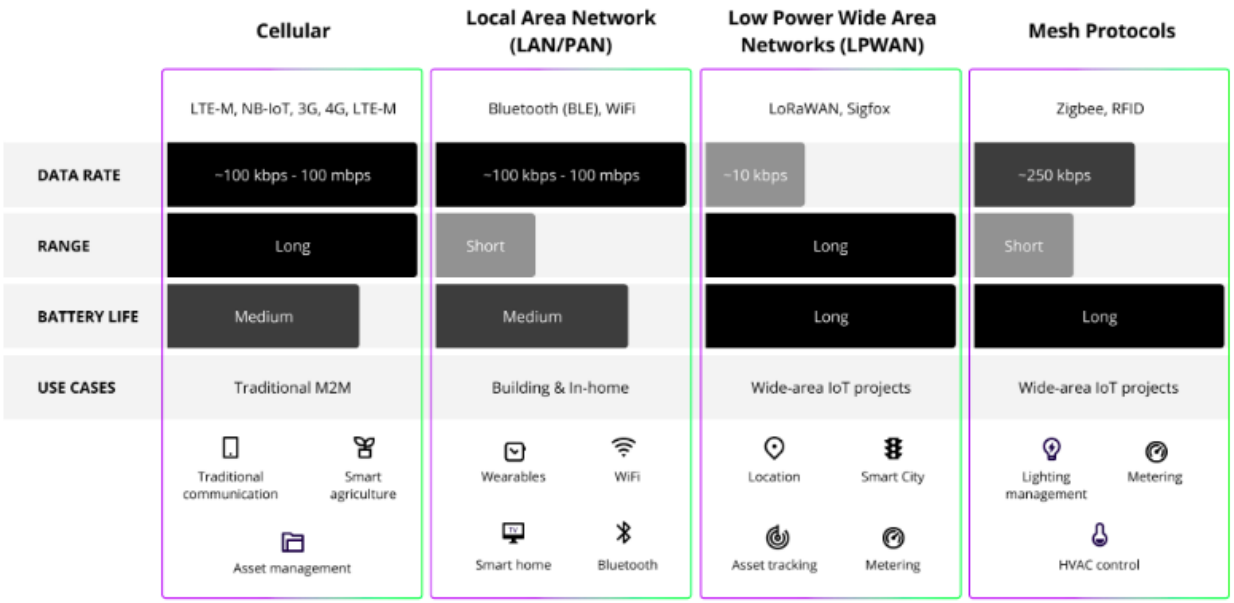
Η αρχιτεκτονική τριών επιπέδων καθορίζει την κύρια ιδέα του IoT, αλλά δεν αρκεί για έρευνα στο IoT, επειδή η έρευνα συχνά επικεντρώνεται σε λεπτότερες πτυχές. Γι' αυτό, έχουμε πολλές περισσότερες πολυεπίπεδες αρχιτεκτονικές που προτείνονται στη βιβλιογραφία. Το ένα είναι η αρχιτεκτονική πέντε επιπέδων, η οποία περιλαμβάνει επιπλέον τα επίπεδα processing και business. Τα πέντε επίπεδα τώρα είναι τα επίπεδα perception, transport, processing, application, and business (βλ. Σχήμα 1). Ο ρόλος των επιπέδων perception και application είναι ίδιος με την αρχιτεκτονική στα τρία επίπεδα. Περιγράφουμε τη λειτουργία των υπόλοιπων τριών επιπέδων [19]:

- Το επίπεδο **transport** μεταφέρει τα δεδομένα του αισθητήρα από το επίπεδο perception στο επίπεδο processing και αντίστροφα μέσω δικτύων όπως wireless, 3G, LAN, Bluetooth, RFID και NFC. [19]
- Το επίπεδο **processing** είναι επίσης γνωστό ως στρώμα ενδιάμεσου λογισμικού. Αποθηκεύει, αναλύει και επεξεργάζεται τεράστιες ποσότητες δεδομένων που προέρχονται από το επίπεδο transport. Μπορεί να διαχειριστεί και να παρέχει ένα ποικίλο σύνολο υπηρεσιών στα κατώτερα

στρώματα. Χρησιμοποιεί πολλές τεχνολογίες, όπως βάσεις δεδομένων, υπολογιστικό νέφος και big data processing modules. [19]

- Το **business** επίπεδο διαχειρίζεται ολόκληρο το σύστημα IoT, συμπεριλαμβανομένων των εφαρμογών, των μοντέλων επιχειρήσεων και κέρδους και του απορρήτου των χρηστών. Το business επίπεδο δεν εμπίπτει στο πεδίο εφαρμογής αυτής της εργασίας. Ως εκ τούτου, δεν το συζητάμε περαιτέρω. [19]

❖ Με βάση παράγοντες όπως η κάλυψη δικτύου και το διαθέσιμο εύρος ζώνης που χρησιμοποιείται από τη κάθε συσκευή ως ακολούθως [20], [16]:



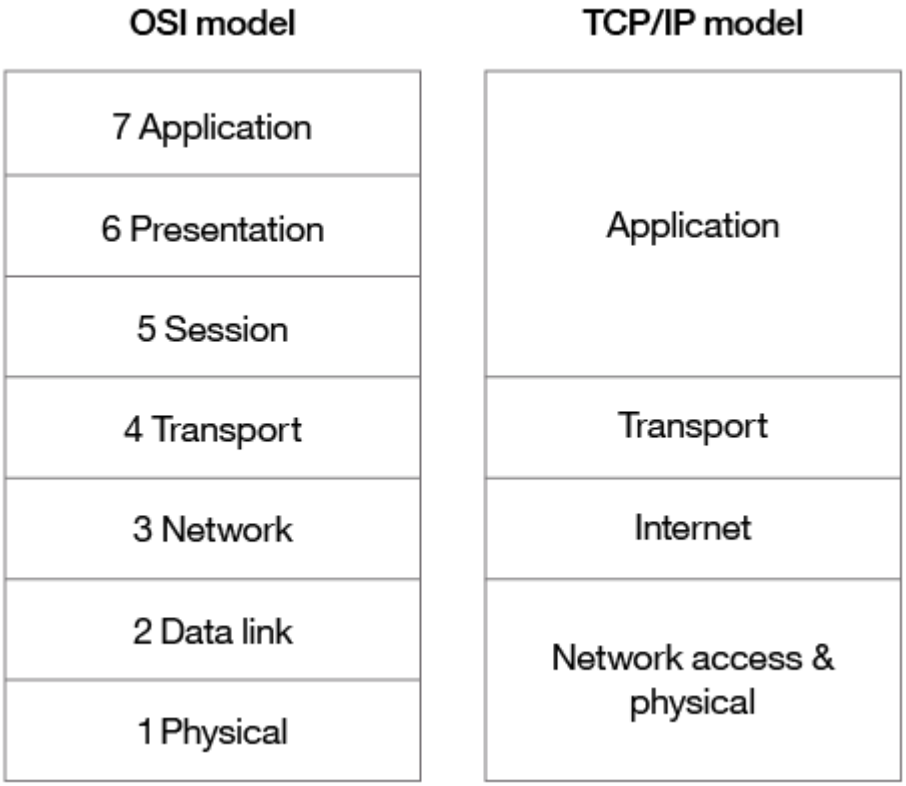
Σχήμα 2: Κατηγοριοποίηση με βάση συγκεκριμένους παράγοντες

- **1.Cellular: LTE-M vs. NB-IoT**
  - Το LTE-M και το NB-IoT ανήκουν και τα δύο σε δίκτυα ευρείας περιοχής χαμηλής κατανάλωσης (LPWAN) και και τα δύο μπορούν να λειτουργήσουν σε ζώνη 4G. Αυτά τα ανοιχτά πρότυπα εισήχθησαν και τα δύο από το 3GPP (3rd Generation Partnership Project) και έχουν σχεδιαστεί για αξιόπιστες, ασφαλείς λειτουργίες χαμηλής κατανάλωσης αλλά διαφέρουν ως προς τη συχνότητα, το εύρος, την ασφάλεια, το κόστος και την κατανάλωση ενέργειας. Παρόλα αυτά, θεωρούνται μια από τις πιο δημοφιλείς λύσεις για το IoT αφού μπορούν να καλύψουν μεγάλες περιοχές. [20]
  - Αποτελώντας μια σταθερή λύση στην αγορά καταναλωτών κινητής τηλεφωνίας, εξελίσσονται, παρέχοντας αξιόπιστη και υψηλού εύρους ζώνης συνδεσιμότητα IoT. Μέχρι το 2026, το NB-IoT και το LTE-M θα καλύπτουν πάνω από το 60% των 3,6 δισεκατομμυρίων συνδέσεων δικτύου LPWA. [20]
- **2. LAN/PAN: WiFi vs. BLE**
  - Τα τοπικά δίκτυα και τα προσωπικά δίκτυα περιοχής (LAN/PAN) είναι οικονομικά αποδοτικά, ωστόσο, η μετάδοση δεδομένων είναι περιορισμένη λόγω του τοπικού περιβάλλοντος. Το WiFi και το

Bluetooth ανήκουν σε αυτήν την κατηγορία και χρησιμοποιούνται συνήθως για λύσεις συνδεσιμότητας IoT. [20]

- **3. LPWAN**
    - Τα δίκτυα ευρείας περιοχής χαμηλής ισχύος (LPWAN) είναι ένα νέο σύνολο ασύρματων πρωτοκόλλων που μπορούν κυριολεκτικά να συνδέσουν όλους τους τύπους αισθητήρων IoT και να διευκολύνουν πολυάριθμες εφαρμογές που έχουν κατασκευαστεί ειδικά για την υποστήριξη μεγάλων έργων IoT. Αυτά τα δίκτυα μπορούν να χρησιμοποιηθούν από συσκευές για την επικοινωνία σε μεγάλες περιοχές με τη βοήθεια μικρών φθηνών μπαταριών με χαμηλή κατανάλωση ενέργειας. Σε σύγκριση με τα κυψελωτά δίκτυα, τα LPWAN είναι μια οικονομικά αποδοτική και μακροπρόθεσμη λύση. [20]
- **4. Mesh protocols**
    - Λόγω της χωρητικότητας μικρής εμβέλειας, τα πρωτόκολλα Mesh είναι εξαιρετικές λύσεις για έργα IoT μεσαίας εμβέλειας με τις μεταφορές δεδομένων σε κοντινή απόσταση. Στα δίκτυα Mesh, η επικοινωνία μεταξύ των κόμβων αισθητήρων διεξάγεται με κατανεμημένο τρόπο για να φτάσουμε στην απόδραση που είναι η προσέγγιση αντίθεσης της μεταφοράς δεδομένων στον κεντρικό διανομέα. [20]

❖ Τα πρωτόκολλα δικτύου που χρησιμοποιεί κάθε συσκευή επακριβώς τοποθετημένα στο OSI layer [16]



[16]

Σχήμα 3: το πρωτόκολλο OSI και TCP/IP

❖ Την κατανάλωση ισχύος της κάθε συσκευής [16]

Η μετάδοση δεδομένων από μια συσκευή καταναλώνει ενέργεια. Η μετάδοση δεδομένων σε μεγάλες αποστάσεις απαιτεί περισσότερη ισχύ από ό,τι σε μικρή απόσταση. Πρέπει να λάβετε υπόψη την πηγή ενέργειας – όπως μπαταρία, ηλιακό στοιχείο ή πυκνωτή – μιας συσκευής και τον συνολικό κύκλο ζωής της. Ένας μακρύς και διαρκής κύκλος ζωής όχι μόνο θα προσφέρει μεγαλύτερη αξιοπιστία αλλά θα μειώσει το λειτουργικό κόστος. Ενδέχεται να ληφθούν μέτρα για την επίτευξη μεγαλύτερης διάρκειας ζωής του τροφοδοτικού. Για παράδειγμα, για να παρατείνετε τη διάρκεια ζωής της μπαταρίας, μπορείτε να θέσετε τη συσκευή σε κατάσταση αναστολής λειτουργίας όποτε είναι σε αδράνεια. Μια άλλη βέλτιστη πρακτική είναι να μοντελοποιήσετε την κατανάλωση ενέργειας της συσκευής κάτω από διαφορετικά φορτία και διαφορετικές συνθήκες δικτύου για να διασφαλίσετε ότι η χωρητικότητα τροφοδοσίας και αποθήκευσης της συσκευής ταιριάζει με την ισχύ που απαιτείται για τη μετάδοση των απαραίτητων δεδομένων χρησιμοποιώντας τις τεχνολογίες δικτύωσης που υιοθετήσατε. [16]

- Το Intermittent connectivity της κάθε συσκευής [16]:

Οι συσκευές IoT δεν είναι πάντα συνδεδεμένες. Σε ορισμένες περιπτώσεις, οι συσκευές έχουν σχεδιαστεί για να συνδέονται περιοδικά. Ωστόσο, μερικές φορές ένα αναξιόπιστο δίκτυο μπορεί να προκαλέσει την πτώση των συσκευών λόγω προβλημάτων συνδεσιμότητας. Μερικές φορές ζητήματα ποιότητας της υπηρεσίας, όπως η αντιμετώπιση παρεμβολών ή διαμάχης καναλιών σε ασύρματο δίκτυο χρησιμοποιώντας κοινό φάσμα. Τα σχέδια θα πρέπει να ενσωματώνουν διακοπτόμενη συνδεσιμότητα και να αναζητούν οποιεσδήποτε διαθέσιμες λύσεις για την παροχή αδιάλειπτης υπηρεσίας, εάν αυτό είναι κρίσιμος παράγοντας για το σχεδιασμό τοπίου IoT. [16]

- Το Interoperability της κάθε συσκευή [16]:

Οι συσκευές λειτουργούν με άλλες συσκευές, εξοπλισμό, συστήματα και τεχνολογία. είναι διαλειτουργικά. Με τόσες πολλές διαφορετικές συσκευές που συνδέονται στο IoT, η διαλειτουργικότητα μπορεί να είναι μια πρόκληση. Η υιοθέτηση τυπικών πρωτοκόλλων είναι μια παραδοσιακή προσέγγιση για τη διατήρηση της διαλειτουργικότητας στο Διαδίκτυο. Τα πρότυπα συμφωνούνται από τους συμμετέχοντες στον κλάδο και αποφεύγουν πολλαπλά διαφορετικά σχέδια και κατευθύνσεις. Με τα κατάλληλα πρότυπα και τους συμμετέχοντες που συμφωνούν με αυτά, μπορεί να αποφευχθούν ζητήματα ασυμβατότητας, επομένως ζητήματα διαλειτουργικότητας. [16]

- Την ασφάλεια της κάθε συσκευής [16]:

Η ασφάλεια είναι προτεραιότητα. Η επιλογή τεχνολογιών δικτύωσης που εφαρμόζουν ασφάλεια από άκρο σε άκρο, συμπεριλαμβανομένου του ελέγχου ταυτότητας, της κρυπτογράφησης και της προστασίας ανοιχτής θύρας είναι ζωτικής σημασίας. Το IEEE 802.15.4 περιλαμβάνει ένα μοντέλο ασφαλείας που παρέχει χαρακτηριστικά ασφαλείας που περιλαμβάνουν έλεγχο πρόσβασης, ακεραιότητα μηνύματος, εμπιστευτικότητα μηνυμάτων και προστασία επανάληψης, τα οποία υλοποιούνται από τεχνολογίες που βασίζονται σε αυτό το πρότυπο, όπως το ZigBee. [16]

- Το χρήστη που τα χρησιμοποιεί [8]:
  - Με αυτό το τρόπο μπορούμε εμείς να έχουμε μία γενικότερη κατανόηση των διαφόρων τομέων που υπάρχουν ήδη ή που θα υπάρξουν για τις συσκευές IoT στο μέλλον.
- Τα δεδομένα που τα ίδια συλλέγουν,χρησιμοποιούν ή επεξεργάζονται [21]:
  - Αν τα δεδομένα αυτά είναι πχ οικονομικής φύσεως δεδομένα, φυσικά δεδομένα (όπως θερμοκρασία, υγρασία κτλ.) κ.ο.κ.
- Και πολλές ακόμα κατηγοριοποιήσεις που μπορούν να προστεθούν σε αυτή τη λίστα

2.1.3 Η χρήση των IoT και παραδείγματα συσκευών

Προσπαθώντας να μην προτιμήσουμε συγκεκριμένα κάποιο ερευνητή και έτσι κάποια ειδική κατηγοριοποίηση, κρίνεται σημαντικό για αρχή να δοθεί έμφαση στις διάφορες κατηγορίες των συσκευών IoT καθώς κάθε μία από αυτές θα έχει διαφορετικές ικανότητες όσον αφορά το υλικό της (μνήμη RAM, επεξεργαστική ισχύς κτλ) και τη χρήση της (καταναλωτική - Consumer, βιομηχανική - Industrial, επιχειρησιακή - Enterprise). Επιλέγουμε λοιπόν την κατηγορία εκείνη η οποία θα μας επιτρέψει να συνεχίσουμε το κεφάλαιο αυτό προσθέτωντας όσο το δυνατόν περισσότερα παραδείγματα συσκευών για να κατανοήσουμε καλύτερα το εύρος των δικτύων IoT:

Η κατηγορία «**Consumer-Καταναλωτής**» αποτελείται από συσκευές, οι οποίες προορίζονται να χρησιμοποιηθούν από καταναλωτές και όχι από επαγγελματίες. [8]

Η «**Enterprise-Επιχείρηση**» περιγράφει την κατηγορία συσκευών που χρησιμοποιούνται από εταιρείες ή έχουν εγκατασταθεί/συναρμολογηθεί από επαγγελματική υπηρεσία. [8]

Η τελευταία κατηγορία «**Industrial-Βιομηχανία**» είναι συσκευές IoT για παραγωγή εντός μίας βιομηχανίας.[8]

Συνολικά, οι διαφορετικές περιοχές για κάθε κατηγορία κατανεμήθηκαν ως εξής [8]:

Consumer

- Smart Home devices
- Wearables
- Connected home automation and alarm systems

Enterprise

- Smart city devices
- Environment sensors (for big buildings or fields)
- Medical devices
- Vehicles (transportation)
- Sensors for bigger buildings
- Alarm systems (for business)

Industrial

- Machine sensors
- Machine control systems
- Industrial sensors

Οι παραπάνω κατάλογοι δεν είναι εξαντλητικοί, αλλά μπορούν να προσφέρουν μια καλή πρώτη εικόνα στις διάφορες κατηγορίες των συσκευών IoT που υπάρχουν και κυκλοφορούν στην αγορά. [8]

Συνεχίζουμε λοιπόν αναφέροντας κάποιες συγκεκριμένες συσκευές που ανήκουν στη κάθε μία από τις προαναφερθείσες κατηγορίες:

Για τη κατηγορία **Consumer** έχουμε:

- ★ Smart Home devices
    - Smart TVs
    - Smart lighting systems

    - Smart thermostats
    - Smart pet and lawn care
    - Smart kitchen appliances
- ★ Wearables
    - Fitness Trackers
    - ECG monitors
    - Smartwatches
    - Smart Jewelry
    - Body Sensors
    - Smart Clothing
    - Smart Headphones
- ★ Connected home automation and alarm systems
    - Smart door locks and garage door openers
    - Smart security cameras and systems
    - Smart household monitors

Για τη κατηγορία **Enterprise** έχουμε:

- ★ Smart city devices
    - Air quality monitoring
    - Smart transportation
    - Smart Roads
    - Waste Management
    - Smart grids
    - Surveillance Cameras
    - Smart Parking
- ★ Environment sensors (for big buildings or fields)
    - Temperature Sensors
    - Pressure Sensors
    - Humidity Sensors
    - Air quality Sensors
    - Motion Sensors
    - Light Sensors
- ★ Medical devices
    - Wearable ECG monitors
    - Connected inhalers
    - Blood glucose/pressure monitoring
    - Pulse oximeters
    - Implantable devices
    - Robotic Surgeon devices
    - Infusion and Insulin pumps
- ★ Vehicles (transportation)
    - Smart Cars
    - Smart Buses
    - Ένας γενικός όρος για ένα όχημα με προηγμένα ηλεκτρονικά. Οι μικροεπεξεργαστές χρησιμοποιούνται σε κινητήρες αυτοκινήτων από τα τέλη της δεκαετίας του 1960 και έχουν αυξηθεί σταθερά σε χρήση σε όλο τον κινητήρα και το σύστημα μετάδοσης κίνησης για να βελτιώσουν τη

σταθερότητα, το φρενάρισμα και τη γενική άνεση. Μπορεί να υπάρχουν εκατό ή περισσότεροι μικροεπεξεργαστές σε ένα αυτοκίνητο σήμερα και γενικότερα κάτω από τα Smart Vehicles εντάσσονται πολλά οχήματα τα οποία έχουν προηγμένες λειτουργίες και κυρίως μπορούν να επικοινωνήσουν με το ίντερνετ όπως αναφέραμε στον ορισμό του IoT στην αρχή της ενότητας

- ★ Sensors for bigger buildings
    - Τα ίδια με τα Environment Sensors μόνο που χρησιμοποιούνται για διαφορετικό σκοπό και συνήθως έχουν πιο προηγμένες λειτουργίες όσον αφορά την επεξεργαστική ισχύ τους ή την ακρίβεια του ίδιου του Sensor
- ★ Alarm systems (for business)
    - σειρήνα πολιτικής άμυνας, επίσης γνωστή ως σειρήνες ανεμοστρόβιλου ή σειρήνες αεροπορικής επιδρομής
    - συστήματα συναγερμού πυρκαγιάς
    - συναγερμός αυτόματης κλήσης, γνωστός και ως συναγερμός κοινότητας.

<u>Για τη κατηγορία **Industrial** έχουμε:</u>

- ★ Machine sensors
    - Pressure,Motion,Temperature,Chemical,Smoke,Infrared Light,Vibration and Proximity Sensors
    - Γυροσκόπιο
    - Environmental monitoring for space hygiene or quality of service for a given product
- ★ Machine control systems
    - Γενικά είναι αυτά τα συστήματα τα οποία μπορούν να ελεγχθούν από απόσταση
    - Smart Lighting System
    - Air Conditioning System
    - Air Quality System
    - Waste management System
    - Heat Controller System
- ★ Industrial sensors
    - Παρεμφερή με τα machine sensors, αλλά εξειδικευμένα για την εκάστοτε βιομηχανία και επεκτείνονται από επιταχυνσιόμετρα μέχρι και ανάλυση του αέρα ενός δωματίου για σκόνη όπως στις κατασκευές πυραύλων στη NASA/SpaceX κτλ ή στην αυτόματη μέτρηση του βάρους για ένα συγκεκριμένο προϊόν σε αλυσίδες παραγωγής κτλ.

2.2 5G-6G Networks and IoT

2.2.1. Η διαδρομή προς το 6G Networking και οι κύριες διαφορές με το 5G

Μέσα από την ανάπτυξη της έκτης γενιάς (6G) ασύρματης επικοινωνίας νέες ψηφιακές εγκληματολογικές προκλήσεις θα προκύψουν για μελλοντικά δίκτυα IoT με δυνατότητα 6G, ενώ την ίδια στιγμή κάποιες τεχνολογίες IoT είναι αδύνατο να λειτουργήσουν χωρίς την ικανότητα πρόσβασης σε μία δικτύωση ανώτερης γενιάς 6G-and-beyond. Θα γίνει έτσι εδώ μία σύντομη ανάλυση μεταξύ των 5G και 6G δικτύων υπογραμμίζοντας τις διαφορές τους, καθώς και τις κύριες τεχνολογίες που θα μπορούν να προκύψουν μέσα από

τα 6G δίκτυα στη συνέχεια ώστε να μπορέσουμε αργότερα να αναλύσουμε καλύτερα τα περιβάλλοντα 6G IoT Networks και τις νέες προκλήσεις που αυτά εισάγουν. [9]

Η ανάπτυξη της τεχνολογίας ασύρματης επικοινωνίας έκτης γενιάς (6G) αναμένεται να προσφέρει μετάδοση δεδομένων εξαιρετικά υψηλής ταχύτητας και προηγμένη απόδοση δικτύου από την τρέχουσα πέμπτη γενιά (5G) και να είναι πλήρως λειτουργική μέχρι τη δεκαετία του 2030. Αυτή η εξέλιξη θα έχει σημαντικό αντίκτυπο και θα προσθέσει βελτιώσεις στην ψηφιακή εκτεταμένη πραγματικότητα (XR), στα αυτόνομα συστήματα, στα δίκτυα ad hoc οχημάτων (VANETs), στην τεχνητή νοημοσύνη (AI), στις υποβρύχιες επικοινωνίες, στην τεχνολογία blockchain, στη διάχυτη βιοϊατρική πληροφορική και στις έξυπνες πόλεις του Διαδικτύου των Πραγμάτων (IoT). Η πανταχού παρούσα φύση αυτού του μεγάλης κλίμακας IoT με δυνατότητα 6G που προσφέρει ταχύτερες δυνατότητες συνδεσιμότητας και ενσωματώνει επίγεια και μη δίκτυα όχι μόνο θα δημιουργήσει νέα ζητήματα ασφάλειας δεδομένων και απορρήτου, αλλά θα προσφέρει επίσης έναν θησαυρό ψηφιακών αποδεικτικών στοιχείων χρήσιμων για τους ψηφιακούς ιατροδικαστές που διερευνούν περιστατικά ασφαλείας και εγκλήματος στον κυβερνοχώρο Ωστόσο, για τους ψηφιακούς ιατροδικαστές, η συλλογή, η διατήρηση και η ανάλυση αποδεικτικών στοιχείων θα αποτελέσουν προτεραιότητα στην επιτυχή ανάπτυξη των δικτύων IoT 6G. [9]

Η τεχνολογία ασύρματης επικοινωνίας πέμπτης γενιάς (5G) υπήρξε βασικός παράγοντας για τον πολλαπλασιασμό και την ανάπτυξη των εφαρμογών Διαδικτύου των Πραγμάτων (IoT) που έχει δει δισεκατομμύρια συσκευές να συνδέονται με τεχνολογίες ασύρματης επικοινωνίας. Σε σύγκριση με ασύρματες τεχνολογίες, όπως 2G/3G/4G, Wi-Fi, Bluetooth κ.λπ., το 5G προσφέρει βελτιωμένη καθυστέρηση, αποτελεσματικότητα φάσματος, αξιοπιστία και ρυθμό μετάδοσης μεταξύ 10 και 20 Gps που είναι 100 φορές υψηλότερος από το 4G . Χρειάστηκε επίσης η επικοινωνία που προηγουμένως περιοριζόταν μόνο στους ανθρώπους για την επικοινωνία μεταξύ ανθρώπων και αντικειμένων. Ωστόσο, το πλήρες δυναμικό των πολλά υποσχόμενων νέων υπηρεσιών IoT από την εκτεταμένη πραγματικότητα (XR), την τεχνητή νοημοσύνη (AI), τα αυτόνομα συστήματα και την τηλεϊατρική έως την υποβρύχια θαλάσσια επικοινωνία και τα ευφυή δίκτυα ad hoc οχημάτων (VANET) δεν μπορούν να υλοποιηθούν με το 5G. Αυτές οι υπηρεσίες βασίζονται κυρίως σε εξαιρετικά υψηλή αξιοπιστία, υψηλούς ρυθμούς δεδομένων, διαχείριση μη επανδρωμένης κινητικότητας και επικοινωνία μεγάλων αποστάσεων, γεγονός που εκθέτει τους περιορισμούς στις εγγενείς ιδιότητες του 5G. [9]

Αυτοί οι περιορισμοί γέννησαν την ανάπτυξη της ασύρματης επικοινωνίας δικτύου έκτης γενιάς (6G), η οποία στοχεύει στην παροχή βελτιώσεων απόδοσης που απαιτούνται από αυτές τις υπηρεσίες. Μια άλλη πτυχή του 6G είναι ότι θα δημιουργήσει ένα μεγάλης κλίμακας ετερογενές δίκτυο που θα ενσωματώνει επίγεια δίκτυα, διαστημικά δορυφορικά δίκτυα και θαλάσσια δίκτυα. Το 6G θα έχει υψηλό ρυθμό αιχμής μεταξύ 100 Gps και 1 Tbps, χαμηλή καθυστέρηση, έγκαιρη επεξεργασία 0,1 ms, απόδοση φάσματος περίπου 2-3 φορές καλύτερη από το 5G και συνολική απόδοση δικτύου 200 bit/J σε σύγκριση με 100 bit/ J που προσφέρεται από το τρέχον 5G. [9]

Αυτές οι απαιτήσεις υψηλής απόδοσης απαιτούνται επί του παρόντος για να ξεκλειδωθεί η κύρια υιοθέτηση της επαυξημένης/εικονικής πραγματικότητας (AR/VR), η τρισδιάστατη ολογραφική οθόνη, η τηλεϊατρική σε πραγματικό χρόνο, η αναβάθμιση της επανάστασης του κλάδου 4.0 και η κάλυψη των απαιτήσεων των αυτόνομων συστημάτων μεταφοράς . Το 6G θα επιτρέψει τον πολλαπλασιασμό και την επέκταση των συσκευών IoT που υποστηρίζονται από AI που θα βελτιώσουν την εμπειρία του τελικού χρήστη με αυξημένες αλληλεπιδράσεις ανθρώπου-αντικειμένου. Οι στατιστικές δείχνουν ότι η παγκόσμια αγορά 6G εκτιμάται ότι θα φτάσει τα 1773,09 δισεκατομμύρια δολάρια μέχρι το

2035 με την πλειονότητα των έξυπνων και IoT συσκευών να λειτουργούν σε δίκτυα 6G ή να θεωρούνται «έτοιμα» για το 6G. [9]

Υπάρχοντα ζητήματα ασφάλειας και προκλήσεις απορρήτου στα δίκτυα 5G, όπως ο έλεγχος ταυτότητας, ο έλεγχος πρόσβασης, η ακεραιότητα, η διαχείριση ταυτότητας, η εμπιστευτικότητα και η μη άρνηση έχουν επίσης εντοπιστεί στις αναδυόμενες τεχνολογίες 6G. Τα τρέχοντα δίκτυα 5G όχι μόνο έχουν αυξήσει την πανταχού παρουσία των συσκευών IoT, αλλά και την εμφάνιση κακόβουλου λογισμικού και botnet IoT. Ως εκ τούτου, η ικανότητα δικαστικής ανάλυσης συσκευών που έχουν μολυνθεί από κακόβουλο λογισμικό IoT είναι πολύ κρίσιμη στα δίκτυα 5G και πέρα από αυτό. [9]

Επιπλέον, νεότερες προκλήσεις εγκληματολογικής ανάλυσης θα προκύψουν επίσης στις τεχνολογίες αιχμής που ενεργοποιούνται από το 6G που περιλαμβάνουν ταχύτερες πανταχού παρούσες υπηρεσίες και εφαρμογές IoT, όπου διάφοροι αισθητήρες και δίκτυα που βασίζονται σε μεγάλα δεδομένα και βαθιά μάθηση διασυνδέονται σε πραγματικό και εικονικό περιβάλλον. Ως εκ τούτου, αυτή η αύξηση στη συνδεσιμότητα IoT όχι μόνο θα εκθέσει την επιφάνεια επικοινωνίας του δικτύου σε επιδείνωση των απειλών που παρατηρούνται αυτή τη στιγμή στα δίκτυα 5G, αλλά επίσης θα δημιουργήσει μια έξαρση σε διαδεδομένες και επίμονες επιθέσεις και συμβάντα που σχετίζονται με την ασφάλεια που απαιτούν διαφορετικές προσεγγίσεις ψηφιακής εγκληματολογικής έρευνας στα δίκτυα 6G. [9]

Καθώς περισσότερα συνδεδεμένα αντικείμενα και αυτόνομα συστήματα επικοινωνούν απρόσκοπτα μέσω αυξανόμενου εύρους ζώνης συστήματος και βελτιωμένης απόδοσης φάσματος που παρέχεται από δίκτυα 6G, η εγκληματολογική έρευνα και η απόκριση συμβάντος, καθώς και η απόδοση επίθεσης ή ελλείμματος, θα γίνουν πιο απαιτητικές σε αυτό το τεράστιο περιβάλλον δικτύου. Επιπλέον, η διερεύνηση του τεράστιου όγκου δεδομένων για πολύτιμα εγκληματολογικά αντικείμενα για την παροχή μιας ολοκληρωμένης ανάλυσης αποδεικτικών δεδομένων δεν είναι απλώς δύσκολη, αλλά θα γίνεται όλο και πιο δύσκολη και σχεδόν αδύνατη σε πλήρως κατανεμημένα αυτόνομα συστήματα, υποβρύχιες τοποθεσίες και εικονικά και XR περιβάλλοντα. Ως εκ τούτου, οι ιατροδικαστές και οι ανταποκριτές συμβάντων θα απαιτήσουν εξειδικευμένες μεθόδους, διαδικασίες και εργαλεία για τον εντοπισμό, τη συλλογή, τη διατήρηση και την ανάλυση αποδεικτικών δεδομένων σε μεγάλης κλίμακας ετερογενή περιβάλλοντα δικτύου 6G IoT. [9]

Κρίνεται έτσι σκόπιμο να επικεντρωθούμε στη συνέχεια στις κύριες τεχνολογίες κλειδιά που θα μπορούν να επιτύχουν ένα λειτουργικό δίκτυο 6G.

2.2.2. Some 5G and 6G Key Enabling Technologies

Ξεκινάμε κάνοντας μία σύντομη ανάλυση σε τεχνολογίες που θα παίξουν σημαντικό ρόλο στην ανάπτυξη και καθιέρωση των δικτύων 6G καθώς και τεχνολογίες αιχμής των ήδη υπάρχοντων δικτύων 5G και στη συνέχεια θα δούμε πως αυτές οι τεχνολογίες θα επιβάλουν συγκεκριμένες αλλαγές στο υλικό και στο λογισμικό που θα απαιτείται από τις συσκευές που θα υποστηρίζουν τη δικτύωση 6G καθώς και που αυτές θα είναι απαραίτητες. [9]

2.2.2.1 mURLLC for 6G and URLLC for 5G

Το Ultra Reliable Low Latency Communications - URLLC - είναι ένα βασικό χαρακτηριστικό του 5G που επιτρέπει την επικοινωνία υψηλής αξιοπιστίας και χαμηλής καθυστέρησης. Το Massive Ultra-Reliable and Low-Latency Communications (mURLLC), το οποίο ενσωματώνει το URLLC με μαζική πρόσβαση, αναδεικνύεται ως νέα και σημαντική κατηγορία υπηρεσιών στην επόμενη γενιά (6G) για ευαίσθητες στο χρόνο επισκεψεις (time-

sensitive traffic) και πρόσφατα έχει λάβει τεράστια ερευνητική προσοχή. Ωστόσο, η πραγματοποίηση αποτελεσματικών (efficient), περιορισμένων καθυστερήσεων (delay bounded) και αξιόπιστων (reliable) επικοινωνιών για έναν τεράστιο αριθμό συσκευών του χρήστη (User Equipment) στο mURLLC, είναι εξαιρετικά προκλητική καθώς πρέπει να λαμβάνει ταυτόχρονα υπόψη την καθυστέρηση, την αξιοπιστία και τις μαζικές απαιτήσεις πρόσβασης. [24]

2.2.2.2 NOMA

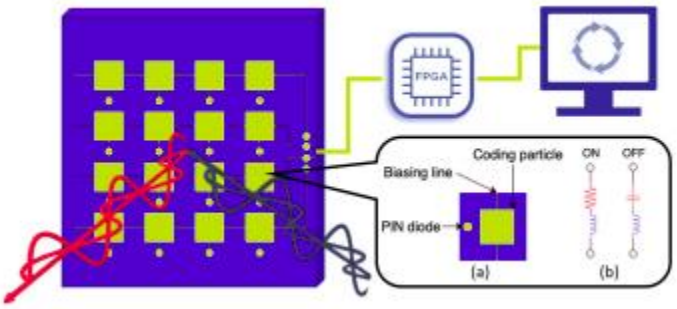
Τα συστήματα μη ορθογώνιας πολλαπλής πρόσβασης (NOMA) επιτρέπουν την εξυπηρέτηση χρηστών με το ίδιο μπλοκ πόρων, δηλαδή συχνότητα ή χρόνο, πολυπλέκωντας το σήμα των χρηστών. Έχουν λάβει μεγάλο ενδιαφέρον τα τελευταία χρόνια για τα κυψελωτά δίκτυα 5G, αλλά και νέες τεχνολογίες προσπαθούν να το προσαρμόσουν και για την επόμενη γενιά δικτύωσης 6G. Η ικανότητα του NOMA να εξυπηρετεί μεγάλο αριθμό χρηστών μοιράζοντας τους ίδιους πόρους χρόνου και συχνότητας είναι το κεντρικό κίνητρο πίσω από την υιοθέτησή του στο 5G βέβαια. Παρέχει υψηλή απόδοση συσκευής, υψηλή απόδοση μετάδοσης, αυξημένη κάλυψη, χαμηλή καθυστέρηση και τεράστια δικτύωση. [25]

Οι έξυπνες ανακλαστικές επιφάνειες (Intelligent reflecting surfaces - IRS) που θα αναλυθούν στη συνέχεια ή οι έξυπνες επιφάνειες με δυνατότητα επαναδιαμόρφωσης (RIS) είναι μια πιθανή προσέγγιση για την αύξηση της απόδοσης μετάδοσης βελτιώνοντας τη διάδοση του σήματος τροποποιώντας τυπικά παθητικά ανακλαστικά στοιχεία για τη τεχνολογία 6G και την υιοθέτηση του NOMA σε αυτό το τρόπο δικτύωσης 6G. [25]

2.2.2.3 RIS - IRS

Οι έξυπνες επιφάνειες με δυνατότητα επαναδιαμόρφωσης (RIS) ή οι έξυπνες ανακλαστικές επιφάνειες (IRS), θεωρούνται ως μία από τις πιο υποσχόμενες και επαναστατικές τεχνικές για τη βελτίωση του φάσματος ή/και της ενεργειακής απόδοσης των ασύρματων συστημάτων. Σημειώνουμε εδώ ότι το RIS και το IRS υποδηλώνουν την ίδια τεχνολογία και δεν έχει οριστεί ακόμα ένα σαφές όνομα για αυτήν. Αυτές οι συσκευές είναι σε θέση να αναδιαμορφώσουν το περιβάλλον ασύρματης διάδοσης ρυθμίζοντας προσεκτικά τις μετατοπίσεις φάσης ενός μεγάλου αριθμού παθητικών ανακλαστικών στοιχείων χαμηλού κόστους. [10]

Ένα RIS είναι μια επίπεδη επιφάνεια που αποτελείται από μια σειρά παθητικών ανακλαστικών στοιχείων, καθένα από τα οποία μπορεί ανεξάρτητα να επιβάλει την απαιτούμενη μετατόπιση φάσης στο εισερχόμενο σήμα. Με βάση τα συγκεκριμένα υλικά των ανακλαστικών στοιχείων, το RIS μπορεί να ταξινομηθεί σε δομές που βασίζονται σε διάταξη κεραίας και σε δομές με βάση μία μετα-επιφάνεια. Προσαρμόζοντας προσεκτικά τις μετατοπίσεις φάσης όλων των ανακλώσιμων στοιχείων, τα ανακλώμενα σήματα μπορούν να διαμορφωθούν εκ νέου ώστε να διαδίδονται προς τις επιθυμητές κατευθύνσεις τους. Λόγω των ραγδαίων εξελίξεων στα μεταϋλικά, ο συντελεστής ανάκλασης κάθε στοιχείου μπορεί να διαμορφωθεί εκ νέου σε πραγματικό χρόνο για να προσαρμοστεί στο δυναμικά κυμαινόμενο περιβάλλον ασύρματης διάδοσης. Ένα σύστημα RIS μπορεί να φανεί στο ακόλουθο σχήμα [10]:



[10]

Σχήμα 4: ένα σύστημα RIS

2.2.2.4 mmWave

Το mmWave αναφέρεται συγκεκριμένα στο ραδιοφάσμα μεταξύ 24 GHz και 100 GHz. Αυτή η περιοχή αναφέρεται ως 5G υψηλής ζώνης και χρησιμοποιείται καλύτερα σε πυκνοκατοικημένες περιοχές. Αυτή είναι μια σημαντική διάκριση επειδή το φάσμα 5G δεν δημιουργείται όλο εξίσου. Για παράδειγμα, τα σήματα 5G χαμηλής ζώνης έχουν σχεδιαστεί για επικοινωνία μεγάλων αποστάσεων, ενώ το 5G υψηλής ζώνης είναι το καλύτερο για εφαρμογές μικρής εμβέλειας και υψηλής απόδοσης. Η μεσαία ζώνη πέφτει κάπου στη μέση, εξισορροπώντας το εύρος και την απόδοση. Οι οργανισμοί συχνά χρησιμοποιούν και τις τρεις ζώνες στο δίκτυό τους για την επίτευξη συγκεκριμένων επιχειρηματικών στόχων. [26]

Βέβαια η επικοινωνία κυμάτων χιλιοστών (mmWave), που αρχικά οραματιζόταν ως μία από τις τρεις βασικές τεχνολογίες στα δίκτυα 5G, δεν έχει υιοθετηθεί ευρέως. Συγκεκριμένα μέχρι στιγμής βλέπουμε ότι έχει χρησιμοποιηθεί και αναπτυχθεί πρακτικά κυρίως το φάσμα μεταξύ 26 GHz έως και 39 GHz. Τα βασικά εμπόδια της επικοινωνίας mmWave περιλαμβάνουν την ευαισθησία του σε μπλοκαρίσματα, την περιορισμένη κάλυψη και τη σοβαρή απώλεια διαδρομής. Ωστόσο, ορισμένες καινοτόμες εφαρμογές, όπως η καθηλωτική εικονική πραγματικότητα, οι ολογραφικές προβολές υψηλής πιστότητας, τα ψηφιακά δίδυμα, η συνδεδεμένη ρομποτική μέσω αυτόνομων συστημάτων, το βιομηχανικό διαδίκτυο των πραγμάτων (Industrial IoT), το ευφυές σύστημα μεταφοράς και οι διεπαφές υπολογιστών εγκεφάλου, αναμένεται να υποστηρίζονται από επικοινωνίες 6G-and-beyond . Αυτές οι εφαρμογές συνεπάγονται απαιτήσεις υψηλής ποιότητας υπηρεσίας (QoS), όπως εξαιρετικά υψηλοί ρυθμοί δεδομένων, εξαιρετικά υψηλή αξιοπιστία και εξαιρετικά χαμηλή καθυστέρηση, οι οποίες δεν μπορούν να υποστηριχθούν εύκολα από τα υπάρχοντα συστήματα. [26]

Λόγω των προαναφερθέντων ζητημάτων υιοθέτησης του mmWave στην ήδη υπάρχον τεχνολογία 5G δεν γνωρίζουμε ακόμα πόσο σημαντικός θα είναι ο ρόλος του στην καθιέρωση του 6G λόγω της έλλειψης του φάσματος που έχει χρησιμοποιηθεί μέχρι στιγμής. [26]

2.2.2.5 VLC

Δεδομένου ότι οι πόροι φάσματος κάτω από 6 GHz έχουν εξαντληθεί και οι ζώνες συχνοτήτων κυμάτων χιλιοστών (mmWave) όπως τα 26 GHz μέχρι τα 39 GHz έχουν ήδη χρησιμοποιηθεί για τη χρήση 5G, είναι απαραίτητο να διερευνηθούν ζώνες υψηλότερης συχνότητας για επικοινωνία, όπως η επικοινωνία terahertz και η επικοινωνία ορατού φωτός (VLC) για να καλυφθούν οι απαιτήσεις υψηλότερης χωρητικότητας και εξαιρετικά υψηλού

ποσοστού εμπειρίας. Το ορατό φως αναφέρεται συνήθως σε ηλεκτρομαγνητικά κύματα 380~790THz (το εύρος μήκους κύματος είναι 380~790nm). Το υποψήφιο φάσμα καλύπτει περίπου 400 THz. Τα χαρακτηριστικά του μεγάλου εύρους ζώνης και της εύκολης πραγματοποίησης της επικοινωνίας εξαιρετικά υψηλής ταχύτητας κάνουν το VLC να γίνει ένα πιθανό συμπλήρωμα στα μελλοντικά συστήματα επικοινωνίας κινητών.[31]

2.2.2.6 OWC

Το Optical Wireless Communications (OWC) πρόκειται για ασύρματες επικοινωνίες που χρησιμοποιούν το οπτικό φάσμα, συμπεριλαμβανομένου του υπέρυθρου, του ορατού φωτός και του υπεριώδους, ως μέσο μετάδοσης. Τα συστήματα OWC χρησιμοποιούν ορατό φως για να μεταφέρουν πληροφορίες, κοινώς αναφερόμενες ως Επικοινωνίες Ορατού Φωτός, οι οποίες έχουν προσελκύσει μεγάλη προσοχή τα τελευταία χρόνια. [27]

2.2.2.7 IR

Η υπέρυθρη ακτινοβολία (IR), επίσης γνωστή ως θερμική ακτινοβολία, είναι αυτή η ζώνη στο φάσμα της ηλεκτρομαγνητικής ακτινοβολίας με μήκη κύματος πάνω από το κόκκινο ορατό φως μεταξύ 780 nm και 1 mm.

2.2.2.8 UV

Η περιοχή UV καλύπτει το εύρος μήκους κύματος 100-400 nm και χωρίζεται σε τρεις ζώνες: UVA (315-400 nm), UVB (280-315 nm) και UVC (100–280 nm).

2.2.2.9 OCC

Η Optical Camera Communication (OCC) είναι μια πρόσφατη τεχνολογία με υψηλές δυνατότητες ταχείας εφαρμογής στην κοινωνία. Αυτή η τεχνολογία τυποποιήθηκε ως μέρος της τεχνολογίας Visible Light Communication (VLC). Αυτό που διαφοροποιεί το OCC από το VLC είναι ότι στην πρώτη, ο δέκτης δεν βασίζεται σε διακριτές φωτοδιόδους, αλλά σε αισθητήρες εικόνας, που συνήθως απαντώνται σε όλα τα σύγχρονα smartphone. Δεδομένου ότι υπάρχει μια ιλιγγιώδης αύξηση της διείσδυσης στην αγορά αυτών των συσκευών για τα επόμενα χρόνια, η τεχνολογία OCC είναι ιδιαίτερα ελκυστική και με αρκετές εφαρμογές που έχουν ήδη προβλεφθεί ή δοκιμαστεί, όπως οι επικοινωνίες οχημάτων, η τοποθέτηση και η οριοθέτηση εσωτερικών χώρων, η μετάδοση και η ψηφιακή σήμανση μεταξύ άλλων. Το OCC, και το VLC στο σύνολό του, θεωρούνται πιθανές τεχνολογίες της έκτης γενιάς (6G) ασύρματων επικοινωνιών. [28]

Τα συστήματα OCC μπορούν γενικά να ταξινομηθούν σύμφωνα με τον αριθμό των στοιχείων σε κάθε άκρο της ζεύξης επικοινωνίας. Από την πλευρά της πηγής, η κατηγορία Screen-to-Camera (S2C), που ονομάζεται επίσης και display-camera ή screen-camera, προβλέπει τη χρήση εκατοντάδων ή χιλιάδων LED ως πομπών. Αυτή η τεχνολογία έχει επομένως τεράστιες δυνατότητες εφαρμογής, καθώς ο αριθμός των εμπορικών οθονών LED έχει αυξηθεί ακόμη πιο γρήγορα από τον αριθμό των smartphone, λόγω της ανάπτυξης της αγοράς αυτών των συσκευών, των ψηφιακών πινακίδων και των σύγχρονων ηλεκτρονικών ειδών ευρείας κατανάλωσης. [28]

2.2.2.10 FSO

Το FSO (free space optics) είναι μια τεχνολογία οπτικής επικοινωνίας στην οποία τα δεδομένα μεταδίδονται με διάδοση φωτός στον ελεύθερο χώρο επιτρέποντας οπτική συνδεσιμότητα. Δεν απαιτείται καλώδιο οπτικών ινών. Η λειτουργία του FSO είναι παρόμοια

με τα δίκτυα OFC (Optical Fiber Cable), αλλά η μόνη διαφορά είναι ότι οι οπτικές δέσμες αποστέλλονται μέσω ελεύθερου αέρα αντί των πυρήνων OFC που είναι γυάλινες ίνες. Το σύστημα FSO αποτελείται από έναν οπτικό πομποδέκτη και στα δύο άκρα για να παρέχει δυνατότητα πλήρους διπλής όψης (αμφίδρομη). Η επικοινωνία FSO δεν είναι νέα τεχνολογία. Υπήρχε από τον 8ο αιώνα αλλά τώρα είναι πιο εξελιγμένο. Το FSO είναι μια τεχνολογία LOS (line of sight), όπου η επικοινωνία δεδομένων, φωνής και βίντεο επιτυγχάνεται με μέγιστο ρυθμό μετάδοσης δεδομένων 10 Gbps μέσω πλήρους αμφίδρομης (αμφίδρομης) συνδεσιμότητας.[29]

2.2.2.11 Li-Fi

Ήδη δημοφιλές στο Ηνωμένο Βασίλειο και σε άλλες ευρωπαϊκές χώρες, το Li-Fi είναι ένα σύστημα Επικοινωνιών Ορατού Φωτός (VLC). Το Li-Fi σημαίνει Light Fidelity. Η επικοινωνία Li-Fi μπορεί να μεταδίδει δεδομένα ασύρματα σε απίστευτα υψηλές ταχύτητες. Λειτουργώντας ως ένα είδος φωτός κώδικα Μορς, η τεχνολογία Li-Fi χρησιμοποιεί λαμπτήρες LED για να εκπέμπει σύντομες εκρήξεις φωτός που μεταφέρουν δεδομένα ασύρματα σε δέκτες που συλλέγουν και επεξεργάζονται τα δεδομένα. [30]

Ενώ οι εκπομπές Li-Fi είναι μη ανιχνεύσιμες στο ανθρώπινο μάτι, το VLC εκμεταλλεύεται πλήρως το ευρύτερο φάσμα συχνοτήτων του ορατού φωτός. Η τεχνολογία αμφίδρομης μετάδοσης του Li-Fi το καθιστά ικανό να μεταφέρει ταχύτητες έως και 224 Gbps. [30]

2.2.3 Wireless network communication and performance technologies

Για να ενεργοποιηθούν και να ενσωματωθούν γεω-ασύρματες κινητές επικοινωνίες, ειδικά επίγεια, διαστημικά και υποβρύχια αυτόνομα δίκτυα, το 6G θα πρέπει να παρέχει πλήρη ασύρματη κάλυψη και ασύρματη συνδεσιμότητα εξαιρετικά μεγάλων αποστάσεων με καθυστέρηση μικρότερη από 1 ms. Το 6G θα χρειαστεί να υποστηρίζει μαζικές εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης (mURLLC) σε ακραία ή έκτακτα συμβάντα με χωρικά και χρονικά μεταβαλλόμενες πυκνότητες συσκευών, μοτίβα κυκλοφορίας, φάσμα και διαθεσιμότητα υποδομής. Αυτό περιλαμβάνει πολλά υποσχόμενες λύσεις στο τρέχον φάσμα επικοινωνίας από τις οποίες θα επωφεληθεί το 6G. Έχει προταθεί η χρήση πλήρους αμφίδρομης επικοινωνίας (full duplex) που βασίζονται σε THz (Terahertz) για τη διασφάλιση αξιοπιστίας και υψηλής φασματικής απόδοσης. Αυτή η χρήση ενός εύρους ζώνης ευρέος φάσματος επιτρέπει κανάλια ευρείας ζώνης, χαμηλή καθυστέρηση, εξαιρετικά υψηλό εύρος ζώνης και υποστήριξη μεταφοράς δεδομένων με πολύ υψηλή ταχύτητα. [9]

Άλλες αναγνωρισμένες τεχνολογίες ενεργοποίησης κλειδιών περιλαμβάνουν τη χρήση και την εφαρμογή κωδικοποίησης καναλιών, προσωρινής αποθήκευσης άκρων, μη ορθογώνιας πολλαπλής πρόσβασης (NOMA) στο πλαίσιο επικοινωνίας χιλιοστών κυμάτων (mmWave) και οπτικών Συστημάτων ασύρματης επικοινωνίας (OWC), όπως η επικοινωνία ορατού φωτός (VLC), η υπέρυθρη ακτινοβολία (IR) ή τα φάσματα υπεριώδους (UV). Τα εξαιρετικά χαρακτηριστικά του OWC το καθιστούν μια πολλά υποσχόμενη συμπληρωματική επιλογή των συστημάτων ασύρματης επικοινωνίας που βασίζονται σε ραδιοσυχνότητες (RF) και ως εκ τούτου έχει αναγνωριστεί ως τεχνολογία που επιτρέπει μελλοντικές επικοινωνίες δικτύου 6G. Μία από τις πιο υποσχόμενες τεχνολογίες OWC περιλαμβάνει οπτική επικοινωνία κάμερας (OCC), οπτική επικοινωνία ελεύθερου χώρου (FSO) και VLC. Το VLC διαδίδει τη μεταφορά δεδομένων μέσω δέσμης ορατού φωτός, μπορεί να προσφέρει υψηλή

ταχύτητα εσωτερικού χώρου, εγγυάται το απόρρητο και την ασφάλεια της μετάδοσης και ως εκ τούτου μπορεί να αναπτυχθεί σε ένα ευρύ φάσμα του φάσματος. Τα VLC διαθέτουν την ικανότητα να παρέχουν φωτισμό και ασύρματη ευρυζωνική επικοινωνία ταυτόχρονα. Πολλές ερευνητικές πλατφόρμες όπως το OpenVLC έχουν επίσης αναπτυχθεί για να επιταχύνουν την εφαρμογή και την επικύρωση των σχεδίων VLC . Η επιτυχής ανάπτυξή του έχει ήδη επιτευχθεί στη ροή βίντεο HD υψηλής ποιότητας και στην εφαρμογή σε πιστότητα φωτός (Li-Fi). Το Li-Fi κρίνεται ισχυρά ότι είναι πιο κατάλληλο για υποβρύχια επικοινωνία, επειδή τα ραδιοκύματα δεν μπορούν να χρησιμοποιηθούν υποβρύχια, καθώς τα κύματα απορροφώνται έντονα από το νερό μέσα σε λίγα πόδια από τη μετάδοση. [9]

Επιπλέον, το 6G θα περιλαμβάνει την εφαρμογή λύσεων βαθιάς μάθησης και μηχανικής μάθησης (ML) για την επίτευξη μέγιστης βελτιστοποίησης δικτύου . Η χρήση της βαθιάς μάθησης και της μηχανικής μάθησης, η ευφυΐα αιχμής και οι αναδιαμορφώσιμες έξυπνες επιφάνειες (RIS) θα βοηθήσουν στη διατήρηση της αυξημένης απόδοσης ως εγγενή προβλήματα στα ασύρματα δίκτυα. Τα τρέχοντα προβλήματα επικοινωνίας ασύρματου δικτύου που επιλύονται με την εφαρμογή συνόλων κανόνων που προκύπτουν από την ανάλυση συστήματος δεν θα ισχύουν πλέον. Η εφαρμογή εκτίμησης και ανίχνευσης καναλιών πολλαπλής εισόδου και πολλαπλών εξόδων (MIMO), ευφυής κοινή χρήση φάσματος , σπονδυλωτή αναγνώριση, αποκωδικοποίηση καναλιών έχει προταθεί για τη βελτίωση της κατάστασης της απόδοσης του δικτύου σε αρχιτεκτονικές 6G. [9]

2.2.4. Transceiver and antenna technologies

Για την παροχή αξιόπιστης απόδοσης ασύρματης επικοινωνίας δικτύου στα προτεινόμενα δίκτυα 6G, οι νέοι πομποί, πομποδέκτες και κεραίες και οι εξελίξεις για την επικοινωνία THz είναι ζωτικής σημασίας και ειδικά ο σχεδιασμός και η ανάπτυξη κεραιών μεγάλης κλίμακας που θα βελτιώσουν την αποδοτικότητα του φάσματος των ασύρματων συστημάτων κινητής επικοινωνίας. Πρέπει έτσι να σχεδιαστούν και να αναπτυχθούν συνδυασμένες συσκευές που βασίζονται σε ηλεκτρονικά και φωτονικά μέσα που μπορούν να φιλοξενήσουν ασύρματα τη μετάδοση και την παράδοση δεδομένων υψηλής ταχύτητας μέσω τεχνολογιών όπως αναλύθηκαν την αμέσως προηγούμενη ενότητα εποπτικά. Εναλλακτικά, απαιτούνται ολοκληρωμένα υβριδικά συστήματα πομποδεκτών που μπορούν να αξιοποιήσουν και να χρησιμοποιήσουν σταθμούς βάσης πολλαπλών λειτουργιών σε διάφορες συχνότητες, συμπεριλαμβανομένων των φασμάτων μικροκυμάτων, mmWave και THz. Επιπλέον, θα απαιτηθεί η ανάπτυξη πολυτροπικών μικρο-LED πομπών για την υποστήριξη υψηλής ταχύτητας VLC και OWC. [9]

Τα δίκτυα 6G θα επεκταθούν επίσης πέρα από την τρέχουσα πρόσβαση και αποθήκευση δεδομένων 5G από τα κέντρα δεδομένων στην άκρη μέσω της χρήσης τόσο κινητών σταθμών βάσης όσο και σταθερών σταθμών βάσης για την εξυπηρέτηση κέντρων λειτουργίας δικτύου για επίγεια διαστημικά-υποβρύχια δίκτυα. Καθώς ένας μεγάλος όγκος δεδομένων δημιουργείται, μεταδίδεται και μοιράζεται σε πραγματικό χρόνο, θα χρειαστεί επιπρόσθετη πρόσβαση σε εικονικά δίκτυα στο cloud για να επεκταθούν οι δυνατότητες των δικτύων παράδοσης περιεχομένου (CDN) μέσα από τη χρήση υποβρύχιων σταθμών βάσης, από επανδρωμένα εναέρια οχήματα (UAV) και από εναέριους δορυφόρους για δίκτυα 6G. Η απρόσκοπτη ενοποίηση τόσο των κινητών όσο και των σταθερών σταθμών βάσης που αποτελείται από αρχιτεκτονικές δορυφορικών επικοινωνιών και συστημάτων επικοινωνίας

που βασίζονται σε UAV/drone/balloons και υποβρύχια ακουστική, οπτική και ραδιοσυχνοτική επικοινωνία έχουν ήδη εντοπιστεί και κρίνονται ένα απαραίτητο βήμα. Λόγω των ισχυρών συνδέσεων οπτικής επαφής, της κινητικότητας, της ευελιξίας και της ικανότητας παροχής υποστήριξης σε περιοχές όπου οι κυψελωτοί σταθμοί βάσης απουσιάζουν ή δεν λειτουργούν, η χρήση UAV και συστημάτων που βασίζονται σε drone/balloons έχουν θεωρηθεί ζωτικής σημασίας για τις μελλοντικές αρχιτεκτονικές 6G. [9]

2.2.5 Data processing and storage technologies

Τα τρέχοντα δίκτυα 5G IoT χρησιμοποιούν υπολογιστικό νέφος και υποδομές κεντρικής αποθήκευσης δεδομένων για την επεξεργασία και την αποθήκευση τεράστιων δεδομένων IoT. Με το 6G, οι αιχμές και οι κατανεμημένοι υπολογιστές θα γίνουν κυρίαρχες τεχνολογίες για να επιτρέψουν την αποτελεσματική κινητικότητα δεδομένων, επεκτασιμότητα, πρόσβαση και διανομή. Έχουν προταθεί τεχνολογίες χαμηλής κατανάλωσης ενέργειας και ασφαλούς αποθήκευσης δεδομένων που εφαρμόζουν τη χρήση αποκεντρωμένων, χωρίς διακομιστή και αξιόπιστων λύσεων υποδομής για την επεξεργασία και αποθήκευση δεδομένων σε δίκτυα IoT 6G. [9]

Το παραδοσιακό όριο πελάτη-διακομιστή θα εξαλειφθεί και κάθε κόμβος δικτύου (συμπεριλαμβανομένων διαφόρων τερματικών, σταθμών βάσης, πυλών, δρομολογητών, διακομιστών κ.λπ.) θα λειτουργεί όχι μόνο ως εκδότης πληροφοριών αλλά και ως καταναλωτής πληροφοριών. Η αποθήκευση δεδομένων θα επεκταθεί από τις παραδοσιακές υποδομές cloud σε δίκτυα αιχμής και πανταχού παρούσες τελικές συσκευές για μείωση του λανθάνοντος χρόνου και βελτίωση της αξιοπιστίας εξαλείφοντας τη γεωγραφική απόσταση. Οι διακομιστές υπολογιστών Edge θα γίνουν μια κοινή υποδομή που χρησιμοποιείται για την επεξεργασία δεδομένων που δημιουργούνται από συσκευές δικτύου 6G IoT, μειώνοντας έτσι την υπερφόρτωση και την καθυστέρηση δεδομένων. Έχει επίσης προταθεί η χρήση βάσεων δεδομένων εκτός αλυσίδας που χρησιμοποιούν τις εγγενείς ιδιότητες του blockchain. Σε μία εργασία μάλιστα παρουσιάστηκε η χρήση UAV που μπορούν να επικοινωνούν με ασφάλεια χρησιμοποιώντας blockchain μεταξύ τους και με τους διακομιστές επίγειων σταθμών στο λεγόμενο δίκτυο edge. [9]

2.3 IoT Networks

Στο παρόν κεφάλαιο θα προσπαθήσουμε να κάνουμε μία εισαγωγή στην ετερογένεια των δικτύων IoT δίνοντας σαφή παραδείγματα τόσο για το τρόπο λειτουργίας συγκεκριμένων δικτύων τα οποία θα εμπεριέχονται στην ευρύ ορολογία του Internet of Things, όσο και συγκεκριμένες προκλήσεις εγκληματολογικού ενδιαφέροντος οι οποίες θα προκύψουν μέσα σε κάθε ένα από τα δίκτυα αυτά. Θα προσπαθήσουμε επίσης να εξηγήσουμε όπου αυτό είναι εφικτό τις διαφορές μεταξύ των παρόντων δικτύων 5G και των μελλοντικών αντίστοιχων δικτύων 6G όπως είναι σε δίκτυα IoT Smart Homes ή/και IoT Wearables και αντίστοιχα θα κάνουμε μία ανάλυση μελλοντικών δικτύων 6G που θα μπορούν να υπάρχουν μόνο μέσω της επέκτασης μας ως προς το 6G για δίκτυα IoT όπως είναι τα Smart Factories και οι κόσμοι XR/VR/AR.

2.3.1 Smart Cities

Μια έξυπνη πόλη είναι μια αστική περιοχή όπου η τεχνολογία και η συλλογή δεδομένων συμβάλλουν στη βελτίωση της ποιότητας ζωής καθώς και στη βιωσιμότητα και την αποτελεσματικότητα των λειτουργιών της πόλης. Οι τεχνολογίες έξυπνων πόλεων που χρησιμοποιούνται από τις τοπικές κυβερνήσεις περιλαμβάνουν τις τεχνολογίες πληροφοριών και επικοινωνιών (ΤΠΕ) και το Διαδίκτυο των Πραγμάτων (IoT).[32]

2.3.1.1 Smart Cities (Smart Vehicles and Drones)

2.3.1.1.1 From Drones to UAV's

Οι συγγραφείς αναγνωρίζουν επιπλέον μια άλλη τρέχουσα τάση στον αναπτυσσόμενο τομέα IoT, δηλαδή τα Unmanned Aerial Vehicles(**UAV**). Γνωστά ως drones για τα δίκτυα 5G, τα UAV (τα οποία είναι 6G enabled) έχουν αιχμαλωτίσει το κοινό ενδιαφέρον. Ορισμένες από τις κορυφαίες εταιρείες logistics, όπως η DHL, η Amazon και η UPS, ξεκίνησαν νέες υπηρεσίες παράδοσης που βασίζονται σε UAV. Χρησιμοποιώντας τεχνολογία drone, αυτές οι εταιρείες logistics ελπίζουν να φέρουν επανάσταση στην παράδοση του πρώτου και του τελευταίου μιλίου σε μεγάλες πόλεις και αγροτικές περιοχές. Δεδομένου ότι οι πρόσφατες εξελίξεις έκαναν τα μοντέλα drones (τα οποία ακόμα ουσιαστικά δεν είναι εμπορικές συσκευές) εύκολα προσιτά, οι πωλήσεις και οι εγγραφές αυξάνονται συνεχώς. Σύμφωνα με μια πρόσφατη πρόβλεψη, η παγκόσμια αγορά drones αναμένεται να φτάσει σε αξία 43 δισεκατομμυρίων δολαρίων μέχρι το τέλος του 2024.[1]

Μεταξύ άλλων κρίσιμων εφαρμογών, τα UAV χρησιμοποιούνται για την εκτέλεση εργασιών όπου ο χρόνος και το κόστος πρέπει να μειωθούν στο ελάχιστο. Σε περίπτωση ακραίων καταστάσεων, για παράδειγμα μετά από καταστροφή τυφώνα,ερευνητές προτείνουν τη χρήση drones για την εγκατάσταση σταθμών βάσης και την παροχή κυψελοειδούς κάλυψης στη δεδομένη περιοχή που βρίσκεται σε κίνδυνο. Η ίδια τεχνική θα μπορούσε επίσης να εφαρμοστεί σε πυκνοκατοικημένες αστικές περιοχές (π.χ. στάδια), προκειμένου να μεγιστοποιηθεί η κάλυψη 5G με σχετικά φθηνό τρόπο.[1]

2.3.1.1.2. Smart Vehicles (AAV's)

Αναμφίβολα, ένα από τα εμπορικά σήματα της έξυπνης πόλης είναι τα έξυπνα συστήματα μεταφοράς της, πιο συγκεκριμένα τα λεγόμενα Autonomous Automated Vehicles(**AAV**). Εξοπλισμένα με αισθητήρες για επικοινωνία όχημα με όχημα (V2V) και όχημα με υποδομή (V2I), τα έξυπνα αυτοκίνητα και τα λεωφορεία μπορούν να παρέχουν τις απαραίτητες πληροφορίες σε επιβάτες, οδηγούς ή φορείς για αποτελεσματική και ασφαλή κυκλοφορία στην πόλη. Ορισμένοι από τους σύγχρονους κατασκευαστές αυτοκινήτων, όπως η Tesla, η BMW, η Mercedes και η Daimler, έχουν ήδη κυκλοφορήσει οχήματα με χαρακτηριστικά αυτόνομης οδήγησης. Οι εταιρείες τεχνολογίας όπως η Google και η Uber έχουν επίσης επιδείξει πρωτότυπα αυτόνομης οδήγησης σε πραγματικούς δρόμους. Σύμφωνα με τον πάροχο επιχειρηματικών πληροφοριών IHS Markit, έως το 2035, θα υπάρχουν σχεδόν 11,8 εκατομμύρια συνδεδεμένα οχήματα που θα προσφέρουν αυτοματοποιημένη υποστήριξη οδήγησης και άλλες σύγχρονες υπηρεσίες εντός του οχήματος.[1]

2.3.1.2 6G Smart Cities (Vanet’s, UAV’s and Satellite IoT’s)

2.3.1.2.1. Vanet’s

Καθώς οι παγκόσμιες επιχειρήσεις, κυβερνητικοί εκπρόσωποι και οργανισμοί δεσμεύονται για την ταχεία επιτάχυνση και τη μετάβαση σε οχήματα μηδενικών εκπομπών άνθρακα έως το 2035, ο στόχος της ανάπτυξης ασφαλών και πλήρως αυτόνομων οχημάτων έχει επίσης επιταχυνθεί παράλληλα. Τα τρέχοντα επίγεια ασύρματα δίκτυα δεν είναι σε θέση να ανταποκριθούν στις απαιτήσεις των μελλοντικών VANET (Vehicular ad hoc network ή αλλιώς V2V - Vehicle to Vehicle, τα οποία είναι 6G enabled) και θα απαιτήσουν τόσο εναέρια όσο και διαστημικά δορυφορικά δίκτυα να αντισταθμίσουν για την επίτευξη απρόσκοπτης επικοινωνίας αυτόνομων οχημάτων οπουδήποτε στον πλανήτη. Τα υπάρχοντα ασύρματα δίκτυα, συμπεριλαμβανομένης της τεχνολογίας που βασίζεται σε RF και του 5G, υφίστανται απώλεια επικοινωνίας και πακέτων δεδομένων λόγω ελλείψεων που προκαλούνται από την αύξηση του αριθμού των οχημάτων, την υψηλή κινητικότητα και τον μεγάλο όγκο κίνησης δικτύου που δημιουργείται και διασκορπίζεται στην επικοινωνία όχημα με όχημα (V2V). Ωστόσο, η τρέχουσα τεχνολογία 5G δεν περιλαμβάνει το VLC ως ολοκληρωμένη τεχνολογία για VANET και το 6G προβλέπεται να συμπεριλάβει και να ενσωματώσει το VLC ως τεχνολογία ενεργοποίησης για τις επικοινωνίες οχημάτων. [9]

Ως εκ τούτου, για την υποστήριξη των ευφυών VANET και της ασφάλειας των αυτόνομων οχημάτων, η αύξηση της αξιοπιστίας και η χαμηλή καθυστέρηση της επικοινωνίας V2V μπορούν να καλυφθούν μόνο από τις εγγενείς ιδιότητες και την υποδομή ανάπτυξης των δικτύων 6G. Η τεχνολογία 6G σε συνδυασμό με την εφαρμογή της βαθιάς μάθησης, την επικοινωνία υψηλής ταχύτητας OWC, THz και τη βελτιστοποίηση μέσω δικτύου χρησιμοποιώντας αλγόριθμους μηχανικής μάθησης παρέχουν μια βιώσιμη λύση για την επίλυση των τρεχουσών ανεπάρκειων επικοινωνίας δικτύου στα VANET. [9]

2.3.1.2.2. UAV’s

Επιπλέον αρκετές πρόσφατες μελέτες έχουν διερευνήσει την εφαρμογή του 6G για UAV. Οι μελέτες υπογράμμισαν τον ρόλο των UAV στην παροχή της πανταχού παρούσας κάλυψης δικτύου ασύρματης επικοινωνίας 6G λόγω του χαμηλού κόστους, της ευελιξίας ανάπτυξης και χαμηλή κατανάλωση ενέργειας. Τα UAV θα λειτουργούν ως συσκευές δικτύου αιχμής και συσκευές αισθητήρων και θα μπορούν να επικοινωνούν απρόσκοπτα με άλλα UAV για ενημερώσεις δικτύου σε πραγματικό χρόνο σε γεωγραφικές τοποθεσίες του εναέριου χώρου, ειδικά σε περιπτώσεις έκτακτης ανάγκης και να μεταδίδουν δεδομένα μεταξύ τους και μεταξύ άλλων σταθμών βάσης. Αυτή η επικοινωνία μπορεί να επιτευχθεί μόνο με καλύτερη και πιο αξιόπιστη συνδεσιμότητα που παρέχεται από την τεχνολογία 6G. Τα μελλοντικά UAV που θα χρησιμοποιούν ασύρματη επικοινωνία 6G θα μπορούσαν με ασφάλεια να μοιράζονται και να αποθηκεύουν δεδομένα (τραβηγμένα βίντεο και εικόνες υψηλής ποιότητας) σε κατανεμημένα δίκτυα blockchain σε πραγματικό χρόνο εξοικονομώντας χώρο αποθήκευσης δεδομένων, επεξεργασία και ισχύ μπαταρίας, τα οποία είναι εγγενώς περιορισμένα σε UAV, όπως π.χ. ως drones. Τα UAV που είναι εξοπλισμένα με πομποδέκτες επικοινωνίας θα είναι απεριόριστα σε συγκεκριμένες τοποθεσίες και εμπόδια, γεγονός που θα τους επιτρέπει να παρέχουν ευρύτερη κυψελωτή κάλυψη σε επιθυμητές τοποθεσίες και υψόμετρα . Ως εκ τούτου, τα UAV θα είναι πολύ χρήσιμα για την υποστήριξη δικτύων 6G IoT, συμπεριλαμβανομένων των ευφυών VANET και των υποδομών αυτόνομης οδήγησης. [9]

2.3.1.2.3. Satellite IoT

Τέλος σημαντική είναι και η αναφορά των Satellite IoT's, δηλαδή η επέκταση της κάλυψης επίγειων επικοινωνιών δικτύου σε μη επίγεια ύψη χρησιμοποιώντας δορυφόρους χαμηλής τροχιάς. Αυτή θα είναι εφικτή με την τεχνολογία 6G. Αυτό το νέο περιβάλλον δικτύου IoT μη επίγειων υποδομών με δυνατότητα 6G περιλαμβάνει τη χρήση δορυφόρων και UAV όπου οι συμβατικές τεχνολογίες κινητής/κινητής τηλεφωνίας είναι δύσκολο αν όχι αδύνατο να εφαρμοστούν. Προτείνονται μοντέλα που αντιμετωπίζουν ζητήματα κατανάλωσης ενέργειας σε μελλοντικά δορυφορικά δίκτυα IoT 6G χρησιμοποιώντας σχήματα μη ορθογώνιας πολλαπλής πρόσβασης (NOMA) για δορυφορική επικοινωνία στο Διαδίκτυο χαμηλής τροχιάς σε τέτοια Smart Cities και παγκόσμιες υποδομές. [9]

Ως εκ τούτου, ενεργοποιημένα από την επικοινωνία THz και τη χαμηλή κατανάλωση ενέργειας, μπορεί να αναπτυχθεί ένας μεγάλος αριθμός δορυφόρων χαμηλής τροχιάς για την επέκταση της κάλυψης στο Διαδίκτυο, την παροχή πρόσβασης στο Διαδίκτυο σε πραγματικό χρόνο σε απομακρυσμένες τοποθεσίες και την υποστήριξη θαλάσσιων/υποθαλάσσιων δικτύων. Αυτό το νέο υπολογιστικό περιβάλλον αιχμής δορυφόρων που επικοινωνούν σε πραγματικό χρόνο χρησιμοποιώντας εύρος ζώνης υψηλής ταχύτητας και όχι μόνο θα συμπληρώσει τα υπάρχοντα επίγεια οικοσυστήματα. [9]

2.3.2 Smart Buildings and Facilities

Τα έξυπνα κτίρια (Smart Buildings) ή έξυπνες εγκαταστάσεις (Smart Facilities) είναι εκείνα τα κτίρια που χρησιμοποιούν συστήματα, υπηρεσίες και τεχνολογία που βασίζονται σε τεχνολογία πληροφοριών και επικοινωνιών για τη βελτιστοποίηση της απόδοσης της εγκατάστασης.[34] Κάτω από έναν τέτοιο ευρύ ορισμό μπορούμε να εναποθέσουμε λοιπόν τα Smart Homes ιδιωτών ή αντίστοιχα τα Smart Offices για το middle level enterprise και τέλος τα Smart Factories για το higher level enterprise πλέον σε επίπεδο παραγωγής.

2.3.2.1 Smart Buildings (Smart Homes/Office and Smart Factories)

2.3.2.1.1. Smart Homes/Office

Οι εφαρμογές Smart Building υποστηρίζουν την εξατομίκευση ελέγχοντας το περιβάλλον διαβίωσης και εργασίας. Ένα σύστημα που σχηματίζεται από αισθητήρες και ενεργοποιητές στοχεύει να βελτιώσει την άνεση των κατοίκων, συνήθως ακόμη και χωρίς την παρέμβασή τους. Επιπλέον, επιτρέποντας στους ιδιοκτήτες ή τους διαχειριστές να παρακολουθούν την ιδιοκτησία από απόσταση, τα έξυπνα οικιακά συστήματα συμβάλλουν στη συντήρηση και την ασφάλεια του κτιρίου. Τα κλιματιστικά, τα συστήματα θέρμανσης δαπέδου, τα ψυγεία, τα πλυντήρια ρούχων και τα φώτα θα μπορούσαν να ελέγχονται μέσω του Διαδικτύου για εξοικονόμηση ενέργειας, νερού και άλλων πόρων. Εκτός από τη βιωσιμότητα και την αποτελεσματικότητα, οι λύσεις έξυπνων κτιρίων θα μπορούσαν επίσης να προσφέρουν βοήθεια σε καταστάσεις έκτακτης ανάγκης. Για παράδειγμα, οι συναγερμοί πυρκαγιάς θα μπορούσαν να ενεργοποιηθούν αυτόματα, με βάση τις μετρήσεις των αισθητήρων θερμοκρασίας και των ανιχνευτών καπνού. [1]

Μέχρι το 2023, η αγορά έξυπνων κατοικιών αναμένεται να φτάσει τα 141,2 δισεκατομμύρια δολάρια, που θα σημαίνει αύξηση 17% σε σύγκριση με το 2019. Ωστόσο, ενώ τα έξυπνα χαρακτηριστικά του σπιτιού και του γραφείου φέρνουν κατανοητά οφέλη στην καθημερινή μας ζωή και αυξάνουν την άνεσή μας, συνεπάγονται επίσης μεγάλες επιφάνειες επίθεσης και έτσι εγείρουν κρίσιμους προβληματισμούς όσον αφορά την έννοια της εμπιστοσύνης, της ιδιωτικής ζωής και της ασφάλειας. [1]

2.3.2.1.2. Industrial IoT (IIoT) and Smart Factory

Αρχικά θα προσπαθήσουμε να δώσουμε ένα σχετικά καλό ορισμό του Industrial Internet of Things (IIoT). Το παρόν εγχείρημα βέβαια είναι δύσκολο καθώς ακόμα ο συγκεκριμένος κλάδος βρίσκεται σε ενεργή ανάπτυξη και αλλάζει συνεχώς. Οι περισσότεροι ερευνητές ωστόσο θα συμφωνήσουν:

Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT) : Πρόκειται για ένα σύστημα που περιλαμβάνει δικτυωμένα έξυπνα αντικείμενα, κυβερνοφυσικά περιουσιακά στοιχεία, σχετικές γενικές τεχνολογίες πληροφοριών και προαιρετικές πλατφόρμες υπολογιστικού νέφους ή αιχμής, που επιτρέπουν σε πραγματικό χρόνο, έξυπνη και αυτόνομη πρόσβαση, συλλογή, ανάλυση, επικοινωνία και ανταλλαγή πληροφορίας διαδικασίας, προϊόντος ή/και υπηρεσίας, εντός του βιομηχανικού περιβάλλοντος, ώστε να βελτιστοποιηθεί η συνολική αξία παραγωγής. Αυτή η τιμή μπορεί να περιλαμβάνει: τη βελτίωση της παράδοσης προϊόντων ή υπηρεσιών, την ενίσχυση της παραγωγικότητας, τη μείωση του κόστους εργασίας, τη μείωση της κατανάλωσης ενέργειας και τη μείωση του κύκλου κατασκευής κατά παραγγελία. [13]

Αναφέρουμε ότι στη βιβλιογραφία υπάρχει μία μεγάλη έλλειψη έρευνας από security threats τα οποία μπορεί να υπάρχουν στο ευρύτερο λοιπόν IIoT, καθώς ακόμα δεν έχει εγκατασταθεί πουθενά ένα τέτοιο απόλυτο δίκτυο (ούτε και σε μικρά περιβάλλοντα ή χώρες), το οποίο μπορεί να περιλαμβάνει εργοστάσια παραγωγής νερού, μεταφοράς, παραγωγής, εμπόριο, εξόρυξη πόρων, γεωργικές διαδικασίες, παραγωγή ενέργειας, αλλά και σταθμούς τηλεπικοινωνιών, τα οποία όλα είναι ικανά να επικοινωνούν μεταξύ τους, ώστε να επιτύχουν το στόσο που αναφέραμε στον ορισμό του IIoT παραπάνω.

Για αυτό το λόγο **εστιάζουμε στην έννοια του Smart Factory**, το οποίο αναφέρεται σε μία **συγκεκριμένη** βιομηχανία η οποία πρόκειται για ένα κυβερνο-φυσικό σύστημα που χρησιμοποιεί προηγμένες τεχνολογίες για να αναλύει δεδομένα, να οδηγεί αυτοματοποιημένες διαδικασίες και να μαθαίνει μέσω τεχνητής νοημοσύνης πως να βελτιώνει τη παραγωγή, τη μείωση του κόστους εργασίας, τη μείωση της κατανάλωσης ενέργειας και τη μείωση του κύκλου κατασκευής κατά παραγγελία **για ένα δεδομένο εργοστάσιο**. [15] [13]

Με βάση τς παραπάνω λοιπόν 2 ορισμούς βλέπουμε ότι η κύρια διαφορά μεταξύ του IIoT και του Smart Factory είναι ότι το ένα αναφέρεται γενικευμένα σε ένα δίκτυο το οποίο συνδέει πολλαπλά εργοστάσια και βιομηχανίες βελτιώνοντας συνολικά τη παραγωγή μίας πόλης,μίας χώρας και γενικότερα μιας περιοχής, ενώ το 2ο αναφέρεται σε μία συγκεκριμένη βιομηχανία, η οποία και ενδεχομένως να μπορεί να υποστηρίξει μία τέτοια κατεύθυνση προς την διασύνδεση των μηχανημάτων της.

2.3.2.2 6G Smart Buildings and Facilities

2.3.2.2.1 6G for Smart Homes/Office

Η ενεργειακή μετάβαση που ξεκίνησε από την ενεργειακή παγκόσμια πολιτική και ο αυξανόμενος αντίκτυπος της κατανάλωσης ανανεώσιμων πηγών ενέργειας στα ακίνητα απαιτούν μια πρόσθετη αποτελεσματική αντίληψη της τοπικής παραγωγής ενέργειας και κατανάλωσης ενέργειας. Η εξισορρόπηση της κατανάλωσης ενέργειας μεταξύ παραγωγής ενέργειας και αγοράς ενέργειας μπορεί να επιτευχθεί μόνο με ένα αποτελεσματικό, αξιόπιστο και οικονομικά αποδοτικό σύστημα διαχείρισης ενέργειας. Η θερμική ενέργεια για τη θέρμανση και το ζεστό νερό και η ηλεκτρική ενέργεια πρέπει να χρησιμοποιείται για την τροφοδοσία των κτιρίων μέσω μέσων με μειωμένες εκπομπές CO2. Επιπλέον, πολλές άλλες εργασίες σε μια σύγχρονη ιδιοκτησία πρέπει να μπορούν να επιλυθούν οικονομικά με τη βοήθεια ψηφιακών στοιχείων. [16]

Η παραγωγή τοπικών δεδομένων επομένως σε έξυπνα κτίρια και έξυπνες πόλεις από αισθητήρες, ενεργοποιητές και μετρητές οφείλει να χρησιμοποιεί κατάλληλη ραδιοτεχνολογία όπως π.χ. Bluetooth LE, ZigBee, EnOcean, Z-Wave, KNX-RF. Η διαχείριση της μετάδοσης δεδομένων σε διακομιστές εφαρμογών και σύννεφα, όπου θα μπορούσαν να αναπτυχθούν οι εφαρμογές, θα πρέπει να γίνεται με κεντρική μετάδοση στα κτίρια μέσω πυλών(gateways). Η τοπική δημιουργία ημερομηνίας μπορεί να διαχειρίζεται πλατφόρμες λογισμικού με γρήγορες συνδέσεις με διαφορετικές ραδιοφωνικές τεχνολογίες IoT. Η ψηφιοποίηση των ακινήτων βασίζεται στην αποκεντρωμένη παραγωγή ενέργειας, αποθήκευση ενέργειας και διανομή ενέργειας, εγκατάσταση ευφυών κτιριακών δικτύων και δημιουργία πραγματικών προστιθέμενων αξιών με νέες εφαρμογές για κατοίκους και διοικήσεις. [16]

Οι ψηφιακές λύσεις για τον κλάδο των ακινήτων αφορούν επομένως κατά βάση την ενέργεια, από την κλασική αγορά πηγών ενέργειας, μέσω τεχνικών συστημάτων, έως διαδικασίες βελτιστοποιημένες για τη μείωση του CO2. Επιπλέον, η ευφυής δικτύωση κτιρίων είναι σημαντική ως βάση για την ολοκληρωμένη λειτουργία ακινήτων και διαδικασιών και η χρήση ψηφιακών στοιχείων μπορεί να δημιουργήσει πραγματική προστιθέμενη αξία για τους κατοίκους και τη διοίκηση. Η ακόλουθη επιλογή ψηφιακών υπηρεσιών θα πρέπει να ενσωματωθεί στην ακίνητη περιουσία [16]:

- Απομακρυσμένη πρόσβαση και έλεγχος παραγωγής, κατανάλωσης και αποθήκευσης ενέργειας (Ηλιακή κ.λπ.),
- Έξυπνη μέτρηση (ηλεκτρικό ρεύμα, θέρμανση, νερό κ.λπ.),
- Έλεγχος έξυπνου σπιτιού και έξυπνου κτιρίου με νέες έννοιες λειτουργίας,
- Έλεγχος φωτός και αντηλιακή προστασία,
- Έλεγχος συσκευής: τηλεχειριστήριο, έλεγχος σκηνής, μείωση κατανάλωσης αναμονής (αυτόματη ενεργοποίηση)
- Μεγιστοποίηση της αυτοκατανάλωσης,
- Έλεγχος HVAC, συμπεριλαμβανομένης της παρακολούθησης και της πρόληψης της ποιότητας του αέρα,
- Σταθεροποίηση δικτύου με χρήση buffers και έλεγχος της τοπικής παραγωγής ενέργειας,
- Ολοκληρωμένο σύστημα μέτρησης: παράδοση δεδομένων για τιμολόγηση, ενοικίαση εξοπλισμού και επιπλέον κόστος,
- Παρακολούθηση κινδύνου καπνού, ελεύθερου νερού,
- Έλεγχος πρόσβασης και ασφάλεια,
- Κόμβος κινητικότητας ενός τετάρτου: παράδοση δεδομένων χρέωσης,
- Κόμβος κινητικότητας συντονισμού: υπολογισμός και ρύθμιση ισχύος φόρτισης για τον συντονισμό της διαθέσιμης ισχύος δικτύου, της χωρητικότητας παραγωγής και της ζήτησης των χρηστών,

- Παρακολούθηση τεχνικού εξοπλισμού σε κτίρια (π.χ. CHP, μετατροπέας DC/AC,…) και
- Έλεγχος πολυμέσων (FTTH, τηλεόραση, Διαδίκτυο, τηλέφωνο): παράδοση δεδομένων χρέωσης (εάν είναι διαθέσιμα από τον πάροχο).

Αισθητήρες, ενεργοποιητές, μετρητές, τεχνολογία επικοινωνίας και κατανεμημένες υπολογιστικές πλατφόρμες σε πραγματικό χρόνο θα είναι βασικές τεχνολογίες για την παρακολούθηση, τον έλεγχο και τη μέτρηση του διάφορου ηλεκτρικού εξοπλισμού. Αυτές οι συλλεγόμενες πληροφορίες θα χρησιμοποιηθούν ως είσοδος για πολλούς τύπους αλγορίθμων πρόβλεψης μοντέλων (π.χ. AI) των οποίων η έξοδος υποστηρίζει αποφάσεις για την επίτευξη των στόχων του μέλλοντος. Έτσι για μια κατάλληλη δομή ελέγχου, είναι απαραίτητο να σταθεροποιηθεί ένα πλέγμα με μια αρχιτεκτονική που βασίζεται στον κατάλληλο συνδυασμό κεντρικού και αποκεντρωμένου ελέγχου. [16]

Ο στόχος λοιπόν είναι να δημιουργηθεί η βέλτιστη κατάλληλη αρχιτεκτονική για μια κοινή Πλατφόρμα Επικοινωνίας (IoT, δίκτυα κινητής τηλεφωνίας και η καλύτερη συγχώνευση) για την προσφορά κατάλληλων εφαρμογών μέσω διακομιστή cloud edge. Μια έξυπνη αστική περιοχή μπορεί να αναπτυχθεί για να επιτρέψει τη διαλειτουργικότητα μεταξύ συσκευών ή εφαρμογών σε περιβάλλον αστικής περιοχής. Τα μαζικά δεδομένα IoT, η παρακολούθηση της ενέργειας και του εξοπλισμού, η αποκεντρωμένη αποδοτική παραγωγή, κατανάλωση και διανομή ενέργειας αποτελούν τη βάση για τη βελτιστοποίηση της χρήσης διαφορετικών ενεργειακών πόρων. [16]

Σε αυτό το πλαίσιο χρησιμοποιούνται ο χρηματοοικονομικός ενεργειακός έλεγχος και η επικοινωνία με το δίκτυο. Το επίπεδο πολυπλοκότητας αυτής της αρχιτεκτονικής αυξάνεται σημαντικά λαμβάνοντας υπόψη τις προσεγγίσεις διαχείρισης της ζήτησης στην εξίσωση, διαφορετικούς τύπους ανανεώσιμων πηγών ενέργειας, συστήματα αποθήκευσης μπαταριών, ηλεκτρικά οχήματα, απόκριση ζήτησης και δυναμική τιμολόγηση. Η υψηλή πυκνότητα των κόμβων μέτρησης και η ποσότητα των δεδομένων που πρέπει να μεταδοθούν μέσω χαμηλού κόστους τερματικών σημείων είναι ικανή να συμβεί μόνο με ψηφιοποίηση στα κτίρια, ώστε να συλλέγεται αυτή η ποσότητα δεδομένων από τις συσκευές IoT μέσω 6G Edge Cloud. Είναι επίσης δυνατές οι απευθείας συνδέσεις με δίκτυα 5G-and-beyond, αλλά προκειμένου όλες οι προαναφερθείσες ανάγκες να μπορούν να γίνονται αρκετά οικονομικά η σύνδεση στο 6G κρίνεται απαραίτητη. [16]

Σε επίπεδο επιχειρηματικής εφαρμογής που αναπτύσσεται σε διακομιστή Cloud Edge μπορεί να γίνει επιλογή υπηρεσιών. Βελτιστοποίηση της λειτουργίας με διεύθυνση της ισχύος κατανάλωσης και παραγωγής και με χρήση συστημάτων άμεσης ή έμμεσης αποθήκευσης. Μέσω της χρήσης αλγορίθμων που πραγματοποιούν μη γραμμικές πράξεις που καθοδηγούνται από παραμέτρους επιχειρηματικής και ζήτησης. Οι αλγόριθμοι είναι δυναμικοί προσαρμοσμένοι ή αυτομάθητοι (πρόγνωση-μοντέλο). Η απομακρυσμένη συντήρηση για τοπική παραγωγή ενέργειας (CHP, PV,…) και τοπική αποθήκευση ενέργειας, έξυπνη μέτρηση για παραγωγή και κατανάλωση ενέργειας (ρεύμα, θέρμανση και ψύξη, νερό,…) μπορεί να διαχειρίζεται εξ αποστάσεως μέσω δικτύων 6G και νέες ιδέες λειτουργίας για έλεγχο θέρμανσης και ψύξης, έλεγχο φωτός και έλεγχο κλείστρου μπορούν να βρεθούν και άμεσα έτσι να εφαρμοστούν. [16]

Η παρακολούθηση διαφορετικού εξοπλισμού, π.χ. θέρμανση και ψύξη, φως, κλείστρο, κλίμα εσωτερικού χώρου, ποιότητα αέρα, αποφυγή μούχλας, ανίχνευση καπνού και πυρκαγιάς, ανίχνευση νερού, έλεγχος εισόδου και ασφάλεια είναι η βάση μιας ιδέας ψηφιοποίησης. Περαιτέρω εφαρμογές είναι η μίσθωση ηλεκτρικής ενέργειας για τη χρήση της αποκεντρωμένης παραγόμενης ενέργειας και το ολοκληρωμένο λογιστικό σύστημα για τη δημιουργία λογιστικών δεδομένων. Θα πρέπει επίσης να αναπτυχθεί ο κόμβος

κινητικότητας σε αστικές περιοχές για την ενοικίαση ηλεκτρικών οχημάτων, ο υπολογισμός και ο έλεγχος της ηλεκτρικής ισχύος των σταθμών φόρτισης για τον συντονισμό της παροχής ενέργειας της παραγωγής ενέργειας και τη δημιουργία δεδομένων για λογιστική χρήση. [16]

2.3.2.2.2 6G for Industrial IoT (IIoT) and Smart Factories

Η πιθανή εφαρμογή της τεχνολογίας ασύρματης επικοινωνίας 6G στο Industrial IoT (IIoT) για τη βελτιστοποίηση καλύτερων βιομηχανικών λειτουργιών και διαδικασιών παραγωγής μεγάλης κλίμακας έχει εντοπιστεί και συζητηθεί. Συγκεκριμένα, η εφαρμογή της τεχνολογίας 6G με δυνατότητα AI μπορεί να χρησιμοποιηθεί για την επίτευξη και την επιτάχυνση του έξυπνου αυτοματισμού και τη βελτίωση των χαμηλών εκπομπών άνθρακα και της αποδοτικότητας της βιομηχανίας. Τα ζητήματα ασφάλειας και απορρήτου ήταν επίσης η κινητήρια δύναμη πίσω από την εφαρμογή τεχνολογιών με δυνατότητα 6G στο IIOT. Ορισμένες επικοινωνίες δικτύου μεταξύ συστημάτων βιομηχανικού ελέγχου και εγκαταστάσεων μπορούν να αντικατασταθούν χρησιμοποιώντας την τεχνολογία OWC. Το VLC βέβαια θεωρείται πολύ πιο ασφαλές λόγω των δεδομένων που μεταδίδονται σε ευθεία οπτική γωνία, η οποία διατηρεί υψηλή πυκνότητα δεδομένων και λιγότερη παραμόρφωση δεδομένων σε σύγκριση με την τρέχουσα επικοινωνία ραδιοκυμάτων. [13]

2.3.3 Smart Healthcare and Wearables.

2.3.3.1 Smart Healthcare and Wearables

2.3.3.1.1 Smart Healthcare

Για τη βελτιστοποίηση των πρακτικών της τρέχουσας φροντίδας ασθενών και την εφαρμογή νέων χαρακτηριστικών, η έξυπνη υγειονομική περίθαλψη εστιάζει σε περιβάλλοντα που οδηγούνται από την τεχνολογία πληροφοριών και επικοινωνιών, εστιάζοντας κυρίως στην αποτελεσματική και αποδοτική τεχνολογία IoT και αυτοματισμό διαδικασιών. Στα έξυπνα νοσοκομεία (Smart Hospitals), υπάρχουν τρεις βασικές κατηγορίες εγκαταστάσεων: ιατρικό προσωπικό, ασθενής και υπηρεσίες διαχείρισης. Οι αποφάσεις ενδονοσοκομειακής διαχείρισης που υποστηρίζουν συστήματα, είναι υψίστης σημασίας και αυτές οι κατηγορίες υγειονομικής περίθαλψης οφείλουν να αντιμετωπίζονται γρήγορα. [22]

Οι φορητοί υπολογιστές, οι έξυπνες πόλεις και το προσωπικό συνδέονται με τη διαχείριση Smart Healthcare System μέσω του διαδικτύου που ενσωματώνει πολλά συστήματα ψηφιακών συσκευών IoT. Αυτό το σύστημα καθιστά δυνατή την αναγνώριση και τεκμηρίωση ασθενών σε νοσοκομεία, την τακτική επίβλεψη του ιατρικού προσωπικού και την παρακολούθηση εξοπλισμού και βιοτικών δειγμάτων. Στον φαρμακευτικό τομέα, η έξυπνη υγειονομική περίθαλψη χρησιμοποιείται επίσης για την παρασκευή και διανομή των φαρμάκων, τον έλεγχο της αποθήκης, την καταπολέμηση της παραχάραξης και τις πρόσθετες απαιτούμενες διαδικασίες. Για να πραγματοποιηθεί μια αξιόπιστη, ασφαλής και αποτελεσματική διανομή νοσοκομειακού υλικού που χρησιμοποιεί, μπορεί να εκδοθεί μια ειδική κατανομή ετικετών RFID (Radio Frequency Identification) για κάθε άτομο και τα δεδομένα μπορούν να μεταδοθούν σε μια συσκευή που παρακολουθεί και ανακτά εύκολα τα δεδομένα μέσω των φορητών εφαρμογών. [22]

Η δημιουργία ενός πλαισίου λειτουργικού ελέγχου βοηθά επίσης στην εκτέλεση εργασιών όπως η επιλογή πόρων, η παρακολούθηση της ποιότητας και η ανάλυση επιτυχίας όσον αφορά τη λήψη αποφάσεων, και μπορεί να ελαχιστοποιήσει το κόστος των

ασθενών, να βελτιστοποιήσει τη χρήση των πόρων και να βοηθήσει τα νοσοκομεία να κάνουν συστάσεις στη διαχείριση. Οι ασθενείς μπορούν να ελέγχουν διάφορα χαρακτηριστικά όσον αφορά τις υπηρεσίες υγειονομικής περίθαλψης, όπως υπηρεσίες φυσικής εξέτασης, ψηφιακές διαβουλεύσεις και εμπειρίες γιατρού-ασθενούς. Τέτοια ηλεκτρονικά συστήματα θα επιτρέψουν οι διαδικασίες της ιατρικής περίθαλψης των ασθενών να γίνουν πιο αποδεκτές και πιο απλές. Με έγκαιρο τρόπο, οι ασθενείς περιμένουν και λαμβάνουν όλο και πιο ζωντανή φροντίδα. Συνοπτικά, το αποτέλεσμα της έξυπνης υγειονομικής περίθαλψης είναι ο μετασχηματισμός, η ανάπτυξη και ο εκσυγχρονισμός. [22]

2.3.3.1.2 Wearables

Η σύγχρονη τεχνολογία φορητών συσκευών εμπίπτει σε ένα ευρύ φάσμα χρηστικότητας, συμπεριλαμβανομένων των έξυπνων ρολογιών, των ιχνηλατών γυμναστικής, των ακουστικών VR, των έξυπνων κοσμημάτων, των γυαλιών με δυνατότητα web και των ακουστικών Bluetooth. Τα wearables λειτουργούν διαφορετικά, ανάλογα με την κατηγορία στην οποία ανήκουν, όπως υγεία, φυσική κατάσταση ή ψυχαγωγία. Κατά κύριο λόγο, η τεχνολογία wearable λειτουργεί ενσωματώνοντας μικροεπεξεργαστές, μπαταρίες και συνδεσιμότητα στο Διαδίκτυο, ώστε τα δεδομένα που συλλέγονται να συγχρονίζονται με άλλα ηλεκτρονικά είδη, όπως κινητές συσκευές ή φορητούς υπολογιστές. [33]

Τα φορητά είναι ενσωματωμένα με ενσωματωμένους αισθητήρες που παρακολουθούν τις σωματικές κινήσεις, παρέχουν βιομετρική αναγνώριση ή βοηθούν στην παρακολούθηση τοποθεσίας. Για παράδειγμα, οι ιχνηλάτες δραστηριότητας ή τα έξυπνα ρολόγια -- οι πιο συνηθισμένοι τύποι φορητών συσκευών -- διαθέτουν λουράκι που τυλίγεται γύρω από τον καρπό του χρήστη ώστε αυτοί να παρακολουθούν τις σωματικές δραστηριότητες του χρήστη ή ζωτικής σημασίας λειτουργίες του σώματος του κατά τη διάρκεια της ημέρας. [33]

Ενώ τα περισσότερα wearable ρούχα είτε φοριούνται στο σώμα είτε συνδέονται με ρούχα, ορισμένα λειτουργούν χωρίς καμία φυσική επαφή με τον χρήστη. Άλλα φορέματα χρησιμοποιούν απομακρυσμένους έξυπνους αισθητήρες και επιταχυνσιόμετρα για να παρακολουθούν τις κινήσεις και την ταχύτητα, ενώ ορισμένα χρησιμοποιούν οπτικούς αισθητήρες για τη μέτρηση του καρδιακού ρυθμού ή των επιπέδων γλυκόζης. Ένας κοινός παράγοντας μεταξύ αυτών των φορητών συσκευών τεχνολογίας είναι το γεγονός ότι όλα παρακολουθούν δεδομένα σε πραγματικό χρόνο. [33]

2.3.3.2 6G for Healthcare and Wearables

Το IoT εφαρμόζεται σε διάφορους τομείς για τη βελτίωση της παροχής υπηρεσιών υγειονομικής περίθαλψης. Αυτές περιλαμβάνουν την απομακρυσμένη παρακολούθηση της υγείας σε πραγματικό χρόνο, την τηλεϊατρική, την υγειονομική περίθαλψη στο σπίτι και τους ηλικιωμένους και τον εντοπισμό και την πρόληψη χρόνιων ασθενειών. Οι φορητές συσκευές, οι βιο-ενσωματωμένες συσκευές και τα ευφυή συστήματα βιο-νανο αναπτύσσονται με ταχεία ταχύτητα για τη διευκόλυνση των υπηρεσιών υγειονομικής περίθαλψης σε πραγματικό χρόνο. Αυτές οι συσκευές IoT βοηθούν στην ανίχνευση βιολογικών και χημικών αλλαγών γύρω από έναν ασθενή και στέλνουν τα συγκεντρωμένα δεδομένα σε περιβάλλοντα κέντρων δεδομένων ακμών ή ομίχλης για περαιτέρω επεξεργασία. Ωστόσο, η επιτάχυνση και η πρόοδός του εμποδίζονται από την αξιοπιστία και την καθυστέρηση της επικοινωνίας

δεδομένων από λειτουργικούς αισθητήρες και κόμβους που μεταφέρουν δεδομένα σε αυτά τα κέντρα δεδομένων. [9]

Αυτές οι συσκευές IoT χρησιμοποιούν επί του παρόντος πρότυπα επικοινωνίας μικρής εμβέλειας, όπως Bluetooth Low Energy (BLE) και ZigBee, τα οποία επιφέρουν σημαντικές καθυστερήσεις. Αν και το ZigBee είναι κατάλληλο για έξυπνες εφαρμογές υγείας, ενέχει κίνδυνο για την ασφάλεια των ευαίσθητων δεδομένων ασθενών που ανταλλάσσονται μέσω του δικτύου και δεν εφαρμόζεται συνήθως σε smartphone σε σύγκριση με το BLE . Ομοίως, τα πρότυπα επικοινωνίας μεγάλης εμβέλειας όπως το Wi-Fi και το NB-IoT που λειτουργούν σε δίκτυα GSM, LTE, 4G και 5G δεν προσφέρουν αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης ή υψηλής ταχύτητας σε σύγκριση με πιθανές τεχνολογίες 6G όπως THz, mURLLC ή VLC. Διάφορες μελέτες περιγράφουν την πιθανή χρήση των UAV που υποστηρίζονται από blockchain και AI στις μελλοντικές έξυπνες εφαρμογές υγείας και τηλεχειρουργικής με δυνατότητα 6G για να διευκολύνουν καλύτερα την απομακρυσμένη, αξιόπιστη και ασφαλή παροχή έξυπνων υπηρεσιών υγειονομικής περίθαλψης. [9]

2.3.4 XR/AR/VR

2.3.4.1 XR/AR/VR environments

2.3.4.1.1. Virtual Reality (VR)

Η εικονική πραγματικότητα (VR) είναι μια προσομοιωμένη εμπειρία που χρησιμοποιεί παρακολούθηση πόζας και τρισδιάστατες οθόνες κοντά στα μάτια για να δώσει στον χρήστη μια καθηλωτική αίσθηση ενός εικονικού κόσμου. Οι εφαρμογές της εικονικής πραγματικότητας περιλαμβάνουν την ψυχαγωγία (ιδίως βιντεοπαιχνίδια), την εκπαίδευση (όπως ιατρική ή στρατιωτική εκπαίδευση) και τις επιχειρήσεις (όπως εικονικές συναντήσεις).

Επί του παρόντος, τα τυπικά συστήματα εικονικής πραγματικότητας χρησιμοποιούν είτε ακουστικά εικονικής πραγματικότητας είτε περιβάλλοντα πολλαπλών προβολών για να δημιουργήσουν κάποιες ρεαλιστικές εικόνες, ήχους και άλλες αισθήσεις που προσομοιώνουν τη φυσική παρουσία ενός χρήστη σε ένα εικονικό περιβάλλον. Ένα άτομο που χρησιμοποιεί εξοπλισμό εικονικής πραγματικότητας είναι σε θέση να κοιτάζει γύρω από τον τεχνητό κόσμο, να κινείται μέσα σε αυτόν και να αλληλεπιδρά με εικονικά χαρακτηριστικά ή αντικείμενα. Το εφέ δημιουργείται συνήθως από ακουστικά VR που αποτελούνται από μια οθόνη τοποθετημένη στο κεφάλι με μια μικρή οθόνη μπροστά στα μάτια, αλλά μπορεί επίσης να δημιουργηθεί μέσα από ειδικά σχεδιασμένα δωμάτια με πολλές μεγάλες οθόνες. Η εικονική πραγματικότητα συνήθως ενσωματώνει ακουστική και βίντεο ανατροφοδότηση, αλλά μπορεί επίσης να επιτρέπει άλλους τύπους αισθητηριακής και δυνάμενης ανατροφοδότησης μέσω απτικής τεχνολογίας.

2.3.4.1.2. Augmented Reality (AR)

Το AR μπορεί να οριστεί ως ένα σύστημα που ενσωματώνει τρία βασικά χαρακτηριστικά: έναν συνδυασμό πραγματικού και εικονικού κόσμου, αλληλεπίδραση σε πραγματικό χρόνο και ακριβή τρισδιάστατη καταγραφή εικονικών και πραγματικών αντικειμένων. Οι επικαλυπτόμενες αισθητηριακές πληροφορίες μπορεί να είναι εποικοδομητικές (δηλαδή προσθετικές στο φυσικό περιβάλλον) ή καταστροφικές (δηλαδή απόκρυψη του φυσικού περιβάλλοντος).Αυτή η εμπειρία είναι άψογα συνυφασμένη με τον φυσικό κόσμο, έτσι ώστε να γίνεται αντιληπτή ως μια εμβυθιστική πτυχή του πραγματικού

περιβάλλοντος.Με αυτόν τον τρόπο, η επαυξημένη πραγματικότητα αλλάζει τη συνεχή αντίληψη κάποιου για ένα περιβάλλον πραγματικού κόσμου, ενώ η εικονική πραγματικότητα αντικαθιστά πλήρως το πραγματικό περιβάλλον του χρήστη με ένα προσομοιωμένο.

Η επαυξημένη πραγματικότητα μπορεί να χρησιμοποιηθεί για τη βελτίωση φυσικών περιβαλλόντων ή καταστάσεων και προσφέρει εμπλουτισμένες εμπειρίες αντιληπτικά. Με τη βοήθεια προηγμένων τεχνολογιών AR (π.χ. προσθήκη όρασης υπολογιστή, ενσωμάτωση καμερών AR σε εφαρμογές smartphone και αναγνώριση αντικειμένων) οι πληροφορίες σχετικά με τον περιβάλλοντα πραγματικό κόσμο του χρήστη γίνονται διαδραστικές και ψηφιακά επεξεργασμένες. Οι πληροφορίες για το περιβάλλον και τα αντικείμενά του επικαλύπτονται στον πραγματικό κόσμο. Αυτές οι πληροφορίες μπορεί να είναι εικονικές. Η επαυξημένη πραγματικότητα είναι κάθε εμπειρία που είναι τεχνητή και προσθέτει στην ήδη υπάρχουσα πραγματικότητα. Βλέποντας παραδείγματος χάριν άλλες πραγματικές ανιχνευόμενες ή μετρημένες πληροφορίες, όπως ηλεκτρομαγνητικά ραδιοκύματα που επικαλύπτονται σε ακριβή ευθυγράμμιση με το σημείο που πραγματικά βρίσκονται στο διάστημα. Η επαυξημένη πραγματικότητα έχει επίσης πολλές δυνατότητες στη συγκέντρωση και την ανταλλαγή σιωπηρής γνώσης. Οι τεχνικές επαύξησης εκτελούνται συνήθως σε πραγματικό χρόνο και σε σημασιολογικά πλαίσια με περιβαλλοντικά στοιχεία. Οι καθηλωτικές αντιληπτικές πληροφορίες συνδυάζονται μερικές φορές με συμπληρωματικές πληροφορίες, όπως σκορ σε ζωντανή ροή βίντεο ενός αθλητικού γεγονότος. Αυτό συνδυάζει τα πλεονεκτήματα τόσο της τεχνολογίας επαυξημένης πραγματικότητας όσο και της τεχνολογίας heads up display (HUD).

2.3.4.1.3. Extended Reality (XR)

Η εκτεταμένη πραγματικότητα (XR) είναι ένας γενικός όρος που αναφέρεται στην επαυξημένη πραγματικότητα (AR), στην εικονική πραγματικότητα (VR) συνολικά. Η τεχνολογία προορίζεται να συνδυάσει ή να αντικατοπτρίζει τον φυσικό κόσμο με έναν «ψηφιακό δίδυμο κόσμο» ικανό να αλληλεπιδρά μαζί του,δίνοντας στους χρήστες μια καθηλωτική εμπειρία με το να βρίσκονται σε ένα εικονικό ή επαυξημένο περιβάλλον.

Τα πεδία της εικονικής πραγματικότητας και της επαυξημένης πραγματικότητας αναπτύσσονται ραγδαία και εφαρμόζονται σε ένα ευρύ φάσμα τομέων όπως η ψυχαγωγία, ο κινηματογράφος, το μάρκετινγκ, η ακίνητη περιουσία, η εκπαίδευση, η εκπαίδευση, η συντήρηση και η εξ αποστάσεως εργασία. Η εκτεταμένη πραγματικότητα έχει τη δυνατότητα να χρησιμοποιηθεί για κοινή προσπάθεια στο χώρο εργασίας, εκπαίδευση, εκπαιδευτικούς σκοπούς, θεραπευτικές θεραπείες και εξερεύνηση και ανάλυση δεδομένων.

Η εκτεταμένη πραγματικότητα λειτουργεί χρησιμοποιώντας την απόκτηση οπτικών δεδομένων που είτε είναι προσβάσιμα τοπικά είτε κοινοποιούνται και μεταφέρονται μέσω δικτύου και στις ανθρώπινες αισθήσεις. Επιτρέποντας απαντήσεις σε πραγματικό χρόνο σε ένα εικονικό ερέθισμα, αυτές οι συσκευές δημιουργούν προσαρμοσμένες εμπειρίες. Η πρόοδος στο 5G και στο edge computing θα μπορούσε να βοηθήσει στους ρυθμούς δεδομένων, να αυξήσει τη χωρητικότητα των χρηστών και να μειώσει την καθυστέρηση. Αυτές οι εφαρμογές πιθανότατα θα επεκτείνουν την εκτεταμένη πραγματικότητα στο μέλλον.

2.3.4.2 6G for XR/AR/VR

Ξεκινάμε την παρούσα αναφέροντας την καθοριστική επίδραση που θα έχει η επικοινωνία δικτύου 6G στα IoT και θα κάνει τα XR,VR και AR πολύ πιο mainstream, με

αυτόνομη και σε πραγματικό χρόνο επικοινωνία μεταξύ των διαφόρων κόμβων δικτύου σε εικονικούς κόσμους. Αυτό θα δημιουργήσει εναλλακτικές πραγματικότητες όπου οι χρήστες μπορούν να αναπαραστήσουν τον εαυτό τους όπως θέλουν, σχεδόν σε οποιαδήποτε μορφή επιθυμούν μέσω των avatar τους. [9]

Προβλέπεται ότι το μέγεθος της αγοράς αυτής της τεχνολογίας θα φτάσει τα 393 δισεκατομμύρια δολάρια μέχρι το 2025 και θα εξαπλωθεί σε διάφορα περιβάλλοντα όπως η ψυχαγωγία, η τεχνητή νοημοσύνη, η ρομποτική και η υγειονομική περίθαλψη με εκτεταμένες βραχυπρόθεσμες δυνατότητες ανάπτυξης. Οι νεότερες συσκευές IoT θα ενσωματωθούν με τεχνολογία 6G-ready με δυνατότητα AI που επιτρέπει τη χρήση αυτών των συσκευών για την επικάλυψη αντικειμένων στον πραγματικό κόσμο. [9]

Στην υγειονομική περίθαλψη, το εφαρμοσμένο AR με ασύρματη επικοινωνία υψηλής ταχύτητας 6G θα χρησιμοποιηθεί για πρακτικές τηλεϊατρικής, τηλεπαρακολούθησης και τηλεχειρουργικής. Σημαντικά μειονεκτήματα έχουν εντοπιστεί σε υπάρχοντα συστήματα τηλεχειρουργικής 5G, όπως η Virtual Interactive Presence and Augmented Reality (VIPAR), τα οποία περιλαμβάνουν λανθάνουσα κατάσταση και κακή επικοινωνία δεδομένων και δικτύου μεταξύ απομακρυσμένων και τοπικών σταθμών. Η τεχνολογία 6G έχει επίσης προβλεφθεί ότι θα τροφοδοτήσει την ψυχαγωγία των καταναλωτών επόμενης γενιάς, ειδικά σε εφαρμογές παιχνιδιών και κοινωνικών μέσων. [9]

2.4 Security Challenges and Risks

2.4.1 Smart Cities (Smart Vehicles and Drones)

2.4.1.1.Security Challenges and Risks for UAV’s - Drones

Παρά τα προφανή πλεονεκτήματα των δικτύων UAV, η εφαρμογή τους περιορίζεται από ανησυχίες για την ασφάλεια. Το 2011, η ασφάλεια των μη επανδρωμένων οχημάτων αυξήθηκε όταν τα ιρανικά στρατεύματα κατέλαβαν ένα αμερικανικό RQ-170. Ο κίνδυνος των εχθρών να ξεκινήσουν επιθέσεις δικτύου υπάρχει κάθε φορά που χρησιμοποιούνται δίκτυα UAV για εργασίες όπως η επικοινωνία μάχης και ο εντοπισμός σε επικίνδυνες συνθήκες. Κατά τη διάρκεια του πολέμου Ρωσίας-Ουκρανίας το 2022, ο στρατός της Ουκρανίας σχημάτισε μικρές ομάδες για να επιτεθεί σωματικά στα ρωσικά drones με τη βοήθεια όπλων λέιζερ. Ο συγγραφέας αυτός εξηγεί πώς οι εισβολείς μπορούν να επωφεληθούν από την παραβίαση της επικοινωνίας μεταξύ UAV και απομακρυσμένων ομολόγων τους, καθιστώντας τα ευάλωτα. [23]

Με την πρόσφατη ανάγνωση, είναι σαφές ότι η επικοινωνία UAV που βασίζεται στο IoT δεν είναι ασφαλής. Τα UAV με ευαίσθητες πληροφορίες για στρατιωτικές αποστολές μπορεί να τεθούν σε κίνδυνο. Όσον αφορά την ασφάλεια, αποστολές υψηλών προδιαγραφών όπως στρατιωτικές εφαρμογές π.χ. Η αναγνώριση, η έρευνα, η διάσωση και η επιθεώρηση γραμμών ηλεκτρικής ενέργειας απαιτούν περισσότερη ασφάλεια και υπάρχουσες μελέτες παρέχουν σύντομες αξιολογήσεις ή έρευνες που περιορίζονται σε λίγες μόνο επιθέσεις ασφαλείας ή αντίμετρα. Δεδομένου ότι δεν κυκλοφόρησε συστηματική μελέτη στον τομέα των δικτύων UAV που βασίζονται στο IoT, έχουμε ελλιπή ακόμα στοιχεία για να μπορούμε να συνειδητοποιήσουμε το πλήρες εύρος των προβλημάτων που θα προκύψουν σε περίπτωση που δίκτυα UAV παραβιαστούν. Υπάρχει ανάγκη για προκαταρκτική μελέτη πρόσφατων επιθέσεων και απαιτούνται τεχνολογίες επικοινωνίας που διατηρούν λειτουργικά τα UAV περιορισμένης ισχύος. [23]

2.4.1.2.Security Challenges and Risks for IoV

Η γρήγορη ανάπτυξη και εφαρμογή του IoV(**Internet of Vehicles**) θα φέρει ορισμένες νέες προκλήσεις, ειδικά όσον αφορά την ασφάλεια. Διάφοροι εισβολείς έχουν ήδη προσπαθήσει να εκμεταλλευτούν τα κανάλια επικοινωνίας των AAV και να ενεργοποιήσουν κακόβουλες οδηγίες που επηρεάζουν το σύστημα πέδησης και κινητήρα. Για παράδειγμα, ένα έξυπνο όχημα θα μπορούσε να τεθεί σε κίνδυνο κατά τη διάρκεια μιας ενημέρωσης του λειτουργικού συστήματος και να αξιοποιηθεί για την αλλαγή των δεδομένων αισθητήρων που αποστέλλονται σε άλλα οχήματα μέσω της διεπαφής V2V και V2I. Με τον ίδιο τρόπο, μια κακόβουλη εφαρμογή smartphone θα μπορούσε να επιτεθεί σε ένα έξυπνο όχημα ή μια μονάδα οδικής εγκατάστασης (RSU) μέσω της διεπαφής ηλεκτρονικών συσκευών από όχημα προς καταναλωτή (V2CE). Επιπλέον, τα παραβιασμένα AAV θα μπορούσαν να χρησιμοποιηθούν για τη δημιουργία ενός botnet και την εκκίνηση μεγάλων επιθέσεων DDoS όπως αυτή που αναφέρθηκε στη προηγούμενη ενότητα. [1]

Ιδιαίτερα ενδιαφέρον από την άποψη της εγκληματολογίας είναι το σύστημα Infotainment Vehicle, επειδή αποθηκεύουν έναν τεράστιο όγκο δεδομένων που σχετίζονται με τον χρήστη (π.χ. το ιστορικό πλοήγησης του οχήματος, αρχεία καταγραφής κλήσεων και λίστες επαφών, φωτογραφίες, βίντεο κ.λπ.) . Οι επαγγελματίες εγκληματολόγοι θα μπορούσαν να χρησιμοποιήσουν αυτές τις πληροφορίες για να προσδιορίσουν τις ευθύνες σε τροχαία ατυχήματα ή κυβερνοεπιθέσεις. Επιπλέον, σε περίπτωση ατυχήματος, μπορούσαν να εξετάσουν τα αρχεία των αισθητήρων από τα γειτονικά αυτοκίνητα. Εφόσον οι ενσωματωμένες λύσεις προληπτικής παρακολούθησης αστικών περιοχών όπως το MobEyes ή το Pics-on-Wheels καταγράφουν το περιβάλλον κατά την οδήγηση, οι επαγγελματίες εγκληματολόγοι θα μπορούσαν ακόμη και να αναζητήσουν στο δίκτυο οχημάτων υλικό βίντεο του ατυχήματος. Φυσικά, η μαζική ανάπτυξη αισθητήρων και ο τεράστιος όγκος δεδομένων IoV φέρνει τις παραδοσιακές εγκληματολογικές πρακτικές σε αμφισβήτηση και απαιτεί νέες, έξυπνες εγκληματολογικές τεχνικές για αυτόνομα οχήματα. [1]

2.4.2 Smart Buildings and Facilities

2.4.2.1.Security Challenges and Risks for Smart Homes/Office

Ορισμένες οικιακές συσκευές που είναι συνδεδεμένες στο Διαδίκτυο, για παράδειγμα, είναι προγραμματισμένες να πραγματοποιούν αυτοέλεγχο και να ζητούν επισκευή σε περίπτωση τεχνικού προβλήματος. Εάν υπάρχει ανάγκη για επισκευές, το έξυπνο σύστημα κτιρίου θα μπορούσε να εξασφαλίσει την πρόσβαση του τεχνικού στη σπασμένη συσκευή. Οι εγκληματίες μπορεί να προσελκύονται από αυτό το χαρακτηριστικό και να χειραγωγούν το σύστημα προκειμένου να εισέλθουν στο σπίτι ενώ οι κάτοικοι λείπουν. Στο πλαίσιο ενός έξυπνου εργοστασίου, τα ευφυή χαρακτηριστικά μπορεί να δημιουργήσουν νέες ευκαιρίες για ad-hoc attacks όπως η βιομηχανική κατασκοπεία και το σαμποτάζ στον κυβερνοχώρο. [1]

Τέλος, τα έξυπνα οικιακά συστήματα ενδέχεται να εισάγουν ορισμένες νέες φυσικές απειλές στον κυβερνοχώρο. Οι αισθητήρες για ανίχνευση έκτακτης ανάγκης (π.χ. αναγνωριστικό διαρροής αερίου) υποτίθεται ότι ειδοποιούν αυτόματα μια εξωτερική υπηρεσία έκτακτης ανάγκης και ανοίγουν όλες τις πόρτες και τα παράθυρα στο κτίριο. Ωστόσο, μια αδίστακτη συσκευή που υποδύεται αυτούς τους αισθητήρες μπορεί να

χρησιμοποιηθεί για να αφήσει έναν εισβολέα να εισέλθει, ή ακόμα χειρότερα: να μπλοκάρει την ειδοποίηση της μονάδας έκτακτης ανάγκης και να κλειδώσει τις εξόδους. [1]

2.4.2.2.Security Challenges and Risks for Smart Factories

Στην παραδοσιακή διαδικασία παραγωγής τώρα, η ασφάλεια της παραγωγής επιτυγχανόταν με φυσική απομόνωση που πραγματοποιούνταν με βάση την αυστηρή διαχείριση δικαιωμάτων πρόσβασης. Το έξυπνο εργοστάσιο (smart factory) είναι συνδεδεμένο εκ φύσεως και το ουσιαστικό μέρος των εργοστασιακών δικτύων συνδέεται με ασύρματα δίκτυα και πιο εκτεταμένα εταιρικά συστήματα. Οι συσκευές που εμπλέκονται στη διαδικασία κατασκευής γίνονται προσβάσιμες σε μη εξουσιοδοτημένες επιθέσεις. Για το λόγο αυτό, ο κίνδυνος της κυβερνοασφάλειας δημιουργεί μεγαλύτερη ανησυχία σε ένα τέτοιο περιβάλλον από ό,τι σε ένα παραδοσιακό περιβάλλον εγκαταστάσεων παραγωγής. Τέτοιες ανησυχίες πρέπει να αντιμετωπιστούν στο πλαίσιο της συνολικής έξυπνης εργοστασιακής αρχιτεκτονικής. [15]

Κάθε σύστημα πληροφοριών και επικοινωνίας ορίζεται συχνότερα μέσω τριών θεμελιωδών αρχών, γνωστών ως τριάδα της CIA: εμπιστευτικότητα (confidentiality), προσβασιμότητα (accessibility) και ακεραιότητα (integrity). Η εμπιστευτικότητα σχετίζεται με τη διασφάλιση της προστασίας των επιθεωρήσεων ιδιοκτησίας από μη εξουσιοδοτημένες οντότητες. Η ακεραιότητα επικεντρώνεται στην προστασία των περιουσιακών στοιχείων από μη εξουσιοδοτημένες τροποποιήσεις, ενώ η διαθεσιμότητα είναι ένα χαρακτηριστικό που σχετίζεται με την παροχή πρόσβασης στα περιουσιακά στοιχεία σε εξουσιοδοτημένες οντότητες ανά πάσα στιγμή. Η διαθεσιμότητα και η ακεραιότητα είναι υψίστης σημασίας στο σύστημα παραγωγής, επειδή τα κενά δεδομένων και τα ψευδή δεδομένα μπορούν να οδηγήσουν σε σημαντικές αλλαγές στις ίδιες τις διαδικασίες που αναλαμβάνει κάθε μηχάνημα ή την παραγωγή. [15]

Πολλές επιθέσεις υποκινούνται από πολιτικούς λόγους, αλλά μπορεί επίσης να υποκινούνται και από οικονομικούς λόγους. Οι κυβερνοεπιθέσεις σε ένα έξυπνο εργοστάσιο συχνά επιδιώκουν έναν από τους ακόλουθους τρεις στόχους [15]:

- κλοπή προσωπικών δεδομένων τελικών πελατών. Οι εγκληματίες χρησιμοποιούν ένα μοναδικό ολοκληρωμένο σύστημα CRM (Customer Relationship Management) και μπορούν μέσω αυτού, για παράδειγμα, να αποκτήσουν πρόσβαση στο λειτουργικό σύστημα του έξυπνου εργοστασίου (smart factory) μέσω προμηθευτών θέρμανσης και κλιματισμού,
- Διακοπή ολόκληρου του συστήματος, η οποία μπορεί να προκαλέσει δραματικές απώλειες που σχετίζονται με επιθέσεις χάκερ,
- Βιομηχανική κατασκοπεία και δολιοφθορά. Τα τεχνολογικά τρωτά σημεία μπορούν να αξιοποιηθούν για την κλοπή πνευματικής ιδιοκτησίας και την απόκτηση σημαντικού ανταγωνιστικού πλεονεκτήματος έναντι των ανταγωνιστών.

Παρόλο που τα συστήματα παραγωγής σε ένα έξυπνο εργοστασιακό περιβάλλον έχουν σχεδιαστεί και ρυθμιστεί με τέτοιο τρόπο ώστε να είναι απομονωμένα, και υπάρχει μεγάλη εμπιστοσύνη σε τέτοια συστήματα, πραγματοποιούνται ελάχιστοι έλεγχοι ακεραιότητας για την πρόληψη κακόβουλης δραστηριότητας. Συστήματα και μηχανήματα που είναι δυνητικά αδύναμοι κρίκοι στην αλυσίδα ασφαλείας και μπορούν να χρησιμοποιηθούν κακόβουλα για να βλάψουν κατασκευασμένα προϊόντα ή να προκαλέσουν

βλάβες είναι τα MES (Manufacturing Execution System), HMI (Human Machine Interfaces) και βιομηχανικές συσκευές IoT. [15]

Λόγω του υψηλού επιπέδου διασύνδεσης των στοιχείων παραγωγής και πληροφορικής και της ολοκλήρωσης με βάση την τεχνολογία πληροφοριών, η λειτουργία της φυσικής παραγωγικής διαδικασίας εξαρτάται από την ομαλή λειτουργία των υπηρεσιών πληροφορικής και επικοινωνίας που οδηγούν σε αυτές. Για το λόγο αυτό, τα έξυπνα εργοστασιακά δίκτυα αντιμετωπίζουν νέες απειλές για την ασφάλεια πληροφοριών και επικοινωνιών σε τέσσερις διαστάσεις: διαθεσιμότητα, πρόσβαση, ακρίβεια και υπευθυνότητα. Κατά συνέπεια, οι έξυπνες εργοστασιακές απειλές για την ασφάλεια προκύπτουν κυρίως μέσα από τα ακόλουθα τέσσερα κανάλια ή μέτωπα [15]:

- Από σφάλματα λογισμικού και δυσλειτουργίες υλικού.
- Από ανοιχτά πρωτόκολλα Διαδικτύου που χρησιμοποιούνται σε ένα τέτοιο περιβάλλον και τυπικά δίκτυα.
- Από πολυάριθμα άτομα που εμπλέκονται στην εκτέλεση της παραγωγικής διαδικασίας.
- Από ένα μεγάλο αριθμό συσκευών στις οποίες μπορούμε να έχουμε πρόσβαση μέσω Internet.

Οι τεχνολογίες που βρίσκονται σε ένα έξυπνο εργοστασιακό περιβάλλον απαιτούν λόγω της λειτουργίας τους να φέρουν μαζί τους συγκεκριμένες απαιτήσεις ασφάλειας. Λόγω των διαφορετικών απαιτήσεων που έχουν τέτοιες τεχνολογίες, δημιουργούνται νέες κατηγορίες κινδύνου επειδή αυξάνονται τα τρωτά σημεία και οι απειλές σε όλο το έξυπνο εργοστασιακό περιβάλλον. Όλα τα στοιχεία που βρίσκονται σε ένα τέτοιο δυναμικό σύστημα καθίστανται κρίσιμα για την ασφάλεια καθώς τα βιομηχανικά συστήματα παρακολούθησης γίνονται στόχος κακόβουλων επιθέσεων στον κυβερνοχώρο. Η προστασία των προσωπικών δεδομένων είναι επίσης μια ουσιαστική πτυχή της ασφάλειας του έξυπνου εργοστασιακού περιβάλλοντος. Η προσέγγιση BYOD (Bring Your Own Device) φέρει μαζί της πολλές απειλές. Τα εμπιστευτικά δεδομένα που είναι αποθηκευμένα σε συνδεδεμένες συσκευές, στα οποία είναι δυνατή η πρόσβαση με περισσότερους τρόπους από ποτέ, προσφέρουν έναν τρόπο διείσδυσης στο δίκτυο από τους εισβολείς, αυξάνοντας τον κίνδυνο βιομηχανικής κατασκοπείας. [15]

Οι απειλές μπορεί να προέρχονται από διάφορες πηγές, όπως η δραστηριότητα των εργαζομένων σε ένα τέτοιο περιβάλλον ή οι επιθέσεις hacking. Είναι δυνατό να προκληθούν διάφορες ζημιές στην ίδια την επιχειρηματική διαδικασία και ακόμη και να διακοπεί η επιχείρηση. Μία από τις πιο κρίσιμες απειλές στο έξυπνο εργοστασιακό περιβάλλον είναι η αχρηστία της υπηρεσίας κατ' απαίτηση. Δεδομένης της αυξανόμενης εξάρτησης της υποδομής παραγωγής από την αξιόπιστη λειτουργία των υπηρεσιών πληροφοριών και επικοινωνιών, τα δεδομένα και η πρόσβαση σε αυτές είναι ζωτικής σημασίας. [15]

Οι επιθέσεις DDoS (Distributed Denial of Service) είναι από τις πιο σημαντικές απειλές στο σύγχρονο περιβάλλον παραγωγής. Αυτή η επίθεση επιδιώκει να απαγορεύσει σε νόμιμους χρήστες την πρόσβαση σε μια ιδιοκτησία σε περιβάλλον παραγωγής. Χρησιμοποιούν πολλαπλά ευάλωτα συστήματα που έχουν μολυνθεί με κακόβουλο λογισμικό, και μια τέτοια απειλή είναι δύσκολο να προστατευτεί για οποιαδήποτε εξωτερικά προσβάσιμη διεπαφή. [15]

2.4.3 Smart Healthcare and Wearables

2.4.3.1.Security Challenges and Risks for Healthcare

Μεταξύ όλων των τομέων που βασίζονται στο IoT, ο τομέας της υγειονομικής περίθαλψης είναι ίσως ο πιο ευάλωτος σε μεγάλες επιθέσεις ασφαλείας. Αυτό θα μπορούσε να εξηγηθεί με τη διαοργανωτική φύση των εφαρμογών IoT σε αυτόν τον τομέα, καθώς και με την ετερογένεια, τον κατακερματισμό και τη διευρυμένη επιφάνεια επίθεσης. Έτσι, ενώ μεταμορφώνουν τη βιομηχανία υγειονομικής περίθαλψης και βελτιώνουν την ανθρώπινη ζωή, οι συσκευές απομακρυσμένης παρακολούθησης της υγείας προκαλούν ορισμένες νέες ανησυχίες σχετικά με την προστασία και την ασφάλεια των ιατρικών δεδομένων των χρηστών. [1]

Οι ιχνηλάτες γυμναστικής (Fitness Trackers), για παράδειγμα, θα μπορούσαν να στοχοποιηθούν από κακόβουλους παράγοντες που θέλουν να χρησιμοποιήσουν τα συγκεντρωμένα δεδομένα για παράνομα οικονομικά οφέλη, π.χ. πουλώντας τα σε ασφαλιστικές εταιρείες ή εκβιάζοντας τον ιδιοκτήτη της παραβιασμένης συσκευής. Ο αυξανόμενος αριθμός περιπτώσεων κλοπής ιατρικής ταυτότητας δεν προκαλεί έκπληξη, δεδομένης της υψηλής αξίας των ιατρικών δεδομένων. Σε γενικές γραμμές, το μέγεθος της αγοράς των εφαρμογών και υπηρεσιών mHealth αποτιμήθηκε πάνω από 86,4 δισεκατομμύρια δολάρια το 2018 και αναμένεται να σημειώσει σύνθετη ετήσια αύξηση άνω του 29,6% από το 2019 έως το 2025. [1]

2.4.3.2.Security Challenges and Risks for Wearables

Τα Wearables, όπως τα βραχιόλια γυμναστικής, έχουν επίσης αποκτήσει σημασία στην ιατροδικαστική επιστήμη (Forensics) για έναν ακόμα λόγο, δηλαδή ως πηγή ψηφιακών αποδεικτικών στοιχείων. Είναι προγραμματισμένα να λειτουργούν παθητικά στο φόντο της καθημερινής ζωής των χρηστών και να δημιουργούν δεδομένα με ενσωματωμένους αισθητήρες (π.χ. μέτρηση απόστασης που διανύθηκε, καρδιακών παλμών, θερμοκρασίας σώματος, κατανάλωσης θερμίδων, ρυθμού ύπνου-εγρήγορσης κ.λπ.). Ως εκ τούτου, θα μπορούσαν να παρέχουν μεγάλο όγκο ιατροδικαστικών δεδομένων που θα μπορούσαν να χρησιμοποιηθούν για να αντικρούσουν την ψευδή μαρτυρία ενός υπόπτου ή για να εντοπίσουν τις δραστηριότητες του θύματος, κοντά στη στιγμή του συμβάντος. Έτσι, αρχικά σχεδιασμένες για την παρακολούθηση της κατάστασης της υγείας ενός χρήστη, οι εφαρμογές που βασίζονται στο IoT θα μπορούσαν επίσης να παίξουν το ρόλο του λεγόμενου «ψηφιακού μάρτυρα». Για το λόγο αυτό, η μελέτη των έξυπνων ρολογιών και των ανιχνευτών ζωνών γυμναστικής έχει γίνει ακόμη πιο ελκυστική στην ιατροδικαστική πρακτική. [1]

Ένας άλλος λόγος είναι η αυξανόμενη δημοτικότητα αυτών των συσκευών. Τα έξυπνα ρολόγια είναι η τρέχουσα κορυφαία κατηγορία φορητών συσκευών με 74 εκατομμύρια αποστολές. Ωστόσο, μέχρι σήμερα, υπάρχουν πολύ λίγες μελέτες που έχουν διεξαχθεί σχετικά με το πώς τα έξυπνα ρολόγια ή άλλες φορητές συσκευές θα μπορούσαν να χρησιμοποιηθούν ως πηγή ψηφιακών στοιχείων. Με την έρευνα αυτού του θέματος, θα πρέπει να δοθεί ιδιαίτερη προσοχή στα θέματα που σχετίζονται με το απόρρητο, καθώς τα δεδομένα που συλλέγονται θα μπορούσαν να είναι εξαιρετικά ευαίσθητα. [1]

Ο αυξανόμενος αριθμός περιστατικών ασφάλειας και προστασίας της ιδιωτικής ζωής υπογραμμίζει μόνο την ανάγκη για καινοτόμες, πολύπλευρες προσεγγίσεις, διαφορετικές και πολύ πιο ισχυρές από την καθιερωμένη μεθοδολογία ψηφιακής εγκληματολογίας. [1]

2.4.4. XR/AR/VR

Η εφαρμογή της τεχνολογίας 6G στον εικονικό κόσμο αναμφίβολα όχι μόνο θα βελτιώσει την υιοθέτηση και την εμπειρία των χρηστών, αλλά θα αυξήσει επίσης τον πολλαπλασιασμό των εικονικών εγκλημάτων στον κυβερνοχώρο, των παρενοχλήσεων και των βλαβών στον κυβερνοχώρο. Εγκλήματα πραγματικού κόσμου διαπράττονται καθημερινά σε εικονικούς κόσμους ήδη βέβαια, συμπεριλαμβανομένου του ξεπλύματος βρώμικου χρήματος, της κλοπής ψηφιακών περιουσιακών στοιχείων όπως οι μη ανταλλάξιμα μάρκες (NFTs), της σεξουαλικής παρενόχλησης και εκμετάλλευσης (δηλαδή του εικονικού βιασμού), του εκφοβισμού ή της καταδίωξης, της ανταλλαγής εικόνων κακοποίησης παιδιών και της προσομοίωσης σεξουαλικής χρήσης με το avatar ενός ατόμου. [9]

Το 2016, ένας παίκτης περιέγραψε ότι ουσιαστικά τον έπιασε ένα άλλο avatar στο παιχνίδι QuiVr VR για πολλούς παίκτες και περιέγραψε ένα περιστατικό βιασμού. Εδώ είναι σημαντικό να αναφερθεί ότι τα Avatar δεν είναι αυτόνομα αλλά ελέγχονται από πραγματικούς ανθρώπους και μπορεί να είναι επιρρεπή σε χειραγώγηση παρόμοια με τα πραγματικά άτομα. Υπάρχουν ήδη αναφερθείσες περιπτώσεις κλοπής εικονικών αντικειμένων που μπορούν να ανταλλάσσονται με εικονικά ή πραγματικά μετρητά ή ακόμα και μέσω σεξουαλικής εκμετάλλευσης από ένα avatar από άλλο. Επίσης, έχουν προκύψει γενικά ζητήματα νομικής ρύθμισης σχετικά με την εφαρμογή τεχνολογιών VR. Πειράματα πραγματικού κόσμου έχουν επίσης πραγματοποιηθεί για να καταδειχθεί η σκοπιμότητα επιθέσεων πλευρικού καναλιού σε εικονικά περιβάλλοντα. Για αυτούς τους λόγους, οι μελλοντικοί εικονικοί κόσμοι παρουσιάζουν ένα μοναδικό σύνολο προκλήσεων όχι μόνο για το σύστημα ποινικής δικαιοσύνης αλλά και για τους ψηφιακούς εγκληματολογικούς ερευνητές στη συλλογή, τη διατήρηση, τη συσχέτιση και την ανάλυση των εγκληματολογικών αποδεικτικών στοιχείων όπως θα δούμε στο επόμενο κεφάλαιο ακόμα πιο αναλυτικά. [9]

Προκλήσεις ψηφιακής εγκληματολογικής έρευνας έχουν εντοπιστεί στο παρελθόν για υπάρχουσες διαδικτυακές πλατφόρμες όπως τα MMORPG (Massive Multiplayer Online Role-Playing Games). Ωστόσο, η έννοια της διεξαγωγής εγκληματολογικών ερευνών που διενεργούνται σε περιβάλλοντα εκτεταμένης και εικονικής πραγματικότητας (XR/VR) είναι ένας νέος τομέας για τις περισσότερες υπηρεσίες επιβολής του νόμου σε όλο τον κόσμο. Η έλλειψη δικαιοδοσίας και γεωγραφικών ορίων σε αυτά τα περιβάλλοντα καθιστά επίσης σημαντική πρόκληση την ιατροδικαστική έρευνα. Ως εκ τούτου, καθιστά δύσκολο, αν όχι αδύνατο, τον προσδιορισμό του εύρους των ψηφιακών εγκληματολογικών ερευνών και των ορίων ενός τόπου εγκλήματος. Έχουν προταθεί διάφορες ρυθμίσεις που περιλαμβάνουν ενέργειες επιτήρησης από οργανισμούς που θα παίξουν τον ίδιο ρόλο με την αστυνομία, τους ερευνητές και την κυβέρνηση σε εικονικούς κόσμους. Ωστόσο, προς το παρόν, η έρευνα που επικεντρώνεται σε εγκληματολογικές μεθοδολογίες και τεχνικές για τη συλλογή αποδεικτικών τεχνουργημάτων σε περιβάλλοντα εικονικής πραγματικότητας βρίσκεται ακόμη στο αρχικό της στάδιο. Επιπλέον, δεν υπάρχουν πολλά ψηφιακά εγκληματολογικά εργαλεία κατάλληλα για εγκληματολογικές έρευνες συστημάτων IoT και VR λόγω της συμβατότητας με το σύστημα που εξετάζεται και λόγω της ποικιλίας του υπάρχοντος υλικολογισμικού και λειτουργικών συστημάτων. Ως εκ τούτου, η ιατροδικαστική ετοιμότητα και η μελλοντική έρευνα σε πλαίσια και η ανάπτυξη εργαλείων που θα επιτρέψουν στους ερευνητές να διεξάγουν έγκυρες ιατροδικαστικές έρευνες στο εγγύς μέλλον είναι ζωτικής σημασίας. [9]

2.5 IoT Forensics

Η αγορά IoT έχει και θα συνεχίσει να παρουσιάζει εκθετική ανάπτυξη κατά την τρέχουσα δεκαετία. Ξεκινώντας από τα 157 δισεκατομμύρια δολάρια το 2016, η αξία της αγοράς του IoT προβλέπεται να φτάσει σε ανώτατο όριο αγοράς που θα εκτείνεται στα 771 δισεκατομμύρια δολάρια μέχρι το 2026. Η Cisco προέβλεψε ότι μέχρι το έτος 2030, 500 δισεκατομμύρια αντικείμενα θα συνδεθούν και θα συνδεθούν στο Διαδίκτυο. Οι πάροχοι υπηρεσιών Cloud το έχουν δει ως ευκαιρία για τη δημιουργία νέων επιχειρηματικών μοντέλων. [1]

Ωστόσο, η διασφάλιση ολόκληρου του δικτύου IoT δεν είναι εύκολη υπόθεση. Σε αντίθεση με τις συμβατικές υπολογιστικές συσκευές που βασίζονται σε παραδοσιακές σουίτες ασφάλειας δικτύου, όπως η προστασία τελικού σημείου και τα τείχη προστασίας, η επικοινωνία IoT αποτελείται από ατελείωτο αριθμό πρωτοκόλλων, δυνατοτήτων συσκευών και προτύπων. Έτσι, η ασφάλεια του IoT βασίζεται στην ασφάλιση κάθε επιπέδου του μοντέλου OSI και εκτείνεται έτσι σε σχεδόν όλα τα γνωστά πρωτόκολλα. [1]

Συνεπώς, τα εργαλεία ασφάλειας IoT και εγκληματολογίας έχουν μεγάλη ζήτηση. Αυτό ισχύει για όλους τους τομείς που βασίζονται στο IoT, όπως η υγειονομική περίθαλψη, οι έξυπνες οικιακές συσκευές, οι βιομηχανικές μηχανές, η αλυσίδα εφοδιασμού και η διαχείριση αποθεμάτων, το έξυπνο δίκτυο, η επιτήρηση και οι έξυπνες πόλεις, μέρη μόνο των κατηγοριών των συσκευών IoT όπως είδαμε στη προηγούμενη ενότητα. Κατά αυτό το τρόπο οδηγούμαστε στην επιστήμη της εγκληματολογίας IoT ή αλλιώς IoT Forensics. [1]

Το IoT Forensics θα μπορούσε να εκληφθεί ως υποδιαίρεση του Digital Forensics, περισσότερα για το οποίο θα δούμε στο επόμενο κεφάλαιο. Ωστόσο, ενώ η πειθαρχία του DF είναι εδώ και πολύ καιρό τόσο στον ακαδημαϊκό χώρο όσο και στη βιομηχανία, το IoT Forensics είναι ένας σχετικά νέος και ανεξερεύνητος τομέας. Ο σκοπός του IoT Forensics είναι παρόμοιος με αυτόν του Digital Forensics, ο οποίος είναι ο εντοπισμός και η εξαγωγή ψηφιακών πληροφοριών με νόμιμο και ιατροδικαστικό τρόπο. Εκτός από μια συγκεκριμένη συσκευή ή αισθητήρα IoT, τα εγκληματολογικά δεδομένα θα μπορούσαν να συλλεχθούν από το εσωτερικό δίκτυο (π.χ. ένα τείχος προστασίας ή έναν δρομολογητή) ή από το cloud. Κατόπιν αυτού, το IoT Forensics θα μπορούσε να χωριστεί σε τρεις κατηγορίες: επίπεδο συσκευής IoT, εγκληματολογία δικτύου και εγκληματολογία cloud. [1]

Μια θεμελιώδης διαφορά μεταξύ Digital Forensics και IoT Forensics μπορεί να φανεί από την πηγή των αποδεικτικών στοιχείων. Σε αντίθεση με το παραδοσιακό DF, όπου τα συνήθη αντικείμενα εξέτασης είναι υπολογιστές, smartphone, tablet, διακομιστές ή πύλες, στο IoT Forensics οι πηγές αποδείξεων θα μπορούσαν να είναι πολύ πιο εκτεταμένες, συμπεριλαμβανομένων των συστημάτων παρακολούθησης βρεφών ή ασθενών, In-Vehicle Infotainment (IVI) συστήματα, φανάρια, ακόμη και ιατρικά εμφυτεύματα σε ανθρώπους και ζώα. [1]

Η ασφάλεια κάθε αισθητήρα, συσκευής επικοινωνίας και αποθήκευσης cloud εντός του δικτύου IoT, είναι σχεδόν αδύνατη. Εάν συμβεί ένα περιστατικό, ένα από τα πρώτα καθήκοντα που εκτελούν οι επαγγελματίες εγκληματολόγοι είναι να καθορίσουν το εύρος του προβλήματος. Ωστόσο, σε αντίθεση με τις πρακτικές ασφάλειας IoT, οι εγκληματολογικές τεχνικές (IoT Forensics) δεν στοχεύουν στην ελαχιστοποίηση της ζημίας, αλλά στον εντοπισμό της προέλευσης της επίθεσης/ελλείμματος ή των ευθυνών των διαφορετικών μερών. [1]

2.5.1. Σημασία και χρησιμότητα των IoT Forensics τεχνικών

2.5.1.1. Εκτεταμένη Επιφάνεια Επίθεσης

Η τεχνολογία Machine-Machine (M2M) έχει επεκταθεί ραγδαία τα τελευταία χρόνια, αλλά παρά τα πλεονεκτήματα και τις ευρείες προοπτικές αυτής της προηγμένης ιδέας, το M2M είναι ένα παράδειγμα τύπου επικοινωνίας ιδιαίτερα ευάλωτου σε κυβερνοεπιθέσεις. Συνδέεται με μεγάλο αριθμό τερματικών και μεγάλη ποσότητα ενσωματωμένου υλικού (όπως ετικέτες τοποθεσίας και έξυπνους αισθητήρες) που αυξάνει την επιφάνεια επίθεσης και το θέτει σε υψηλότερο κίνδυνο. Το ίδιο ισχύει και για το IoT που εξελίχθηκε στα θεμέλια που έθεσε η τεχνολογία M2M. [1]

Αντίστοιχα, οι συσκευές IoT με δημόσιες διεπαφές εκτίθενται σε μεγαλύτερα επίπεδα κινδύνου επειδή θα μπορούσαν να φέρουν ένα κακόβουλο λογισμικό στο ιδιωτικό δίκτυο από έναν λιγότερο ασφαλή δημόσιο χώρο. Τα συχνά παρατηρούμενα περιστατικά περιλαμβάνουν κλοπή ταυτότητας και διαρροή δεδομένων, πρόσβαση και χρήση εκτυπωτών συνδεδεμένων στο Διαδίκτυο, παραβίαση κόμβων, χειραγώγηση μονάδων CCTV που βασίζονται σε σύννεφο, SQL injections , phishing, απάτη που σχετίζεται με ασφαλίσεις, διαδικτυακό εκφοβισμό, ransomware και κακόβουλο λογισμικό που στοχεύει συγκεκριμένες συσκευές, όπως συσκευές VoIP και έξυπνα οχήματα. [1]

Οι κυβερνοεπιθέσεις θα μπορούσαν επίσης να έχουν μεγάλη κλίμακα και να επηρεάσουν τις παγκόσμιες επιχειρήσεις ή να δημιουργήσουν χάος στο χρηματιστήριο. Για παράδειγμα, οι συσκευές IoT μπορούν να χρησιμοποιηθούν για την εκτόξευση επιθέσεων κατανεμημένης άρνησης υπηρεσίας (DDoS) εναντίον ιστότοπων τρίτων, εταιρικών δικτύων ή κυβερνητικών ιδρυμάτων. Η δεύτερη μεγαλύτερη επίθεση DDoS μέχρι στιγμής έλαβε χώρα τον Οκτώβριο του 2016 και απευθύνθηκε στην Dyn, έναν καθιερωμένο πάροχο DNS. Χρησιμοποιώντας ένα κακόβουλο λογισμικό που ονομάζεται Mirai, οι εισβολείς δημιούργησαν ένα botnet από παραβιασμένες συσκευές IoT όπως έξυπνες τηλεοράσεις, κάμερες IP, εκτυπωτές κ.λπ. [1]

Ως αποτέλεσμα, υπήρξαν παρατυπίες για πολλούς ιστότοπους, συμπεριλαμβανομένων πλατφορμών όπως Amazon, Twitter, PayPal, Visa, AirBnB, Netflix, Spotify, Tumblr, The New York Times, Reddit και GitHub. Η Gartner έχει υπολογίσει ότι έως το 2020, περισσότερες από το ένα τέταρτο των επιθέσεων θα αφορούν σε κίνδυνο ανόμοιες συσκευές. [1]

2.5.1.2. Νέες απειλές για τη φυσική ασφάλεια στον κυβερνοχώρο

Ερευνητές δηλώνουν ότι χρησιμοποιώντας τη δύναμη της τεχνολογίας IoT, τα εικονικά εγκλήματα θα μπορούσαν να ξεπεράσουν τα όρια του κυβερνοχώρου και να απειλήσουν μέχρι και την ανθρώπινη ζωή. Οι συγγραφείς αναφέρουν μια περίπτωση από τον Ιανουάριο του 2017, όταν ο Οργανισμός Τροφίμων και Φαρμάκων των ΗΠΑ (FDA) δημοσίευσε μια προειδοποίηση ότι ορισμένα μοντέλα βηματοδότη (μια συσκευή που χρησιμοποιείται από ασθενείς με καρδιακή αρρυθμία για τη ρύθμιση των συσπάσεων του καρδιακού μυός) ήταν ευάλωτα στο hacking. [1]

Μια άλλη ευπάθεια εντοπίστηκε στη διαδικασία σύνδεσης στην πύλη μιας έξυπνης ηλεκτρικής σκούπας LG, επιτρέποντας σε μια ομάδα ερευνητών να έχουν πρόσβαση σε ζωντανή ροή βίντεο από το εσωτερικό του σπιτιού του ιδιοκτήτη. Σε ένα παρόμοιο περιστατικό, μονάδες CCTV για παρακολούθηση βρεφών (κοινώς γνωστές ως "κάμερες νταντάς") έγιναν πρόσβασιμες και το υλικό έγινε διαθέσιμο στο κοινό. Οι έξυπνες κλειδαριές,

για παράδειγμα, θα μπορούσαν να προγραμματιστούν ώστε να ξεκλειδώνουν εάν μια συγκεκριμένη συσκευή εντοπιστεί από το ασύρματο δίκτυο του κτίριου, επιτρέποντας σε έναν εγκληματία να έχει πρόσβαση στο σπίτι ή στο γραφείο κάποιου. Ένα σενάριο με θανατηφόρες συνέπειες θα ήταν εύλογο εάν μια έξυπνη κλειδαριά είναι προγραμματισμένη να κλειδώνει όταν ανιχνεύεται πυρκαγιά ή διαρροή αερίου. [1]

Μια τέτοια κατάσταση θα μπορούσε να είναι αποτέλεσμα μιας σκόπιμης επίθεσης ή συνέπεια μιας δυσλειτουργίας λόγω ανεπαρκούς σχεδίασης και έλλειψης προσαρμογής του συστήματος. Έτσι, ενώ διάφοροι τύποι επιθέσεων έχουν ήδη βιωθεί, το IoT εισάγει νέες κυβερνο-φυσικές απειλές στους χρήστες και τους ιατροδικαστές. Με άλλα λόγια, το IoT θα μπορούσε να μετατρέψει ορισμένους από τους υπάρχοντες ψηφιακούς κινδύνους μετατρέποντάς τους από απειλές για το απόρρητο και την ψηφιακή ασφάλεια σε απειλές φυσικής ασφάλειας. [1]

2.5.1.3. Ψηφιακά Ίχνη

Ο όρος ψηφιακά ίχνη χρησιμοποιείται για να περιγράψει μια πληροφορία (αποθηκευμένη σε smartphone και συσκευές IoT) η οποία είναι σε θέση να αποδείξει ή να διαψεύσει ορισμένες υποθέσεις, και επομένως θα μπορούσε να βοηθήσει τους επαγγελματίες της εγκληματολογίας να βρουν απαντήσεις και να ανασυνθέσουν τη σκηνή του εγκλήματος. Για παράδειγμα, τα ψηφιακά ίχνη μπορεί να παρέχουν πληροφορίες σχετικά με το πότε απενεργοποιήθηκε ένας έξυπνος συναγερμός στο σπίτι ή για το πότε άνοιξε μια συγκεκριμένη πόρτα. Επίσης, οι πληροφορίες που συλλέγονται από έναν ανιχνευτή καπνού ή μονοξειδίου του άνθρακα θα μπορούσαν να προσδιορίσουν την ακριβή στιγμή και το σημείο όπου ξεκίνησε η φωτιά στο κτίριο. [1]

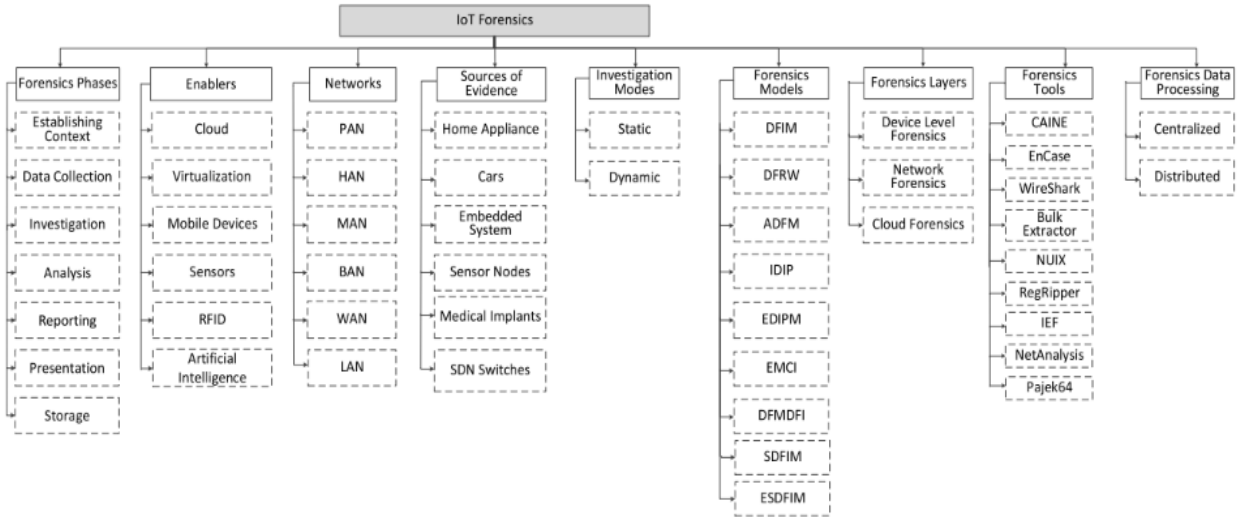
Φορητές συσκευές όπως τα έξυπνα ρολόγια ή οι ιχνηλάτες γυμναστικής μπορούν να χρησιμοποιηθούν για την αναγνώριση ενός ατόμου μέσω των βιομετρικών του πληροφοριών (π.χ. καρδιακοί παλμοί). Παραδείγματα τέτοιων εγκληματολογικών τεχνουργημάτων μπορεί να περιλαμβάνουν αποθηκευμένες μικρογραφίες εικόνων και θραύσματα των ροών της κάμερας, καθώς και κρυφά συμβάντα που ενεργοποιούνται από τους αισθητήρες, και πλήρη αρχεία καταγραφής συμβάντων που είναι αποθηκευμένα στη βάση δεδομένων της εφαρμογής. Ασφαλώς, αυτά τα αρχεία περιλαμβάνουν ευαίσθητες προσωπικές πληροφορίες σχετικά με την ταυτότητα, την τοποθεσία, τη δραστηριότητα των χρηστών, καθώς και γενικές συνδέσεις και χρονολογία, και επομένως πρέπει να συλλέγονται και να αναλύονται με ιδιαίτερη προσοχή στη δεοντολογία και το απόρρητο. [1]

3. IoT Digital Forensics

3.1. Ταξινόμηση των IoT Digital Forensics

Αυτή η ενότητα περιγράφει την ταξινόμηση της εγκληματολογίας του IoT που απεικονίζεται στο σχήμα 5. Τα χαρακτηριστικά αυτής της ταξινόμησης περιλαμβάνουν φάσεις εγκληματολογίας, ενεργοποιητές, δίκτυα, πηγές αποδεικτικών στοιχείων, τρόπους έρευνας, εγκληματολογικά μοντέλα, επίπεδα εγκληματολογίας, εργαλεία εγκληματολογίας και επεξεργασία εγκληματολογικών δεδομένων, όπως φαίνεται και στο σχήμα. Στο τέλος του παρόν υποκεφαλαίου θα παρουσιαστούν και τα Point of Focus των Digital Forensics που είναι ένα διαφορετικό approach από αυτά που βλέπουμε παρακάτω στο σχήμα για τα Digital Forensics.

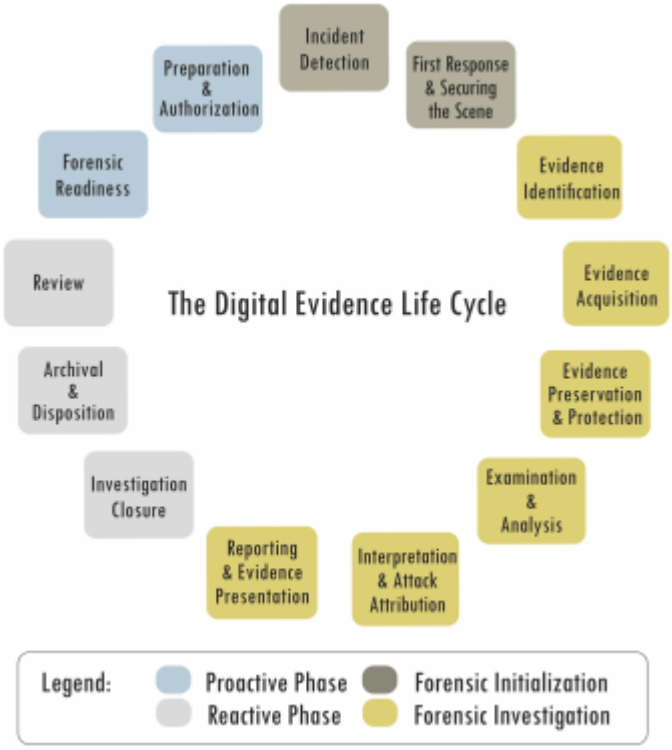
Στη συνέχεια οι παρακάτω ιδιότητες συζητούνται εν συντομία. [64]



Σχήμα 5: Η ταξινόμηση των IoT Forensics

3.1.1. Forensics phases

Μια τυπική εγκληματολογική έρευνα IoT ξεκινά με τον καθορισμό του πλαισίου. Η ομάδα έρευνας εφαρμόζει πολλές μετρήσεις ασφαλείας, όπως λογισμικό και εργαλεία ασφαλείας, στα τεράστια δεδομένα που πρόκειται να συλλεχθούν από διαφορετικές τοποθεσίες [6]. Η επιβολή του νόμου που σχετίζεται με την έρευνα, όπως η νομοθεσία περί ιδιωτικού απορρήτου, πνευματικών δικαιωμάτων και τεχνολογίας πληροφοριών, μεταξύ άλλων, επιβεβαιώνονται εκ νέου και συμφωνούνται πλήρως από τον ερευνητή πριν από την πραγματική έρευνα. Στη συνέχεια συλλέγονται στοιχεία από διάφορες πηγές, τα οποία διερευνώνται και αναλύονται περαιτέρω στην επόμενη φάση. Με βάση τα στοιχεία, το τελικό συμπέρασμα αναφέρεται στο έγγραφο και παρουσιάζεται στα ενδιαφερόμενα μέρη. Στην τελική φάση, τα δεδομένα που συλλέχθηκαν και οι τελικές εκθέσεις αρχειοθετούνται σε ψηφιακή μορφή για μελλοντική χρήση. [64]



[1]

Σχήμα 6: Forensics Evidence Life Cycle

Στη συνέχεια θα αναλύσουμε καθε μία από τις 6 μεθόδους που αφορούν το forensics κομμάτι λοιπόν. [1]

3.1.1.1. Evidence Identification

Το πρώτο και ίσως το πιο ουσιαστικό μέρος κάθε ιατροδικαστικής εξέτασης είναι η αναζήτηση αποδεικτικών στοιχείων. Η αναγνώριση στο πλαίσιο του IoT είναι ιδιαίτερα δύσκολη, καθώς σε ορισμένες περιπτώσεις οι εξεταστές δεν γνωρίζουν καν πού αποθηκεύονται φυσικά τα δεδομένα που διερευνήθηκαν. Ακόμη και μια απλή εργασία όπως η εύρεση της παραβιασμένης συσκευής IoT και η ανακατασκευή της σκηνής του εγκλήματος μπορεί να είναι προκλητική. Οι ακόλουθες γραμμές εξηγούν ποια προβλήματα αντιμετωπίζουν οι ερευνητές κατά τη διάρκεια αυτού του πρώτου βήματος του Κύκλου Ζωής της Έρευνας Εγκληματολογικών Ερευνών. [1]

3.1.1.1.1. Πεδίο εφαρμογής του συμβιβασμού και της ανασυγκρότησης της σκηνής του εγκλήματος:

Το πλαίσιο του IoT, ωστόσο, συνεπάγεται σε πραγματικό χρόνο και αυτόνομη αλληλεπίδραση μεταξύ διαφόρων κόμβων, γεγονός που καθιστά σχεδόν αδύνατη την ανακατασκευή του τόπου του εγκλήματος και τον προσδιορισμό του εύρους της ζημίας, λόγω της εξαιρετικά δυναμικής φύσης της επικοινωνίας. [1]

3.1.1.1.2. Διάδοση συσκευών και δεδομένων:

Οι επαγγελματίες εγκληματολόγοι όχι μόνο πρέπει να προσδιορίσουν τι είναι χρήσιμο για την έρευνα, αλλά και να απορρίψουν τα άσχετα δεδομένα, γεγονός που καθιστά δύσκολη την έγκαιρη ανάλυση. [1]

3.1.1.1.3 Τοποθεσία δεδομένων:

Τα δεδομένα που προέρχονται από ιχνηλάτες γυμναστικής, έξυπνα ρολόγια, έξυπνα ρούχα ή μεγαλύτερα κινητά αντικείμενα, όπως αυτοκίνητα, ποδήλατα και drones, δεν είναι σταθερά σε μια συγκεκριμένη γεωγραφική θέση. [1]

3.1.1.1.4 Τύπος συσκευής:

Σε αντίθεση με την παραδοσιακή επιστήμη της ψηφιακής εγκληματολογίας, όπου τα αντικείμενα εγκληματολογικού ενδιαφέροντος συνήθως περιορίζονται σε διαφορετικούς τύπους συστημάτων ηλεκτρονικών υπολογιστών ή κινητών τηλεφώνων, η πηγή αποδεικτικών στοιχείων σε υποθέσεις με επίκεντρο το IoT θα μπορούσε να είναι ετερογενής: ξεκινώντας από ένα αυτόνομο όχημα που προκάλεσε θανατηφόρο ατύχημα, σε μια έξυπνη τοστιέρα που άναψε κατά τη διάρκεια της νύχτας και προκάλεσε φωτιά στο νοικοκυριό. [1]

3.1.1.2. Evidence Acquisition

Υποθέτοντας ότι η σχετική συσκευή IoT έχει αναγνωριστεί επιτυχώς, το δεύτερο βήμα θα ήταν η συλλογή των αποδεικτικών δεδομένων. Ωστόσο, σε αυτό το σημείο οι ερευνητές πρέπει να αντιμετωπίσουν ένα άλλο πρόβλημα: μέχρι σήμερα, δεν υπάρχει καθοδήγηση ή τυποποιημένη μέθοδος για τη συλλογή αποδεικτικών στοιχείων από μια συσκευή IoT με ιατροδικαστικά ορθό τρόπο. [1]

3.1.1.2.1 Έλλειψη εκπαίδευσης και αδύναμη διαχείριση γνώσης:

Η NIST Forensics Science Challenges Report προσδιορίζει την ανάγκη για εκπαίδευση στο cloud για τους πρώτους ανταποκριτές και τους ερευνητές. Ερευνητές προτείνουν επίσης ότι οι υπηρεσίες επιβολής του νόμου θα πρέπει να οργανώσουν προγράμματα κατάρτισης για τους πρώτους ανταποκριτές τους, προκειμένου να τους καθοδηγήσουν πώς να αποκτούν ψηφιακά στοιχεία με ιατροδικαστικό τρόπο. [1]

3.1.1.2.2. Κρυπτογράφηση δεδομένων:

Αναμφίβολα, η κρυπτογράφηση ήταν πάντα ένα από τα πιο απαιτητικά ζητήματα στην Ψηφιακή Εγκληματολογία. Σήμερα, για τη βελτίωση της εμπιστοσύνης των καταναλωτών, πολλά λειτουργικά συστήματα και πλατφόρμες παρέχουν ολοκληρωμένη υποστήριξη για κρυπτογράφηση. Οι αλγόριθμοι επιτρέπουν στους χρήστες να κωδικοποιήσουν τα δεδομένα πριν τα στείλουν στο cloud και να τα αποκρυπτογραφήσουν αφού επιστρέψουν στο δικό τους σύστημα. [1]

3.1.1.2.3. Προδιαγραφές ετερογενούς λογισμικού και/ή υλικού:

Μια άλλη τεχνική πρόκληση που σχετίζεται με την εξαγωγή στοιχείων από συσκευές IoT είναι ότι κάθε κατασκευαστής υιοθετεί διαφορετικό υλικό και λειτουργικά συστήματα. Εκτός από αυτήν την πολυπλοκότητα, τα πρωτόκολλα επικοινωνίας των συσκευών IoT μπορεί να είναι εξίσου διαφορετικά, είτε πρόκειται για ZigBee, WiFi, Bluetooth κ.λπ. [1]

3.1.1.2.4. Απόρρητο και ηθικά ζητήματα από την πρόσβαση σε προσωπικά δεδομένα:

Πέρα από τις τεχνικές προκλήσεις, το απόρρητο είναι ένα σημαντικό ζήτημα που πρέπει να λαμβάνεται υπόψη κατά τη συλλογή δεδομένων. Οι συσκευές IoT, όπως οι ιχνηλάτες φυσικής κατάστασης ή τα απομακρυσμένα συστήματα παρακολούθησης της υγείας, ασχολούνται με ευαίσθητες προσωπικές πληροφορίες, συμπεριλαμβανομένων των ιατρικών αρχείων, των συνταγών ή της τρέχουσας κατάστασης υγείας των χρηστών. Για να μην παραβιάζονται οι συμφωνίες εμπιστευτικότητας με τους πελάτες τους, οι πάροχοι υπηρεσιών cloud αρνούνται να δώσουν στις αρχές πρόσβαση στην κοινόχρηστη μνήμη, επειδή μπορεί επίσης να περιέχει δεδομένα πελατών που δεν σχετίζονται με την έρευνα. [1]

3.1.1.2.5. Ιατροδικαστική αξία αποδεικτικών στοιχείων:

Ορισμένοι πάροχοι υπηρεσιών IoT σταματούν να υποστηρίζουν τα πλαίσια τους και προσπαθούν να παρέχουν ενημερώσεις ασφαλείας. Αυτό ισχύει ιδιαίτερα για εταιρείες, μέρος της διευρυνόμενης σκηνής των start-up, που αποφασίζουν να επικεντρωθούν σε νέα προϊόντα και να σταματήσουν να υποστηρίζουν τα παλιά. Τα δεδομένα που συλλέγονται από τέτοιες συσκευές IoT είναι λιγότερο πολύτιμα, επειδή θα μπορούσαν εύκολα να τα χειριστεί ένας χάκερ που εκμεταλλεύτηκε τα τρωτά σημεία ασφαλείας. [1]

3.1.1.2.6 Έλλειψη κοινού εγκληματολογικού μοντέλου στο IoT:

Η θεωρία και η πράξη δεν διαθέτουν μια κοινά αποδεκτή και έγκυρη προσέγγιση απόκτησης για συστήματα IoT. Ανάλογα με την περίπτωση, το αρμόδιο ανακριτικό όργανο επιλέγει διαφορετικές μεθόδους. Ωστόσο, μια άτυχη επιλογή μεθοδολογίας θα μπορούσε να έχει πολλές πιθανές επιπλοκές. [1]

3.1.1.3. Evidence Preservation and Protection

Σε περίπτωση που οι ερευνητές βρουν μια πιθανώς παραβιασμένη συσκευή και καταφέρουν να συλλέξουν δυνητικά χρήσιμα δεδομένα, θα πρέπει να αντιμετωπίσουν μια άλλη πρόκληση: πώς να διατηρήσουν τα συγκεντρωμένα δεδομένα και να εγγυηθούν την ακεραιότητά τους [1]

3.1.1.3.1. Εξασφάλιση της αλυσίδας φύλαξης:

Στην περίπτωση του IoT Forensics, τα δεδομένα αποδεικτικών στοιχείων πρέπει να συλλέγονται από πολλούς απομακρυσμένους διακομιστές, γεγονός που περιπλέκει σημαντικά την αποστολή της διατήρησης της κατάλληλης Chain of Custody. Επιπλέον, η μορφή των δεδομένων που συλλέγονται από μια συγκεκριμένη συσκευή IoT μπορεί να διαφέρει από τη μορφή των δεδομένων που είναι αποθηκευμένα στο cloud. Αυτό οφείλεται

στο γεγονός ότι πριν αποθηκευτεί, επεξεργαζόταν με αναλυτικούς αλγόριθμους. Τέλος, πρέπει να επιστραφεί στην αρχική του μορφή πριν από την εκτέλεση της ανάλυσης, διαφορετικά δεν θα γίνει δεκτό στο δικαστήριο. [1]

Διάφοροι μελετητές υποστηρίζουν την ιδέα μιας Ψηφιακής Αλυσίδας Επιμέλειας (DCoC). Ορισμένοι προτείνουν τη χρήση τεχνολογίας blockchain για την προστασία της ασταθούς φύσης των ψηφιακών στοιχείων σε ένα εξαιρετικά αποκεντρωμένο περιβάλλον. [1]

3.1.1.3.2. Περιορισμός διάρκειας ζωής:

Μια άλλη πρόκληση στη διατήρηση δεδομένων σχετίζεται με τον περιορισμένο χώρο μνήμης στις συσκευές IoT. Λόγω του γεγονότος ότι τα συστήματα IoT λειτουργούν συνεχώς, τα δεδομένα θα μπορούσαν εύκολα να αντικατασταθούν, με αποτέλεσμα την πιθανότητα να λείπουν στοιχεία. [1]

3.1.1.3.3. Το(α) πρόβλημα(α) του Cloud Forensic:

Η συνέργεια μεταξύ cloud και IoT έχει προκύψει επειδή το cloud διαθέτει χαρακτηριστικά που επιτρέπουν και ωφελούν την επέκταση του IoT. Ωστόσο, το cloud αποτελείται από ένα τεράστιο ποσό ζητημάτων ασφαλείας. [1]

3.1.1.3.4. Ασφάλεια αποδεικτικών στοιχείων ανάλογα με την ανάπτυξη και/ή το μοντέλο υπηρεσίας του Cloud (PaaS, SaaS, IaaS):

Από την σκοπιά της εγκληματολογίας, η απόκτηση αποδεικτικών στοιχείων σε SaaS και PaaS αφορά κυρίως τους παρόχους υπηρεσιών, ενώ στην εγκληματολογία του IaaS, οι ερευνητές πρέπει να ασχοληθούν τόσο με τους παρόχους υπηρεσιών όσο και με τους πελάτες. Επομένως, η διερεύνηση δεδομένων ενός χρήστη IaaS μπορεί να απαιτεί λιγότερους περιορισμούς, αλλά στην περίπτωση του SaaS οι πληροφορίες αποδεικτικών στοιχείων πρόσβασης μπορεί να είναι ελάχιστες ή να λείπουν εντελώς. [1]

3.1.1.3.5. Προστασία Δεδομένων και Έλλειψη Διαφάνειας στις υπηρεσίες Cloud:

Όταν μιλάμε για υπολογιστικό νέφος, η αποθήκευση και η προστασία δεδομένων εκτελούνται συνήθως από τον προμηθευτή του IaaS. Δεδομένου ότι ο αριθμός των παρόχων επεκτείνεται, ο χρήστης έχει πολλές ευκαιρίες για να επιλέξει (π.χ. Google Cloud, AWS, Microsoft Azure, iCloud και πολλά άλλα). Αντίστοιχα, αλλάζουν και τα κριτήρια που χρησιμοποιούν οι πελάτες για να κρίνουν την ποιότητα της υπηρεσίας. Το 2018, μια μελέτη των Delphi σχετικά με τα κριτήρια για την επιλογή ενός παρόχου υπηρεσιών cloud προσδιόρισε τη λειτουργικότητα και την ευελιξία, αλλά και τη νομική συμμόρφωση, τη σύμβαση και τη γεωγραφική θέση των διακομιστών, ως τα κορυφαία χαρακτηριστικά ποιότητας της υπηρεσίας. [1]

3.1.1.3.6. Περίοδος αποθήκευσης δεδομένων στο Cloud:

Στις περισσότερες περιπτώσεις, η περίοδος αποθήκευσης δεδομένων καθορίζεται από τον πάροχο της υπηρεσίας. Η νομοθεσία σε διαφορετικές χώρες καθορίζει εάν θα αποθηκεύονται δεδομένα και για πόσο χρονικό διάστημα. Στις χώρες της ΕΕ, η περίοδος

αυτή μπορεί να κυμαίνεται από 6 μήνες έως 10 χρόνια, ανάλογα με τον τύπο των δεδομένων. Για τις ΗΠΑ, η περίοδος καθορίζεται μεμονωμένα, ωστόσο, υπάρχουν προμηθευτές που βρίσκονται σε χώρες όπου δεν υπάρχει νομική πρόβλεψη για ελάχιστη ή μέγιστη περίοδο αποθήκευσης, δημιουργώντας φυσικά προϋποθέσεις για τη διάπραξη εγκλημάτων. [1]

3.1.1.4. Examination and Evidence Analysis

3.1.1.4.1. Ανάλυση από άκρο σε άκρο:

Λόγω του γεγονότος ότι οι κόμβοι IoT λειτουργούν συνεχώς, παράγουν εξαιρετικά μεγάλο όγκο δεδομένων. Έχοντας αυτό υπόψη, είναι κατανοητό ότι η ανάλυση από άκρο σε άκρο των υπαρχουσών πληροφοριών υπερβαίνει τις ικανότητες ενός μόνο ερευνητή ή ακόμη και μιας μονάδας διερεύνησης. [1]

3.1.1.4.2. Προέλευση δεδομένων:

Ως ζωτικό μέρος οποιασδήποτε διαδικασίας έρευνας, η προέλευση των δεδομένων παρέχει στους εξεταστές πληροφορίες σχετικά με την ιδιοκτησία και το ιστορικό τροποποιήσεων των αντικειμένων δεδομένων. Σε αντίθεση με τις παλιομοδίτικες εξετάσεις ψηφιακής εγκληματολογίας, στο IoT Forensics υπάρχει λιγότερη βεβαιότητα για το από πού προέρχονται τα δεδομένα, καθώς και για το ποιος ή τι δημιούργησε ή/και τροποποίησε το αντικείμενο δεδομένων. Ο βαθμός στον οποίο θα μπορούσε να διευκρινιστεί η προέλευση των δεδομένων εξαρτάται από το μοντέλο cloud ή από την προθυμία του προμηθευτή να συνεργαστεί με τις αρχές. [1]

3.1.1.4.3. Time Lining και περιορισμένη συσχέτιση αποδεικτικών στοιχείων:

Η συντριπτική πλειονότητα των συσκευών IoT δεν αποθηκεύει μεταδεδομένα (π.χ. πληροφορίες ώρας και γεωχωρικού χώρου, πληροφορίες πνευματικών δικαιωμάτων, ημερομηνία δημιουργίας και τελευταίας τροποποίησης). Αυτό πρακτικά καθιστά σχεδόν αδύνατη τη συσχέτιση και τη λογική συνέπεια των στοιχείων, που συλλέγονται από πολλούς κόμβους IoT. Υπάρχει έτσι το πρόβλημα της ενοποιημένης γραμμής ώρας, στην περίπτωση του οποίου διαφορετικές πηγές παρουσιάζουν διαφορετικές αναφορές ζώνης ώρας, ζητήματα λοξής/μετακίνησης ρολογιού και ερμηνείες χρονικών σφραγίδων. Χωρίς χρονικές πληροφορίες, οι ερευνητές μπορούσαν μόνο να κάνουν εικασίες σχετικά με τις αιτιώδεις συνδέσεις. [1]

3.1.1.4.4. Νομικά θέματα:

Ένα από τα κύρια σημεία αναφέρεται στην αντικρουόμενη νομική καθοδήγηση σε περίπτωση διασυνοριακών εγκλημάτων, συμπεριλαμβανομένης της απουσίας σαφών διαδικαστικών και συμβατικών συμφωνιών. Ένα μεμονωμένο αρχείο θα μπορούσε να αναλυθεί σε πολλαπλά μπλοκ δεδομένων που βρίσκονται σε διαφορετικούς κόμβους και ως εκ τούτου εμπίπτουν σε διαφορετικές δικαιοδοσίες. Στη χειρότερη περίπτωση, αυτό οδηγεί σε παραβίαση του νόμου στην πολιτεία όπου διεξάγεται πραγματικά η ιατροδικαστική πρακτική. Το γεγονός ότι κάθε χώρα έχει τους δικούς της κανονισμούς, αυξάνει έτσι

σημαντικά τον χρόνο, το κόστος και τη δυσκολία που σχετίζεται με μια συγκεκριμένη έρευνα. [1]

3.1.1.5. Interpretation and Attack Attribution

Όλες οι διαδικασίες έρευνας στοχεύουν στον εντοπισμό εγκληματικών μερών. Ωστόσο, ακόμη και αν τα στοιχεία υποστηρίζουν ότι ένας συγκεκριμένος κόμβος IoT είναι η αιτία του εγκλήματος, αυτό δεν σημαίνει ότι η συσκευή που έχει εντοπιστεί θα οδηγήσει τους ερευνητές στους εγκληματίες. [1]

3.1.1.5.1. Έλλειψη πληροφοριών χρήστη/ανωνυμία IP:

Οι περισσότεροι από τους παρόχους υπηρεσιών cloud διατηρούν φιλικές προς το χρήστη πολιτικές και απαιτούν ελάχιστες πληροφορίες κατά την εγγραφή τους σε μια υπηρεσία. Η υιοθέτηση εργαλείων σκοταδισμού IP, μαζί με τα προαναφερθέντα εύχρηστα χαρακτηριστικά πολλών συστημάτων cloud, περιπλέκει σοβαρά τον εντοπισμό ενός εγκληματία. [1]

3.1.1.5.2. Κοινή χρήση πόρων και προσδιορισμός υποχρεώσεων:

Πρέπει να επισημανθεί ότι ορισμένα συμβάντα ένδειξης παρουσίας (π.χ. ανίχνευση κίνησης ή άνοιγμα πόρτας) δεν αποκαλύπτουν απαραίτητα την ταυτότητα κάποιου. Στο παρακάτω παράδειγμα, ο συναγερμός απενεργοποιήθηκε πριν ανοίξει η πόρτα του σπιτιού και μπει ένα άτομο στο κτίριο. Από τη μία πλευρά, τα ψηφιακά ίχνη υποδηλώνουν ότι ο ιδιοκτήτης του σπιτιού έδωσε την εντολή και μπήκε στο σπίτι τους. Από την άλλη πλευρά, ο ιδιοκτήτης του σπιτιού θα μπορούσε επίσης να είχε εκδώσει την εντολή εξ αποστάσεως και έτσι να παραχωρήσει σε κάποιον άλλο πρόσβαση στο κτίριο. [1]

3.1.1.6. Reporting and Evidence Presentation

Η παρουσίαση των ευρημάτων μιας υπόθεσης με επίκεντρο το IoT θέτει ορισμένες νέες προκλήσεις. Υπάρχουν νομικά συστήματα (π.χ. το νομικό σύστημα των ΗΠΑ) που απαιτούν την παρουσίαση των αποδεικτικών στοιχείων ενώπιον μιας επιτροπής ενόρκων στην αίθουσα του δικαστηρίου. Πριν ανακριθούν και επιλεγούν από τον δικαστή και/ή τους δικηγόρους, οι πιθανοί ένορκοι επιλέχθηκαν από την κοινότητα χρησιμοποιώντας μια εύλογα τυχαία μέθοδο. Αυτό σημαίνει ότι η κριτική επιτροπή πιθανότατα έχει μόνο βασική κατανόηση του cloud computing και της εγκληματολογίας, με βάση τα μέσα ενημέρωσης ή την προσωπική τους εμπειρία με την τεχνολογία IoT. Θα ήταν μια πρόκληση να τους εξηγήσουμε τις τεχνικές λεπτομέρειες πίσω από μια τόσο περίπλοκη αρχιτεκτονική στον πολύ περιορισμένο χρόνο της δοκιμής. [1]

3.1.2. Enablers

Μετά τα forensics phases που συζητήθηκαν στο 3.1.1 ο ερευνητής θα πρέπει να κοιτάξει τα enablers των συσκευών IoT. Το IoT αποτελείται από διάφορες τεχνολογίες, όπως κόμβους αισθητήρων, κινητές συσκευές, εικονικοποίηση, cloud, αναγνώριση ραδιοσυχνοτήτων (RFID), εξοπλισμό δικτύου και Τεχνητή Νοημοσύνη (AI). Αυτές οι

τεχνολογίες διαδραματίζουν μεμονωμένους ρόλους κατά τη διαδικασία της εγκληματολογικής έρευνας. Οι βασικές συσκευές IoT, όπως οι κόμβοι αισθητήρων και οι κινητές συσκευές, χρησιμοποιούνται για τη συλλογή στοιχείων από τον τόπο του εγκλήματος μετά την επίθεση. Το cloud και η τεχνολογία εικονικοποίησης παρέχουν υποστήριξη κατ' απαίτηση, επεκτάσιμη, ελαστική, υπολογιστική ως υπηρεσία κατά τη διάρκεια ολόκληρης της διαδικασίας εγκληματολογίας. Το RFID χρησιμοποιείται εκτενώς σε συσκευές αισθητήρων για την αναγνώριση αντικειμένων. Ο εξοπλισμός δικτύου, όπως οι δρομολογητές, οι μεταγωγείς και οι μεταγωγείς δικτύωσης που καθορίζονται από το λογισμικό (SDN), επιτρέπουν την παρακολούθηση της ανίχνευσης πακέτων. Οι τεχνικές τεχνητής νοημοσύνης χρησιμοποιούνται εκτενώς για την ανάλυση των δεδομένων που συλλέγονται. [64]

3.1.3. Networks

Τα χαρακτηριστικά δικτύου αναφέρονται στον τύπο του δικτύου που συνδέεται με συσκευές IoT στον τόπο του εγκλήματος. Ο τύπος δικτύου διαδραματίζει σημαντικό ρόλο κατά τη διαδικασία έρευνας και διασφαλίζει ότι η περιοχή της περιοχής καλύπτεται και τηρείται η επιβολή του νόμου. Το Τοπικό Δίκτυο (LAN), το Μητροπολιτικό Δίκτυο (MAN) και το Προσωπικό Δίκτυο Περιοχής (PAN) χρησιμοποιούνται ευρέως για τη διασύνδεση συσκευών IoT εντός περιορισμένου εύρους. Παραδείγματα αυτών των δικτύων είναι κάμερες παρακολούθησης που είναι εγκατεστημένες σε δρόμους και εμπορικά κέντρα. Οι οικιακές συσκευές, όπως πλυντήρια ρούχων και ψυγεία, είναι συνδεδεμένες στο Home Area Network (HAN). Το cloud computing παίζει σπουδαίο ρόλο για τις συσκευές IoT όσον αφορά την αποθήκευση και την επεξεργασία δεδομένων. Οι συσκευές IoT συνδέονται στο Δίκτυο ευρείας περιοχής (WAN) για να ενσωματώσουν τις εφαρμογές cloud μέσω API. [64]

3.1.4. Sources of evidence

Οι πληροφορίες που σχετίζονται με το έγκλημα στο IoT και τα cybersecurity incidents γενικότερα μπορούν να συλλεχθούν από τις διαφορετικές σκηνές του εγκλήματος εστιάζοντας στην βασική πηγή αποδεικτικών στοιχείων. Στο IoT, τα δεδομένα μπορούν να βρίσκονται κυρίως στις συσκευές, όπως οι οικιακές συσκευές, οι κόμβοι αισθητήρων, τα ιατρικά εμφυτεύματα, τα ενσωματωμένα συστήματα και τα αυτοκίνητα. Αν και οι χώροι μνήμης των εφαρμογών IoT είναι χαμηλοί, πολύτιμες πληροφορίες αποστέλλονται στον κεντρικό υπολογιστή επεξεργασίας για επεξεργασία μέσω του δικτύου. Δεδομένα, όπως το αρχείο καταγραφής συστήματος και η προσωρινή μνήμη cache, μπορούν να χρησιμοποιηθούν ως πηγές αποδεικτικών στοιχείων. Αυτά τα δεδομένα μπορούν να ανακτηθούν ανιχνεύοντας πολλές συσκευές δικτύου, όπως δρομολογητές, SDN και μεταγωγείς, μεταξύ άλλων. [64]

3.1.5. Investigation modes

Ο τρόπος έρευνας κατηγοριοποιεί το είδος της έρευνας με βάση το χρονοδιάγραμμα της έρευνας. Η στατική λειτουργία είναι η παραδοσιακή μέθοδος έρευνας που εκτελείται μετά τον εντοπισμό της επίθεσης στο σύστημα IoT. Ως αποτέλεσμα της επίθεσης, τα δεδομένα IoT έχουν ήδη καταστραφεί ή διαγραφεί. Η στατική λειτουργία ανακτά δεδομένα χρησιμοποιώντας γενικό σειριακό δίαυλο και σάρωση κρυφής μνήμης, μεταξύ άλλων. Η διερεύνηση της εγκληματολογίας του IoT απαιτεί μερικές φορές το σύστημα να είναι ζωντανό

κατά τη διάρκεια της διαδικασίας για την ανακάλυψη νέων δεδομένων, όπως ανοικτή σύνδεση δικτύου, αποθήκες μνήμης και διεργασίες που εκτελούνται, για την εξαγωγή σημαντικών πηγών αποδεικτικών στοιχείων. Αυτός ο τύπος λειτουργίας έρευνας είναι γνωστός ως δυναμικός τρόπος. [64]

3.1.6. Forensics models

Στη βιβλιογραφία έχουν συναντηθεί διάφορα Forensics model όπως το DFRWS, ADFM, IDIP που έχουν βρεθεί στο [62], το DFIM, DFRW, ADFM, IDIP, EDIPM, EMCI, DFMDFI, SDFIM, ESDFIM που βρέθηκαν στο [64].

Σύντομα τα μοντέλα αυτά έχουν ως ακολούθως:

DFRWS [62]:
- Έχει 6 φάσεις: Identification, Collection, Examination record and Analyses and Presentation
- Άλλοι ερευνητές [62] χρησιμοποιούν αυτό το μοντέλο με τις 6 φάσεις και άλλοι ουσιαστικά το ίδιο με μία φάση ακόμα, το decision [64]

DFRW [64]:
- Έχει 7 φάσεις: Identification, Collection, Examination record and Analyses, Presentation and decision

ADFM [62] [64]:
- Έχει διαχωριστεί από το DFRWS/DFRW προσθέτωντας 3 ακόμα φάσεις: preparation, approach strategy, and return of evidence

IDIP [62] [64]:
- Αποτελείται από 5 φάσεις: Readiness Phase, Deployment Phase, Physical Crime Scene Phase and Digital Crime Scene Investigation Phase and review
- Αναπτύσσεται περαιτέρω στο μοντέλο EDIPM [64]

EDIPM [64]:
- Προσθέτει 2 επιπλέον βήματα στο IDIP: traceback and dynamite
-

DFIM [64]:
- Το Digital Forensics Investigation Model (DFIM) είναι ένα μοντέλο τεσσάρων φάσεων που στοχεύει κυρίως στην αποκάλυψη κρυμμένων στοιχείων στα δεδομένα που συλλέγονται. Ωστόσο, δεν ενδιαφέρεται για τα πραγματικά στοιχεία, δηλαδή τα φυσικά στοιχεία, τα οποία είναι δυσμενή στην περίπτωση του IoT

EMCI [64]:
- Περιλαμβάνει 13 βήματα: awareness, authorization, planning, notification, identify evidence, collection of evidence, transport of evidence, storage of evidence, examination of evidence, hypothesis, presentation of hypothesis, proof of hypothesis, and archive storage

DFMDFI [64]:
- Στηρίζεται σε four-tier iterative approach
- Το 1ο tier ασχολείται με preparation, identification, authorization, and communication
- Το 2ο tier ασχολείται με τους κανόνες που σχετίζονται με collection, preservation, and documentation.

- Το 3ο tier ασχολείται με τους κανόνες που σχετίζονται με examination, exploratory testing and analysis,
- Το 4ο tier τέλος ασχολείται με το να παρέχει αποτελέσματα, reviews και αναφορές

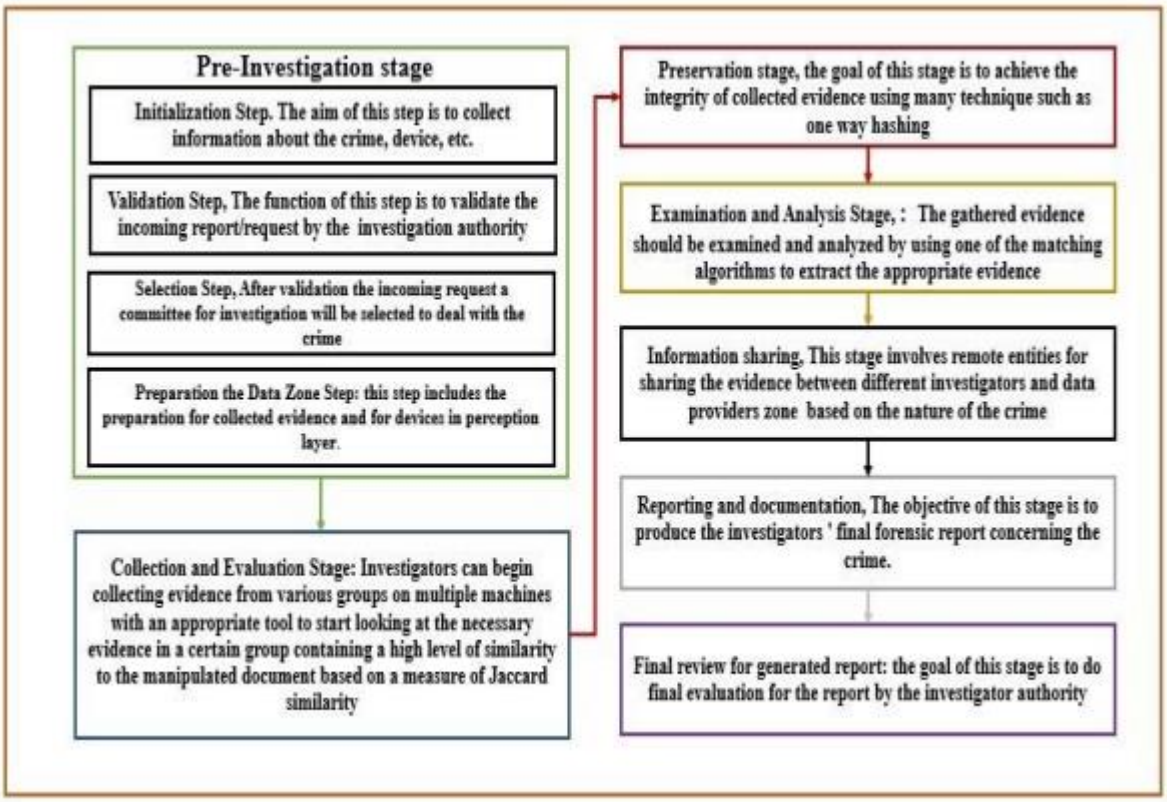
SDFIM [64]:

- Το SDFIM χωρίζει το digital forensic investigation process σε 11 φάσεις:
- preparation, securing the scene, survey & recognition, documentation of scene, communication shielding, evidence collection, preservation, examination, analysis, presentation, result & review

ESDFIM [64]:

- Το ESDFIM χωρίζει το digital forensic investigation process σε 6 φάσεις:
- Preparation, acquisition and preservation, examination and analysis, information sharing, presentation, review

Στο σχήμα 7 στη συνέχεια παρουσιάζονται τα βήματα του πλαισίου DFIM ενώ παρατίθενται στη συνέχεια και η μέθοδος DFIF. Στα frameworks ανά χρονολογία μπορούν να βρεθούν επίσης διαφορα frameworks σε συνδυασμό με τα βήματα και τα στάδια τους έτσι όπως έχουν βρεθεί χρονολογικά.



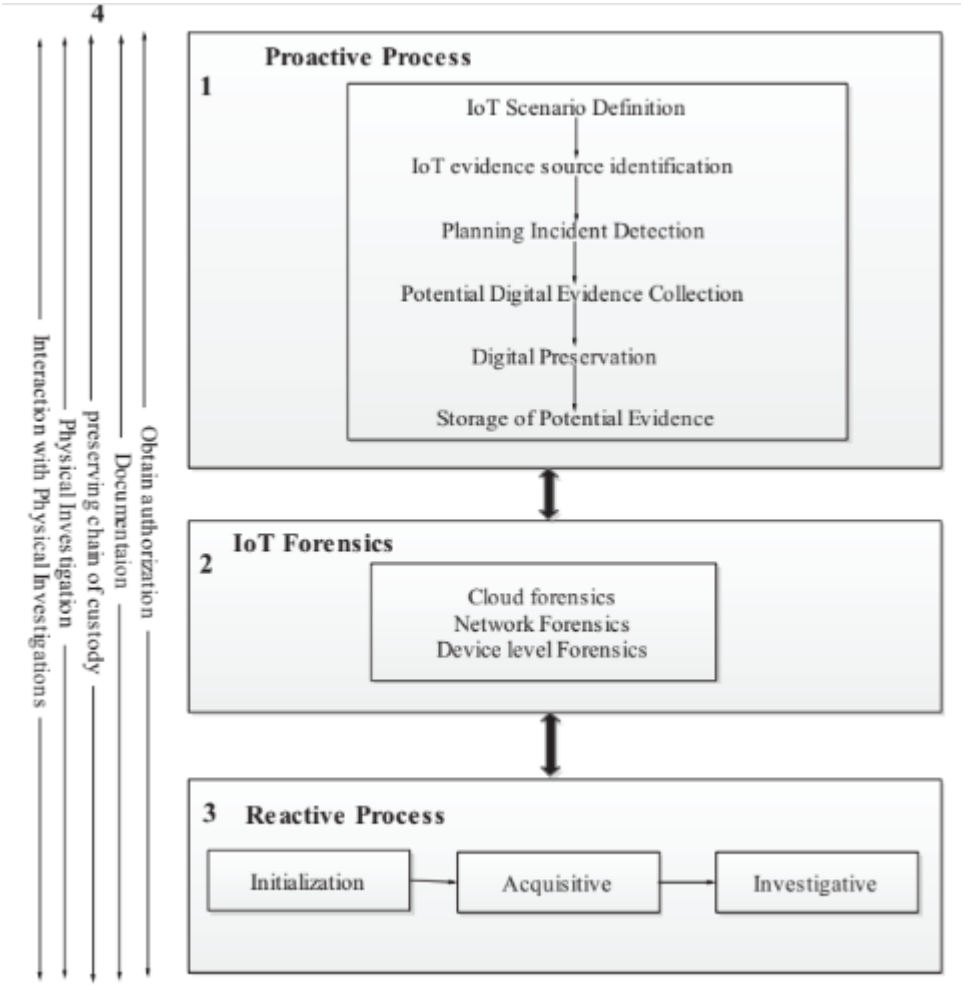
[11]

Σχήμα 7: Τα στάδια του DFIM

Πολλά ακόμα μοντέλα υπάρχουν παρόλα αυτά όπως το DFIF το οποίο συναντήθηκε στο [4]

3.1.6.1. DFIF-IoT

Το DFIF-IoT έχει παρουσιαστεί ως ένα γενικό πλαίσιο που συμμορφώνεται με το διεθνές πρότυπο ISO/IEC 27043:2015. Επιπλέον, αυτό το πλαίσιο έχει κατασκευαστεί με συνδυασμό τριών διακριτών ενοτήτων και συγκεκριμένα: Proactive process, IoT Forensics και reactive (investigation) διαδικασία. Η προληπτική διαδικασία παρουσιάζεται ως διαδικασία DFR που επιτρέπει στα περιβάλλοντα IoT να σχεδιάζουν και να προετοιμάζονται για πιθανά συμβάντα. Περιλαμβάνει υποδιεργασίες: Ορισμός σεναρίου IoT, Αναγνώριση πηγής αποδεικτικών στοιχείων IoT, Ανίχνευση συμβάντων προγραμματισμού, συλλογή πιθανών ψηφιακών αποδεικτικών στοιχείων, ψηφιακή διατήρηση και αποθήκευση πιθανών αποδεικτικών στοιχείων. Στη συνέχεια, είναι το IoT Forensics που αποτελείται από τα εξής: Cloud Forensics, Network Forensics (NF) και Device-Level Forensics (DLF). Ακολουθεί η Αντιδραστική Διαδικασία που αποτελείται από διαδικασίες Εκκίνησης, Απόκτησης και Διερεύνησης. Η αντιδραστική διαδικασία στο DFIF-IoT παρουσιάζεται ως απόκριση μετά το συμβάν που διεξάγεται εάν εντοπιστεί ένα πιθανό συμβάν ασφαλείας. Τέλος είναι οι ταυτόχρονες διεργασίες που έχουν ληφθεί αυτολεξεί από το ISO/IEC 27043: 2015. Το σχήμα 8 δείχνει το πλαίσιο DFIF-IoT. [4]



[4]

Σχήμα 8: DFIF-IoT Framework

3.1.7. Forensics layers

Η εγκληματολογία IoT αποτελείται από τρία επίπεδα: συσκευή, δίκτυο και εγκληματολογία σε επίπεδο cloud. Στην εγκληματολογία σε επίπεδο συσκευής, ο ερευνητής συλλέγει αποδεικτικά δεδομένα κυρίως από συσκευές IoT, όπου τα δεδομένα αποθηκεύονται με ακρίβεια στην τοπική μνήμη. Η εγκληματολογία σε επίπεδο δικτύου συλλέγει δεδομένα από συσκευές δικτύου για να κρίνει ή να κατηγορήσει έναν ύποπτο. Οι συσκευές IoT συνήθως επικοινωνούν μεταξύ τους μέσω κάποιου δικτύου, π.χ. LAN, WAN, MAN, PAN, κ.λπ. Τα δίκτυα περιέχουν χρήσιμα δεδομένα που μπορούν να λειτουργήσουν ως αξιόπιστα στοιχεία, όπως δεδομένα καταγραφής δικτύου και πληροφορίες κρυφής μνήμης. Οι περισσότερες συσκευές IoT έχουν χαμηλές δυνατότητες επεξεργασίας και αποθήκευσης. Συνδέονται με το κέντρο δεδομένων cloud για αποθήκευση ή επεξεργασία δεδομένων. Το Cloud Forensics ασχολείται με την εγκληματολογική έρευνα για δεδομένα IoT που είναι αποθηκευμένα στο cloud σε περίπτωση επίθεσης. [64]

3.1.8. Forensics tools

Η ιατροδικαστική έρευνα των επιθέσεων IoT εκτελείται από καλά εκπαιδευμένους εμπειρογνώμονες που έχουν καλή γνώση της πληροφορικής και της επιβολής του νόμου. Παρόλο που η διερεύνηση της εγκληματολογίας του IoT περιλαμβάνει πολλές προκλήσεις, δηλαδή τεράστιο όγκο συλλογής δεδομένων και ανάλυση δεδομένων σε πραγματικό χρόνο, αυτές οι προκλήσεις μπορούν να αντισταθμιστούν με τη βοήθεια των διαφόρων εργαλείων εγκληματολογίας. Το Computer Aided Investigative Environment (CAINE) είναι ένα διαδραστικό και ανοιχτού κώδικα εργαλείο εγκληματολογίας που υποστηρίζει πολλαπλές φάσεις εγκληματολογίας. Το EnCase χρησιμοποιείται για την εκτέλεση αναλύσεων για εγκληματολογικές εικόνες, δεδομένα και αρχεία. Το Wireshark χρησιμοποιείται ως επί το πλείστον για εγκληματολογική ανάλυση δικτύου. Ο κύριος περιορισμός του Wireshark είναι ότι δεν λειτουργεί καλά με τα μεγάλα δεδομένα δικτύου. Το Bulk Extractor βοηθά στη σάρωση και την εξαγωγή πληροφοριών, π.χ. αριθμών καρτών, διευθύνσεων email, διευθύνσεων ιστού και αριθμών τηλεφώνου από τις εικόνες του δίσκου και τα αρχεία καταλόγου. Το NUIX χρησιμοποιείται για τη σάρωση ενός τεράστιου όγκου δεδομένων και διαδικασιών που οδηγεί στην εξαγωγή χρήσιμων πληροφοριών αργότερα που θα χρησιμοποιηθούν για σκοπούς ανάλυσης. Το RegRipper χρησιμοποιείται κυρίως για τη σάρωση των αρχείων μητρώου των Windows. Το IEF χρησιμοποιείται για τη σάρωση των εγκληματολογικών εικόνων και ενός ευρέος φάσματος δεδομένων που εξάγονται από το ιστορικό Διαδικτύου, το ιστορικό συνομιλιών και τα λειτουργικά συστήματα. Το NetAnalysis βοηθά στη σάρωση των εγκληματολογικών εικόνων και δεδομένων που σχετίζονται με το ιστορικό του Διαδικτύου. Το Pajek64 βοηθά στην ανάλυση μεγάλου όγκου δεδομένων που σχετίζονται με το δίκτυο. [64]

Περισσότερα ακόμα εργαλεία και λογισμικά θα δούμε αναλυτικότερα στο Κεφάλαιο 5. Εκεί αφού εξετάσουμε διάφορα εργαλεία και λογισμικά ανα δίκτυο στη συνεχεια θα έχουμε ένα συγκεντρωτικό πίνακα με όλα τα εργαλεία και τις μεθόδους που συναντήθηκαν στην εργασία αυτή.

3.1.9. Forensics data processing

Η επεξεργασία των εγκληματολογικών δεδομένων αναφέρεται στον τρόπο με τον οποίο διεξάγεται η τοποθεσία υπολογισμού της εγκληματολογικής έρευνας. Στην κεντρική εγκληματολογία δεδομένων, τα εγκληματολογικά δεδομένα αποθηκεύονται σε έναν κεντρικό

διακομιστή υψηλής ασφάλειας, στον οποίο μπορούν να έχουν πρόσβαση σε διαφορετικές τοποθεσίες εξουσιοδοτημένοι ερευνητές. Η κεντρική επεξεργασία δεδομένων είναι χαμηλού κόστους και εξαιρετικά ασφαλής και προσφέρει εξαιρετικό έλεγχο στους διαχειριστές. Η επεξεργασία κατανεμημένων δεδομένων αναφέρεται στο πότε τα εγκληματολογικά δεδομένα και οι υπολογισμοί βρίσκονται σε κατανεμημένους διακομιστή. Έχει χαμηλή καθυστέρηση και χαμηλή καθυστέρηση αλλά χαμηλή ασφάλεια και υψηλό εύρος ζώνης. [64]

Πέρα από το παραπάνω καθοδηγητικό τρόπο όπου τα DF θα μπορούσαν να γίνουν στα IoT στη βιβλιογραφία συναντήσαμε και τα 1-2-3 Zones:

3.1.10. Τα Points of Focus - The 1-2-3 Zones of Digital Forensics

Στο IoT DF θα περιλαμβάνει το να γνωρίζουμε πού να κοιτάξουμε. Χωρίς να προσεγγίσουμε την εγκληματολογία του IoT με αυτόν τον τρόπο, θα χαθεί πολύτιμος χρόνος ψάχνοντας σε λάθος μέρη για άσχετα στοιχεία. Αυτό το έγγραφο προτείνει μια μέθοδο που βασίζεται σε ζώνη για την προσέγγιση των ερευνών που σχετίζονται με το IoT. [14]

3.1.10.1 Zone 1:

Η εσωτερική ζώνη όπου καταγράφεται όλο το υλικό, το λογισμικό και τα δίκτυα (π.χ. Bluetooth και Wi-Fi) που σχετίζονται με μια σκηνή εγκλήματος και λαμβάνεται μια απόφαση σχετικά με το τι είναι σχετικό με την υπόθεση και τι μπορεί να περιέχει στοιχεία που θα είναι χρήσιμα για την υπόθεση. Το IoTware σε αυτά τα δίκτυα, όπως οι έξυπνοι ελεγκτές θερμοκρασίας, μπορεί να είναι χρήσιμο ακόμη και μόνο για τα αναγνωριστικά των ετικετών τους (αναγνωριστικό ετικέτας) και την κατάστασή τους, π.χ. σε ύπνο, ξύπνιο και ενεργό/μετάδοση κ. [14]

3.1.10.2. Zone 2:

Σε αυτή τη ζώνη βρίσκονται όλες οι συσκευές και το λογισμικό που βρίσκονται στα όρια του δικτύου και που παρέχουν ένα μέσο επικοινωνίας μεταξύ των εσωτερικών και εξωτερικών δικτύων. Αυτή η ζώνη κρατά όλες όλες τις συσκευές με δημόσια προβολή των εν λόγω δικτύων. Οι εγκληματολογικές έρευνες συνήθως περιλαμβάνουν τον εντοπισμό αυτών των στοιχείων, την καταλογογράφηση τους και την ανάκτηση οποιωνδήποτε διαθέσιμων σχετικών αποδεικτικών στοιχείων από αυτά. Οι συσκευές σε αυτήν τη ζώνη μπορεί να περιλαμβάνουν συστήματα πρόληψης και ανίχνευσης εισβολής (IPS και IDS) και τείχη προστασίας δικτύου. [14]

3.1.10.3. Zone 3:

Αυτή η ζώνη καλύπτει όλο το υλικό και το λογισμικό που βρίσκεται εκτός του εν λόγω δικτύου. Αυτή η ζώνη περιλαμβάνει στοιχεία από όλα τα δεδομένα των παρόχων cloud, κοινωνικών δικτύων, παρόχων υπηρεσιών Διαδικτύου (ISP) και κινητών δικτύων. Υπηρεσίες που βασίζονται στο Διαδίκτυο και στο Διαδίκτυο, εικονικές διαδικτυακές ταυτότητες αντικειμένων, δίκτυο αιχμής, στοιχεία διαδικτυακής εργασίας (π.χ. 2 HAN γειτόνων), αποδεικτικά στοιχεία που βασίζονται σε συσκευές π.χ. αρχεία καταγραφής από ετικέτες RFID και αναγνώστες. συσκευές πύλης ή άκρων, κ.λπ. [14]

Η εφαρμογή αυτής της προσέγγισης θα είναι στη διακριτική ευχέρεια των ερευνητών DF και μπορεί να γίνει παράλληλα (όλες οι Ζώνες ερευνώνται ταυτόχρονα) ή μπορεί να προσδιοριστεί μια Ζώνη μεγαλύτερης προτεραιότητας (αυτό μπορεί να βασίζεται στην περιγραφή της αναφερόμενης συχνότητας και την πιθανώς την περιοχή με τον μεγαλύτερο αντίκτυπο) και μπορεί να ληφθεί απόφαση να επικεντρωθεί πρώτα σε αυτό. [14]

Η απόκριση σε ψηφιακές επιθέσεις που σχετίζονται με το IoT χρησιμοποιώντας τις Ζώνες 1-2-3 που περιγράφονται παρέχει στους ερευνητές DF μια χρήσιμη μέθοδο για τον σχεδιασμό και τη συστηματική προσέγγιση των ερευνών και τον αποτελεσματικό εντοπισμό πιθανών OOFI. Αυτή η προσέγγιση μειώνει την πολυπλοκότητα που θα συναντηθεί σε περιβάλλοντα IoT και διασφαλίζει ότι οι ερευνητές μπορούν να επικεντρωθούν σε σαφώς προσδιορισμένες περιοχές και αντικείμενα κατά την προετοιμασία για έρευνες. [14]

3.2 IoT Digital Forensics guidelines and Frameworks

3.2.1. ο οδηγός ACPO

Είναι σαφές ότι οι τρέχουσες ενέργειες που αναλαμβάνουν οι ανακριτές, ανεξάρτητα από τη μεθοδολογία εγκληματολογίας που ακολουθείται, υποστηρίζονται από τον οδηγό ACPO (Association of Chief Police Officers). Ο οδηγός ACPO περιγράφει οδηγίες για τον ερευνητή ώστε να αποκτήσει και να αναλύσει νομίμως τα αποδεικτικά στοιχεία, αλλά καθώς τα αποδεικτικά στοιχεία μπορεί να έχουν πολλές μορφές και υπάρχουν πολλά διαφορετικά σενάρια στα οποία μπορεί να εμπλέκονται αυτά τα στοιχεία, πρέπει να υπάρχει ένα αποτελεσματικό πλαίσιο για να το υποστηρίξει. Με αυτό το σκεπτικό, ο ανακριτής στον τόπο του εγκλήματος πρέπει να ακολουθεί τις κατευθυντήριες γραμμές που ορίζει η ACPO διασφαλίζοντας ότι πραγματοποιείται ανάλυση των δεδομένων, συλλέγοντας όλα τα σχετικά δεδομένα σε ένα αποτελεσματικό και πολυμήχανο θέμα. [6]

Ο οδηγός ACPO παραθέτει αρχές για ηλεκτρονικά αποδεικτικά στοιχεία που βασίζονται σε υπολογιστή και παρατίθεται παρακάτω [6]:

Αρχή 1: «Καμία ενέργεια που λαμβάνεται από τις υπηρεσίες επιβολής του νόμου ή τους πράκτορές τους δεν θα πρέπει να αλλάζει δεδομένα που διατηρούνται σε υπολογιστή ή μέσα αποθήκευσης, τα οποία ενδέχεται στη συνέχεια να βασιστούν στο δικαστήριο». [6]

Αρχή 2: «Σε περιπτώσεις όπου ένα άτομο θεωρεί απαραίτητο να έχει πρόσβαση σε πρωτότυπα δεδομένα που τηρούνται σε υπολογιστή ή σε μέσα αποθήκευσης, αυτό το άτομο πρέπει να είναι ικανό να το πράξει και να μπορεί να αποδείξει τη συνάφεια και τις συνέπειες των πράξεών του». [6]

Αρχή 3: Θα πρέπει να δημιουργηθεί και να διατηρηθεί μια διαδρομή ελέγχου ή άλλο αρχείο όλων των διαδικασιών που εφαρμόζονται σε ηλεκτρονικά αποδεικτικά στοιχεία που βασίζονται σε υπολογιστή. Ένα ανεξάρτητο τρίτο μέρος θα πρέπει να μπορεί να εξετάσει αυτές τις διαδικασίες και να επιτύχει το ίδιο αποτέλεσμα. [6]

Αρχή 4: Ο υπεύθυνος της έρευνας (ο υπεύθυνος της υπόθεσης) έχει τη συνολική ευθύνη για τη διασφάλιση της τήρησης του νόμου και αυτών των αρχών. [6]

3.2.2. Τα περισσότερα Frameworks ανά χρονολογία

Και μία λίστα με frameworks μέχρι και το 2019 όπως παρέχονται στο [11] :

Framework	Comments	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5	Stage 6	Stage 7
VMcKemmis h	Το McKemmish είναι το πρώτο προτεινόμενο μοντέλο για την ψηφιακή εγκληματολογία. Αυτό το πλαίσιο δεν διατηρεί τα στάδια μείωσης και επανεξέτασης για τα συλλεγόμενα στοιχεία.	Identification And Collection	Preservation	Examination	Presentation			
NIST	Το μοντέλο NIST περιέχει τα βασικά στάδια της διαδικασίας έρευνας. Δεν λαμβάνει υπόψη τις αρχές ασφάλειας και απορρήτου.	Collection	Identification And preservation	Examination	Analysis	Reporting		
Martini	Αυτό το πλαίσιο δεν έχει κανένα στάδιο αξιολόγησης, είτε σε αρχικά στάδια είτε σε μεταγενέστερα στάδια. Το προτεινόμενο πλαίσιο δεν λαμβάνει υπόψη το απόρρητο των συλλεγόμενων αποδεικτικών στοιχείων, επειδή δεν υπάρχει κανένα στάδιο ή ενέργεια για την παροχή άδειας για τη συλλογή δεδομένων για εξουσιοδοτημένο ερευνητή.	Identification	Preservation	Collection	Examination And Analysis	Reporting and Presentation		

Beebe	Το πλαίσιο Beebe περιέχει τα κύρια στάδια της τυπικής ψηφιακής εγκληματολογίας με ορισμένα πρόσθετα στάδια, όπως το στάδιο προετοιμασίας για την προετοιμασία της έκθεσης που περιέχει την εντολή αίτησης για έρευνα. Αυτό το μοντέλο δεν έχει καμία πρόταση για την ενίσχυση της ασφάλειας των συλλεγόμενων αποδεικτικών στοιχείων ούτε σε επίπεδο μεταφοράς αποδεικτικών στοιχείων από πλευρά σε πλευρά ή σε επίπεδο αποθήκευσης αποδεικτικών στοιχείων. Ένα άλλο αδύναμο σημείο αυτού του μοντέλου είναι ο περιορισμός της ακρίβειας για τη διαδικασία έρευνας Προετοιμασία απόκρισης περιστατικού	Collection	Preservation and store	Analysis	Presentation	Incident Closer		

IDIP (αναφορά και στο 3.1.6)	Το προτεινόμενο μοντέλο διαφέρει από τα τυπικά μοντέλα, ξεκινώντας από το στάδιο ετοιμότητας, το οποίο παρουσιάζει την προετοιμασία των λειτουργιών και της υποδομής. Στη συνέχεια, το επόμενο στάδιο αναφέρεται στο στάδιο ανάπτυξης που μπορεί να είναι μέρος του σταδίου ετοιμότητας, αυτό το στάδιο εγκατάστασης όλου του απαραίτητου λογισμικού και ανακάλυψης του εγκλήματος. Μετά από αυτό, ξεκινούν τα κύρια στάδια της τυπικής διαδικασίας έρευνας. Και η τελική φάση αναφέρεται στα αποτελέσματα της έρευνας.	Readine ss	Deploym ent	Trace-back	Dynamit e	Review		
Cohn	Το μοντέλο Cohen δεν λαμβάνει υπόψη καμία από τις αρχές ασφάλειας και απορρήτου, όπως αξιολόγηση για τα συλλεχθέντα στοιχεία, αξιολόγηση για τον επιλεγμένο ερευνητή. Άλλο σχόλιο εδώ είναι η αξιολόγηση για την έκθεση που συντάχθηκε πριν	Identifica tion	Collectio n	Collectio n And Preserva tion	Transpor tation Storage	Analysis	Interpret ation And Attribute s	Presenta tion

	από την υποβολή στο δικαστήριο							
Agrawal Framework	Αυτό το πλαίσιο αποτελείται από τα κύρια στάδια της διαδικασίας ψηφιακής εγκληματολογίας. Ένα από τα σχόλια σε αυτό το μοντέλο είναι η ανάγκη για ένα αρχικό στάδιο αξιολόγησης των συλλεγόμενων αποδεικτικών στοιχείων πριν από την έναρξη της διαδικασίας εξέτασης, ένα άλλο σχόλιο αναφέρεται στην επίτευξη των αρχών ασφαλείας είτε μέσω της μεταφοράς των συλλεγόμενων αποδεικτικών στοιχείων είτε στον τόπο αποθήκευσης αποδεικτικών στοιχείων Προετοιμασία Ασφάλεια και αναγνώριση.	Preparation	Securing and recognition.	Evidence Collection	Preservation	Analysis	Presentation	Result And Review
Perumal 1	Αυτό το πλαίσιο δεν έχει κανένα στάδιο αξιολόγησης για την αξιολόγηση των συλλεχθέντων αποδεικτικών στοιχείων ή της παραγόμενης έκθεσης από τη διαδικασία	Planning	Identification	Collection	Analysis	Proof and Defense Result	Review	

	έρευνας.							
Perumal 2	Το Perumal Framework δεν θέτει κανένα κριτήριο για τη συλλογή στοιχείων από την αναγνωρισμένη συσκευή. Καμία ενέργεια για την επίτευξη της ασφάλειας σε αυτό το πλαίσιο. Δεν υπάρχει καμία πρόταση για τη διασφάλιση των όρων και του απορρήτου για τα συλλεχθέντα αποδεικτικά στοιχεία.	Planning	Device Identification Triage	Examination Router or Fog or getaways servers	Lab analysis	Archive and Storage		
Quick and Choo Framework	Αυτό το πλαίσιο θεωρείται ως ένα από τα ισχυρότερα πλαίσια στην ψηφιακή εγκληματολογία. Εκτός από τα τυπικά στάδια της εγκληματολογικής διαδικασίας, αυτό το πλαίσιο διαθέτει ένα στάδιο ανασκόπησης για τα συλλεγόμενα στοιχεία, προκειμένου να βελτιωθεί η ακρίβεια και η απόδοση της διαδικασίας έρευνας.	Commence	Preparation	Identify and collection	Reduction and reviewing.	Evidence analysis.	Presentation	Complete

Στη συνέχεια παρουσιάζονται κάποιες προκλήσεις όπως αυτές μπορούν να βρεθούν στα δίκτυα που είναι 5G+ enabled σε συνδυασμό με κάποιες πιθανές λύσεις τους.

3.3 IoT Digital Forensics in 6G

3.3.1. Digital Forensics Challenges in 6G Environments

3.3.1.1 Satellite IoT and UAVs

Η ταυτοποίηση, η συλλογή, η διατήρηση, ο συσχετισμός και η ανάλυση δορυφορικών συσκευών IoT συμπεριλαμβανομένων των UAV θα είναι πολύ δύσκολη, δεδομένου ότι οι συσκευές θα σχεδιαστούν να λειτουργούν αυτόνομα, σε πραγματικό χρόνο και σε μη επίγεια υψόμετρα και υποβρύχιες τοποθεσίες. Η εγκληματολογική ανάλυση σε μια ποικιλία UAV, συμπεριλαμβανομένων των drones, έχει διεξαχθεί σε μια προσπάθεια εξαγωγής, ανάλυσης και επεξεργασίας εγκληματολογικών αντικειμένων. Το κοινό θέμα σε τέτοιες μελέτες είναι ότι στις περισσότερες περιπτώσεις, οι ερευνητές απαιτούν ανάκτηση των φυσικών συσκευών και πρόσβαση στον OEM (Original Equipment Manufacturer) συμπεριλαμβανομένων των αρχείων καταγραφής πτήσης και των δεδομένων τοποθεσίας που μπορούν να βρεθούν στην ενσωματωμένη μνήμη των drones. [9]

Ωστόσο, οι προκλήσεις σε περιβάλλοντα IoT με δυνατότητα 6G θα περιλαμβάνουν τη φυσική ανάκτηση κατεστραμμένων UAV και δορυφορικών συσκευών IoT που αναπτύσσονται σε μη επίγεια περιβάλλοντα, όπως υποβρύχιες τοποθεσίες και μεγάλα υψόμετρα. Τα στοιχεία των UAV που αποτελούν φυσικό αποδεικτικό στοιχείο μπορούν δυνητικά να είναι διάσπαρτα σε διάφορες τοποθεσίες. Ως εκ τούτου, η δημιουργία μιας υγιούς εγκληματολογικής σύνδεσης μεταξύ ενός ανακτημένου UAV και του σχετικού ελεγκτή ασυρμάτου ή εδάφους για τον προσδιορισμό της ιδιοκτησίας μπορεί να είναι μεγάλη πρόκληση. [9]

Σε ορισμένα σενάρια όπου οι ερευνητές μπόρεσαν να ανακτήσουν ιατροδικαστικά στοιχεία, συχνά δεν είναι δυνατό να συνδεθεί το drone με έναν ύποπτο με βάση δεδομένα που εξάγονται μόνο από το drone. Επιπλέον, τα εγκληματολογικά αντικείμενα αποθηκεύονται σε μια ποικιλία μορφών αρχείων ανάλογα με το OEM του drone που δεν μπορούν να αναλυθούν χρησιμοποιώντας παραδοσιακά ψηφιακά εγκληματολογικά εργαλεία. Στις περισσότερες περιπτώσεις, οι ερευνητές βασίζονται σε μια ποικιλία εργαλείων ανοιχτού κώδικα που δεν έχουν σχεδιαστεί ειδικά για εγκληματολογική ανάλυση drone. Για την αντιμετώπιση αυτών των προκλήσεων απαιτούνται συνεχείς και μελλοντικές κατευθύνσεις έρευνας στην εγκληματολογία των UAV με εξέταση συσκευών που αναπτύσσονται σε μη επίγεια υψόμετρα. [9]

3.3.1.2. Heterogeneous optical wireless networks

Η σύγκλιση ετερογενών δικτύων που αποτελούνται τόσο από δίκτυα ραδιοσυχνοτήτων όσο και από οπτικά ασύρματα δίκτυα θα διαδραματίσει ηγετικό ρόλο στην παροχή υπηρεσιών υψηλής ποιότητας (QoS) που αναμένεται σε ασύρματα δίκτυα επικοινωνίας με δυνατότητα 6G. Αυτό περιλαμβάνει την υβριδική προσέγγιση της ενσωμάτωσης δύο ή περισσότερων ασύρματων τεχνολογιών για αξιοπιστία, αυξημένο χρόνο λειτουργίας, αποδοτικότητα, μειωμένες παρεμβολές, εξισορρόπηση φορτίου δικτύου και βελτιώσεις, ειδικά για απομακρυσμένα και μη επίγεια περιβάλλοντα. Για παράδειγμα, μια υβριδική-διπλή προσέγγιση θα μπορούσε να περιλαμβάνει RF/οπτική, Wi-Fi/LiFi, οπτικό

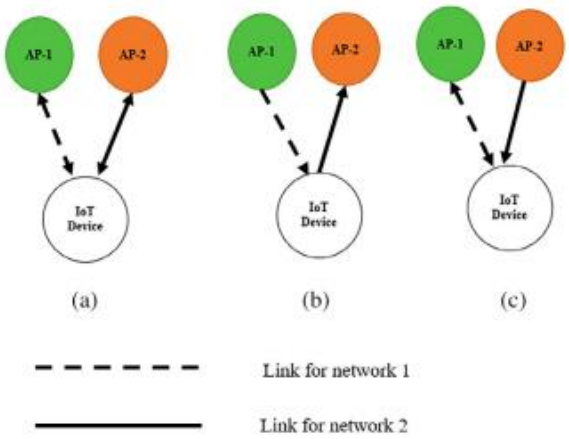
ελεύθερο χώρο (FSO)/VLC, Li-Fi/OCC, femtocell/VLC, επικοινωνία με γραμμή ισχύος (PLC)/VLC, και ούτω καθεξής. [9]

Ωστόσο, η απρόσκοπτη ενσωμάτωση των υφιστάμενων ασύρματων δικτύων ραδιοσυχνοτήτων με οπτικά ασύρματα δίκτυα απαιτεί τεχνολογία δυναμικής διαχείρισης δικτύου, όπως η δικτύωση που καθορίζεται από λογισμικό (Software Defined Networking - SDN), η οποία βασίζεται στις αρχές της εικονικοποίησης δικτύου και στη δημιουργία ξεχωριστών επιπέδων ελέγχου και επιπέδων δεδομένων. Ένα τυπικό υβριδικό σύστημα όπως περιγράφεται από διάφορους ερευνητές, αποτελείται από σενάρια όπου μια συσκευή/τερματικό κινητού τηλεφώνου (δέκτης, πομπός ή πομποδέκτης) έχει πρόσβαση και στα δύο δίκτυα/σημεία πρόσβασης (APs) ταυτόχρονα για ανερχόμενη και κατερχόμενη ζεύξη. Ένα άλλο σενάριο που περιγράφεται σε ένα τέτοιο υβριδικό σύστημα είναι όταν ένα δίκτυο/AP χρησιμοποιείται για uplink και ένα άλλο δίκτυο αποκλειστικά για downlink. Η πρόσβαση σε ένα συγκεκριμένο δίκτυο μπορεί επίσης να ποικίλλει ανάλογα με τον τύπο κίνησης, καθώς διαφορετικές εφαρμογές απαιτούν διαφορετικά επίπεδα QoS, που υποστηρίζονται από μια ποικιλία δικτύων. Το σχήμα 9 δείχνει μια τυπική τοπολογία υβριδικού/ετερογενούς δικτύου. [9]

Αυτός ο τύπος υβριδικής/ετερογενούς τοπολογίας δικτύου σε μελλοντικά δίκτυα IoT 6G δημιουργεί δυσκολίες για την εγκληματολογία δικτύου στον εντοπισμό, τη σύλληψη και τη διατήρηση όλων των πακέτων δικτύου από πολλαπλά δίκτυα και τερματικούς κόμβους που λειτουργούν με ρυθμό μετάδοσης υψηλής ταχύτητας. Η δυσκολία έγκειται επίσης στην απομόνωση, το φιλτράρισμα και την αποκωδικοποίηση συγκεκριμένων πακέτων δεδομένων λαμβάνοντας υπόψη ότι ένα ετερογενές δίκτυο θα αποτελείται από διάφορα πρωτόκολλα δικτύου και μεταδεδομένα που είναι εντελώς ανεξάρτητα το ένα από το άλλο, αλλά συνεργάζονται παράλληλα. Εάν εντοπιστεί παραβίαση δικτύου ή ανωμαλία σε ένα δίκτυο, μπορεί να είναι δύσκολο να αποδοθεί το περιστατικό μόνο στο συγκεκριμένο δίκτυο. Επιπλέον, η εξακρίβωση της ακεραιότητας των δεδομένων που συλλέγονται σε ένα ετερογενές δίκτυο είναι ένα κρίσιμο και δύσκολο έργο για την εγκληματολογία δικτύου. Το εύρος, το μέγεθος και η πολυπλοκότητα των δεδομένων καθιστούν δύσκολο για τους ερευνητές να διατηρήσουν την ακεραιότητα των δεδομένων. [9]

Κάθε μία από τις τεχνολογίες OWC έχει μοναδικές αρχιτεκτονικές, που διαφέρουν μεταξύ τους ως προς την τεχνική διαμόρφωσης, το σύστημα μετάδοσης, το σύστημα λήψης και το σύστημα επικοινωνίας. Η χρήση επομένως κρυπτογράφησης και μετάδοσης σημάτων OWC υψηλής απόδοσης θα είναι πολύ δύσκολη αν όχι αδύνατη. [9]

Οι τρέχουσες μελέτες για το OWC ειδικά το πρότυπο IEEE 802.15.7 του VLC έχουν επικεντρωθεί κυρίως στην αξιολόγηση της απόδοσης και στη βελτιστοποίηση για τη βελτίωση της αξιοπιστίας και της κάλυψης της μελλοντικής επικοινωνίας δικτύου IoT σε εσωτερικά και εξωτερικά περιβάλλοντα.. Επιπλέον, η διεξαγωγή εγκληματολογικών δικτύων ήχου θα απαιτήσει μια ποικιλία εξειδικευμένων εργαλείων και τεχνικών για βαθιά επιθεώρηση και ανάλυση πακέτων σε ετερογενή δίκτυα 6G IoT. [9]



[9]

Σχήμα 9: Υβριδικό/ετερογενές τοπολογία δικτύου (α) και τα 2 δίκτυα για ανεβασμα και κατέβασμα (β) δίκτυο 1 για κατέβασμα και δίκτυο 2: για ανεβασμα (γ) δίκτυο 1 για ανέβασμα και κατέβασμα και δίκτυο 2 για ανέβασμα

3.3.1.3. 6G edge computing environments

Όπως συζητήθηκε και προηγουμένως, οι βασικές τεχνολογίες ενεργοποίησης που θα υποστηρίζουν ετερογενή δίκτυα IoT με δυνατότητα 6G θα στεγαστούν σε περιβάλλοντα υπολογιστών αιχμής που αποτελούν τεράστια κέντρα δεδομένων και βάσεις δεδομένων στην περιφέρεια του δικτύου, όπου θα είναι πιο κοντά σε συσκευές και αισθητήρες. Τα συγκεντρωτικά δεδομένα που είναι αποθηκευμένα σε πολλούς διακομιστές υπολογιστών αιχμής από πολλαπλά δίκτυα IoT, θα μπορούσε να είναι δύσκολο να εντοπιστούν και να συλλεχθούν λόγω του τεράστιου όγκου και της πολυπλοκότητας των δεδομένων. [9]

Για παράδειγμα, ορισμένα από τα δεδομένα μπορεί να είναι αποθηκευμένα σε διαφορετικές μορφές ή κρυπτογραφημένα και μπορεί να απαιτούν παρακολούθηση δικτύου σε πραγματικό χρόνο, γεγονός που το καθιστά πιο δύσκολο για τους ιατροδικαστές. Επιπλέον, λόγω των περιορισμένων δυνατοτήτων υπολογισμού και αποθήκευσης των περιβαλλόντων υπολογιστών άκρων, οι κόμβοι ακμής συχνά εκφορτώνουν εργασίες υπολογισμού στο νέφος εάν δεν διαθέτουν τους πόρους υπολογισμού που απαιτούνται για την κάλυψη των απαιτήσεων απόδοσης, ώστε η τελική συσκευή να μπορεί να λάβει απόκριση εντός εύλογου λανθάνοντος χρόνου. Ως εκ τούτου, τα σχετικά εγκληματολογικά τεχνουργήματα μπορεί να είναι πτητικά ή μη μόνιμα σε διακομιστές άκρων και τοποθεσίες βάσεων δεδομένων. Τα αποδεικτικά δεδομένα μπορεί να διασπείρονται σε πολλούς διακομιστές cloud, καθιστώντας τη συλλογή και τη διατήρηση δύσκολη ή αδύνατη σε ορισμένα σενάρια. Ως εκ τούτου, πρέπει να εξεταστούν νέες ψηφιακές εγκληματολογικές προσεγγίσεις και μέθοδοι που θα επιτρέψουν τη διεξαγωγή συντονισμένων και υγιών εγκληματολογικών ερευνών σε αυτά τα ετερογενή δίκτυα IoT με δυνατότητα 6G. [9]

3.3.2. Digital Forensics Solutions in 6G Environments

Δεν υπάρχει αμφιβολία ότι η ανάπτυξη της ασύρματης τεχνολογίας 6G θα έχει βαθύ αντίκτυπο στο μέλλον της ασύρματης επικοινωνίας και θα ενεργοποιήσει το Διαδίκτυο των Πάντων (Internet of Everything - IoE). Ωστόσο, όπως προσδιορίσαμε από αυτήν την έρευνα, οι ιατροδικαστικοί ερευνητές αντιμετωπίζουν πολλές σημαντικές ψηφιακές εγκληματολογικές προκλήσεις. Σε αυτή την ενότητα, επισημαίνουμε διάφορες ψηφιακές εγκληματολογικές προσεγγίσεις και ερευνητικές κατευθύνσεις για την αντιμετώπιση αυτών των προκλήσεων. Συζητάμε επίσης τις ευκαιρίες ιατροδικαστικής έρευνας και την ετοιμότητα για μελλοντικά δίκτυα 6G και πέραν του IoT.

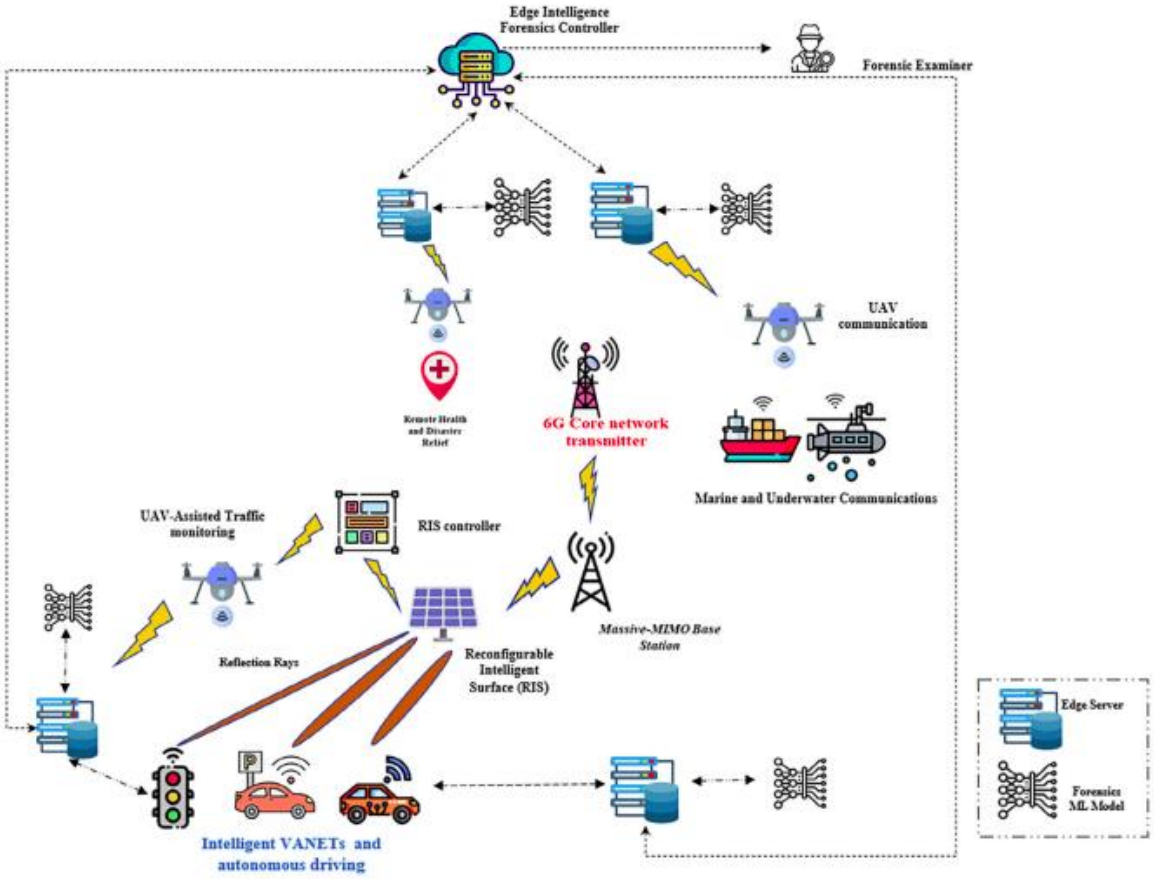
3.3.2.1 Edge intelligence forensics

Η μελλοντική επικοινωνία δικτύων 6G θα χρησιμοποιεί ασύρματα δίκτυα αιχμής για να παρέχει όχι μόνο υπηρεσίες παράδοσης και υπολογισμού περιεχομένου χαμηλής καθυστέρησης, αλλά και τοπική απόκτηση, συγκέντρωση και επεξεργασία δεδομένων. Πρόσφατες μελέτες έχουν προτείνει τη χρήση προσεγγίσεων ομοσπονδιακής μάθησης (Federated Learning - FL) και μηχανικής μάθησης (ML) για τη βελτιστοποίηση της απόδοσης του δικτύου και τη χαμηλή καθυστέρηση και τη βελτίωση του απορρήτου των δεδομένων χρήστη σε αυτόνομα περιβάλλοντα IoT και τα οραματιζόμενα ασύρματα δίκτυα 6G. Στην ψηφιακή εγκληματολογία, έχουν προταθεί προσεγγίσεις και μεθοδολογίες μηχανικής μάθησης (ML) για την αντιμετώπιση του συνεχώς αυξανόμενου όγκου, της πολυπλοκότητας και της ποικιλομορφίας των δεδομένων. Αυτές οι προσεγγίσεις όταν συνδυαστούν θα μπορούσαν να επιτρέψουν την απρόσκοπτη αναγνώριση και συλλογή εγκληματολογικών δεδομένων από δίκτυα αιχμής 6G IoT. Τα Edge Intelligence forensics προσφέρουν έτσι επιπρόσθετη γνώση στην άκρη των κόμβων για τον εντοπισμό και τη συλλογή αποδεικτικών εγκληματολογικών τεχνουργημάτων από μεγάλα σύνολα δεδομένων δικτύου 6G IoT για εγκληματολογική ανάλυση και εξέταση χρησιμοποιώντας προηγμένες προσεγγίσεις από federated και machine learning αλγορίθμους. [9]

Για παράδειγμα, μια βιώσιμη προσέγγιση στην εγκληματολογία αιχμής (Edge Intelligence Forensics) θα είναι η εφαρμογή της τεχνητής νοημοσύνης για τον εντοπισμό και τη συλλογή εγκληματολογικών αποδεικτικών στοιχείων χρησιμοποιώντας μοντέλα ML αυτομάθησης από εξαιρετικά κατανεμημένους διακομιστές αιχμής δικτύου 6G IoT όπως φαίνεται στο σχήμα 10. Στο δεδομένο σενάριο, τα UAV ως συσκευές edge, παρέχουν μια επέκταση στην επικοινωνία ασύρματου δικτύου 6G. Για ευφυή VANET και αυτόνομα συστήματα, τα UAV δεν είναι σε θέση να παρέχουν σχεδιασμό διαδρομής ή να λαμβάνουν έξυπνες αποφάσεις λόγω υψηλού υπολογισμού, επεξεργασίας δεδομένων και κατανάλωσης ενέργειας. Λόγω αυτών των περιορισμών, τα UAV προωθούν την επικοινωνία δεδομένων στους κοντινούς διακομιστές άκρων (που έχουν υψηλότερες δυνατότητες) για να εκτελέσουν αυτές τις ενέργειες. Τα έξυπνα οχήματα και τα έξυπνα συστήματα κυκλοφορίας προωθούν επίσης δεδομένα που έχουν ληφθεί σε κοντινούς διακομιστές αιχμής για αποφάσεις αυτόνομης οδήγησης και διαχείριση της κυκλοφορίας σε πραγματικό χρόνο. [9]

Ομοίως, σε θαλάσσιες και υποβρύχιες τοποθεσίες, τα UAV προωθούν πακέτα δεδομένων σε κοντινούς διακομιστές και κρυφές μνήμες για επικοινωνία δεδομένων σε πραγματικό χρόνο. Σε κάθε σενάριο, οι διακομιστές ακμών αναπτύσσονται τοπικά με προσαρμοστικά εγκληματολογικά μοντέλα ML που βασίζονται στην ανίχνευση ανωμαλιών FL που διέπεται από έναν ελεγκτή ευφυΐας άκρων (Edge Intelligence Controller). Αυτή η προσέγγιση επιτρέπει την ακριβή αναγνώριση και ταξινόμηση των επιθέσεων στα δίκτυα IoT

6G, τα οποία μπορούν να παρακολουθούνται, να συλλέγονται και να αναλύονται από τον ιατροδικαστή μέσω του ελεγκτή. Λόγω του υψηλού όγκου και της πολυπλοκότητας των δεδομένων, η εγκληματολογία αιχμής μπορεί να βοηθήσει τους ερευνητές να εξοικονομήσουν χρόνο στην ανάλυση μεγάλων δεδομένων κατά τη διάρκεια των εγκληματολογικών ερευνών, να βοηθήσουν στην απόκριση συμβάντων σε πραγματικό χρόνο σε γνωστές επιθέσεις και να διευκολύνουν τον εντοπισμό ανωμαλιών κυκλοφορίας δικτύου. Τα μοντέλα ML μπορούν να εκπαιδευτούν για συγκεκριμένα περιβάλλοντα δικτύου 6G IoT για τον εντοπισμό μοτίβων δικτύου και υπογραφών για εγκληματολογική ανάλυση. [9]



Σχήμα 10: Edge intelligence forensics σε 6G IoT networks

3.3.2.2 XR/VR forensics

Η ανάπτυξη της τεχνολογίας ασύρματης επικοινωνίας 6G θα πολλαπλασιάσει τη χρήση εφαρμογών XR/VR σε αντίθεση με τα τρέχοντα δίκτυα 4G και 5G. Επομένως, απαιτούνται έγκυρες μεθοδολογίες και εργαλεία εγκληματολογίας για την ανάκτηση αποδεικτικών δεδομένων και την ανακατασκευή των δραστηριοτήτων των χρηστών σε εικονικά περιβάλλοντα. Οι τρέχουσες ερευνητικές μελέτες έχουν επικεντρωθεί στον τρόπο με τον οποίο η εικονική πραγματικότητα θα μπορούσε να χρησιμοποιηθεί για την υποστήριξη αστυνομικών ερευνών ή να χρησιμοποιηθεί για τη διδασκαλία εννοιών ψηφιακής εγκληματολογίας. Ωστόσο, υπάρχει έλλειψη ερευνητικών μελετών που επικεντρώνονται σε ψηφιακές εγκληματολογικές έρευνες σε περιβάλλοντα XR/VR. Επιπλέον, υπάρχει έλλειψη εγκληματολογικών εργαλείων ειδικά για την αναγνώριση, συλλογή, διατήρηση και ανάλυση

ψηφιακών αντικειμένων σε περιβάλλοντα XR/VR. Σε μία έρευνα διεξήχθη μια εγκληματολογική ανάλυση των καθηλωτικών κοινωνικών εφαρμογών εικονικής πραγματικότητας. Οι συγγραφείς ανακάλυψαν τεχνουργήματα από την πλευρά του πελάτη και βάσει δικτύου που δημιουργήθηκαν χρησιμοποιώντας το HTC Vive και το Oculus Rift. Οι εφαρμογές VR που αναλύθηκαν περιλαμβάνουν τα Steam, Bigscreen, Rec Room, Altspacevr και Facebook Spaces. Περιορισμένα αποδεικτικά δεδομένα σχετικά με τις δραστηριότητες των χρηστών ανακτήθηκαν από αρχεία καταγραφής που δημιουργήθηκαν από τις εφαρμογές VR που είναι εγκατεστημένες σε έναν σταθμό εργασίας υπολογιστή με Windows. Τα υπολείμματα δεδομένων της εγκληματολογικής αξίας ανακτήθηκαν με επιτυχία μόνο από την επιθεώρηση πακέτων δικτύου μιας μεμονωμένης εφαρμογής VR στα πειράματά τους. Λαμβάνοντας υπόψη στο όχι και τόσο μακρινό μέλλον, η ανάπτυξη του XR/VR θα κινηθεί προς την πλήρη εφαρμογή εικονικών εμπειριών, περιουσιακών στοιχείων και περιβαλλόντων, συμπεριλαμβανομένου του «μετασύμπαντος», η μελέτη καταλήγει στο συμπέρασμα ότι υπάρχει περιθώριο για περαιτέρω έρευνα και ανάπτυξη εργαλείων σε αυτόν τον εκκολαπτόμενο τομέα της ψηφιακής εγκληματολογίας. [9]

3.3.2.3 Optical wireless network forensics

Σε σενάρια που απαιτούν ψηφιακή εγκληματολογία και απόκριση συμβάντων σε επιθέσεις στον κυβερνοχώρο, συμπεριλαμβανομένων επιθέσεων έγχυσης και επανάληψης μηνυμάτων σε τοπολογίες δικτύου OWC, θα απαιτείται η διεξαγωγή εγκληματολογικών δικτύων με χρήση εξειδικευμένων εργαλείων. Σε αντίθεση με τα παραδοσιακά σήματα που βασίζονται σε RF, το sniffing, η λήψη και η αποκωδικοποίηση σημάτων OWC απαιτούν εξειδικευμένο υλικό και λογισμικό. Σε μία μελέτη, πηνία δέκτη (που επεξεργαζονται σήματα και αποκωδικοποιούν πλαίσια δεδομένων και εκτείνονται σε πολλαπλό υλικό και λογισμικό) σχεδιάστηκαν για την επιτυχή ανίχνευση και λήψη σημάτων VLC με βάση τα σχήματα διαμόρφωσης Variable Pulse Position Modulation (VPPM) και On–Off Keying (OOK). Ωστόσο, το sniffing σημάτων VLC που βασίζονται σε άλλα σχήματα, συμπεριλαμβανομένου του Color Shift Keying (CSK) και των προηγμένων σχημάτων διαμόρφωσης, όπως το DCO-OFDM (οπτικό OFDM με πόλωση συνεχούς ρεύματος) και το ACO-OFDM (οπτικό OFDM με ασύμμετρη κοπή) θα απαιτήσει διαφορετική προσέγγιση. [9]

Μια άλλη μελέτη περιέγραψε την πολυπλοκότητα της ανίχνευσης δεδομένων VLC για ανάλυση. Η μελέτη απαιτούσε τη χρήση μιας εξελιγμένης διάταξης συσκευής που περιλαμβάνει ένα τηλεσκόπιο και μια φωτοδίοδο PIN που ακολουθείται από έναν ενισχυτή trans-impedance amplifier σε απόσταση 30 m για την ανίχνευση δεδομένων σε ένα σενάριο VLC. Αυτό υπογραμμίζει περαιτέρω την ανάγκη για ανάπτυξη απλούστερων και λιγότερο περίπλοκων εργαλείων για την ανίχνευση της κυκλοφορίας δικτύου VLC για ανάλυση. [9]

Δεδομένου ότι το ορατό φως δεν μπορεί να διαπεράσει αντικείμενα, τα κανάλια VLC μπορούν εύκολα να μπλοκαριστουν κατά τη διάρκεια της ζωντανής καταγραφής της κυκλοφορίας ακόμη και με την εφαρμογή τεχνικών MIMO για τον μετριασμό της ατμοσφαιρικής απορρόφησης, της απώλειας όρασης (LOS) και του φαινομένου σκίασης. Αυτό αναπόφευκτα καθιστά προβληματική την ανακάλυψη δικτύου για τους ιατροδικαστές. [9]

Τα μελλοντικά ερευνητικά προγράμματα θα πρέπει επίσης να επικεντρωθούν σε νέες μεθόδους και εργαλεία που απαιτούνται για τη λήψη και ανάλυση δεδομένων δικτύου σε άλλα συστήματα OWC, συμπεριλαμβανομένων των υποβρύχιων οπτικών ασύρματων επικοινωνιών (underwater optical wireless communications - UOWCs) που μεταδίδουν

δεδομένα χρησιμοποιώντας φορείς όπως ακουστικά κύματα, κύματα RF και οπτικά κύματα, ειδικά σε υποβρύχιες τοποθεσίες που μπορεί να είναι επιρρεπείς σε παρεμβολές σήματος ή απώλεια. [9]

4. Μέθοδοι και εφαρμογές Cyber Physical Systems & Digital Twins

4.1 Εισαγωγή στα CPS και DT

Όπως μπορούμε να καταλάβουμε καλύτερα και απο το κεφάλαιο 2 υπάρχουν πάρα πολλά διαφορετικά βήματα τα οποία κάποιος ερευνητής θα πρέπει να ακολουθήσει ώστε να πραγματοποιήσει εγκληματολογική έρευνα DF σε συσκευές IoT. Πρέπει κάποιος να έχει μια πολύ καλή εικόνα του κλάδου του DF γενικότερα γνωρίζοντας πολύ καλά τα DF phases, ενώ στη συνέχεια πρέπει να είναι αρκετά εξοικειωμένος με την εκάστοτε συσκευή IoT για να μπορεί να γνωρίζει τα enablers της κάθε συσκευής. Η ετερογένεια όμως των δικτύων IoT αναγκάζουν τελικά τον κάθε ερευνητή να γίνεται συγκεκριμένος με τις συσκευές στις οποίες θελει να πραγματοποιήσει εγκληματολογική έρευνα.

Σε αυτό το πλαίσιο στη συνέχεια στο παρόν κεφάλαιο θα εξετάσουμε τα μέρη που αποτελούν το ψηφιακό κομμάτι της τεχνολογίας των IoT συσκευών, δηλαδή ειδικότερα τα CPS και τα DT των διαφόρων δικτύων IoT. Με αυτό το τρόπο θα έχουμε μια καλύτερη εικόνα τόσο των εφαρμογών του κάθε επιμέρους δικτύου, όσο και των ειδικων λειτουργιών που κάθε φορά κάποιος ερευνητής καλείται να γνωρίζει καθώς αναλύει εγκληματολογικά ένα συγκεκριμένο δίκτυο.

Θα δούμε ότι πολλές φορές κάποιοι ερευνητές χρειάζεται να γνωρίζουν τις εφαρμογές των CPS και των DT στα IoT. Μέσω αυτών θα καλεστουν να καλύψουν την μεγάλη ετερογένεια τους, όπως στα smart homes ή τα smart cars όπου ειδικές εφαρμογές που υποστηρίζουν όλα τα διαφορετικά CPS ενός smart car ή ενός smart home ενώνονται σε ένα γενικότερο application ώστε να μπορεί να γίνει DF analysis μέσω αυτής της εφαρμογής ή αλλιώς ξεχωριστό DF analysis θα πρέπει να πραγματοποιηθεί για τη κάθε μια συσκευή IoT.

Αντίστοιχα πολλές φορές το DT counterpart θα είναι και αυτό καθοριστικής σημασίας σε άλλα δίκτυα όπως στα drones όπου για να πραγματοποιηθεί DF analysis σε σμήνη drones θα πρέπει ο ερευνητής να γνωρίζει το χειρισμό τους μέσα από εργαλεία των DT μέσω των οποίων αυτά ελέγχονται (εφαρμογές τέτοιες είναι πχ στη παροχή δικτύου μέσω των drones) ή αντίστοιχα στα δίκτυα των Sattelite IoT όπου ένας ερευνητής θα καλεστεί να πραγματοποιήσει DF analysis μέσω ή στα DT των δορυφόρων καθώς οι ίδιοι οι δορυφόροι δε θα μπορούν προφανώς να αναλυθούν μέσω του υλικού τους.

Αφού καλύψουμε λοιπόν στο κεφάλαιο αυτό κάποιες βασικές αρχές των τεχνολογιών CPS και DT ανά δίκτυο όπως χωρίστηκαν στο κεφάλαιο 2 και όπου αυτά υπάρχουν, στη συνέχεια θα παρουσιάσουμε μεθόδους ανάλυσης DF στο κεφάλαιο 5 ανά συγκεκριμένο δίκτυο για να δούμε πως έχουν πραγματοποιηθεί αυτές οι έρευνες συγκεκριμένα όσο περισσότερο γίνεται χωρίς να παρέχουν μόνο ένα γενικότερο πλαίσιο εγκληματολογικής έρευνας όπως στο κεφάλαιο 3.

4.1.1 Τι είναι το CPS

Ορισμοί του CPS βρέθηκαν στο [40], [39], [37], [36], [35], [13]. Γενικότερα χωρίς να χρειάζεται να μπούμε σε ολοκληρωτικό βάθος για την αρχιτεκτονική των συστημάτων αυτών

μπορούμε να πούμε ότι τα κυβερνοφυσικά συστήματα (CPS) είναι έξυπνα σύνθετα συστήματα που έχουν σχεδιαστεί μέσω της ενοποίησης κυβερνο-φυσικών υποσυστημάτων ή εξαρτημάτων ή/και προϋπαρχόντων εξαρτημάτων κυβερνοφυσικών συστημάτων, έτσι ώστε να εμφανίζονται και να λειτουργούν ως ενιαία μονάδα σε σχέση με το εξωτερικό κόσμο (σε άλλα συστήματα). Η ολοκλήρωση του υποσυστήματος περιλαμβάνει τόσο μια κατάλληλη χωρική διάταξη των υποσυστημάτων, όσο και μια επαρκή διασύνδεση, επικοινωνία και συνεργασία των υποσυστημάτων. [40]
Τα CPS έτσι είτε [40]:

- Συλλέγουν πληροφορίες χρησιμοποιώντας διάφορους αισθητήρες και άλλες (μακρινές) εισόδους επικοινωνίας ή
- Επεξεργάζονται τις συλλεγόμενες πληροφορίες για να υπολογίσουν συμπεράσματα που αντιπροσωπεύουν ορισμένες αποφάσεις ελέγχου ή
- που χρησιμεύουν για την προετοιμασία τέτοιων αποφάσεων ελέγχου, ή
- κοινοποιούν τα αποτελέσματα της επεξεργασίας πληροφοριών εγκαίρως χρησιμοποιώντας διάφορες μνήμες ή στο χώρο χρησιμοποιώντας διαφορετικά μέσα επικοινωνίας και ενεργοποιητές, ή
- Εφαρμόζουν όλες αυτές τις λειτουργίες πραγματοποιώντας ένα πλήρες σύστημα ελέγχου, ή
- Εφαρμόζουν ένα υποσύνολο αυτών των συναρτήσεων πραγματοποιώντας π.χ. ένα σύστημα παρακολούθησης ή διάγνωσης.

Ενώ τα φυσικά συστήματα περιλαμβάνουν τα φυσικά περιβάλλοντα που απαιτούν έλεγχο και επιτήρηση, τα συστήματα στον κυβερνοχώρο αναφέρονται στις ενσωματωμένες συσκευές, που ονομάζονται επίσης μηχανικά συστήματα επόμενης γενιάς. Τα τελευταία είναι υπεύθυνα για την επεξεργασία πληροφοριών και την επικοινωνία με το κατανεμημένο περιβάλλον στο οποίο τοποθετείται το σύστημα που βασίζεται στο CPS. Επίσης σε ένα σύστημα που βασίζεται στο CPS, το δίκτυο επικοινωνίας, οι αισθητήρες και οι ενεργοποιητές αποτελούν τη διεπαφή που εξυπηρετεί το σκοπό της σύνδεσης του φυσικού κόσμου με την αρχιτεκτονική του κυβερνοχώρου. Ο όρος CPS δεν διαφέρει πολύ από το Internet of Things (IoT) και υπάρχει μια ορισμένη επικάλυψη μεταξύ των εφαρμογών τους. **Το IoT αναφέρεται ως υποσύνολο του CPS σε πρόσφατη έρευνα.** [39]

4.1.2 Τι είναι το DT

Αντίστοιχα ορισμοί του DT βρέθηκαν στα [53], [41], [52], [35] και [46]. Εν συντομία η γενική ιδέα ενός ψηφιακού δίδυμου DT αναφέρεται σε ένα νέο μέσο προσομοίωσης που βασίζεται σε CPS και IoT παρέχοντας συγχρονισμό σε πραγματικό χρόνο με τα συστήματα παραγωγής. Η ανάλυση μεγάλων δεδομένων και η Τεχνητή Νοημοσύνη (AI) σε συνδυασμό με DT εφαρμόζουν παρακολούθηση, λήψη αποφάσεων και πρόβλεψη αποτυχίας σε πραγματικό χρόνο, ενισχύοντας τη συνεργασία μεταξύ ενός χειριστή και της έξυπνης μηχανής. [41]

«Μια εννοιολογική ιδέα» του ψηφιακού δίδυμου προτάθηκε για πρώτη φορά από τον Grieves το 2002 για τη διαχείριση του κύκλου ζωής του προϊόντος (PLM) και ονομάστηκε «Εννοιολογική Ιδανική για τη Διαχείριση Κύκλου Ζωής Προϊόντος». Η ιδέα περιείχε τρία στοιχεία: τα εικονικά και τα πραγματικά συστήματα, καθώς και τη συνεχή ανταλλαγή πληροφοριών μεταξύ των δύο συστημάτων. Μέσω της επικοινωνίας δεδομένων σε πραγματικό χρόνο μεταξύ του φυσικού κόσμου και του ψηφιακού του αντίστοιχου, το DT αναμενόταν να διαδραματίσει ρόλο σε όλο τον κύκλο ζωής ενός προϊόντος. Το 2010, ο όρος

«ψηφιακό δίδυμο» υιοθετήθηκε από την Εθνική Υπηρεσία Αεροναυτικής Διαστήματος (NASA), η οποία τον όρισε ως εξής: «Ένα ψηφιακό δίδυμο είναι μια ολοκληρωμένη πολυφυσική, πολλαπλής κλίμακας, πιθανολογική προσομοίωση ενός οχήματος ή συστήματος που χρησιμοποιεί τα καλύτερα διαθέσιμα φυσικά μοντέλα, ενημερώσεις αισθητήρων, ιστορικό στόλου κ.λπ., για να αντικατοπτρίζουν τη ζωή του αντίστοιχου ιπτάμενου δίδυμου» [41]

Το DT συνήθως περιγράφεται ως η συνολική δομή των φυσικών οντοτήτων και των εικονικών αντίστοιχων οντοτήτων και η σύνδεση δεδομένων μεταξύ τους. Είναι η ψηφιακή μορφή φυσικών αντικειμένων, που επιτρέπει στα δεδομένα να μεταδίδονται απρόσκοπτα στον φυσικό και εικονικό κόσμο, έτσι ώστε η τεχνολογία των υπολογιστών να μπορεί να χρησιμοποιηθεί για την εξερεύνηση, τη διαχείριση οντοτήτων και τη βελτίωση της απόδοσής τους σε οντότητες. [52]

Στο εξατομικευμένο σύστημα σχεδίασης και κατασκευής, η DT δημιουργεί ένα ψηφιακό μοντέλο και έναν εικονικό ορισμό για το σύστημα παραγωγής για να βοηθήσει στην υλοποίηση της ψηφιοποίησης και του αυτοματισμού στη διαδικασία σχεδιασμού και κατασκευής. Στο πλαίσιο της βιομηχανίας 4.0, το DT παρέχει μια καλή βάση για μαζική εξατομίκευση. Ταυτόχρονα, φυσικά αντικείμενα όπως υλικά, προσωπικό και εξοπλισμός μπορούν επίσης να ενσωματωθούν σε ψηφιακή μορφή για να αποκτήσουν ενοποιημένη και αποτελεσματική διαχείριση. Επιπλέον, αυτό επιτρέπει την πραγματοποίηση πρόσθετης έξυπνης συντήρησης, απομακρυσμένης παρακολούθησης σε πραγματικό χρόνο, πρόβλεψης κατάστασης και άλλων προηγμένων λειτουργιών. [52]

4.1.3 Διαφορές μεταξύ CPS και DT

Το CPS σχηματίζει ένα σύστημα συστημάτων μέσω μιας σύνδεσης δικτύου από έναν αριθμό αισθητήρων, ενεργοποιητών και συσκευών ελέγχου. Μέσω αυτού του συστήματος CPS, λαμβάνονται και αναλύονται πληροφορίες για τον πραγματικό κόσμο και τα επεξεργασμένα αποτελέσματα εφαρμόζονται στον φυσικό κόσμο ξανά μέσω ενός συστήματος ενεργοποιητή. Αυτό το παράδειγμα διαφέρει από τα συμβατικά απλά συστήματα ελέγχου στο ότι είναι ένα αμφίδρομο σύστημα που αλληλεπιδρά στενά με τον πραγματικό κόσμο. Στον πραγματικό κόσμο στον οποίο ζούμε, υπάρχουν κοινωνικές υποδομές όπως συστήματα μεταφορών, κτίρια, σπίτια, ηλεκτρονικά είδη, ηλεκτρικά δίκτυα και το Διαδίκτυο και ρομπότ στον πραγματικό χώρο. Ένα σύστημα που περιλαμβάνει τέτοιες οντότητες του πραγματικού κόσμου ονομάζεται φυσικό σύστημα. Ο κόσμος του κυβερνοχώρου αναφέρεται συλλογικά σε έναν εικονικό υπολογιστικό χώρο που δημιουργείται από υπολογιστές και Διαδίκτυο που εκτελεί λειτουργία για τον έλεγχο κόμβων αισθητήρων του φυσικού συστήματος. Το CPS εκτελεί τη λειτουργία της περιβαλλοντικής παρακολούθησης μέσω μιας ποικιλίας αισθητήρων που μπορούν να ανιχνεύσουν αλλαγές που συμβαίνουν στον πραγματικό κόσμο. Το φυσικό σύστημα αναγνωρίζει, αναλύει και προβλέπει το φαινόμενο του πραγματικού κόσμου με βάση τις πληροφορίες που λαμβάνονται από αισθητήρες. Οι πληροφορίες ελέγχου που προκύπτουν εφαρμόζονται ως είσοδος του συστήματος πραγματικού κόσμου, το οποίο μετατρέπει το σύστημα του πραγματικού κόσμου προς την επιθυμητή κατεύθυνση, π.χ. ένα αυτο-οδηγούμενο αυτοκίνητο που τρέχει προς τον προορισμό. [35]

Διάφορες ηλεκτρονικές συσκευές, οικιακές συσκευές, συσκευές επικοινωνίας, αυτοκίνητα κ.λπ. που χρησιμοποιούνται κυρίως στην καθημερινή ζωή είναι εξοπλισμένες με εξειδικευμένους υπολογιστές. Ένα ειδικό σύστημα ενσωματωμένο για να χρησιμεύσει ως ο

εγκέφαλος των συσκευών ονομάζεται ενσωματωμένα συστήματα. Τα ενσωματωμένα συστήματα όπως τα έξυπνα τηλέφωνα, οι συσκευές αναπαραγωγής MP3, οι κάμερες, τα συστήματα πλοήγησης και οι ανιχνευτές πυρκαγιάς μπορούν εύκολα να εντοπιστούν στην καθημερινή μας ζωή. Αυτά τα συστήματα που χαρακτηρίζονται από επεξεργασία σε πραγματικό χρόνο, σμίκρυνση και χαμηλή κατανάλωση ενέργειας, λειτουργούν ανεξάρτητα για την επίτευξη συγκεκριμένων στόχων χωρίς αλληλεπίδραση με άλλα συστήματα. Οι ηλεκτρονικές συσκευές εξοπλισμένες με ενσωματωμένα συστήματα μπορούν να θεωρηθούν ως μονοκατευθυντικά και κλειστά φυσικά συστήματα επειδή λειτουργούν σύμφωνα με τις απαιτήσεις των χρηστών. Αυτά τα συμβατικά ενσωματωμένα συστήματα δεν λαμβάνουν υπόψη τις αλλαγές στο συνολικό σύστημα κατά τον έλεγχο του φυσικού συστήματος σύμφωνα με τη λειτουργία του λογισμικού. [35]

Στην περίπτωση του CPS, η κατάσταση του συστήματος αλλάζει ανάλογα με τις αλληλεπιδράσεις με το περιβάλλον, τον χρόνο και τους ανθρώπους. Το ενσωματωμένο σύστημα εκτελεί μόνο μια απλή γραμμική εργασία χωρίς να εξετάζει πλήρως τις συνέπειες αυτών των παραγόντων. Εφαρμόζει έναν απλό μονοκατευθυντικό έλεγχο από τον κόσμο του κυβερνοχώρου στον φυσικό κόσμο. Με την πρόοδο του ελέγχου και της θεωρίας συστημάτων, το ενσωματωμένο σύστημα άρχισε να εξελίσσεται σε μια μορφή στην οποία θα μπορούσε να ενεργοποιηθεί η αμφίδρομη γεφύρωση με τον άνθρωπο. [35]

Ως αποτέλεσμα, το CPS έχει αναδειχθεί ως ένα νέο παράδειγμα που περιλαμβάνει φυσικές οντότητες στον πραγματικό κόσμο, το οποίο πρόκειται να επεκτείνει την έννοια των ενσωματωμένων συστημάτων. Προκειμένου να δούμε τα συστήματα του κυβερνοχώρου και τα φυσικά συστήματα ολοκληρωμένα, είναι απαραίτητο να κατανοήσουμε πρώτα τις εγγενείς διαφορές μεταξύ των δύο συστημάτων. Το φυσικό σύστημα αλλάζει ανάλογα με το χρόνο και τον χώρο ενώ το υπάρχον ενσωματωμένο σύστημα λειτουργεί ανάλογα με τη λογική. Καθώς ένα αυτοοδηγούμενο αυτοκίνητο προσαρμόζει τη διαδρομή και την ταχύτητα οδήγησης ανάλογα με το χρόνο και τις συνθήκες κυκλοφορίας οδικώς, έτσι και η κατάσταση του CPS αλλάζει ανάλογα με τις διακυμάνσεις του χρόνου και του χώρου. Από την άλλη πλευρά, στην περίπτωση του κυβερνοχώρου, το αποτέλεσμα της λειτουργίας του λογισμικού αλλάζει ανάλογα με τη ροή της λογικής, η οποία απαιτεί μηχανικούς υπολογισμούς για τη λειτουργία του σχετικού υλικού. Δεδομένου ότι οι αρχές λειτουργίας των δύο συστημάτων (CPS έναντι ενσωματωμένου συστήματος) είναι θεμελιωδώς διαφορετικές μεταξύ τους, υπάρχει ανάγκη για μέσο συγχρονισμού για σωστή αλληλεπίδραση μεταξύ των δύο συστημάτων στην περίπτωση του ενσωματωμένου συστήματος στον κυβερνοχώρο. [35]

Το CPS έχει ήδη αρχίσει να διεισδύει στην κοινωνία μας και η ορατή αλλαγή έχει αρχίσει να συντελείται. Στις ΗΠΑ, επτά βασικά πεδία εφαρμογής του CPS προτάθηκαν ως εξής: Smart Factory, Smart Traffic System, Smart Grid, Smart Healthcare System, Smart Home/Building System, Smart Defense System και Smart Disaster Response System. Για παράδειγμα, αισθητήρες που συνδέονται σε δρόμους, κτίρια και γέφυρες παρέχουν βασικές πληροφορίες για τον τρισδιάστατο χάρτη εγκαταστάσεων. Έτσι, το CPS αναμένεται να βελτιώσει δραματικά την αποδοτικότητα και την παραγωγικότητα σε διάφορους τομείς όπως η γεωργία ακριβείας, ο έλεγχος κτιρίων, η αντιμετώπιση καταστροφών, η ενέργεια, η κατασκευή και η βιομηχανία και οι κοινωνικές υποδομές κ.λπ. Μπορεί να ειπωθεί ότι η πλατφόρμα CPS είναι μια πλατφόρμα σε πλατφόρμα που αποτελείται από πολλές μικρές και απτές ή άυλες πλατφόρμες. Ειδικότερα, η τεχνολογία CPS αναμένεται να παρέχει ένα σύστημα νοημοσύνης μηδενικών ελαττωμάτων που μπορεί να εγγυηθεί υψηλή αξιοπιστία και ασφάλεια για την ευέλικτη αντιμετώπιση απροσδόκητων κρίσεων. [35]

Τα ψηφιακά δίδυμα και τα φυσικά συστήματα στον κυβερνοχώρο (CPS) δεν είναι τα ίδια. Ενώ και οι δύο σχετίζονται με την ενοποίηση του φυσικού και ψηφιακού κόσμου, έχουν

διαφορετικές λειτουργίες και εφαρμογές. Ένα ψηφιακό δίδυμο μπορεί να χρησιμοποιηθεί σε συνδυασμό με ένα CPS για την παρακολούθηση και τον έλεγχο του φυσικού συστήματος, αλλά δεν είναι το ίδιο με το ίδιο το CPS. Το CPS είναι το πραγματικό φυσικό σύστημα, ενώ το ψηφιακό δίδυμο είναι μια εικονική αναπαράστασή του. [35]

4.2 Εφαρμογές και Μέθοδοι σε Smart Cities

4.2.1 Εφαρμογές και Μέθοδοι σε Drones/UAV's

4.2.1.1 Drones as CPS

Τα Drones όπως και κάθε άλλη smart συσκευή πρόκειται για ένα περίπλοκο μηχανισμό που αποτελείται από πολλά διαφορετικά μέρη τα οποία συνολικά καταλήγουν να φτιάχνουν το σύστημα CPS που το αποτελεί. Συγκεκριμένα όπως αναφέρεται πολύ αναλυτικά στο άρθρο [35] το Drone μηχανικά αποτελείται από:

- το σκελετό του
- Σύστημα προώθησης του (Electronic Speed Controller and Propeller)
- Το Flight Controller (FC)
- Battery
- Telemetry (την ασύρματη επικοινωνία μεταξύ του drone και του τηλεχειριστηρίου χειρός, δηλαδή από το Radio Control Transmitter ή το Radio Communication που εφαρμόζει - bluetooth/LTE κτλ)
- Το φορτίο του

Ο τρόπος λοιπόν μέσα από τον οποίο το drone μετατρέπεται σε ένα έξυπνο σύστημα CPS όμως είναι μέσα από τους σενσορες που πλέον αυτά αρχίζουν να υιοθετούν μέσα από location sensors και imaging sensors.

Τα **location Sensors** που χρησιμοποιούνται λοιπόν για τα Drones/UAV's είναι μέσα από δορυφόρους και τις τεχνολογίες ανίχνευσης που αυτοί χρησιμοποιούν (όπως πχ. τριγωνισμός τοποθεσίας μέσα από 3 δορυφόρους)εφόσον το drone χρησιμοποιεί τηλεμετρία με επικοινωνία μέσω δορυφόρων ή μέσα από επιταχυνσιόμετρο και γυροσκόπιο και εκπομπή της πληροφορίας αυτής μέσα από Radio Frequencies στο τηλεχειριστήριο.

Αντίστοιχα τα **Imaging Sensors** τα οποία θα υποστηρίζει το εκάστοτε drone στηρίζονται πάνω σε

1. Χωρική ανάλυση (τι περιοχή και πόσο λεπτομερές μέγεθος)
2. Φασματική ανάλυση (τι χρώματα – ζώνες, ευαισθησία σε μήκος κύματος)
3. Χρονική ανάλυση (πόσο συχνά, ώρα της ημέρας/εποχή/έτος)
4. Ραδιομετρική ανάλυση (πόσο πιο βαθύ βάθος χρώματος)

Και με βάση την ειδική λειτουργία έτσι που το drone θα χρησιμοποιείται (για αγροτικές καλλιέργειες ή για μετάδοση σήματος 5G/6G κτλ) επιλέγεται ο κατάλληλος Imaging Sensor όπου το drone θα μεταφέρει.

Για να κατανοήσουμε τέλος τη πλήρης έκταση που έχουν τα Drones ως CPS τέλος αξίζει να αναφερθούμε σύντομα σε κάποιες τεχνολογίες μέσα από τις οποίες τα Drones θα χρησιμοποιηθούν ευρέως στο Industry 4.0 όπως:

- Στη δημιουργία high quality 3D Maps για τα self driving cars [35]
- Στην άμεση μετάδοση επίγειας επικοινωνίας σε απομονωμένες περιοχές και ταυτόχρονα για την αυτόματη πλοήγηση τόσο των ίδιων των drone όσο και των smart cars μέσα από αυτές [35]

- Και τέλος στην πλήρη αυτόματη πλοήγηση των drone ως autonomous flying machine μέσω deep learning και AI τεχνολογιών και προφανώς μηχανικών εξαρτημάτων [35]

4.2.1.2 Drones as DT

Θα ξεκινήσουμε τη παρούσα παράγραφο αναφέροντας συγκεκριμένα κάποιες εφαρμογές DT και frameworks γενικότερα τα οποία χρησιμοποιούνται για τα UAV's ή Drones. Στη συνέχεια θα δούμε πως μπορούν να χρησιμοποιηθούν τα DT για τη καλύτερη διαχείριση των drones.

4.2.1.2.1 Aeroloop

Το έργο αφορά την ανάπτυξη ενός περιβάλλοντος προσομοίωσης που επιτρέπει στον χρήστη να διεξάγει πειράματα με πολλαπλά εικονικά μη επανδρωμένα εναέρια οχήματα (vUAVs) με φθηνό, ευέλικτο, ελεγχόμενο και ασφαλή τρόπο, πριν δοκιμάσει το σύστημα-λογισμικό και τις αποστολές στον πραγματικό κόσμο. Το σύστημα AeroLoop θα υποστηρίζει λειτουργίες προσομοίωσης λογισμικού in-the-loop και hardware-in-the-loop, ενώ θα εκμεταλλεύεται τις διαθέσιμες μηχανές/μοντέλα προσομοίωσης πτήσης. Θα υποστηρίζει επίσης την ad-hoc επικοινωνία μεταξύ UAV μέσω προσομοιωμένου δικτύου WiFi, καθώς και εικονικές κάμερες στα vUAV. Το σύστημα AeroLoop θα ενσωματωθεί στην ευρύτερη υποδομή του RAWFIE ως εικονική βάση δοκιμών. [45]

4.2.1.2.1 Ardupilot

Το ArduPilot είναι ένα αξιόπιστο, ευέλικτο και ανοιχτού κώδικα σύστημα αυτόματου πιλότου που υποστηρίζει πολλούς τύπους οχημάτων: ελικοπτερα, παραδοσιακά ελικόπτερα, αεροσκάφη σταθερής πτέρυγας, βάρκες, υποβρύχια, ρόβερ και άλλα. Ο πηγαίος κώδικας αναπτύσσεται από μια μεγάλη κοινότητα επαγγελματιών και ενθουσιωδών. Ο καλύτερος τρόπος για να ξεκινήσετε είναι να συμμετάσχετε στο Φόρουμ της ομάδας προγραμματιστών, το οποίο είναι ανοιχτό σε όλους και είναι γεμάτο καθημερινές καλές εξελίξεις. [45]

4.2.1.2.1 Gazepo

Το Gazebo είναι μια πλούσια σε χαρακτηριστικά τρισδιάστατη πλατφόρμα ρομποτικής προσομοίωσης που μπορεί να συνδυαστεί με μια ποικιλία κινητήρων φυσικής και μοντέλων αισθητήρων και μέσω κατάλληλων πρόσθετων μπορεί να χρησιμοποιηθεί για δοκιμές SITL/HITL. [45]

4.2.1.2.1 Airsim

Το AirSim είναι μια πιο πρόσφατη πλατφόρμα που προσφέρει φυσικά και οπτικά ρεαλιστικές προσομοιώσεις μέσω της χρήσης του Unreal Engine και επικεντρώνεται στο να επιτρέπει στους προγραμματιστές αυτόνομων συστημάτων να παράγουν μεγάλες ποσότητες δεδομένων εκπαίδευσης που χρησιμοποιούνται από αλγόριθμους μηχανικής μάθησης. Και οι δύο προσομοιωτές υποστηρίζουν μια ποικιλία δημοφιλών πρωτοκόλλων επικοινωνίας, αλλά είναι αρκετά βαρύ ως προς τους απαιτούμενους πόρους, γεγονός που

καθιστά πιο δύσκολη την εκτέλεση προσομοιώσεων που περιλαμβάνουν μεγάλο αριθμό οχημάτων. [45]

4.2.1.2.1 UTSim

Το UTSim είναι ένα άλλο πρόσφατο πλαίσιο προσομοίωσης που βασίζεται στη μηχανή παιχνιδιών Unity που επικεντρώνεται στη μελέτη ζητημάτων ολοκλήρωσης της εναέριας κυκλοφορίας όπως οι αλγόριθμοι αίσθησης και αποφυγής, πλοήγησης και σχεδιασμού διαδρομής. Το κύριο μειονέκτημα είναι ότι τα σενάρια δοκιμών μπορούν να υλοποιηθούν μόνο χρησιμοποιώντας τη δική του διεπαφή χρήστη, χωρίς να προσφέρει δυνατότητες ενοποίησης σχετικά με τα πιο δημοφιλή πλαίσια εφαρμογών στον τομέα των drone, όπως το DroneKit και το ROS, και τα αντίστοιχα πρωτόκολλα επικοινωνίας, π.χ., το MAVLink. [45]

4.2.1.2.1 Χρησιμότητα των DT για τα Drones

Μία από τις πιο προηγμένες χρήσεις των DT για τα Drones είναι πάνω στην αξιολόγηση των CPS τους που τα απαρτίζουν.Υπάρχει μια ποικιλία προσεγγίσεων για την αξιολόγηση συστημάτων που λειτουργούν σε δυναμικά περιβάλλοντα. Μια ευρεία έννοια που μπορεί να χρησιμοποιηθεί σε όλα τα στάδια του κύκλου ζωής (σχεδιασμός-κατασκευή-λειτουργία) τέτοιων συστημάτων είναι αυτή του digital twin (DT). Η προβλεπόμενη χρήση καθορίζει τα μοντέλα που θα χρησιμοποιηθούν. Μπορεί να ποικίλλει από την επίτευξη καλύτερου σχεδιασμού ή κατασκευής, έως την εκτέλεση προσομοιώσεων what-if για την πρόβλεψη αστοχιών ή τη βελτιστοποίηση της απόδοσης. [45]

Για παράδειγμα, συνδυάζει μια προσομοίωση δυναμικής οχήματος ενός εικονικού οχήματος, που είναι το ψηφιακό δίδυμο του πραγματικού, και μια προσομοίωση κυκλοφορίας, η οποία παρέχει τη συμπεριφορά των άλλων συμμετεχόντων στην κυκλοφορία, κατά τη φάση ανάπτυξης των λειτουργιών αυτοματοποιημένης οδήγησης για τον εντοπισμό κρίσιμων σεναρίων και τη βελτίωση της παρεχόμενης λειτουργικότητας. Από την άλλη πλευρά, παρουσιάζει ένα ρομποτικό σύστημα που χρησιμοποιεί προγνωστική επικύρωση χρόνου εκτέλεσης μέσω προσομοίωσης προοπτικής προκειμένου να πετύχει τον στόχο του διασφαλίζοντας ταυτόχρονα την ασφάλειά του. Για να το πετύχει αυτό, χρησιμοποιεί τον προσομοιωτή ρομπότ Stage για να αξιολογήσει σε πραγματικό χρόνο όλες τις πιθανές ενέργειες του δέντρου αναζήτησης αποφάσεων (που προέρχονται από το ρομπότ και το δυναμικό περιβάλλον), προβλέπει τις συνέπειές τους και επιλέγει την καταλληλότερη. Επίσης, προτείνει την παρακολούθηση χρόνου εκτέλεσης των στοιχείων λογισμικού μέσω της εκτέλεσης του DT του (που θεωρούνται αφηρημένες προδιαγραφές) σε ένα προσομοιωμένο περιβάλλον προκειμένου να εντοπιστούν και να μετριαστούν κακόβουλες συμπεριφορές. [45]

Οι συγγραφείς υποστηρίζουν ότι σε συστήματα λογισμικού η επαλήθευση εκτός σύνδεσης πριν από την ανάπτυξη πρέπει να συνοδεύεται από ποσοτική διαδικτυακή επαλήθευση των βασικών απαιτήσεων κατά το χρόνο εκτέλεσης προκειμένου να επιτευχθεί αξιοπιστία και προσαρμοστικότητα του λογισμικού, μέσω της αναγνώρισης και μερικές φορές της πρόβλεψης παραβιάσεων απαιτήσεων. [45]

4.2.2 Εφαρμογές και Μέθοδοι σε Smart Vehicles/Vanet’s

4.2.2.1 Smart Vehicles as CPS

Προκειμένου να ενοποιηθούν οι υπολογισμοί και οι φυσικές διαδικασίες, έχουν αναπτυχθεί πολλά κυβερνοφυσικά συστήματα (CPS) στην αυτοκινητοβιομηχανία. Με την ευρεία χρήση της άφθονης πληροφορίας στον κυβερνοχώρο και την πρόοδο της τεχνολογίας υλικού, έχουν προταθεί πολλές προσεγγίσεις για να ξεπεραστούν οι προκλήσεις: διαδραστικότητα, εξατομίκευση και συνέχεια. [36]

1) Διαδραστικότητα

Ο Mark Weiser πρότεινε ότι η πανταχού παρούσα νοημοσύνη απαιτεί ευκολότερη αλληλεπίδραση ανθρώπου-υπολογιστή που είναι προσαρμόσιμη στο ιδίωμα αλληλεπίδρασης των ανθρώπων. Ορισμένα έργα έχουν προτείνει φυσικούς τρόπους αλληλεπίδρασης των χρηστών με τα αυτοκίνητα, όπως χειρονομίες, αίσθηση αφής, φωνή. Για παράδειγμα, η διεπαφή χειρονομίας για οχήματα όχι μόνο διευκολύνει τον οδηγό να εκτελεί ορισμένες εργασίες, αλλά αυξάνει επίσης την ασφάλεια μειώνοντας σημαντικά την οπτική ζήτηση και τον γνωστικό φόρτο εργασίας. Μια δονητική-απτική ζώνη μέσης σχεδιάστηκε επίσης για να δίνει οδηγίες στροφή προς στροφή χρησιμοποιώντας την απτική αντίληψη του ανθρώπινου δέρματος. Η Mercedes-Benz παρουσίασε την πρώτη γενιά του Linguatronic, ενός συστήματος εντολών και ελέγχου που βασίζεται στην ομιλία για αυτοκίνητα. Το σύστημα ομιλίας επιτρέπει την πλήρη λειτουργία hands-free του κινητού τηλεφώνου. [36]

2) Εξατομίκευση

Ορισμένα έργα έχουν προταθεί για την παροχή εξατομικευμένων υπηρεσιών. Για παράδειγμα, το Affective Intelligent Driving Agent (AIDA), ένα νέο προσωπικό ρομπότ στο αυτοκίνητο που αναπτύχθηκε από ερευνητές του MIT, μπορεί όχι μόνο να διαβάσει τη διάθεση του οδηγού από την έκφραση του προσώπου, αλλά και να ανταποκριθεί με κοινωνικά κατάλληλο και κατατοπιστικό τρόπο. Επιπλέον, η AIDA έχει την ικανότητα να μελετά τις οδηγικές συνήθειες και την εμπειρία των οδηγών, ώστε να μπορεί να λαμβάνει σημαντικές αποφάσεις και συμπεράσματα για τους οδηγούς. Το Ford Sync μπορεί επίσης να παρέχει πληροφορίες πλοήγησης, κίνησης και ψυχαγωγίας σύμφωνα με τις απαιτήσεις και τις προτιμήσεις των χρηστών. [36]

3) Συνέχεια

Σε ορισμένα έργα όπως το MirrorLink και το Sonnenberg, το έξυπνο τηλέφωνο είναι ενσωματωμένο στο έξυπνο αυτοκίνητο. Οι MirrorLink και Sonnenberg ενσωμάτωσαν το έξυπνο τηλέφωνο με το αυτοκίνητο μέσω WLAN, Bluetooth, USB ή DPWS (Devices Profile for Web Services). Το έξυπνο τηλέφωνο και το έξυπνο αυτοκίνητο συνδέονται άψογα και ορισμένες υπηρεσίες και διεπαφές χρήστη μπορούν να μετεγκατασταθούν από φορητές συσκευές σε συστήματα ενημέρωσης και ψυχαγωγίας αυτοκινήτου. Το OnStar επιτρέπει στους ανθρώπους να ελέγχουν και να παρακολουθούν εξ αποστάσεως τα αυτοκίνητά τους χρησιμοποιώντας τα έξυπνα τηλέφωνά τους. Η ενσωμάτωση έξυπνων τηλεφώνων με αυτοκίνητα μπορεί να διατηρήσει τη συνέχεια των υπηρεσιών μεταξύ των χώρων του κυβερνοχώρου και των φυσικών χώρων. [36]

Καποια απο τα συστήματα CPS που αναφέρονται στο [36] είναι τα ακόλουθα:

A. Sensor-based status monitoring and control

- Status monitoring module: Η κατάσταση του αυτοκινήτου μπορεί να παρακολουθείται εξ αποστάσεως, όπως τα χιλιόμετρα, η κατάσταση των θυρών του αυτοκινήτου (ανοιχτές / κλειστές). [36]
- Surveillance module: Η δουλειά αυτής της μονάδας είναι να διατηρεί μια απομακρυσμένη επιτήρηση για το περιβάλλον του αυτοκινήτου και το περιβάλλον έξω από το αυτοκίνητο. [36]
- Lock and control module: Οι άνθρωποι μπορούν να ελέγχουν τις συσκευές στο αυτοκίνητο χρησιμοποιώντας έξυπνα τηλέφωνα. Το έξυπνο τηλέφωνο μπορεί να χρησιμοποιηθεί ως κλειδί για να κλειδώσετε τις πόρτες ή τα παράθυρα του αυτοκινήτου. [36]
- Alarm module: Οι άνθρωποι θα προειδοποιούνται αυτόματα εάν συμβούν απροσδόκητα πράγματα στα αυτοκίνητα. Οι άνθρωποι μπορούν επίσης να ελέγξουν τα αρχεία καταγραφής συναγερμών στο έξυπνο τηλέφωνο. [36]

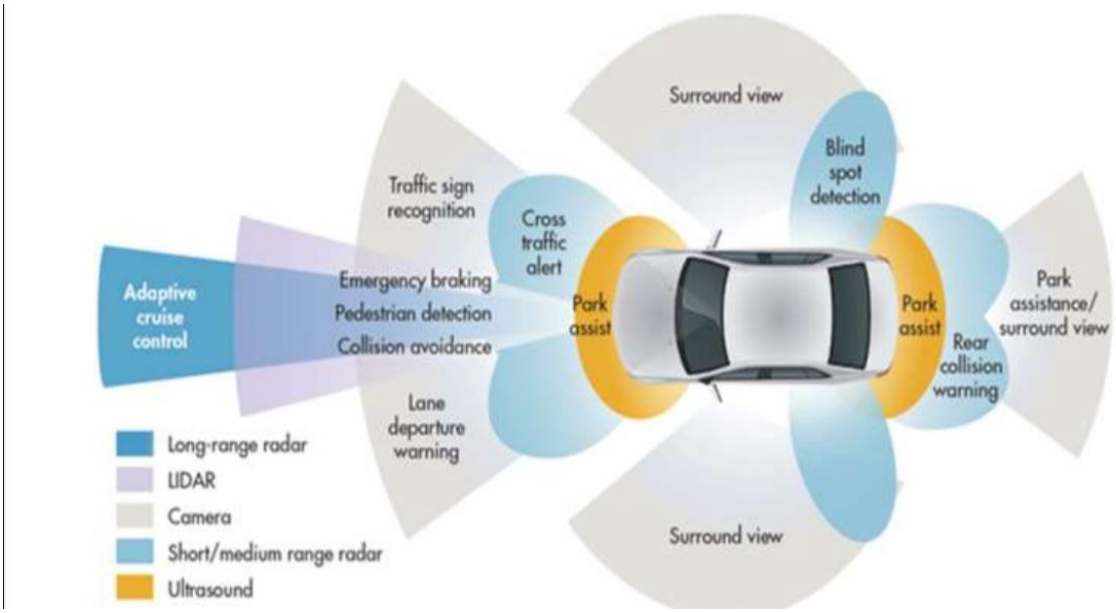
B. Gesture-based environmental control

- 3D modeling for cars: Αποθηκεύσαμε την τρισδιάστατη μοντελοποίηση αυτοκινήτων και συσκευών εντός αυτοκινήτου σε μια ετικέτα NFC. Επιπλέον, αποθηκεύσαμε επίσης πληροφορίες τοποθεσίας των μερών που κάθονται συχνά σε ετικέτες και επικολλήσαμε τις ετικέτες στα μέρη που κάθονται συχνά οι άνθρωποι. Οι χρήστες πρέπει πρώτα να αγγίξουν τις ετικέτες με τα τηλέφωνά τους για να διαβάσουν τις πληροφορίες του τρισδιάστατου μοντέλου και τη θέση του τηλεφώνου. [36]
- Computing the pointing information: Το έξυπνο τηλέφωνο υπολογίζει με ακρίβεια τις πληροφορίες της κατεύθυνσης κατάδειξης. Και το εικονίδιο της συσκευής που δείχνει το έξυπνο τηλέφωνο εμφανίζεται στην οθόνη του τηλεφώνου. [36]
- Recognizing the gestures: Προκατασκευάζουμε αναγνωρίσιμες εντολές αλληλεπίδρασης και τις αντίστοιχες χειρονομίες κάθε εντολής για συσκευές αυτοκινήτου. Όταν οι χρήστες παίρνουν τη συσκευή που επιλέγουν, οι χρήστες κινούν τα χέρια τους και οι χειρονομίες αναγνωρίζονται. Οι αντίστοιχες εντολές ελέγχου αποστέλλονται στις συσκευές μέσω ασύρματης επικοινωνίας. [36]

C. NFC-based media migration

- Event detection: Το συμβάν καταγράφεται όταν οι χρήστες χρησιμοποιούν ένα έξυπνο τηλέφωνο για να αγγίξουν την ετικέτα NFC που είναι τοποθετημένη στο αυτοκίνητο ή να απομακρύνουν το τηλέφωνο από την ετικέτα. Εν τω μεταξύ, το smart phone και η κονσόλα αυτοκινήτου συνδέονται μέσω ασύρματης επικοινωνίας. Οι πληροφορίες σχετικά με την κονσόλα αυτοκινήτου που είναι αποθηκευμένες στην ετικέτα διαβάζονται ταυτόχρονα από το έξυπνο τηλέφωνο. [36]
- Media determination: Ελέγχοντας τις σχετικές εφαρμογές στο τηλέφωνο, όπως Μουσική, Βίντεο και Συλλογή, προσδιορίζεται το μέσο που αναπαράγεται στο τηλέφωνο. Στη συνέχεια, το τηλέφωνο διαβάζει τις πληροφορίες σχετικά με αυτό το μέσο. [36]
- Media migration: Το έξυπνο τηλέφωνο στέλνει τις πληροφορίες πολυμέσων στην κονσόλα αυτοκινήτου και καλείται η σχετική εφαρμογή στην κονσόλα αυτοκινήτου. Μετά από αυτό, τα μέσα αναπαράγονται συνεχώς στην κονσόλα αυτοκινήτου και μπορούν να ελεγχθούν με το έξυπνο τηλέφωνο. [36]

Στο σχήμα 11 παρακάτω φαίνονται μόνο κάποια από τα πολλά συστήματα CPS που έχει ένα smart car



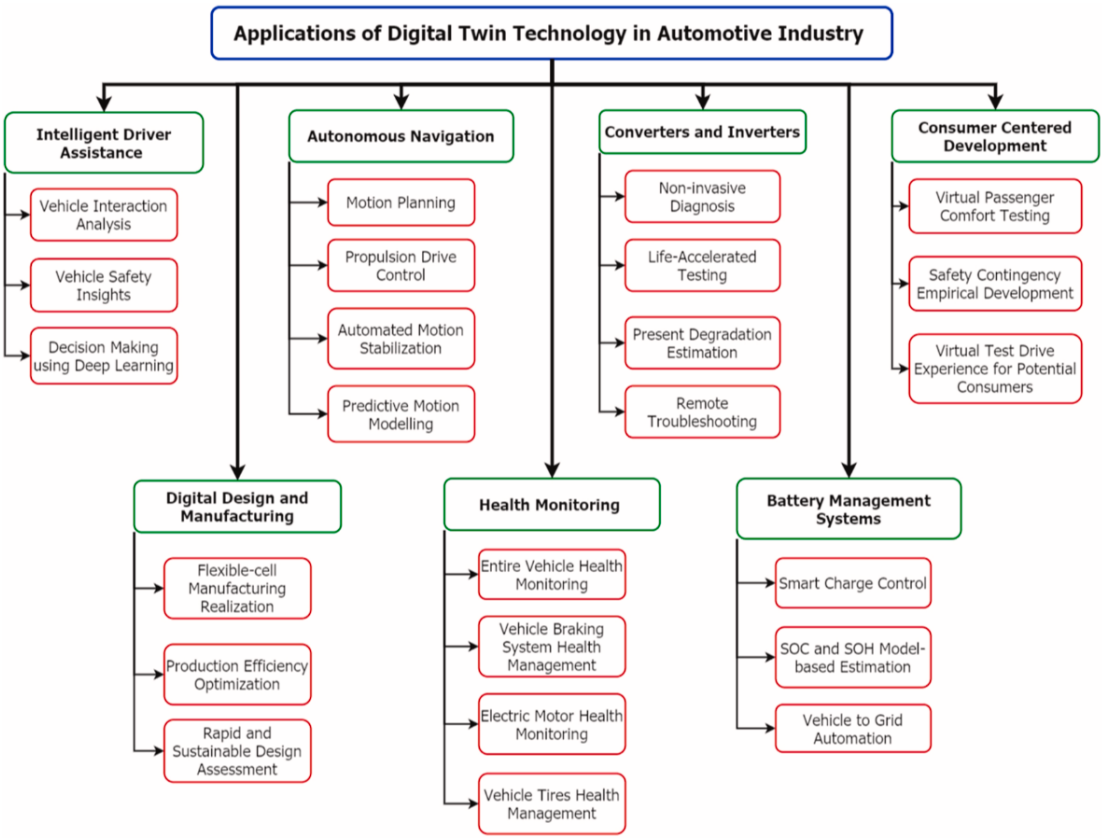
[40]

Σχήμα 11: CPS ενός αυτόνομου οχήματος

4.2.2.2 Smart Vehicles as DT

Τα ηλεκτρικά οχήματα είναι πολύ κατάλληλα για εικονική αναπαράσταση, αλλά οι σύνθετες αλληλεξαρτήσεις του υποσυστήματος αποδεικνύονται πρόκληση όταν εφαρμόζεται ένα ρεαλιστικό μοντέλο. Η κύρια πτυχή της ψηφιακής διπλής τεχνολογίας DT είναι ότι βασίζεται σε μεγάλο βαθμό σε δεδομένα και το σύνολο δεδομένων από τον κύκλο ζωής του οχήματος του επιτρέπει να αναπαράγει ακόμη και διεπιστημονικά χαρακτηριστικά του οχήματος. Αυτό το σύνολο δεδομένων αποτελεί τις πληροφορίες προϊόντος που περνούν από την αρχή της ζωής (BoL) έως το τέλος της ζωής (EoL) και τις πληροφορίες που παράγεται από τον εννοιολογικό ορισμό, τη μοντελοποίηση και την ωρίμανση, και η παραγωγή βιομηχανικής συναρμολόγησης χρησιμοποιείται ως ορυχεία δεδομένων για το DT. [46]

Η εικονική αναπαράσταση σχηματίζεται στη συνέχεια από τη συγχώνευση τρισδιάστατων μοντέλων CAD ή γεωμετρικών σκίτσων, χαρακτηριστικών προφίλ σώματος όπως υπολογιστική δυναμική ρευστών ή θερμικά μοντέλα και αρχέτυπα βασισμένα στη φυσική που αναπαριστούν την κίνηση του αυτοκινήτου. Για ολοκληρωμένη αναπαράσταση, το περιβάλλον του οχήματος πρέπει επίσης να αναπαραχθεί δυναμικά στον ψηφιακό κόσμο, συμπεριλαμβανομένων όλων των συμβατών παραμέτρων που επηρεάζουν τη λειτουργία του οχήματος. Άλλα αρχεία ανθρώπινου χειριστή, όπως η ιστορική πρόοδος του προϊόντος, τα δεδομένα στόλου και τα αρχεία καταγραφής συντήρησης, μπορούν να παρέχουν στο ψηφιακό αρχέτυπο σχετικό πλαίσιο για να αντιπροσωπεύει την τρέχουσα ή μελλοντική κατάσταση του περιβάλλοντος και των εσωτερικών μηχανισμών του. Είναι προφανές ότι η ψηφιακή δίδυμη τεχνολογία προσφέρει μεγάλες δυνατότητες για τη δημιουργία μιας φιλικής προς τους πόρους προσέγγισης δοκιμών και βελτιστοποίησης για ηλεκτρικά οχήματα, και τα έξυπνα οχήματα παράγουν άφθονη αισθητηριακή ανάδραση και δεδομένα σε πραγματικό χρόνο, καθιστώντας τα ιδανικούς υποψηφίους για αναπαραγωγή ως ψηφιακά δίδυμα. Το Σχ. 12 απεικονίζει μια επισκόπηση των εφαρμογών του DT στην αυτοκινητοβιομηχανία. [46]



[46]

Σχήμα 12: Εφαρμογές της τεχνολογίας digital twin στο κλάδο της αυτοκινητοβιομηχανίας

Συνοπτικά απο το [46] DT systems είναι τα ακόλουθα:

- Predictive mobility and autonomous motion control
- Advanced driver assistance systems (**ADAS**)
    - Η χρήση της ασαφούς λογικής στα συστήματα ADAS DT είναι θεμελιώδης για τη διευκόλυνση της μετάβασης από τα ημιαυτόνομα οχήματα στα αυτόνομα οχήματα.
- Vehicle health monitoring and management (**IVHM**)
    - Integrated Vehicle Health management -> Το IVHM διαπιστώνει ότι το υποσύστημα λειτουργεί στην κανονική του κατάσταση, χωρίς απρόβλεπτη βλάβη. Στο πλαίσιο αυτού του παραδείγματος, τα ψηφιακά δίδυμα προσφέρουν στους κατασκευαστές αυτοκινήτων αυξημένη ικανότητα να διαγνώσουν ανώμαλες καταστάσεις και να προβλέψουν την υπολειπόμενη ωφέλιμη ζωή των αφαιρετικών εξαρτημάτων του οχήματος χωρίς καμία ανάγκη επιτόπιων δοκιμών, βελτιώνοντας έτσι την ασφάλεια και την ικανοποίηση του ιδιοκτήτη.
- Battery management systems and intelligent charging
    - Battery Management Systems (**BMS**) -> Διάφοροι τύποι αισθητήρων, ενεργοποιητών, συμπεριλαμβανομένων των χειριστηρίων βρίσκονται στο EV BMS. Το BMS μετρά τη χωρητικότητα της μπαταρίας, την απόσβεση της μπαταρίας κατά τη φόρτιση/εκφόρτιση και τη σωστή απόδοση της μπαταρίας και παρέχει στους χρήστες αυτές τις πληροφορίες σε πραγματικό χρόνο
- Vehicle power electronic converters

- Electric power drive system
    - Modern Electric Power Drive Systems (**EPDS**) -> Τα σύγχρονα συστήματα ηλεκτροκίνησης ισχύος (EPDS) μετρούν σε μεγάλο βαθμό την απόδοση της μετάδοσης κίνησης από οικονομική και τεχνολογική άποψη.

4.2.3 Εφαρμογές και Μέθοδοι σε Satellite IoT

4.2.3.1 Satellite IoT as CPS

2 βασικά συστήματα CPS εξερευνεί το άρθρο [37] το οποίο έχει να κάνει με δίκτυα satellite IoT, με πρώτο να είναι το GNSS. Το σύστημα **GNSS** λαμβάνει την τοποθεσία, η οποία εμφανίζεται σε ψηφιακό χάρτη που παρέχεται από DVD ή εσωτερικό σκληρό δίσκο και ο χρήστης βλέπει την τρέχουσα τοποθεσία. Οι πληροφορίες οδικής κυκλοφορίας αποστέλλονται με καθυστέρηση μερικών λεπτών μέσω του συστήματος πληροφοριών και επικοινωνίας του οχήματος (για παράδειγμα, **VICS** στην Ιαπωνία) και αυτό εμφανίζεται στην οθόνη. Αυτές οι πληροφορίες βρίσκονται σε ξεχωριστό επίπεδο, δεν ενσωματώνονται στα δεδομένα χάρτη. Μια παρόμοια τεχνική μπορεί να παρατηρηθεί με την επαυξημένη πραγματικότητα (AR). Είναι ενσωματωμένο για να φαίνεται σαν μια προσομοίωση ή μια εικόνα στον κυβερνοχώρο να υπερτίθεται στον φυσικό χώρο. [37] Αυτο πρόκειται για το λεγόμενο σύστημα PCPS (pseudo-CPS), ο ορισμός του οποίου ξεφεύγει απο τα πλαίσια της εργασίας αυτής.

Το 2ο σύστημα CPS το οποίο συναντάμε είναι το σύστημα UOS (Urban Operating System). Αυτή η πλατφόρμα λειτουργίας είναι οργανωμένη με τέσσερα επίπεδα: αισθητήρα/ενεργοποιητή, εποπτεία, έλεγχο και εφαρμογή. Το στρώμα αισθητήρα/ενεργοποιητή περιέχει διάφορες συσκευές στον φυσικό κόσμο. Οι πληροφορίες τους συγκεντρώνονται τοπικά και παραδίδονται στο Διαδίκτυο σε πραγματικό χρόνο. Το επίπεδο εποπτείας οργανώνει τις πηγές δεδομένων, διεξάγει αναλύσεις και προσομοιώσεις και το παρέχει στο επίπεδο εφαρμογής. Οι συσκευές IoT παρακολουθούνται και ελέγχονται στο επίπεδο ελέγχου. Το UOS θεωρείται επιχειρηματική λύση παρά εμπορικό πακέτο. Ως εφαρμογή, η Hitachi Ltd. έχει εφαρμόσει το σύστημα σε έργα ανάπτυξης μεγάλης κλίμακας. [37] Αυτό αντίστοιχα πρόκειται για ένα TCPS (True-CPS), ο ορισμός του οποίου επίσης δεν έχει σημασία.

Γενικότερα απο το άρθρο αυτό γίνεται κατανοητό ότι τα συστήματα CPS τα οποία απαρτίζουν τα δίκτυα των δορυφόρων θα χρησιμοποιηθούν σε διάφορες εφαρμογές του Smart City σε συνδυασμό με άλλες συσκευές IoT, ενώ ταυτόχρονα ορίζεται η έννοια των Geo-CPS, δηλαδή των συστημάτων αυτών CPS τα οποία χρειάζονται δορυφορική κάλυψη.

Πιθανές εφαρμογές των Geo CPS: [37]

- Construction industry and construction equipment
- Water resources and infrastructure management
- Environmental conservation and resource management
- Accessibility and mobility
- City Brain in China

4.2.3.1 Satellite IoT as DT

Ορισμένες ερευνητικές μελέτες έχουν εφαρμόσει την ψηφιακή διπλή τεχνολογία στο σχεδιασμό πλαισίων και μεθόδων προστασίας δορυφορικών δικτύων. Για δορυφορική παρακολούθηση και επαλήθευση ασφάλειας, οι Hou et al. παρουσιάζουν ένα πλαίσιο που συνδυάζει ψηφιακά δίδυμα με επαλήθευση χρόνου εκτέλεσης και προτείνουν μια μέθοδο συγχρονισμού κατάστασης για την εξασφάλιση ασφαλούς και αποτελεσματικής επικοινωνίας μεγάλων αποστάσεων μεταξύ δορυφόρων και ψηφιακών δίδυμων. Για την παρακολούθηση της συμπεριφοράς του δορυφόρου σε πραγματικό χρόνο και τη διασφάλιση της αξιοπιστίας των δορυφορικών συστημάτων, οι Shangguan et al. παρουσιάζουν μια προσέγγιση διάγνωσης βλαβών και παρακολούθησης της υγείας (**FD-HM**) που βασίζεται σε ψηφιακά δίδυμα. [47]

Για δορυφορικά-επίγεια δίκτυα, η ταχύτητα κίνησης του δορυφόρου είναι μεγαλύτερη από τον επίγειο σταθμό, γεγονός που μπορεί να προκαλέσει ασυνεπή εξυπηρέτηση και συχνή παράδοση δορυφόρων. Για την επίλυση αυτών των προβλημάτων, οι Zhao et al. προτείνει μια στρατηγική αποθήκευσης με ψηφιακή διπλή υποβοήθηση για δορυφορικά-επίγεια δίκτυα (**INTERLINK**) και ένα σύστημα παράδοσης προσανατολισμένο σε δορυφορική αποθήκευση. Ο αστερισμός του Ιριδίου χρησιμοποιείται ευρέως ως σενάριο προσομοίωσης δορυφορικού δικτύου. Για παράδειγμα, οι Liu et al. προτείνουν ένα έξυπνο πρωτόκολλο δρομολόγησης με επίγνωση της ενέργειας για δορυφορικά δίκτυα και χρησιμοποιούν τον αστερισμό του ιριδίου ως πειραματικό σενάριο για την αξιολόγηση της απόδοσης. Ταυτόχρονα, ορισμένοι μελετητές προσπαθούν να συνδυάσουν ψηφιακά δίδυμα με βιομηχανικές εγκαταστάσεις. [47]

Οι ερευνητές στο [47] στη συνέχεια φτιάχνουν ένα DT για την αναπαράσταση των δορυφόρων και για να μπορέσουν μέσω αυτού να υπολογίσουν αν κάποιος δορυφόρος έχει χτυπηθεί απο αντικείμενο και έχει βγει εκτός τροχιάς. Αυτό είναι ένα application όπου το DT χρησιμοποιείται για αυτό το σύστημα επομένως

4.3 Εφαρμογές και Μέθοδοι σε Smart Buildings and Facilities

4.3.1 Εφαρμογές και Μέθοδοι σε Smart Homes/Office

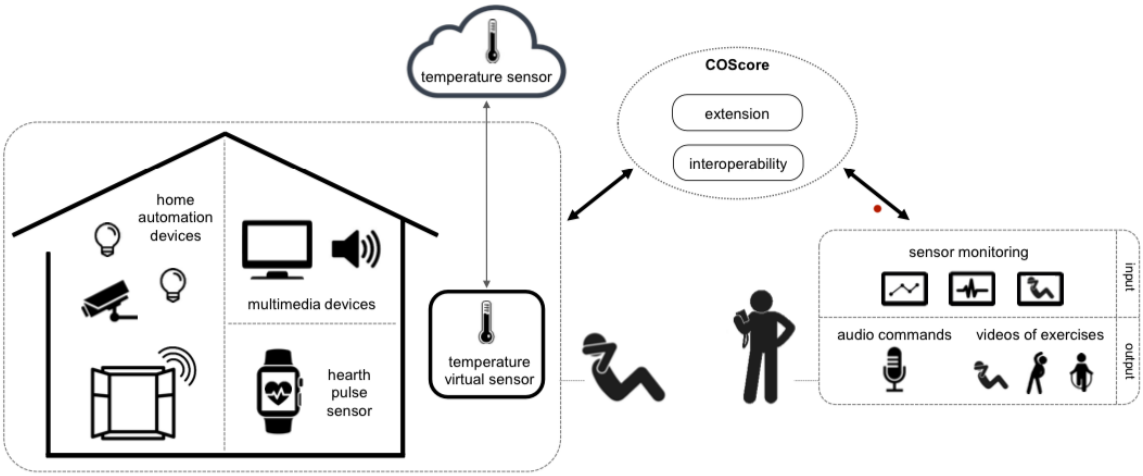
4.3.1.1 Smart Homes as CPS

Μπορούμε να δούμε αυτήν την ετερογένεια των CPS σε ένα παράδειγμα σεναρίου απομακρυσμένης παρακολούθησης της φυσικής δραστηριότητας ενός ατόμου που βρίσκεται στο σπίτι του/της. Αυτός ο χαρακτήρας (αριστερή πλευρά του σχήματος) ζει σε ένα έξυπνο σπίτι με διαφορετικά κυβερνοφυσικά συστήματα. Πρώτον, ένας αριθμός λαμπτήρων, μια κάμερα ασφαλείας και ένας αισθητήρας για την ανίχνευση του ανοίγματος ενός παραθύρου συνδέονται σε ένα σύστημα οικιακού αυτοματισμού. Δεύτερον, μια έξυπνη τηλεόραση και ένα σετ ασύρματων ηχείων αποτελούν μέρος ενός συστήματος πολυμέσων. Τρίτον, ένα έξυπνο ρολόι είναι ένα άλλο CPS που προορίζεται να λάβει τον καρδιακό ρυθμό του χαρακτήρα και, τέλος, ένας εικονικός αισθητήρας διαβάζει την εξωτερική θερμοκρασία, η οποία αποκτάται από μια υπηρεσία τρίτων που είναι διαθέσιμη στο cloud. [38]

Όλα τα αναφερόμενα συστήματα χρησιμοποιούν διαφορετικές τεχνολογίες και πρωτόκολλα επικοινωνίας και δεν μπορούν εύκολα να συνδεθούν για να εκτελέσουν μια κοινή εργασία. Σε αυτή την περίπτωση, ο στόχος του σεναρίου είναι να συνδέσει τον πελάτη (ο χαρακτήρας στο σπίτι) με έναν personal trainer για παράδειγμα (δεξιά πλευρά του

Σχήματος 13). Ο εκπαιδευτής θα λάβει τα δεδομένα θερμοκρασίας, τον καρδιακό ρυθμό και τις εικόνες από την κάμερα ως χρήσιμες πληροφορίες για την παρακολούθηση της δραστηριότητας. Αυτός ο χαρακτήρας μπορεί να στείλει εντολές ήχου που θα αναπαράγονται μέσω των ηχείων και μπορεί επίσης να στείλει βίντεο με νέες ασκήσεις που θα εμφανίζονται στην smart TV. Επιπλέον, αυτή η συμπεριφορά πρέπει να συνυπάρχει με την εργασία ασφαλείας του συστήματος οικιακού αυτοματισμού που θα ηχήσει ένα σήμα συναγερμού μέσω των ηχείων και θα αναβοσβήνουν οι λαμπτήρες εάν ενεργοποιηθεί ο αισθητήρας παραθύρου. [38]

Το κύριο πρόβλημα εδώ είναι να επιτραπεί η σύνδεση μεταξύ των διαφορετικών τμημάτων, μετατρέποντας έτσι κάθε σύστημα σε ένα υποσύστημα μιας ολόκληρης λύσης που επιτρέπει τη διαλειτουργικότητα. [38]

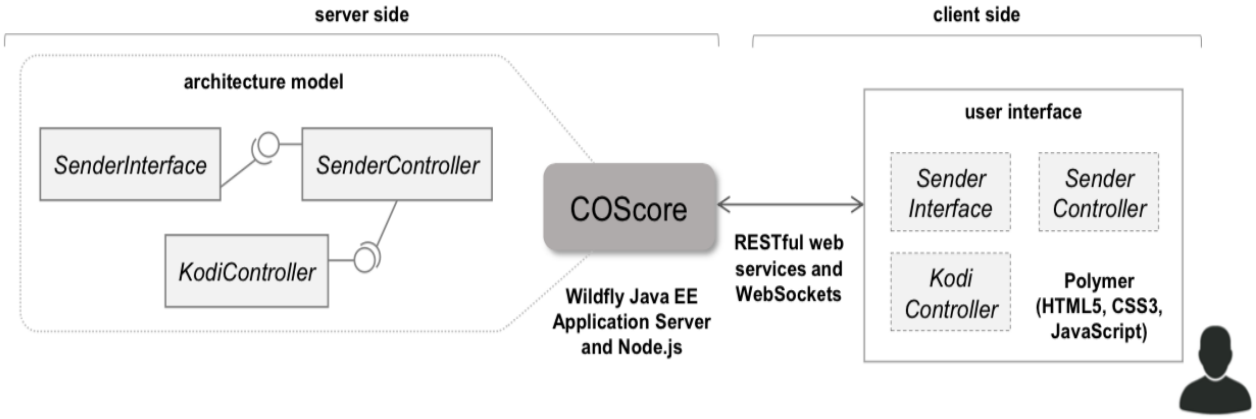


Σχήμα 13: Ετερογενή CPS σε ένα παραδειγματικό σενάριο

Οι συγκεκριμένοι ερευνητες στο [38] αναφέρουν στη συνέχεια το COScore μια τεχνολογία η οποία μπορεί να ενώσει όλα αυτά τα διαφορετικά CPS μεταξύ τους, χρησιμοποιώντας το λογισμικό KODI.

Όπως συζητήθηκε και προηγουμένως για να υποστηριχθεί η επέκταση και η συμπερίληψη διαφορετικών τύπων CPS, οι ερευνητές του [38] ανέπτυξαν τη δική τους τεχνολογική υποδομή (που ονομάζεται COScore). Η ανάπτυξή του βασίζεται στην τεχνολογία CBSE, Model-Driven Engineering (MDE) και τεχνολογία που βασίζεται στο Cloud Computing. Προκειμένου να διευκολυνθεί η κατανόηση αυτού του άρθρου, είναι απαραίτητο να συνοψιστούν οι πιο σχετικές πτυχές αυτής της υποδομής, οι οποίες περιγράφονται παρακάτω. Η πρότασή μας απαιτεί κάθε εφαρμογή χρήστη να ορίζεται ως ένα σύνολο ανεξάρτητων στοιχείων, διαθέσιμα σε μια ποικιλία αποθετηρίων (ιδιοκτησίας ή τρίτου μέρους). Ονομάσαμε αυτά τα στοιχεία ως COTSgets, από το Commercial Off-The-Shelf (COTS) και το GadGETS. Ακολουθώντας το προηγούμενο παράδειγμα, ας υποθέσουμε ότι ένας personal trainer θέλει να στείλει έναν πόρο (ήχος, βίντεο κ.λπ.) σε έναν πελάτη για να αναπαράγει με ένα κέντρο πολυμέσων KODI. [38]

Το **KODI** είναι ένα λογισμικό ανοιχτού κώδικα που παρέχει μια φιλική διεπαφή χρήστη για την αναπαραγωγή (επιπλέον της εγγραφής, προγραμματισμού, προβολής κ.λπ.) αρχείων πολυμέσων που είναι αποθηκευμένα σε τοπικό χώρο αποθήκευσης ή διαθέσιμα από μια απομακρυσμένη διεύθυνση URL ιστού. Επιπλέον, όλες οι ενέργειες μπορούν να εκτελεστούν μέσω ενός API αντί να αλληλεπιδρούν με τη διεπαφή χρήστη. Σε αυτήν την περίπτωση, μπορούμε να δημιουργήσουμε τρία στοιχεία: KodiController, SenderController και SenderInterface (δεξιά πλευρά του σχήματος 14). [38]



Σχήμα 14: Κύρια μέρη της τεχνολογίας COScore

4.3.1.2 Smart Homes as DT

Για να γεφυρωθεί το χάσμα μεταξύ των δεδομένων εκπαίδευσης και των δεδομένων χρήσης του πραγματικού κόσμου, η δημιουργία δεδομένων μπορεί να είναι μια πιθανή λύση, ιδιαίτερα μέσω της έννοιας των ψηφιακών διδύμων. Στο πλαίσιο του HAR(Human Activity Recognition), ένα ψηφιακό δίδυμο θα μπορούσε να είναι ένα εικονικό αντίγραφο ενός σπιτιού στόχου, με τους ίδιους εγκατεστημένους αισθητήρες. Μέσα σε αυτό το ψηφιακό περιβάλλον, ένα ή πολλά avatars μπορούν να προσομοιώσουν ADL μοντελοποιώντας τις συμπεριφορές των κατοίκων. Με αυτόν τον τρόπο, το ψηφιακό δίδυμο μπορεί να χρησιμοποιηθεί για να τελειοποιήσει τους αλγόριθμους πριν από την ανάπτυξή τους στο πραγματικό σπίτι-στόχο. [48]

Επιπλέον, τα ψηφιακά δίδυμα έχουν τη δυνατότητα να παράγουν δεδομένα που αντιπροσωπεύουν ένα ευρύ φάσμα διαμορφώσεων σπιτιών, οικιακών συνηθειών και συμπεριφορών των κατοίκων, επιταχύνοντας έτσι τις προσομοιώσεις, διευκολύνοντας την αυτόματη επισήμανση και εξαλείφοντας το κόστος των φυσικών αισθητήρων. Αυτό το εκτεταμένο σύνολο δεδομένων μπορεί στη συνέχεια να χρησιμοποιηθεί για προ-εκπαίδευση μοντέλων μηχανικής εκμάθησης. Επιπλέον, ένα ψηφιακό δίδυμο μπορεί να βοηθήσει στην αξιολόγηση της σωστής τοποθέτησης και επιλογής αισθητήρων για την αναγνώριση μιας προκαθορισμένης λίστας δραστηριοτήτων. [48]

Τα ψηφιακά δίδυμα μοντέλα έχουν κερδίσει σημαντικό ενδιαφέρον σε διάφορους τομείς εφαρμογών, όπως η κατασκευή, η αεροδιαστημική, η υγειονομική περίθαλψη και η ιατρική. Ενώ τα ψηφιακά δίδυμα για έξυπνα σπίτια είναι σχετικά λιγότερο διερευνημένα, τα ψηφιακά δίδυμα για κτίρια έχουν μελετηθεί εκτενώς. Ngah Nasaruddin et al. ορίζουν το Digital Twin ενός κτιρίου ως την αλληλεπίδραση μεταξύ του εσωτερικού περιβάλλοντος ενός πραγματικού κτιρίου και ενός ρεαλιστικού εικονικού μοντέλου αναπαράστασης του κτιριακού περιβάλλοντος. Αυτό το ψηφιακό δίδυμο επιτρέπει την παρακολούθηση και την απόκτηση δεδομένων σε πραγματικό χρόνο. Για παράδειγμα, ψηφιακά δίδυμα κτιρίων έχουν χρησιμοποιηθεί σε μία έρευνα για τον προσδιορισμό των στρατηγικών θέσεων των αισθητήρων για αποτελεσματική συλλογή δεδομένων. [48]

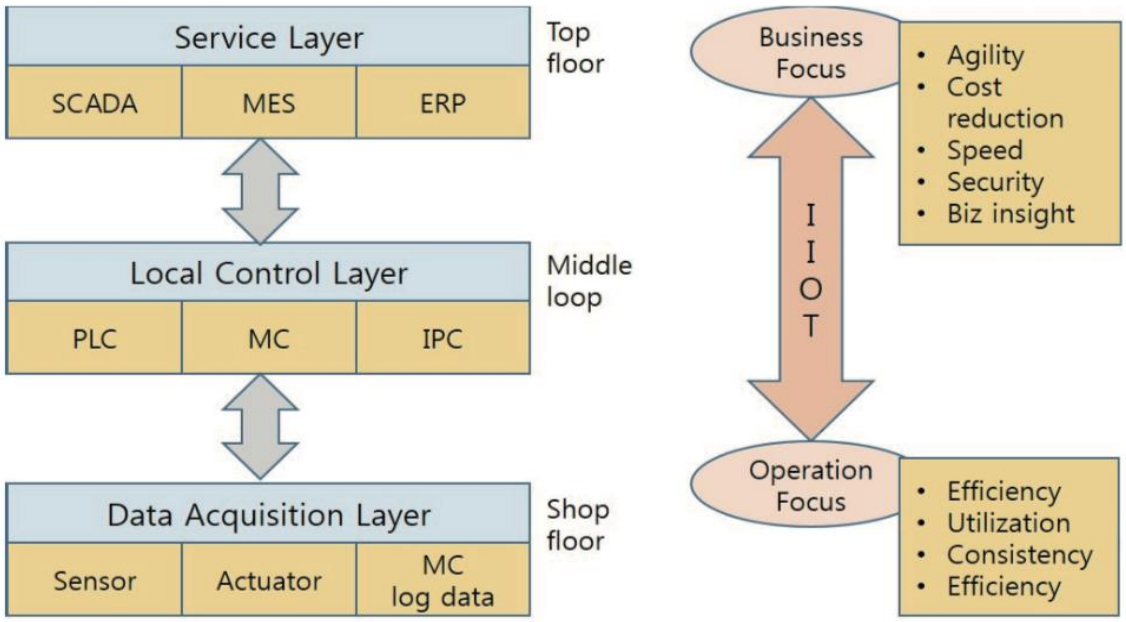
4.3.2 Εφαρμογές και Μέθοδοι σε Industrial IoT (IIoT) και Smart Factories

4.3.2.1 Smart Factories as CPS

Το συνδεδεμένο εργοστάσιο χαρακτηρίζεται τυπικά από μια ιεραρχική δομή, η οποία είναι μια «πυραμίδα αυτοματισμού». Αποτελείται από τρία επίπεδα: επίπεδο απόκτησης δεδομένων, αλλαγή τοπικού ελέγχου και επίπεδο υπηρεσίας. [49]
Δεδομένα αισθητήρα, ενεργοποιητή και δεδομένα καταγραφής μηχανής στο κατάστημα είναι είσοδος για τοπικό έλεγχο αργότερα. Στον μεσαίο βρόχο, ο προγραμματιζόμενος λογικός ελεγκτής (**PLC**), ο μικροελεγκτής (**MC**) και ο βιομηχανικός υπολογιστής (**IPC**) είναι τα ονόματα του διαμεσολαβητή. Στο επίπεδο υπηρεσιών, υπάρχουν δίκτυα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (**SCADA**), Σύστημα Εκτέλεσης Κατασκευής (**MES**) και Σχεδιασμός Πόρων Επιχειρήσεων (**ERP**). Το SCADA είναι μια αρχιτεκτονική συστήματος ελέγχου που χρησιμοποιεί υπολογιστές, δικτυωμένες επικοινωνίες δεδομένων και γραφικές διεπαφές χρήστη για διαχείριση εποπτείας διεργασιών υψηλού επιπέδου. [49]

Η μεταφορά αυτών των περιεκτικών δεδομένων από τα συστήματα Λειτουργικής Τεχνολογίας (OT) στον όροφο του καταστήματος στα συστήματα Πληροφορικής (IT) στον τελευταίο όροφο θα απαιτούσε ειδικές μεθοδολογίες και τεχνικές για την ανάλυση μεγάλων δεδομένων. Η προαναφερθείσα έννοια της πυραμίδας αυτοματισμού απεικονίζεται στο Σχήμα 15. Η παραπάνω αρχιτεκτονική αντιστοιχεί σε πλατφόρμα υπολογισμού/επικοινωνίας, πλατφόρμα λογισμικού και φυσική πλατφόρμα. Στο CPS, οι βασικές ιδιότητες του συστήματος όπως η σταθερότητα, η ασφάλεια και η απόδοση εκφράζονται με όρους φυσικής συμπεριφοράς. [49]

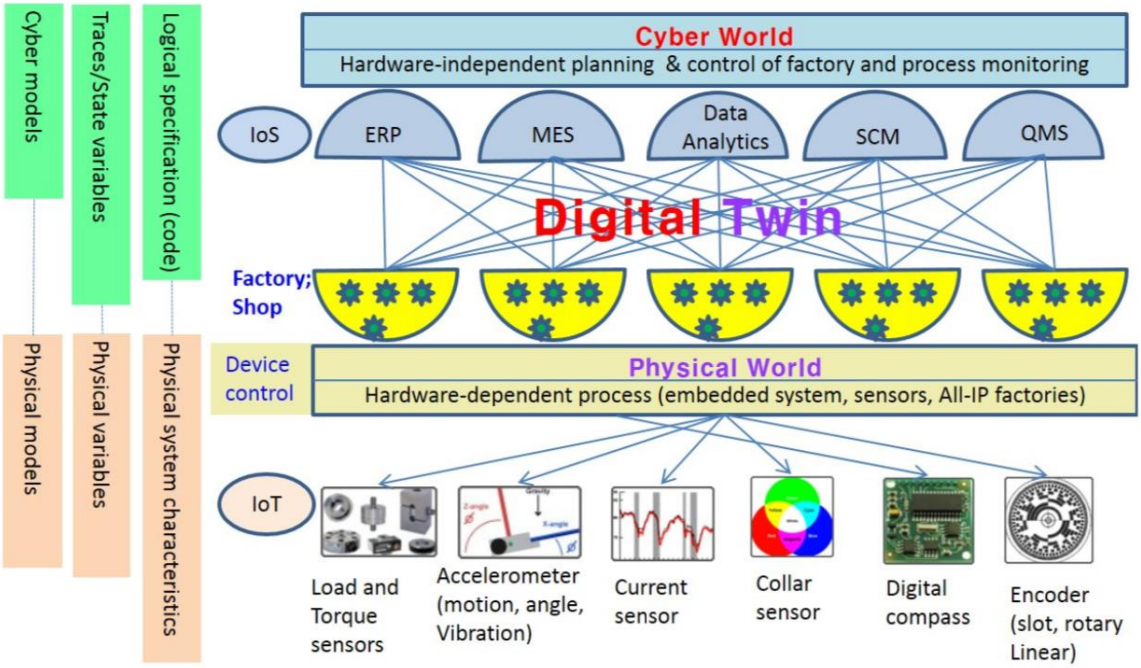
Ένα πρωτότυπο έξυπνου εργοστασίου με δυνατότητα IoT στον τομέα της βιομηχανικής κατασκευής ταινιών βινυλίου έχει αναφερθεί. Το πρόβλημα ποιότητας στο βιομηχανικό βινύλιο έχει αντιμετωπιστεί με χρήση δικτύου αισθητήρων. Η προσομοιωμένη γραμμή κατασκευάζεται από χαλύβδινο οδηγό, ένα διαφανές μπουκάλι νερού, δύο πλακέτες Arduino, τρεις Zigbee και δύο αισθητήρες υπερήχων. [49]



[49]
Σχήμα 15: Η πυραμίδα του αυτοματισμού σε 3 επίπεδα

Το σχέδιο του έξυπνου εργοστασιακού συστήματος ελέγχου και παρακολούθησης που βασίζεται σε ψηφιακό δίδυμο λειτουργεί ως εξής. Όλα τα χαρακτηριστικά του έξυπνου εργοστασίου με αισθητήρες, δίκτυο και σύστημα παλαιού τύπου αντικατοπτρίζονται στο tablet ή τον υπολογιστή που είναι ενσωματωμένο με αναλυτικά δεδομένα μεγάλων δεδομένων στο cloud ή στον κύριο διακομιστή. Όλες οι ενέργειες και οι εργασίες στο κύτταρο παραγωγής και κατασκευής παρακολουθούνται με διαφάνεια στο tablet ή τον υπολογιστή σε πραγματικό χρόνο. Με βάση τα αναλυτικά δεδομένα μεγάλων δεδομένων, το πρόβλημα ποιότητας ή πρόβλημα εγκατάστασης προβλέπεται ή αποτρέπεται προληπτικά. Τα αποτελέσματα της ανάλυσης μεγάλων δεδομένων ανατροφοδοτούνται στο βιομηχανικό πεδίο για την παρακολούθηση και τον έλεγχο της διαδικασίας. [49]

Το σχήμα 16 δείχνει την αρχιτεκτονική CPS που αποτελείται από φυσικούς και ψηφιακούς κόσμους. Στον φυσικό κόσμο, διάφορα δεδομένα αισθητήρων αποκτώνται μέσω ασύρματου και ενσύρματου δικτύου αισθητήρων. Είναι μια διαδικασία που εξαρτάται από το υλικό με ενσωματωμένο σύστημα, πολλαπλούς αισθητήρες και IIoT (Industrial Internet of Things). Στον κόσμο του κυβερνοχώρου, το ERP, το MES, το **SCM** (Supply Chain Management), το **QMS** (Quality Management System) και η ανάλυση δεδομένων εργάζονται για την εφαρμογή του IoS (Internet of Service). Αυτά αντιστοιχούν στην κληρονομιά στη μεταποιητική βιομηχανία. [49]



Σχήμα 16: Εποπτική αρχιτεκτονική CPS - Digital Twin

4.3.2.2 Smart Factories as DT

Στη βιβλιογραφία στο paper [50] αναλύονται κάποιες συγκεκριμένες πλατφόρμες open source μέσω των οποίων μπορούν να χρησιμοποιηθούν DT.

Αυτή η εργασία διερευνά τη συλλογική ικανότητα 5 πλατφορμών ανοιχτού κώδικα, δηλαδή των Eclipse Hono1, Eclipse Ditto2, Apache Kafka3, Influx DB4 και Grafana5. Η συλλογική λειτουργία αυτών των πλατφορμών έχει σχεδιαστεί για να επιτρέπει ψηφιακές δίδυμες δυνατότητες, συμπεριλαμβανομένης της απόκτησης δεδομένων σε πραγματικό

χρόνο IoT, εικονικής αναπαράστασης και διαχείρισης, ανάλυσης σε πραγματικό χρόνο και οπτικοποίησης. Η αρχιτεκτονική ανοιχτού κώδικα αποδεικνύεται με τα «ανοικτά δεδομένα» της βιομηχανίας που διατίθενται από τη Microsoft και έχουν συγκριθεί με καθολικά εργαλεία δοκιμών, όπως το «Apache jmeter», για την κατανόηση της ικανότητας απόδοσης κλιμάκωσης. [50]

Το **Eclipse Hono** παρέχει διεπαφές απομακρυσμένων υπηρεσιών για τη σύνδεση μεγάλου αριθμού συσκευών IoT και την αλληλεπίδραση μαζί τους με ομοιόμορφο τρόπο, ανεξάρτητα από το πρωτόκολλο επικοινωνίας της συσκευής. Η Hono υποστηρίζει συσκευές που επικοινωνούν μέσω κοινών πρωτοκόλλων IoT, στάνταρ, όπως HTTP, MQTT και AMQP. Είναι μια αρχιτεκτονική που βασίζεται σε μικροϋπηρεσίες που χρησιμοποιεί ένα αντιδραστικό μοντέλο προγραμματισμού, επιτρέποντας την οριζόντια κλιμάκωση. Καθώς, μια τέτοια επικοινωνία είναι εύκολη μέσω ενός κοινού API ανεξάρτητα από το πρωτόκολλο της συσκευής. [50]

Το **Eclipse Ditto** είναι ένα πλαίσιο που υποστηρίζει την εφαρμογή προτύπων λογισμικού IoT Digital twins. Οι δυνατότητες του Ditto περιλαμβάνουν:

- αντικατοπτρίζει φυσικά στοιχεία/συσκευές
- λειτουργεί ως «μοναδική πηγή αλήθειας» για ένα φυσικό περιουσιακό στοιχείο
- παρέχει πτυχές και υπηρεσίες γύρω από τις συσκευές
- διατηρεί τον πραγματικό και ψηφιακό κόσμο σε συγχρονισμό.

Το ψηφιακό δίδυμο πλαίσιο της Ditto παρέχει web API για αλληλεπίδραση με ψηφιακά δίδυμα, διασφαλίζει ότι η πρόσβαση μπορεί να γίνει μόνο με εξουσιοδότηση, επιτρέπει ένα προς ένα ή ένα προς πολλά Digital twin αλληλεπιδράσεις και ενσωματώσεις σε άλλες υποδομές υποστήριξης, όπως μεσίτες και συστήματα ανταλλαγής μηνυμάτων. [50]

Το **Apache Kafka** επιτρέπει τη δημιουργία αγωγών δεδομένων για εφαρμογές ροής σε πραγματικό χρόνο. Οι τρεις κύριες δυνατότητες του Kafka είναι:

- δημοσίευση και εγγραφή σε ροή εγγραφών
- αποθήκευση αυτών των εγγραφών με τρόπο ανεκτικό σε σφάλματα
- επεξεργασία τους όπως εμφανίζονται. [50]

Το **Influx DB** είναι μια βάση δεδομένων σειρών σε πραγματικό χρόνο, η οποία είναι απλή στη ρύθμιση και την κλίμακα. Μια βάση δεδομένων χρονοσειρών χρησιμοποιείται για την αποθήκευση αρχείων καταγραφής, πολλαπλών τύπων δεδομένων (π.χ. δεδομένα αισθητήρων), για μια χρονική περίοδο. Το δυνατό σημείο του Influx DB είναι ότι τα δεδομένα γράφονται σε πραγματικό χρόνο και διαβάζονται σε πραγματικό χρόνο, με δυνατότητα εκατομμυρίου εγγραφών ανά δευτερόλεπτο. [50]

Το **Grafana** είναι μια λύση ανάλυσης και παρακολούθησης που παρέχει μοντέλα πηγών δεδομένων προσθέτων και υποστήριξη για πολλές από τις πιο δημοφιλείς βάσεις δεδομένων χρονοσειρών, όπως: Graphite, Prometheus, Elastic search και Influx DB. Το Grafana επιτρέπει στους χρήστες να κάνουν ερωτήσεις, να οπτικοποιούν και να ειδοποιούνται για μετρήσεις και αρχεία καταγραφής από πολλές αποθηκευμένες τοποθεσίες που είναι αποθηκευμένες. [50]

Ο συνδυασμός αυτών των 5 πλατφορμών ανοιχτού κώδικα παρέχει μια καθολική αρχιτεκτονική για το Digital Twin. Αυτή η αρχιτεκτονική παρέχει συνδεσιμότητα IoT και απόκτηση δεδομένων σε πραγματικό χρόνο (Hono), εικονική αναπαράσταση και διαχείριση (Ditto), οριζόντια δεδομένα συνδεσιμότητα αγωγών (Kafka), αποθήκευση δεδομένων χρονοσειρών (Influx DB), ανάλυση δεδομένων και οπτικοποίηση (Grafana). [50]

4.4 Εφαρμογές σε Smart Healthcare and Wearables

4.4.1 Εφαρμογές σε Smart Healthcare

4.4.1.1 Smart Healthcare as CPS

Ο κλάδος του smart healthcare έχει αφενός άπειρες εφαρμογές από τη κατασκευή των φαρμάκων μέχρι και την βοήθεια των ασθενών. Ως εκ τούτου αποτελείται από αμέτρητα συστήματα CPS τα οποία το αποτελουν και τα οποία με τη σειρά τους υπερκαλύπτονται απο άλλους κλάδους τους οποίους έχουμε αναφέρει ήδη.

Ένα paper στο οποίο θα αναφερθούμε αναφέρει πως μπορεί να χρησιμοποιηθεί σε συνδυασμό με τα smart homes [39] και έτσι έχουμε τα ακόλουθα συστήματα CPS:

- Medication Reminder Systems in Smart Homes
- Detection of Pill Ingestion
- Systems for People with Cognitive Impairment
- n-Home Monitoring for High-Risk Pregnancies
- Ambient Technology and E-Diagnostics
- Monitoring Bone Fracture Recovery
- Continuous Edema Assessment

Ο ρόλος του CPS στις εφαρμογές λήψης φαρμάκων είναι πρωταρχικής σημασίας. Είτε η μη τήρηση των συνταγογραφούμενων φαρμάκων είναι σκόπιμη είτε όχι, μπορεί να γίνει ένα περίπλοκο πρόβλημα με σοβαρές συνέπειες. Ορισμένοι παράγοντες μπορεί να συμβάλλουν στην ακούσια μη τήρηση της φαρμακευτικής αγωγής, συμπεριλαμβανομένης της λήθης λόγω γήρανσης ή των γνωστικών φορτίων των ηλικιωμένων. Η σωματική αναπηρία μπορεί επίσης να αποδοθεί σε αμέλεια κατά τη λήψη φαρμάκων. Επιπλέον, η τήρηση της φαρμακευτικής αγωγής καθίσταται δύσκολη για τους ηλικιωμένους, καθώς η ποικιλία των φαρμάκων αυξάνεται λόγω των συνοδών ιατρικών καταστάσεων. Ως αποτέλεσμα, η θεραπεία μπορεί να μειώσει την αποτελεσματικότητά της ή να έχει δυσμενείς επιπτώσεις στην υγεία του ασθενούς υποβαθμίζοντας έτσι την ποιότητα ζωής. Αυξάνει επίσης το ποσοστό εισαγωγής στο νοσοκομείο και το κόστος υγειονομικής περίθαλψης. Επιπλέον, η ακριβής αξιολόγηση του επιπέδου μη συμμόρφωσης του ασθενούς στη φαρμακευτική αγωγή είναι δύσκολο να προσδιοριστεί από τον πάροχο υγειονομικής περίθαλψης [39]

4.4.1.2 Smart Healthcare as DT

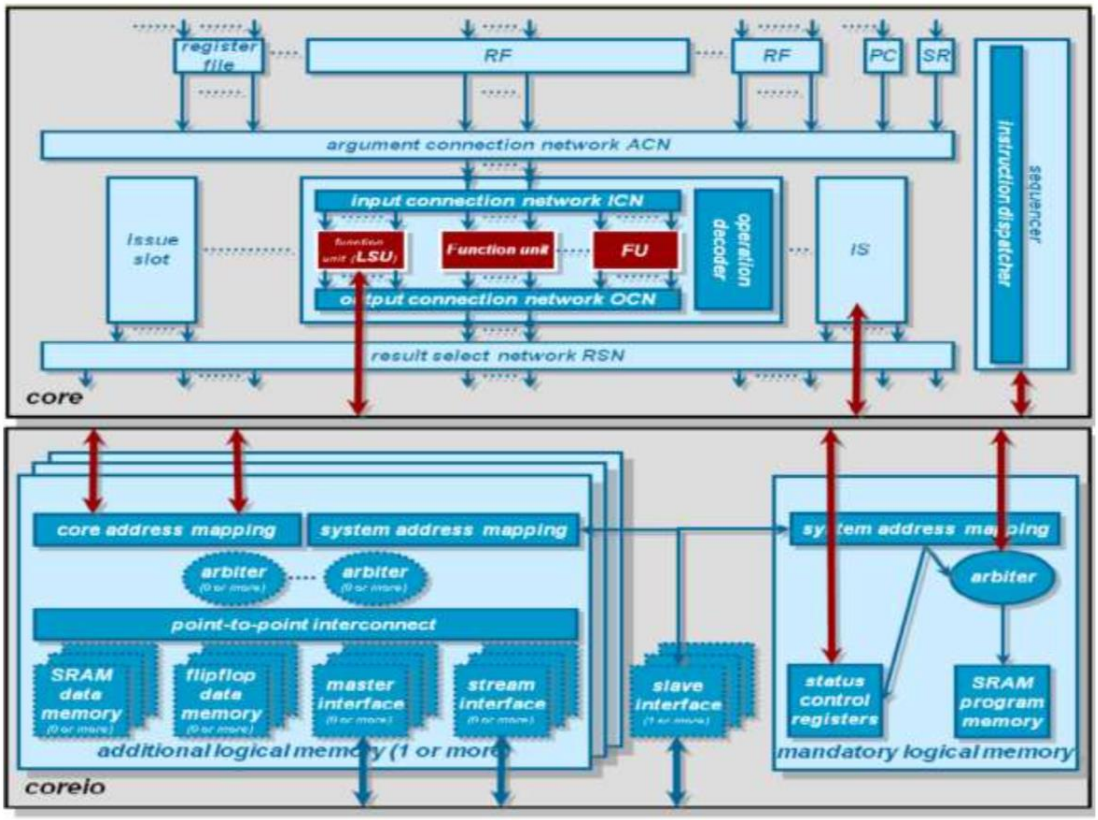
Το άρθρο [51] παρέχει μια καλή εικόνα κάποιων DT τεχνολογιών στην υγειονομική περίθαλψη. Μέσα σε αλλα επισημαίνει ότι η ανάπτυξη ενός Digital Twin μπορεί να είναι μια πολύ περίπλοκη και δαπανηρή εργασία και μπορεί επίσης να αυξήσει την πολυπλοκότητα της παρακολούθησης της υγείας των ασθενών σε ένα νοσοκομείο. Επομένως, η έρευνα που σχετίζεται με τα ψηφιακά δίδυμα πρέπει να καθορίσει ποια δεδομένα συμβάλλουν περισσότερο στην προβλεψιμότητα των αποτελεσμάτων, πώς μπορούν να αξιολογηθούν αυτά τα αποτελέσματα και πώς αυτή η προσέγγιση μπορεί να ενσωματωθεί οικονομικά στην υγειονομική περίθαλψη. Τελικά, ωστόσο, τα Digital Twins μπορούν να βελτιώσουν τις διαγνωστικές και παρακολούθησης ικανότητες, να βελτιώσουν τη θεραπεία και την ευημερία του ασθενούς, να μειώσουν το οικονομικό κόστος και να επεκτείνουν τις επιλογές θεραπείας και τις επιλογές ασθενών όταν εφαρμόζονται επαρκώς. [51]

Ωστόσο, στην υγειονομική περίθαλψη, η έννοια του Ψηφιακού Διδύμου δεν έχει ακόμη καθοριστεί τόσο ξεκάθαρα λόγω της απίστευτης πολυπλοκότητας του ανθρώπου, ενός αντικειμένου του φυσικού κόσμου, για το οποίο πρέπει να δημιουργηθεί ένα Ψηφιακό Δίδυμο. Όσον αφορά τα εξαρτήματα των βιομηχανικών συστημάτων σήμερα, υπάρχει η ελπίδα ότι η μοντελοποίηση θα παρέχει την επιθυμητή ακρίβεια των αποτελεσμάτων. Αλλά δυστυχώς, είναι πολύ πιο δύσκολο να προσφέρουμε καθολικές μεθόδους και προσεγγίσεις για τη διαμόρφωση του ανθρώπινου όντος. Επίσης, παρά τις ανακαλύψεις στη δημιουργία νέων αισθητήρων και μεθόδων συλλογής δεδομένων, η απόκτηση ενημερωμένων δεδομένων για βασικούς δείκτες του ανθρώπινου σώματος σε λειτουργικό τρόπο είναι μια δύσκολη εργασία, η οποία μπορεί να υλοποιηθεί, τις περισσότερες φορές, μόνο σε εργαστηριακή κλινική έρευνα. [51]

4.4.2 Εφαρμογές σε Wearables

4.4.2.1 Wearables as CPS

Το άρθρο [40] αναφέρεται αναλυτικά στα συστήματα CPS τα οποία αποτελούν γενικότερα τα περισσότερα wearables. Τη στιγμή βέβαια που αυτά τα συστήματα ως επί το πλείστον δεν αποτελούνται από επιμέρους συσκευές και λειτουργίες ο μοναδικός τρόπος να περιγράφουν τα συστήματα CPS που το αποτελούν είναι να γίνει μια εκτενής αναφορά στο υλικό το οποίο εμπεριέχεται στη motherboard. Ενώ αυτό είναι σημαντικό για hardware forensic analysis κρίνεται ότι είναι έξω από τους σκοπούς της συγκεκριμένες εργασίας. Παρατίθεται μόνο το σχήμα 17 για να έχουμε μια σύντομη εικόνα:



Σχήμα 17: Γενικευμένη VLIW ASIP αρχιτεκτονική

Όπου φαίνεται η αρχιτεκτονική VLIW προκειμένου να καταλάβουμε που θα πρέπει να εστιάζει ένας Digital Forensics analyst ή που ένας researcher θα έπρεπε να κάνει τροποποιήσεις ώστε να προστεθούν βήματα που θα βοηθήσουν στις μεθόδους DF όπως είδαμε σε άλλες περιπτώσεις

4.4.2.2 Wearables as DT

Η κατασκευή φορητών ιατρικών συσκευών είναι ένας προκλητικός και εξαιρετικά ρυθμιζόμενος τομέας. Λόγω της άμεσης αλληλεπίδρασης με τους ασθενείς, οι εξελίξεις των ιατροτεχνολογικών προϊόντων εξαρτώνται σε μεγάλο βαθμό από τους τελικούς χρήστες, δηλαδή τους ηλικιωμένους, τα άτομα με αναπηρίες ή/και ειδικές ανάγκες και τους φροντιστές τους . Δεδομένου αυτού του χαρακτηριστικού, μένει κανείς να σκεφτεί πώς υποστηρίζεται η κατασκευή φορητών ιατρικών συσκευών από τις τεχνολογικές βελτιώσεις που επιφέρει η DT. [52]

Η DT υποστηρίζει την λιτή παραγωγή και συμβάλλει στη βελτίωση της ασφάλειας και στη μείωση του χρόνου και του κόστους παραγωγής μέσω της βελτιστοποίησης της διαφάνειας. Μερικές από τις περισσότερες λειτουργίες που εισάγει η DT είναι η συγκέντρωση δεδομένων και η ιχνηλασιμότητα, καθιστώντας την DT μια πολλά υποσχόμενη τεχνολογία για φορητές ιατρικές συσκευές. [52]

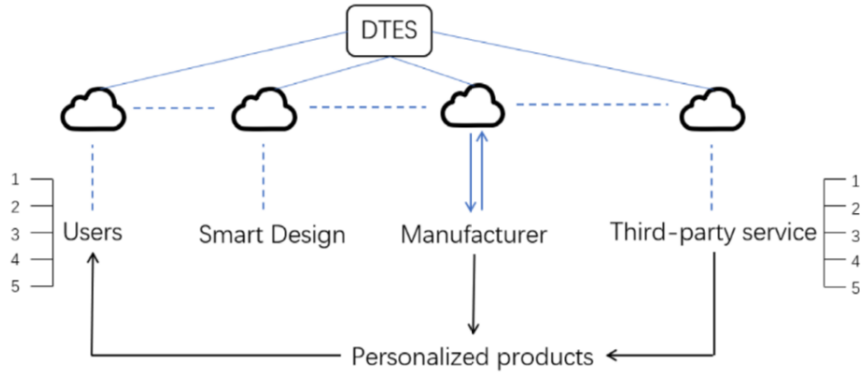
Αυτή η μελέτη [52] προτείνει ένα σύστημα έξυπνων συσκευών με δυνατότητα DT για τη συμμετοχή διαφόρων τύπων ασθενών στην εξατομίκευση και την υπηρεσία υγειονομικής περίθαλψης των φορητών συσκευών τους. Είναι μια αποδεκτή και θεωρητική δομή. Μέσω της διαχείρισης αποδοτικότητας των πληροφοριών όλων των συμμετεχόντων στην κατασκευή, το σύστημα παράγει εξαιρετικά εξατομικευμένες συσκευές άνετα. Με βάση το Διαδίκτυο των πραγμάτων σε φορητές συσκευές, παρέχεται επίσης η λειτουργία συνεχούς παρακολούθηση δομής συστήματος. [52]

Το σύστημα DT-enabled (DTES) είναι ένα εξατομικευμένο σύστημα σέρβις που καλύπτει ολόκληρο τον κύκλο του προϊόντος. Συνδέει όλους τους συμμετέχοντες στο σύστημα σχεδιασμού και κατασκευής μέσω υπηρεσιών cloud. Στο DTES, η συλλογή δεδομένων χρήστη, ο σχεδιασμός, η κατασκευή, οι υπηρεσίες τρίτων και άλλα μέρη διαθέτουν χαρτογράφηση δεδομένων και συμπληρωματικές υπηρεσίες cloud. Ο κατασκευαστής θα διαχειρίζεται κεντρικά τα δεδομένα για να διασφαλίσει ότι η εξατομικευμένη διαδικασία παραγωγής μπορεί να πραγματοποιηθεί ομαλά μεταξύ όλων των συμμετεχόντων. Η δομή του DTES φαίνεται στο Σχήμα 18. [52]

Το DT κάθε χρήστη αποτελείται από δύο είδη εξατομικευμένων δεδομένων: τις εξατομικευμένες παραμέτρους σχεδιασμού και τα δεδομένα που παράγονται από τη μακροχρόνια χρήση του προϊόντος. Τα δεδομένα παραμέτρων χρήστη για το σχεδιασμό πρέπει να εισάγονται από τους χρήστες. Τέτοια δεδομένα θα εξαχθούν από το cloud και θα δημιουργήσουν σχετικά αρχεία σχεδίασης με τη βοήθεια υπολογιστή (CAD), τα οποία θα γίνουν τα αρχεία εισόδου της εξατομικευμένης κατασκευής. Αυτή η διαδικασία είναι η βάση του εξατομικευμένου σχεδιασμού και κατασκευής. Τα δεδομένα που παράγονται κατά τη μακροχρόνια χρήση περιλαμβάνουν φυσιολογικά δεδομένα, παραμέτρους κατάστασης κ.λπ. [52]

Αυτά τα δεδομένα πρέπει να παρακολουθούνται για μεγάλο χρονικό διάστημα και να εφαρμόζονται περαιτέρω. Επομένως, στο DTES, θα αποθηκεύσουμε και θα αρχειοθετήσουμε αυτά τα δεδομένα στο cloud, τα οποία το σύστημα εφαρμογής θα ανακτήσει ανά πάσα στιγμή. Για ορισμένες πρόσθετες λειτουργίες και εξαρτήματα σε

εξατομικευμένα προϊόντα, είναι δύσκολο για τους κατασκευαστές να τα αναπτύξουν εκ νέου και να τα παράγουν επειδή αυτό συνήθως σημαίνει υψηλό κόστος. Η συνεργασία με τρίτους παρόχους υπηρεσιών επιτρέπει στους κατασκευαστές να κατασκευάζουν γρήγορα τα εξατομικευμένα προϊόντα που χρειάζονται. Σε αυτή τη διαδικασία, το DTES μπορεί να λειτουργήσει ως «γέφυρα» μεταξύ των δύο μέσω υπηρεσιών cloud. Οι κατασκευαστές μπορούν να ενσωματώσουν γρήγορα τις πληροφορίες των υπηρεσιών τρίτων και να συνδυάσουν σχετικές υπηρεσίες για να συντομεύσουν το χρόνο της εξατομικευμένης κατασκευής. [52]



[52]
Σχήμα 18: Αρχιτεκτονική DTES

4.5 Εφαρμογές σε XR/AR/VR

4.5.1 XR/AR/VR as CPS

Μόνο η ίδια η συσκευή αποτελεί το CPS ενός XR/AR/VR application. Ως εκ τούτου δεν υπάρχει βιβλιογραφία για το συγκεκριμένο topic

4.5.2 XR/AR/VR as DT

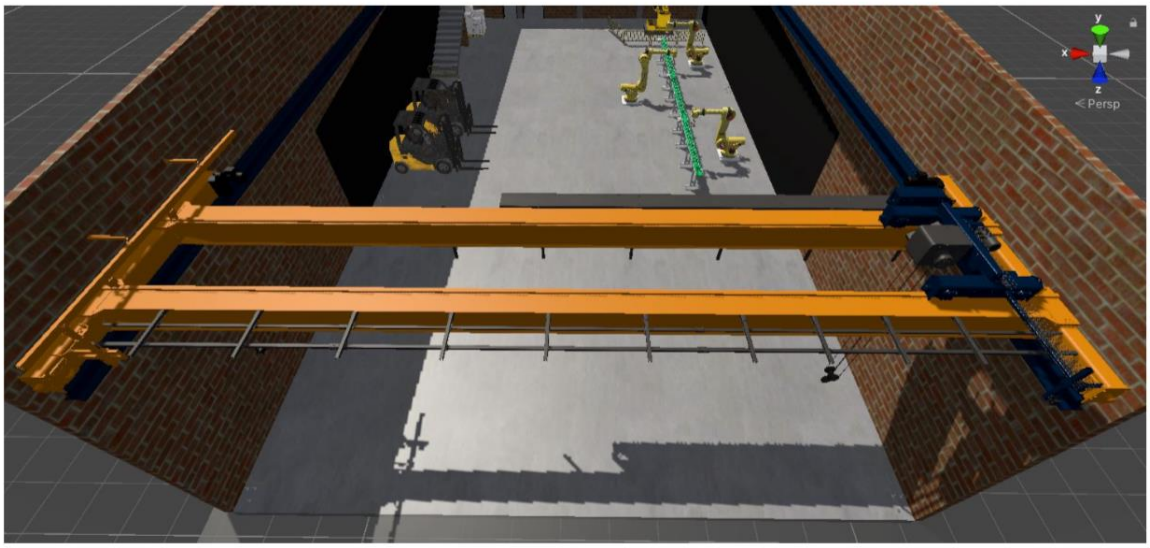
Στο άρθρο [41] συνάντησα τα παρακάτω εργαλεία μέσω των οποίων στήθηκε το software ενός DT application μέσω VR :

- Unity
- OpenXR
- XRTK/MRTK
- HslCommunication
- RestSharp API
- UA-.NETStandard:

Το DT είναι το μοναδικό application που μπορούν να χρησιμοποιηθούν τα περιβάλλοντα αυτά

Σε αυτό το άρθρο χρησιμοποίησαν το XR για να φτιάξουν ένα DT μιας ρόμπας (industrial section) και να μπορούν οι μηχανικοί μέσω αυτού του XR να αναλύσουν καλύτερα τις ιδιότητες του [41] :

Το περιβάλλον που έχτισαν είναι το ακόλουθο:



Σχήμα 19: Ένα μοντέλο στη Unity

Μια ακόμα χρησιμότητα που έχει το XR είναι στην ενίσχυση του DT σε HCLINT-DT όπως φαίνεται και απο το άρθρο [53]

Η μονάδα Annotation Module (AM) εμφανίζεται ως συνοδευτικό της μονάδας DT πέντε διαστάσεων. Το AM λειτουργεί ως μονάδα plug-and-play που εκμεταλλεύεται το HCLINT μαζί με τα παραδείγματα XR. Στην πράξη, κάθε χρήστης που αλληλεπιδρά με το PE ή το VE μπορεί να διαβάσει ή να παράγει σχολιασμούς. Τέτοιοι σχολιασμοί μπορούν να προέρχονται από AR και VR. Στην πρώτη περίπτωση, ένας χρήστης που φοράει οθόνη με κεφαλή AR (π.χ. τα Hololens) μπορεί: (α) να εξατομικεύσει εκείνα τα αντικείμενα του πραγματικού κόσμου που διαθέτουν επίσης έναν κυβερνο-φυσικό αντίστοιχο στο VE και (β) να παρέχει σχολιασμούς, με την παραγωγή περιεχομένου πολυμέσων (π.χ. κειμενικά, οπτικά και φωνητικά δεδομένα). Οι ενότητες **ADTD** και **ASSYST** επεξεργάζονται και αναπαράγουν τέτοιους σχολιασμούς, καθιστώντας τους διαθέσιμους στα αντίστοιχα στοιχεία του VE. Η ρύθμιση VR προσφέρει αντ 'αυτού τη δυνατότητα άμεσης παροχής σχολιασμών στο VE, εκμεταλλευόμενη μια οθόνη τοποθετημένη στο κεφάλι VR. Οι ενημερώσεις που κοινοποιούνται στο VR υποβάλλονται σε επεξεργασία από τις μονάδες ADTD και ASSYST για την εξαγωγή τέτοιων σχολιασμών σε AR. Η προτεινόμενη AM είναι αγνωστική όσον αφορά τον συγκεκριμένο τύπο DT (αντικείμενο, άνθρωπος ή διαδικασία).
Για να απεικονίσουμε οπτικά τον μηχανισμό λειτουργίας του AM και πώς αλληλεπιδρά με το μοντέλο αναφοράς DT, παρουσιάζουμε το νέο Σχήμα 2. Όπως φαίνεται, το AM λειτουργεί σε τρία στάδια, πριν, κατά τη διάρκεια και μετά την εισαγωγή ενός σχολιασμού (ή όχι). Σε αυτό το σχήμα, τα μπλε, μωβ, κίτρινα και πράσινα μπλοκ αντιπροσωπεύουν τις διεπαφές PE, VE, ASSYST και AR/VR, αντίστοιχα. Οι λειτουργίες και οι αλληλεπιδράσεις τους υποστηρίζονται από το ADTD. [53]

Πριν από την ανάγνωση ή τη δημιουργία ενός σχολιασμού, το σύστημα αναγνωρίζει τα αντικείμενα που παρακολουθεί ένας χρήστης. Για το σκοπό αυτό, λαμβάνεται ένα στιγμιότυπο της προβολής χρήστη από το PE ή το VE, ανάλογα με τη διεπαφή που αποφάσισε να χρησιμοποιήσει ο χρήστης (AR vs. VR). Στην περίπτωση του AR, το στιγμιότυπο είναι μια απλή φωτογραφία ή βίντεο που τραβήχτηκε από την κάμερα, με την εικονική πραγματικότητα να περιλαμβάνει το σύνολο των αντικειμένων που βρίσκονται στο frustum της θέασης. Σε αυτό το σημείο, καλείται μια υπηρεσία αναγνώρισης αντικειμένων (που παρέχεται από τη μονάδα ASSYST). Στην περίπτωση του AR, μια τέτοια ενότητα χρησιμοποιεί έναν ή περισσότερους ανιχνευτές αντικειμένων που βασίζονται σε βαθιά μάθηση για την αναγνώριση γνωστών αντικειμένων, μαζί με τις χωρικές τους συντεταγμένες. Αντίθετα, για την εικονική πραγματικότητα, η αναγνώριση συνίσταται στην εξέταση μεταδεδομένων που σχετίζονται με το σύνολο των εξεταζόμενων αντικειμένων. Μόλις αναγνωριστούν τα αντικείμενα στην προβολή χρήστη, η μονάδα ASSYST ανακτά τους σχετικούς σχολιασμούς, εάν υπάρχουν. Εν τω μεταξύ, τα αντικείμενα που αναγνωρίζονται στην προβολή του χρήστη επισημαίνονται για να προτείνουν ποια είναι ενεργά για πιθανές αλληλεπιδράσεις. Τέλος, όταν ο χρήστης αλληλεπιδρά με ένα από αυτά, ένα μενού επικαλύπτεται στη διεπαφή, παρέχοντας τη λίστα με τους υπάρχοντες σχολιασμούς. [53]

4.6 Μέθοδοι και εφαρμογές σε 6G

4.6.1 6G Edge Computing

4.6.1.1 6G Edge as CPS

Τα CPS χαρακτηρίζονται από την απρόσκοπτη συνένωση του φυσικού κόσμου των αντικειμένων υποδομής και του εικονικού κόσμου της επεξεργασίας πληροφοριών. Στο CPS, οι πληροφορίες περιβάλλοντος σχετικά με αντικείμενα υποδομής στο φυσικό χώρο συλλέγονται από αισθητήρες και στη συνέχεια προωθούνται στον κυβερνοχώρο για επεξεργασία. Στη συνέχεια, οι επιχειρησιακές εντολές απελευθερώνονται από τον κυβερνοχώρο και εκτελούνται από ενεργοποιητές για τον έλεγχο αντικειμένων υποδομής. Με βάση τον παραπάνω μηχανισμό λειτουργίας του CPS, είναι λογικό να αξιοποιηθεί το 6g edge computing ή το 6g cloud computing για την ολοκλήρωση της διαδικασίας επεξεργασίας πληροφοριών. Έχοντας κατά νου αυτή την ιδέα, πολυάριθμες ερευνητικές εργασίες έχουν αφιερωθεί στον σχεδιασμό της αρχιτεκτονικής edge computing ή υποβοηθούμενων από cloud edge computing CPS. Για παράδειγμα, ένας ερευνητής σχεδίασε ένα πλαίσιο CPS με υποβοήθηση υπολογιστικού νέφους για τη διάκριση, τον εντοπισμό και την πρόληψη ασθενειών που μεταδίδονται από τα κουνούπια. Στο πλαίσιο, ο φυσικός χώρος είναι υπεύθυνος για την ανίχνευση, τη συλλογή και την εξαγωγή χρήσιμων πληροφοριών σχετικά με τους χρήστες τερματικών. Ο κυβερνοχώρος, που αποτελείται από στρώμα ακμών και στρώμα νέφους, είναι υπεύθυνος για την ανάλυση των δεδομένων που μεταδίδονται από τον φυσικό χώρο. [42]

4.6.1.2 6g Edge as DT

Τα ψηφιακά δίδυμα αντιπροσωπεύουν πραγματικά αντικείμενα ή υποκείμενα με τα δεδομένα, τις λειτουργίες και τις δυνατότητες επικοινωνίας τους στον ψηφιακό χώρο. Για να μειώσουμε τον λανθάνοντα χρόνο και να βελτιώσουμε την αξιοπιστία για εφαρμογές

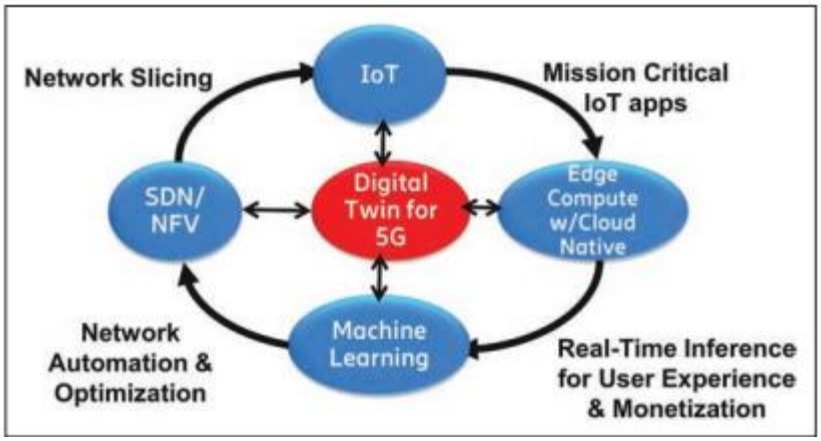
υπολογιστών 6g edge, ενσωματώνουμε ψηφιακά δίδυμα σε ασύρματα δίκτυα και προτείνουμε τα ψηφιακά δίδυμα ασύρματα δίκτυα (**DTWN**). Χαρτογραφώντας συσκευές IoT σε ψηφιακούς δίδυμους σε διακομιστές άκρων, το DTWN βελτιώνει την αποτελεσματικότητα των αλγορίθμων AI και μετριάζει τον αντίκτυπο της αναξιόπιστης επικοινωνίας μεταξύ των χρηστών και των διακομιστών αιχμής. Επιπλέον, το DTWN αλληλεπιδρά με τα φυσικά συστήματα IIoT σε πραγματικό χρόνο μέσω συλλογής δεδομένων και αναλύσεων για να διατηρεί το ψηφιακό επίπεδο συγχρονισμένο με το φυσικό σύστημα. [54]

Έτσι, η ανάλυση κατάστασης λειτουργίας και η βελτιστοποίηση των συσκευών χρήστη μπορούν να πραγματοποιηθούν απευθείας στο DTWN, γεγονός που μειώνει το κόστος του συστήματος. Έχουμε σημειώσει λίγες εργασίες που συζητούν την ενσωμάτωση ψηφιακών διδύμων με φυσικά συστήματα για τη βελτίωση της απόδοσης των κληρονόμων για διαφορετικές εφαρμογές. Για παράδειγμα, κάποιοι συγγραφείς προτείνουν τα πειραματικά ψηφιακά δίδυμα (**EDTs**) που μπορούν να χρησιμοποιηθούν για την υλοποίηση πολύπλοκων αλγορίθμων ελέγχου ή νοητικών μοντέλων. Συγκεκριμένα, οι συγγραφείς κατασκεύασαν ένα γενικό ψηφιακό δίδυμο για σύνθετο εξοπλισμό και πρότειναν μια νέα μέθοδο για τη διαχείριση της υγείας χρησιμοποιώντας ψηφιακά δίδυμα. Σε αυτό το έγγραφο, προτείνουμε την ενσωμάτωση ψηφιακών διδύμων σε δίκτυα αιχμής για να μετριαστεί το χάσμα πόρων μεταξύ των τελικών χρηστών και των Σταθμών Βάσης (BS) για αποτελεσματικό υπολογισμό αιχμής. [54]

Οι κύριες συνεισφορές αυτής της εργασίας συνοψίζονται ως εξής:

- Σχεδιάζεται ένα νέο ψηφιακό δίδυμο μοντέλο ασύρματου δικτύου-DTWN, το οποίο χρησιμοποιεί ψηφιακά δίδυμα για να μετριάσει την αναξιόπιστη και μεγάλη απόσταση επικοινωνίας μεταξύ τελικών χρηστών και διακομιστών αιχμής.
- Ορίζεται το πρόβλημα συσχέτισης άκρων για το DTWN και προτείνεται ένα εξουσιοδοτημένο ομοσπονδιακό πλαίσιο μάθησης με εξουσιοδότηση blockchain για υπολογιστές ακμών στο DTWN.
- Για να βελτιωθεί η αποτελεσματικότητα του προτεινόμενου σχήματος, διαμορφώνεται ένα πρόβλημα βελτιστοποίησης εξετάζοντας από κοινού τη συσχέτιση άκρων και την κατανομή πόρων επικοινωνίας για να ελαχιστοποιηθεί το κόστος χρόνου και αναπτύσσεται ένας αλγόριθμος βασισμένο στην ενίσχυση της εκμάθησης πολλαπλών παραγόντων για την εύρεση της βέλτιστης λύσης στο πρόβλημα. [54]

Η τεχνολογία DT επιτρέπει την εύκολη και οικονομικά αποδοτική πρόσβαση στο 5G με εξαιρετικά ευέλικτες και επαναλαμβανόμενες προσεγγίσεις ανάπτυξης. Επιτρέπει την προληπτική μοντελοποίηση της κυκλοφορίας δεδομένων και των κινδύνων ασφάλειας για σκοπούς δοκιμής/επικύρωσης, οδηγώντας σε λειτουργική και ενεργειακή απόδοση, βοηθώντας στην επιτάχυνση της έρευνας και του χρόνου για την αγορά νέων υπηρεσιών που προκαλούν αναστάτωση. [55]



[55]

Σχήμα 20: Digital Twin για 5G

4.6.2 Εφαρμογές σε Optical Wireless Networks

4.6.2.1 OWN as CPS

Δεν υπάρχουν τέτοιες αντίστοιχες εφαρμογές

4.6.2.2 OWN as DT

Δεν υπάρχουν τέτοιες αντίστοιχες εφαρμογές

5. Εργαλεία και Μέθοδοι DF στα IoT Networks

5.1 Εισαγωγή

Τώρα λοιπόν που έχουμε μια καλύτερη κατανόηση των πολυάριθμων μερών που αποτελούν το digital κομμάτι των συσκευών IoT, μπορούμε να δούμε συγκεκριμένα, καλύτερα και σε μεγαλύτερο βάθος τρόπους μέσω των οποίων μπορεί να πραγματοποιηθεί DF analysis σε κάθε δίκτυο.

5.2 DF in Smart Cities

5.2.1. DF in Drones/UAV's

Βρέθηκαν 2 paper τα οποία αναφέρονται στην DF analysis για τα drones [60], [61]. Το 1ο απο αυτά κάνει μια βιβλιογραφική ανασκόπηση DF αναλύσεων σε drones και προτείνει μια δίκη του μέθοδο χρησιμοποιώντας ML, ενώ το 2ο προτείνει μια νέα μέθοδο DF το CCAFM, το οποίο καλείται να μπορεί να λύσει τα προβλήματα τα οποία παρουσιάζονται συγκεκριμένα για μεθόδους που έχουν να κάνουν με drones.

Ως μέρος της εγκληματολογίας του drone, τα δεδομένα που παράγονται κατά την πτήση, τα οποία καταγράφονται σε αρχεία καταγραφής, μπορούν να υποβληθούν σε επεξεργασία για να αποκαλύψουν διάφορες πτυχές της κίνησης και των λειτουργιών του drone, όπως χρονικές σημάνσεις, διάρκεια πτήσης, ταχύτητα ισχύος, εκτροπή, pitch and roll, υψόμετρο και τύπο drone. Τα δεδομένα πρέπει να είναι ανακτήσιμα για ανάλυση και η κρυπτογράφηση επιβαρύνει αυτή τη δραστηριότητα. Μπορεί να πραγματοποιηθεί οπτικοποίηση της πτήσης με drone για να ενισχυθεί η DF έρευνα εάν τα δεδομένα είναι σε αναγνώσιμη μορφή. [60]

Σε μία έρευνα, το ιατροδικαστικό παράδειγμα του drone διαιρέθηκε στα εξής: ψηφιακή εγκληματολογία και υλικό ή φυσική εγκληματολογία. Επιπλέον, η ψηφιακή εγκληματολογία ταξινομήθηκε ως ο όμιλος διαδικασίας ανάλυσης κυκλοφορίας δικτύου, συμπεριλαμβανομένης της ανάλυσης μηνυμάτων επικοινωνίας από drone προς τον ελεγκτή, ανάλυση αρχείων καταγραφής συστήματος, ανάλυση συστημάτων αρχείων και εγγραφών κάμερας. [60]

Σε μία άλλη έρευνα, οι συγγραφείς προσπάθησαν να μελετήσουν τη δυνατότητα ανάκτησης εικόνας από τη μνήμη ενός drone, την ανακατασκευή της διαδρομής πτήσης και τη σύνδεση ενός κατασχεμένου drone με μια ύποπτη συσκευή διοίκησης και ελέγχου (απατεώνων). Η ανάλυση περιελάμβανε τα ακόλουθα χαρακτηριστικά drone για τους τύπους drone DJI Phantom 3 και 4: μέγιστος χρόνος πτήσης, μέγιστη απόσταση μετάδοσης, συχνότητα λειτουργίας, τύπος σύνδεσης drone-controller, υποστηριζόμενες εφαρμογές για κινητά, ορισμός μνήμης και πληροφορίες πτήσης. Οι συγγραφείς μπόρεσαν να καταλήξουν στο συμπέρασμα ότι το πρότυπο επικοινωνίας που υιοθετήθηκε για την επικοινωνία drone με ελεγκτή εδάφους είναι σημαντικό για τον προσδιορισμό των στοιχείων δεδομένων που μεταφέρονται, γεγονός που μπορεί ουσιαστικά να οδηγήσει στην ανάκτηση αποδεκτών αποδεικτικών στοιχείων από ένα κατασχεμένο drone. [60]

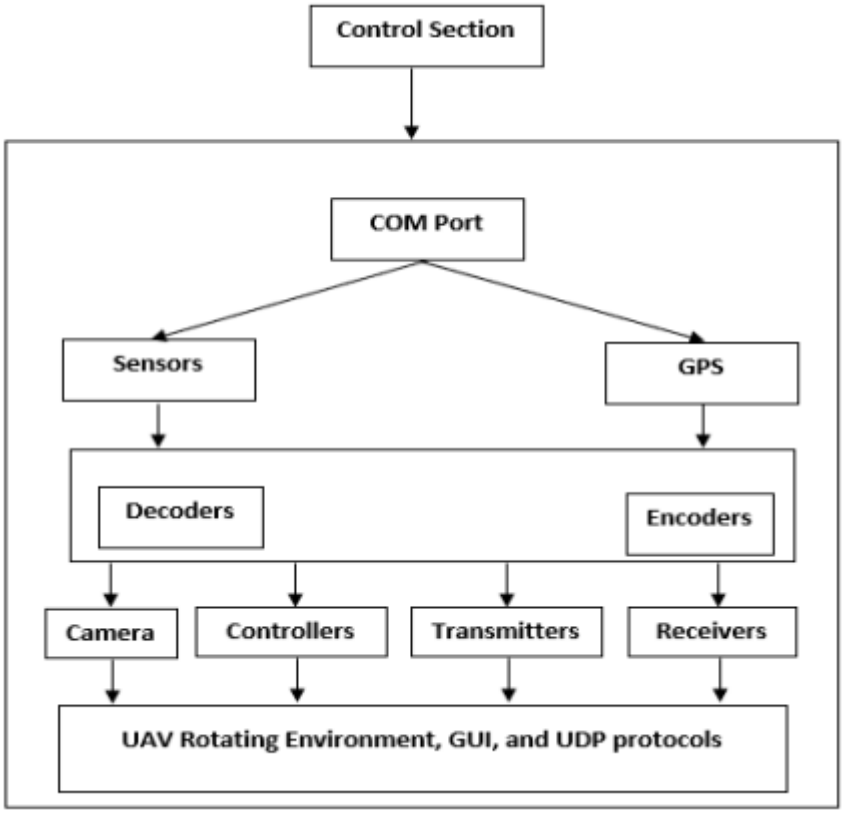
Συνοπτικά, οι υπάρχουσες εργασίες περιλαμβάνουν προτάσεις για την ανάκτηση όλων των δεδομένων των drone με ασφαλή τρόπο, ώστε να αποφευχθεί η παραβίαση στοιχείων. Τα δεδομένα διαφέρουν από το ένα προτεινόμενο πλαίσιο στο άλλο και

εξαρτώνται επίσης από τη διαθεσιμότητα δεδομένων σε διάφορες οικογένειες drone. Με την εμφάνιση των drones της γενιάς 7, ο όγκος των δεδομένων καθώς και η ποικιλομορφία τους θα αυξάνονται μόνο με την πάροδο του χρόνου. [60]

Οι ενισχυμένες προσεγγίσεις παροχής ισχύος που βασίζονται στη μηχανική μάθηση χρησιμοποιούνται για την προστασία των μεταδόσεων UAV από επιθέσεις όπως η υποκλοπή και η εμπλοκή. Η ML μπορεί επίσης να χρησιμοποιηθεί για την ανίχνευση μιας υποκλοπής δημιουργώντας έναν ταξινομητή με βάση τα λαμβανόμενα σήματα που σχετίζονται με επιθέσεις και μη επιθέσεις υποκλοπής. Αυτή η δραστηριότητα βασίζεται σε προηγούμενη εκπαίδευση μοντέλων ML μέσω της παρουσίασης δεδομένων που απεικονίζουν μια επίθεση παρεμβολής ραδιοφωνικού σήματος στον ταξινομητή ML. [60]

Στην ψηφιακή εγκληματολογία, μέσω της ομαδοποίησης κοινών δειγμάτων δεδομένων σε ένα ενιαίο σύμπλεγμα και μέσω της επακόλουθης οπτικοποίησης των συστάδων δεδομένων, μπορούν να παρατηρηθούν κοινά στοιχεία μεταξύ στοιχείων δεδομένων, τα οποία στη συνέχεια μπορούν να επισημανθούν. Μέσω του ορισμού τέτοιων συστάδων για drones και των δεδομένων που δημιουργούνται κατά τη διάρκεια της πτήσης, είναι δυνατό να προβλεφθεί η τροχιά των drones κατά την πτήση και να χαρακτηριστούν είτε ως νόμιμες διαδρομές πτήσης είτε ως παραβιασμένες που συνήθως παρουσιάζονται από αδίστακτα/παραβιασμένα drones. [60]

Στο [61] αναφέρεται ότι τα εγκληματολογικά στοιχεία των συσκευών drone θα μπορούσαν να παρατηρηθούν με τη μορφή δεδομένων που είναι αποθηκευμένα στη μνήμη (πρακτική χρήση εγκληματολογίας μνήμης), δεδομένων ηλεκτρομαγνητικών κυμάτων (EM) και περιεχομένων διαφορετικών αρχείων καταγραφής. Το ESC και το FCB είναι οι πιθανές πηγές στοιχείων μνήμης, τα οποία θα μπορούσαν να αφαιρεθούν απευθείας από τα στοιχεία του ESC και του FCB, αντίστοιχα. Τα εξαρτήματα περιλαμβάνουν δεδομένα ελέγχου πτήσης, δεδομένα καταγραφής πτήσης, πληροφορίες από την εσωτερική μονάδα παρακολούθησης του drone και δεδομένα από τους τοποθετημένους πομποδέκτες και αισθητήρες. Γενικά, οι μεθοδολογίες επεξεργασίας σήματος συμπληρώνουν τη διαδικασία εγκληματολογικής αναγνώρισης και εξαγωγής των δεδομένων. Ωστόσο, τα ψηφιακά στοιχεία, τα οποία εμφανίζονται με τη μορφή σημάτων EM από τους αντίστοιχους πομποδέκτες και τους τοποθετημένους αισθητήρες, μπορούν να καταστήσουν διαθέσιμες περαιτέρω επιβεβαιωτικές πληροφορίες στη διαδικασία έρευνας. Υπό αυτή την έννοια, η TCU θα μπορούσε να αξιοποιηθεί για την εξαγωγή πρωτογενών σημάτων EM, τα οποία θα μπορούσαν να υποβληθούν σε περαιτέρω επεξεργασία για την εξαγωγή των δευτερευόντων επιβεβαιωτικών ψηφιακών στοιχείων. Το σχήμα 21 απεικονίζει την αρχιτεκτονική ενός UAV και τα πρωτόκολλα που υποστηρίζουν τις επικοινωνίες του, τα οποία μπορεί να βοηθήσουν τους ερευνητές να το χρησιμοποιήσουν κατά τη διερεύνηση του drone. [61]



Σχήμα 21: Τι εμπεριέχεται σε μία αρχιτεκτονική UAV

Η υπάρχουσα βιβλιογραφία αποτελείται από διάφορα μοντέλα συλλογής και ανάλυσης που προτείνονται για την εγκληματολογία των drone, μερικά από τα οποία τείνουν προς συγκεκριμένα σενάρια και συστήματα drone. Ως αποτέλεσμα, δεν υπάρχει κατάλληλο και τυποποιημένο μοντέλο συλλογής και ανάλυσης που να βασίζεται σε drone χωρίς κοινά σημεία που να μπορούν να λύσουν μελλοντικά προβλήματα που μπορεί να προκύψουν στην εγκληματολογία των drone. [61]

Για να αντιμετωπιστεί το κενό που αναφέρθηκε παραπάνω, υπάρχει ανάγκη να προσδιοριστεί ένα νέο ολοκληρωμένο εγκληματολογικό μοντέλο συλλογής και ανάλυσης που θα εστιάζει στη συλλογή και την ανάλυση ως ένα βήμα προς την επίλυση του πλεονασμού. Αντίστοιχα, η παρούσα εργασία [61] προτείνει ένα νέο ολοκληρωμένο εγκληματολογικό μοντέλο συλλογής και ανάλυσης (**CCAFM**) που εφαρμόζεται στον τομέα της εγκληματολογίας των drone. Σε σύγκριση με τα υπάρχοντα μοντέλα, το CCAFM ενσωματώνει όχι μόνο την ανακατασκευή, την ανάλυση και τη συλλογή αλλά και τις διαδικασίες διερεύνησης μετά το περιστατικό. [61]

5.2.2. DF in Smart Vehicles/Vanet’s

Πρόσφατα, οι αγωγές εξαρτώνται όλο και περισσότερο από τα δεδομένα αισθητήρων και συμβάντων που καταγράφονται στην ηλεκτρονική μονάδα ελέγχου των οχημάτων και στην υποδομή δεδομένων έξυπνης πόλης. Αυτά τα δεδομένα αισθητήρων περιλαμβάνουν αρχεία ταχύτητας, δεδομένα αερόσακου και αισθητήρα φώτων φρένων και άλλα δεδομένα συμβάντων που μπορούν να βοηθήσουν τον Reconstructionist ατυχήματος να επιβεβαιώσει και να ταξινομήσει φυσικά στοιχεία και στοιχεία κυβερνοεπίθεσης, αποκαλύπτοντας έτσι την πραγματική αιτία ενός συμβάντος. Δεδομένου ότι αυτά τα ψηφιακά δεδομένα ενδέχεται να καταλήξουν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία στο δικαστήριο, θα πρέπει να είναι

ιατροδικαστικά. Ωστόσο, οι πρακτικές που χρησιμοποιούνται κυρίως για την εξαγωγή αυτών των πληροφοριών είναι αντιεπαγγελματικές σε σύγκριση με άλλους τομείς της ψηφιακής εγκληματολογίας και ως εκ τούτου απαιτούν μεγάλη προσοχή από την πλευρά των ερευνητών για τη σωστή διατήρηση και παρουσίαση αποδεικτικών στοιχείων. [63]

Άλλοι ερευνητές εξέτασαν την ασφάλεια της εγκληματολογικής διαδικασίας και της συλλογής δεδομένων σε συστήματα αυτοκινήτων, ρωτώντας την ασφάλεια των πρωτοκόλλων που εμπλέκονται στην επικοινωνία δεδομένων οχημάτων και έξυπνων υποδομών μεταφορών. Προτείνεται ένας μηχανισμός για τη συλλογή και αποθήκευση εγκληματολογικών δεδομένων σε συστήματα αυτοκινήτων, ο οποίος είναι αξιόπιστος, ασφαλής και αποτελεσματικός και θα διατηρεί το απόρρητο των δεδομένων του ιδιοκτήτη του αυτοκινήτου. Το έκαναν αυτό ενσωματώνοντας μια διαγνωστική εφαρμογή smartphone που ονομάζεται **DiaLOG**. που συλλέγει εγκληματολογικά δεδομένα από το αυτοκίνητο και τα στέλνει σε ασφαλή αποθήκευση cloud χρησιμοποιώντας ένα ασφαλές πρωτόκολλο. Είναι ένας μη επεμβατικός τύπος εγκληματολογίας οχημάτων. Ανέλυσαν την απόδοση του προτεινόμενου πρωτοκόλλου χρησιμοποιώντας κάποιο εργαλείο ανάλυσης: **Scyther** και **Casper FDR**, και τα αποτελέσματά τους δεν δείχνουν επιτυχή επίθεση. Ωστόσο, το πρωτόκολλό τους δείχνει ότι σχεδιάστηκε μόνο για την επικοινωνία που πραγματοποιείται μεταξύ της ECU των οχημάτων και της κινητής συσκευής που θα λειτουργεί ως προσωρινή αποθήκευση για τα εγκληματολογικά δεδομένα. Δεν προτείνεται καμία μορφή κρυπτογράφησης ή κατακερματισμού στη διαδικασία επικοινωνίας μεταξύ της εφαρμογής για κινητά και της ασφαλούς αποθήκευσης cloud, καθώς τα δεδομένα μπορούν να υποκλαπούν κατά τη μεταφορά δεδομένων σε ένα μοντέλο επίθεσης από άνθρωπο στη μέση. Ως εκ τούτου, υπονομεύει την ασφάλεια του πρωτοκόλλου για αποθήκευση cloud. Επίσης, έννοιες όπως το ασφαλές νέφος ή η αποθήκευση απομακρυσμένου διακομιστή αναφέρθηκαν μόνο χωρίς μορφή υλοποίησης. Επιπλέον, εάν ένας εισβολέας αποκτήσει πρόσβαση στα δεδομένα στο cloud, ποια είναι τα μέτρα που θα λάβει ο μηχανισμός για να προστατεύσει την ακεραιότητα και την εμπιστευτικότητα των δεδομένων; [63]

Προβλήματα DF σε IoT [63]:

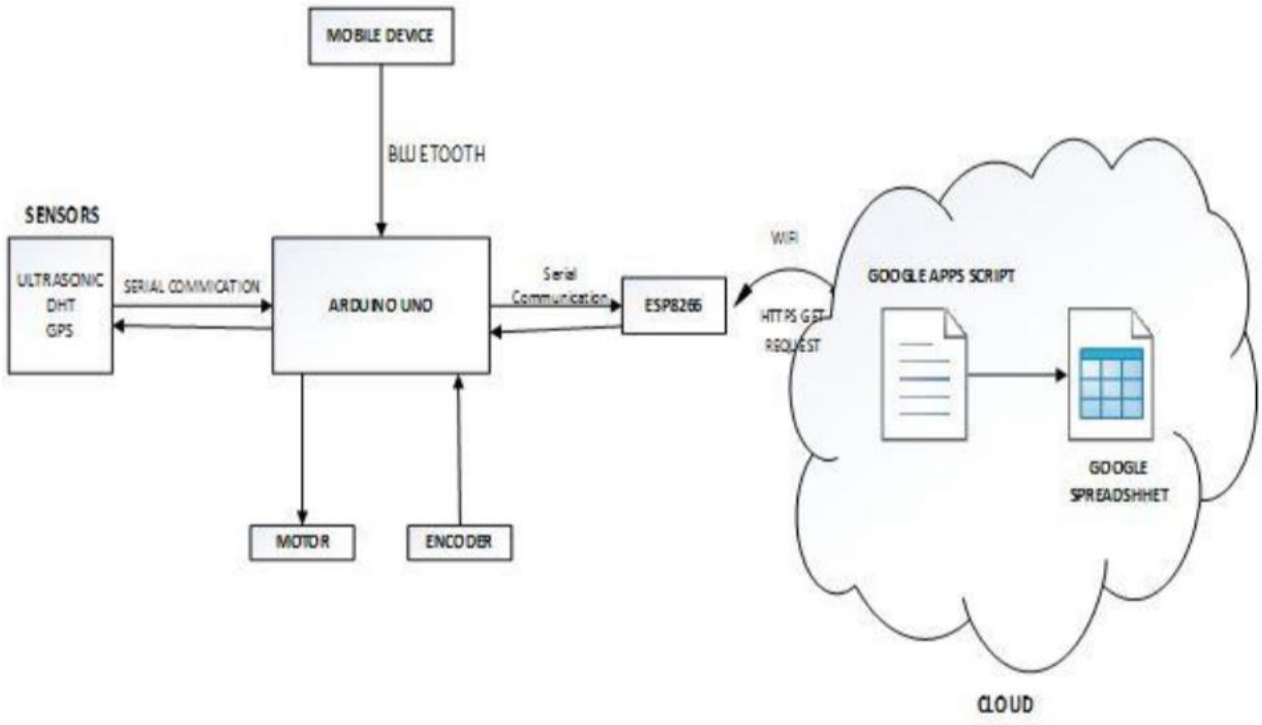
- Storage of Forensic Data
- Issues with the Existing Model of IoT and Forensic Data Storage
    - Το τρέχον σύστημα αισθητήρα νέφους και αποθήκευσης εγκληματολογικών δεδομένων είναι ένα σύστημα που χρησιμοποιεί κλειδιά διεπαφής προγραμματισμού εφαρμογών (κλειδιά API). Τα κλειδιά API χρησιμοποιούνται για δύο σκοπούς: Πρώτον, για την αναγνώριση της εφαρμογής που καλεί ένα API και, δεύτερον, για την επαλήθευση ότι η εφαρμογή που ζητά το API έχει λάβει πρόσβαση για να το κάνει και επομένως είναι ενεργοποιημένη. Παραδείγματα τέτοιων πλατφορμών αποθήκευσης περιλαμβάνουν το **Pushingbox**, το **Xively** και το **Thingspeak**. Τα κλειδιά API είναι κυρίως χρήσιμα κατά τον έλεγχο του αριθμού των κλήσεων που γίνονται σε ένα API, το φιλτράρισμα αρχείων καταγραφής και τον εντοπισμό μοτίβων χρήσης στην επισκεψιμότητα API. Αλλά δεν μπορεί να χρησιμοποιηθεί για ασφαλή εξουσιοδότηση, αναγνώριση μεμονωμένων χρηστών και ταυτοποίηση των δημιουργών ενός έργου με αποτέλεσμα ελαττώματα ασφαλείας με τα τελικά σημεία του. Η εφαρμογή του σε υποδομές αποθήκευσης δεδομένων έξυπνης πόλης AV θα θέσει σε κίνδυνο αυτά τα οχήματα, καθώς μια γέφυρα ασφαλείας με ένα συνδεδεμένο αυτοκίνητο

μπορεί να οδηγήσει σε μια γέφυρα όλων των συνδεδεμένων οχημάτων που χρησιμοποιούν το ίδιο σύστημα.

- Security requirement for secure storage of forensic sensor data
    - Integrity
    - Authenticity
    - Availability
    - Reliability
    - Privacy

Μια πιθανή λύση που προτείνουν απο το [63] είναι:

Τα AV έχουν πρόσβαση στο Διαδίκτυο και συνδεσιμότητα για να υποστηρίζουν την επικοινωνία τους με υποδομές έξυπνων πόλεων και άλλα συνδεδεμένα οχήματα. Αυτό θα επιτρέψει την επικοινωνία και την αποθήκευση των εγκληματολογικών δεδομένων στο cloud (υποδομή έξυπνης πόλης). Η στρατηγική πίσω από τον προτεινόμενο μηχανισμό είναι η καταγραφή των δεδομένων αισθητήρων που δημιουργούνται από ένα AV στο cloud (υποδομή έξυπνης πόλης) μέσω μιας ασφαλούς σύνδεσης δικτύου TLS που χρησιμοποιεί ένα προ-κοινόχρηστο κλειδί για έλεγχο ταυτότητας και κρυπτογράφηση τόσο του πελάτη όσο και του διακομιστή. Η εφαρμογή σεναρίου Google στη μονάδα δίσκου Google είναι ο διακομιστής μας, ενώ το ESP8266 (μονάδα WIFI) που είναι συνδεδεμένο σε ένα Arduino IDE, το οποίο είναι η μονάδα ελέγχου του AV είναι ο πελάτης. Ο μηχανισμός έχει επίσης σχεδιαστεί για να καταγράφει και να κατακερματίζει την κίνηση του δικτύου για να δημιουργήσει μια τεχνική επαλήθευσης για μελλοντική χρήση. Τα δεδομένα που λαμβάνονται μπορούν στη συνέχεια να αναλυθούν και να ταξινομηθούν για ιατροδικαστικούς σκοπούς και για την αποκατάσταση ατυχημάτων. [63]



Σχήμα 22: Η αρχιτεκτονική του συστήματος

Στη συνέχεια αναλύουν με ποια συγκεκριμένα πρωτόκολλα και ποια διαδικασία αυτό μπορεί να εφαρμοστεί επακριβώς

5.2.3. DF in Satellite IoT

Δεν υπάρχουν πολλές μελέτες στην βιβλιογραφία. Μια απο αυτές η [5] αναφέρεται σε ένα πρωτόκολλο που έχουν αναπτύξει για εφαρμογές healthcare που μεταφέρονται μέσω ειδικών δορυφόρων το SmartSat-IIoHT testbed, οι ερευνητές αναλύουν πως θα μπορούσαν να αποφύγουν επιθέσεις Mittre και αναλύουν επακριβώς τη δομή των headlights των πακέτων του πρωτοκόλλου αυτού. Σημειώνουμε μονάχα ότι ολη η δουλειά αυτή μπορεί να γίνει μόνο μέσω των DT counterparts των δορυφόρων.

5.3 DF in Smart Buildings/Facilities

5.3.1. DF in Smart Homes/Office

Υπάρχουν διάσπαρτες απόψεις στη βιβλιογραφία και ήταν δύσκολο να βρούμε συγκεκριμένα κάτι που να μην αναφέρεται σε κάτι συγκεκριμένο ακριβώς λόγω των πολλών CPS που μπορούν να απαρτίζουν ένα smart home ή ένα smart office

Σε μια έρευνα [57] οι ερευνητές παρουσιάζουν σύντομα τις προκλήσεις που έχουν τα smart home forensics:

- The need for standardization
- The need for security-by-design
- The need for forensic-by-design
- The need for forensically sound tools in HAS forensics
- Other factors
    - Οι έξυπνες συσκευές έχουν συνήθως λειτουργίες καταγραφής, οι οποίες μπορεί να περιέχουν χρήσιμες πληροφορίες. Καθώς υπάρχουν τόσες πολλές διαφορετικές τεχνολογίες, προμηθευτές και ενοποιητές συστημάτων, το ερώτημα θα είναι ποια συμβάντα καταγράφονται, σε ποια αρχεία και σε ποια μορφή (βάσης δεδομένων); Κατά τη διάρκεια μιας εγκληματολογικής έρευνας, οι εγκληματολόγοι της βάσης δεδομένων θα πρέπει να είναι σε θέση να παρέχουν ορισμένες διευκρινίσεις.

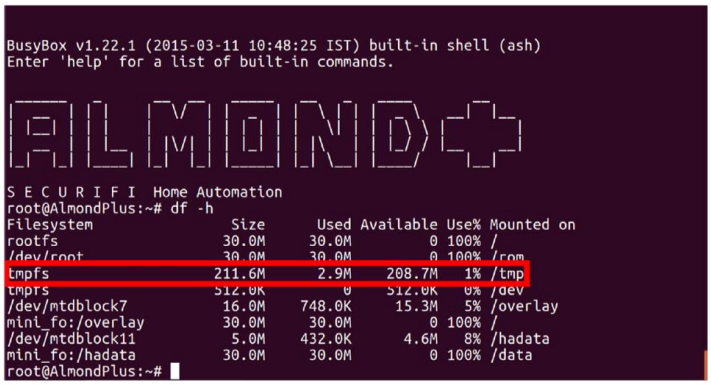
Ενώ στη συνέχεια προτείνουν ένα framework (το οποίο το ονομάζουν HAS forensic framework) με τις ακόλουθες ιδιότητες:

- Phase1:Preparationoff-site
- Phase2:Searchforahomeautomationsystemon-site
- Phase 3: Preserve the HAS “as is”, wherever possible.
- Phase 4: Understanding the specific home automation system
- Phase5:Checksecuritylevel
- Phase6:Locateandacquireevidentialdata
- Phase 7: Process/analyse seized data

Και παρουσιάζουν 2 test cases στα οποία εφαρμόζουν τη παραπάνω διαδικασία

Σε ένα άλλο paper [44] αναφέρεται το Almond+ το οποίο κρατάει αρχεία στο cloud και μέσω terminal για όλες τις smart συσκευές και μπορεί μέσω αυτού να παρατηρηθεί και να χρησιμοποιηθεί το DF analysis. Παρατίθενται μόνο η εικόνα του Almond+ όπου μπορεί να φανεί ότι ανάλυση γίνεται μέσω cloud, terminal και κινητής συσκευής για τον ιδιοκτήτη real time, αλλα και καταγραφή των στοιχείων των συσκευών:

Fig. 2. Top Almond+ touchscreen, Right - companion app, Bottom–Cloud interface.



Σχήμα 23: Το σύστημα ALMOND+

Σε ένα άλλο paper [43] οι ερευνητές κάνουν ανάλυση στο Amazon Alexa και στο google home και επεξηγούνται κάποια πράγματα για αυτές και μόνο τις έτοιμες συσκευές σε περίπτωση που κάποιο smartphone τις εμπεριέχει

Ενώ τέλος στο [17] οι ερευνητές κάνουν ανάλυση σε ακόμα περισσότερες συσκευές και μέσα όπως :

- Streaming Media Player Analysis
- Smart Watch Analysis

- Smart Hub Analysis
- Smart Doorbell and Smart Lock Analysis
- Network Security Application analysis
- Smart Plug Analysis
- Smart Camera Analysis
- Smart Bulb Analysis

Ενώ αναφέρουν και πιθανά threats τα οποία μπορούν να προκύψουν με βάση αυτές τις συσκευές

5.3.2. DF in Industrial IIoT and Smart Factories

Table 2
Existing Security Standards for Industrial Processes/Systems and Automation of Devices.

Reference	Standard	Focus	Security risks	Threat/ Vulnerability	Infosec	Digital forensics	Cybersecurity
[29]	ISA/IEC 62443	Security for control system components	✓	✓	X	X	✓
[29]	ISA/IEC 62443–4–2	Security for Industrial Automation	✓	✓	✓	X	✓
[29]	ISA/IEC 62443–3–3	System Security Requirements	✓	✓	✓	X	✓
[29]	ISA/IEC 62443–4–1	Product Security Development	X	X	X	X	✓
[29]	ISA/IEC 62443–3–2	Security Risk Assessment	✓	✓	✓	X	✓
[30]	NIST-IIoT	Security for IIoT	✓	✓	✓	X	✓
[10]	ISO/IEC 27043	Incident Investigation Principles	✓	X	✓	✓	✓
[31]	NIST-SP800–82	Industrial control system security	✓	X	✓	X	✓
[29]	ISA/IEC 62443–4–2	Technical requirements for IACS components	✓	X	✓	X	✓
[29]	IEC 62351–4	Security for any profiles including MMS - Authentication for MMS - TLS for TCP/IP	X	✓	✓	X	✓
[29]	IEC 62351–5	TLS for TCP/IP profiles and encryption for serial profiles	X	✓	✓	X	✓
[29]	IEC 62351–7	Security through network and system management	✓	✓	✓	X	✓
[29]	IEC62351–8	Role Based Authentication Control	✓	✓	✓	X	✓

Σχήμα 24: Υπάρχουσα security standards για Industrial Processes/Systems

Στο paper [58] αναφέρονται διαφορα standards μέσω των οποίων μπορεί να γίνει πρόβλεψη επίθεσης, επίβλεψη και ασφάλεια δικτύου, αλλα αναφέρεται από τους ερευνητές ότι και τα ιδια τα standards δεν αναφέρουν κάτι συγκεκριμένο. Ο παραπάνω συγκεντρωτικός πίνακας αναφέρει αρκετά από αυτά μαζί με το σε ποιες περιοχές αναφέρεται.

Στο άρθρο [12] απο την άλλη αναφέρεται μια καινούργια μέθοδος, η οποία κάνει ανασκόπηση στα higher layer Forensic Layer των συσκευών (Network-layer, bit-layer, user-layer) καθώς και στα lower-layer physical, ώστε να σχηματιστεί μια πιο καθολική μέθοδος που στηρίζεται σε όλα τα Forensic Layer όπως αυτά φαίνονται και απο το κεφάλαιο 3. Αν και το άρθρο αναφέρεται συγκεκριμένα στα IIoT, η μέθοδος αυτή θα μπορούσε να επεκταθεί και σε αλλα IoT δίκτυα.

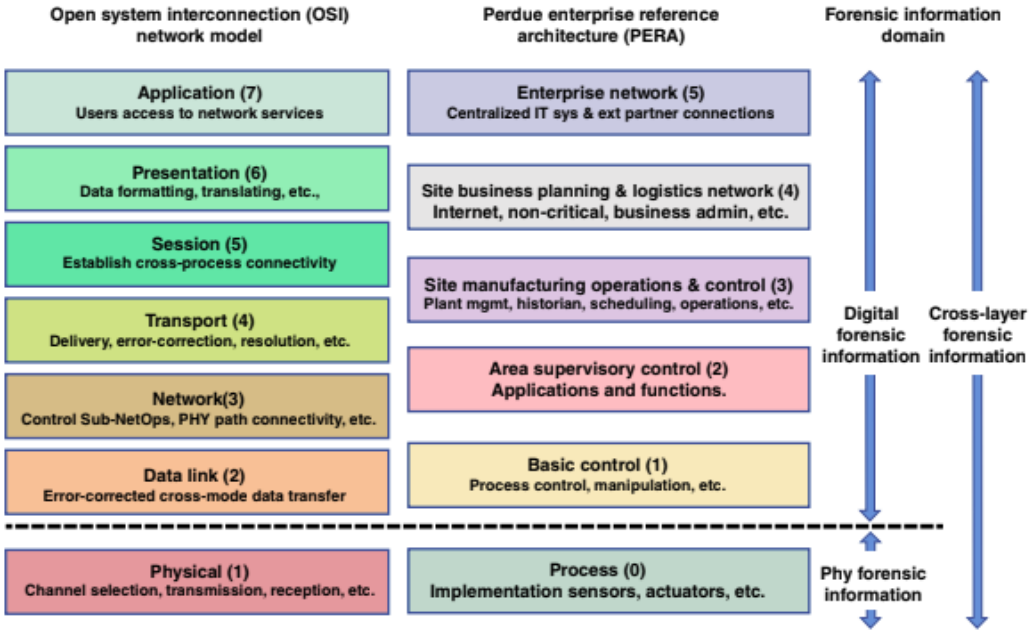
5.3.2.1 IIoT forensic information domains

Η δημιουργία συμφραζομένων των τομέων εγκληματικών πληροφοριών IIoT (ή οποιουδήποτε άλλου τομέα για αυτό το θέμα) απαιτεί την εξέταση συγκεκριμένων λεπτομερειών εφαρμογής και λειτουργίας εντός του στοχευμένου χώρου εφαρμογής. Αυτό περιλαμβάνει την εξέταση του πρωτοκόλλου δικτύου (κανόνες επικοινωνίας, δομή, κ.λπ.) που εξετάζεται.

Το Σχήμα 25 δείχνει τον διαχωρισμό των εγκληματολογικών πληροφοριών στον κυβερνοχώρο με βάση [12]

- στοιχεία που συλλέγονται και αναλύονται σε υψηλότερα επίπεδα (Digital Forensic Information) [12]
- στοιχεία που συλλέγονται και αναλύονται στο χαμηλότερο φυσικό επίπεδο (PHY) [12]

Όπως περιγράφεται λεπτομερώς στις επόμενες ενότητες, αυτός ο λειτουργικός διαχωρισμός εισάγεται για να διαφοροποιηθεί μεταξύ της εγκληματολογικής εκμετάλλευσης του higher-layer digital και του lowest-layer PHY (στο επίπεδο κυματομορφής). [12]



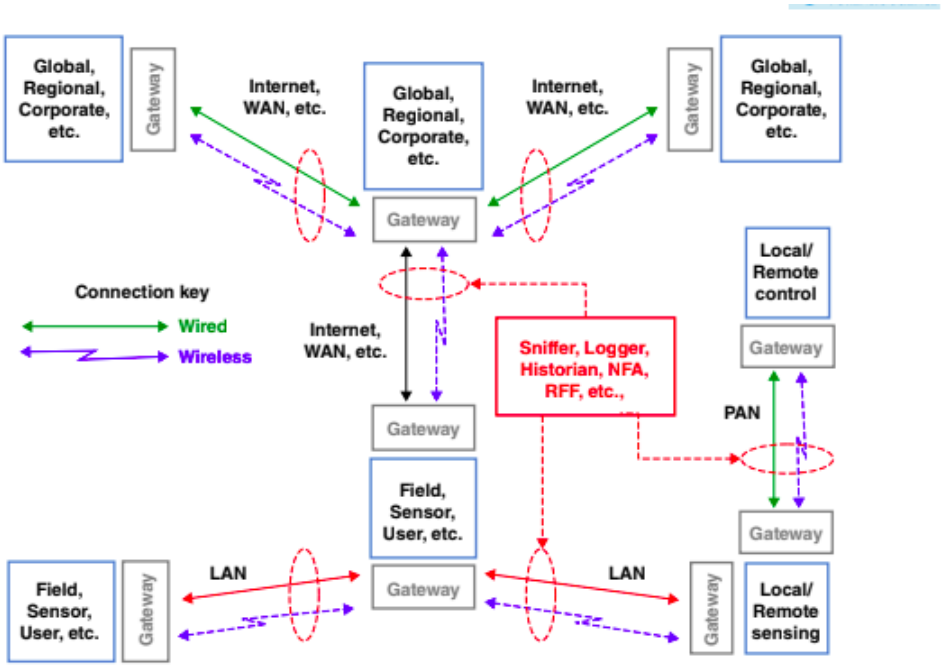
Σχήμα 25: Σχέση μεταξύ της αρχιτεκτονική 7 επιπέδων OSI και της αρχιτεκτονικής 6 επιπέδων PERA

Το σχήμα 26 δείχνει μια γενική αρχιτεκτονική δικτύου IIoT που αποτελείται από διαφορετικούς τύπους ενσύρματων και ασύρματων συνδέσεων επικοινωνίας που μπορούν να χρησιμοποιηθούν ή και όχι σε όλες τις εφαρμογές του IIoT, με όλη την υποδεικνυόμενη διασυνδεσιμότητα. Συλλογικά, τοποθεσίες εντός της επιχείρησης, του εργοστασίου, του πεδίου, του οχήματος κ.λπ., όπου μπορούν να αποθηκευτούν ψηφιακά δεδομένα και η απαιτούμενη επικοινωνιακή διασυνδεσιμότητα, παρέχουν την ευκαιρία για εκμετάλλευση ψηφιακών εγκληματολογικών πληροφοριών υψηλότερου επιπέδου (higher-layer) και χαμηλότερου επιπέδου (physical). Υπάρχει [12]:

(α) υπερπληθώρα άμεσα σχετικών εργασιών για την εκμετάλλευση Ψηφιακών Εγκληματολογικών Πληροφοριών Υψηλών Επιπέδων για προστασία σε επίπεδο δικτύου σε πραγματικό χρόνο, ανίχνευση/άμυνα κυβερνοεπιθέσεων και εγκληματολογική ανάλυση μετά την επίθεση—αυτός ο πλούτος πληροφοριών είναι αποτέλεσμα της ιστορικής έμφασης στην RDD (Resilient Distributed Dataset) στο IT τομέα, [12]

(β) ένας σημαντικός όγκος πληροφοριών που σχετίζονται με την εγκληματολογική ανάλυση χαμηλότερου επιπέδου (physical), ειδικά στον τομέα των δακτυλικών αποτυπωμάτων με ραδιοσυχνότητες (RFF - radio frequency fingerprinting) [12]

(γ) επαρκείς πληροφορίες για να παρακινήσουν την εξέταση των Διασταυρωμένων (cross-layer) Εγκληματολογικών Πληροφοριών σύμφωνα με τις οποίες η υψηλότερου επιπέδου (higher-layer) και η χαμηλότερου επιπέδου (physical) θεωρείται από κοινού ότι υποστηρίζουν την ανάπτυξη μιας επιβεβαιωμένης εγκληματολογικής έρευνας. [12]



Σχήμα 26: Γενική IIoT αρχιτεκτονική δικτύου που αποτελείται από ίντερνετ, WAN, LAN, PAN, RF, wireless διασύνδεση και παρέχει πρόσβαση σε bit-level data/packet sniffing, logging, historian, network forensic analysis και RFF διαδικασίες

5.3.2.1.1. Higher-layer digital forensic information

Οι ψηφιακές εγκληματολογικές πληροφορίες υψηλότερου επιπέδου μπορούν να θεωρηθούν ως ιεραρχία που περιλαμβάνει τρία γενικά επίπεδα, συμπεριλαμβανομένων τεχνικών εγκληματολογικών τεχνικών σε επίπεδο bit (bit-level forensic analysis), σε επίπεδο δικτύου (network-layer forensic analysis) και σε επίπεδο χρήστη (user-layer forensic analysis)- τα διαχωριστικά όρια μεταξύ αυτών των επιπέδων είναι κάπως αυθαίρετα και μπορεί να είναι ασαφή σε ορισμένες εφαρμογές [12].

Η παρακάτω ανασκόπηση τεχνικών ψηφιακής εγκληματολογίας υψηλότερου επιπέδου εξετάζει καθένα από αυτά τα επίπεδα ανεξάρτητα. Ωστόσο, θα πρέπει να σημειωθεί ότι οι τεχνικές που εφαρμόζονται σε ένα επίπεδο συχνά, αν όχι πάντα, έχουν εφαρμογή σε άλλα επίπεδα ή μπορούν να χρησιμοποιηθούν για να επιβεβαιώσουν ευρήματα σε χαμηλότερα επίπεδα. Η εγκληματολογική ανάλυση IIoT χρησιμοποιεί παρόμοιες εγκληματολογικές τεχνικές με άλλες εφαρμογές, επομένως πολλές έρευνες εφαρμογών που δεν είναι συγκεκριμένες για το IIoT περιλαμβάνονται εδώ. Γενικά, υπάρχει έλλειψη εργαλείων και μεθοδολογιών που έχουν σχεδιαστεί ειδικά για να ενσωματώνουν συστήματα SCADA, συμπεριλαμβανομένων των πρωτοκόλλων και των ιδιόκτητων μορφών καταγραφής. Επομένως, η κύρια διαφορά μεταξύ της γενικής ψηφιακής εγκληματολογίας ανώτερου επιπέδου και αυτών που ισχύουν ειδικά για το IIoT δεν έγκειται απαραίτητα στην ίδια την υλοποίηση της τεχνικής, αλλά μάλλον στο ότι απαιτείται ειδική τεχνογνωσία σε επίπεδο συστήματος για τον εντοπισμό και τη συλλογή χρήσιμων δεδομένων. [12]

5.3.2.1.2. Bit-level forensic analysis

Η συλλογή και η ανάλυση των πληροφοριών σε επίπεδο bit εξετάζονται εδώ ως διαφορετική από την ανίχνευση εισβολής δικτύου (Network Intrusion Detection - NID) και την εγκληματολογική ανάλυση δικτύου (Network Forensic Analysis - NFA) που συζητούνται στην επόμενη ενότητα, επειδή πολλές τεχνικές που αναπτύχθηκαν για αυτό το επίπεδο μπορούν να χρησιμοποιηθούν ή να επεκταθούν στο δίκτυο-επίπεδο. Επιπλέον, πληροφορίες σε επίπεδο bit που συλλέγονται από τον προγραμματιζόμενο λογικό ελεγκτή (Programmable Logic Controller - PLC), την απομακρυσμένη τερματική μονάδα (Remote Terminal Unit - RTU), τον αισθητήρα πεδίου, την πύλη επικοινωνίας κ.λπ., μπορούν να χρησιμοποιηθούν για να βοηθήσουν στην ανάλυση μετά την επίθεση παρέχοντας την πιο ακριβή άποψη για τον τρόπο με τον οποίο αποθηκεύονται πραγματικά οι πληροφορίες και βοηθώντας στον προσδιορισμό της αυθεντικότητας της συσκευής. [12]

Οι τεχνικές ταξινόμησης σε επίπεδο bit μπορούν να βοηθήσουν στην αντιμετώπιση πιθανών ελλείψεων σε αυτόνομες ιατροδικαστικές τεχνικές σε επίπεδο δικτύου, όπως η χρήση τέτοιων τεχνικών απουσία σχολίων (πολύ συνηθισμένο σε κακόβουλο κώδικα). Άλλοι τύποι συλλεγόμενων αποδεικτικών στοιχείων μπορούν να τεκμηριωθούν μέσω τεχνικών σε επίπεδο bit, για παράδειγμα, παθητική ψηφιακή εγκληματολογία, βίντεο με χρήση εξαγωγής χαρακτηριστικών βάση pixel για τον εντοπισμό χωροχρονικών πλαστών ή επιθέσεων αντιγραφής. Ο συνδυασμός των αποτελεσμάτων μεμονωμένων τεχνικών από διάφορα συστήματα σε επίπεδο εγκατάστασης και η σύνδεσή τους με εγκληματολογικές πληροφορίες επιπέδου bit που συλλέγονται από συσκευές IIoT δημιουργεί μια ουσιαστική αφήγηση μετά την επίθεση. Ωστόσο, η συλλογή τέτοιων δεδομένων εξαρτάται από τα δεδομένα που αποθηκεύονται αρκετό καιρό μετά από μια επίθεση, ώστε οι ερευνητές να έχουν πρόσβαση όταν χρειάζεται. [12]

Ο όγκος των δεδομένων που συλλέγονται σε επίπεδα higher bit-level analysis συνεχίζει να αυξάνεται σε ένα σημείο όπου οι τεχνικές που χρησιμοποιήθηκαν προηγουμένως χρειάζονται αύξηση προκειμένου να παραχθεί μια έγκαιρη συνεισφορά σε μια εγκληματολογική έρευνα. Για το σκοπό αυτό, η μηχανική μάθηση, η εξόρυξη δεδομένων και η βαθιά εκμάθηση υπόσχονται τη βελτίωση της αποτελεσματικότητας του χειρισμού μεγάλων ποσοτήτων δεδομένων. Ωστόσο, καθώς αναπτύσσονται πρόσθετες τεχνικές όπως αυτές, η χρήση τους πρέπει να λαμβάνεται υπόψη σε σχέση με το παραδεκτό και την επαναληψιμότητα των εγκληματολογικών αποδεικτικών στοιχείων που παρέχονται από αυτές τις μεθόδους. [12]

Ένα άλλο ζήτημα για την εγκληματολογική ανάλυση σε επίπεδο bit είναι ο καθορισμός του εάν οι ερευνητές έχουν άμεση πρόσβαση στα στοιχεία υλικού ή όχι. Για παράδειγμα, έχει γίνει σημαντικός όγκος εργασιών σχετικά με την εγκληματολογία κινητών συσκευών, όπου οι ερευνητές διαθέτουν υλικό στο χέρι και μπορούν να έχουν πρόσβαση στα περιεχόμενα [12]

- συσκευών αποθήκευσης εσωτερικής μνήμης και/ή [12]
- αφαιρούμενων συσκευών αποθήκευσης που περιέχουν χρήστη και πάροχο υπηρεσιών λεπτομέρειες. [12]

5.3.2.1.3. Network-level forensic analysis

Οι τεχνικές σε επίπεδο bit στην προηγούμενη ενότητα μπορούν να επεκταθούν για να εφαρμοστούν σε εγκληματολογική ανάλυση σε επίπεδο δικτύου, όπου η φύση της επίθεσης και η απόδοση επίθεσης αρχίζουν να λαμβάνουν χώρα. Όπως φαίνεται στα

Σχήματα 25 και 26, οι εγκληματολογικές εφαρμογές σε επίπεδο δικτύου IIoT (PERA Layer 1 και υψηλότερο) μπορούν να χρησιμοποιήσουν ορισμένες τεχνικές σε επίπεδο δικτύου άλλων εφαρμογών επικοινωνίας (OSI Layer 2 και υψηλότερο). Ο τύπος των τεχνικών που μπορεί να ληφθούν υπόψη για τη μετάβαση μεταξύ εγκληματολογίας σε επίπεδο bit και σε επίπεδο δικτύου περιλαμβάνει γενικά ανάλυση αρχείων δεδομένων, αντιγραφή εικόνας δίσκου, ασφάλεια συστήματος καταγραφής, ασφάλεια μεταφοράς, ασφάλεια δεδομένων, ανάκτηση δεδομένων , ανάλυση συστήματος αρχείων, σύλληψη και ανάλυση κίνησης δικτύου, έρευνα δικτύου και ανίχνευση IP. [12]

Δεδομένης της φύσης των δεδομένων επιπέδου δικτύου, και ειδικά όταν εξετάζουμε συσκευές IIoT, υπάρχει μια υποτιθέμενη μεταβλητότητα και δυναμική φύση των δεδομένων και της αποθήκευσης της κίνησης δικτύου που μπορεί να μην υπάρχει σε άλλα επίπεδα. Κάποια έργα, περιγράφουν συλλογικά δύο ταξινομήσεις κυκλοφορίας δικτύου, συμπεριλαμβανομένων [12]

- **Catch-it-as-you-can** [12]
- **stop-look-and- listen** [12]

Στα συστήματα «catch-it-as-you-can» όλα τα πακέτα περνούν από ένα σημείο κυκλοφορίας και συλλαμβάνονται. Αυτό απαιτεί μεγάλο όγκο αποθήκευσης δεδομένων και η ανάλυση πραγματοποιείται μετά τη συλλογή δεδομένων, με τις απαιτήσεις χωρητικότητας αποθήκευσης να αυξάνονται για το Cloud computing ως μέρος του εταιρικού συστήματος. Στα συστήματα «stop-look-and-listen» οι επιλεγμένες πληροφορίες αποθηκεύονται για μελλοντική ανάλυση μετά από ένα συμβάν ενεργοποίησης. [12]

Υπάρχουν εργαλεία εγκληματολογικής ανάλυσης δικτύου (Network Forensic Analysis Tools - NFAT) που καταγράφουν την κυκλοφορία του δικτύου, αναλύουν την κίνηση και επιτρέπουν στους διαχειριστές να αναγνωρίζουν, να αναπαράγουν και να απομονώνουν την ανώμαλη δραστηριότητα δικτύου. Τα NFAT διευκολύνουν την οργάνωση των πακέτων κίνησης δικτύου που έχουν συλληφθεί ώστε να θεωρούνται ως συνδέσεις επιπέδου μεταφοράς μεταξύ μηχανών. Όλα τα NFAT παρουσιάζουν τρεις βασικές ιδιότητες: [12]

- συλλογή δεδομένων [12]
- διατήρηση δεδομένων χωρίς αλλοίωση [12]
- επανάληψη δεδομένων [12]

Οι ειδικές τεχνικές που σχετίζονται με την εγκληματολογία δικτύου συνδέονται στενά με τα εργαλεία που χρησιμοποιούνται στη διαδικασία. Δεν επιδιώκουμε να καταλογοποιήσουμε ή να ερευνήσουμε όλα τα διαθέσιμα εργαλεία, δεδομένου ότι τα περιεχόμενα μιας τέτοιας λίστας αλλάζουν δυναμικά. [12]

Οι εγκληματολογικές τεχνικές σε επίπεδο bit και σε επίπεδο δικτύου που συζητήθηκαν μέχρι τώρα και αναφέρονται εδώ αποτελούν μέρος μιας συνολικής στρατηγικής έρευνας που επιδιώκει να περιγράψει εμπειρικά την κυβερνοεπίθεση και να την αποδώσει σωστά στον/στους δράστη/ους. Ωστόσο, τα στοιχεία που συλλέγονται από τις τεχνικές σε επίπεδο bit και σε επίπεδο δικτύου μπορεί να μην είναι επαρκή από μόνα τους όταν εξετάζονται μεμονωμένα. Λαμβάνοντας υπόψη τα οφέλη της επιβεβαίωσης με άλλες πηγές δεδομένων, παράγεται ένα τελικό εγκληματολογικό επίπεδο εντός της ψηφιακής εγκληματολογίας υψηλότερου επιπέδου – τα κορυφαία επίπεδα των μοντέλων OSI και PERA που αντιστοιχούν σε διαδικτυακά δεδομένα που μπορούν να ανακαλυφθούν από εγκληματολόγους [12]

5.3.2.1.4 User-level forensic analysis

Το επίπεδο χρήστη ορίζεται εδώ ως δεδομένα που συλλέγονται από ένα επίπεδο εφαρμογής ή εξάγονται από στοιχεία αποθήκευσης Cloud. Οι παραδοσιακές εγκληματολογικές μέθοδοι πρέπει να τροποποιηθούν ή να δημιουργηθούν νέες μέθοδοι, προκειμένου να φιλοξενηθούν οι μεγάλες ποσότητες δεδομένων που απαιτούνται για τις εγκληματολογικές έρευνες IIoT. Ακόμη και όταν ο όγκος των δεδομένων που συλλέγονται μειώνεται, ο όγκος των ψηφιακών εγκληματολογικών πληροφοριών θα μπορούσε να κατακλύσει μια έρευνα. Όταν συνδυάζονται με άλλες ψηφιακές εγκληματολογικές πληροφορίες higher-layer analysis (που συζητήθηκαν προηγουμένως) ή physical (που συζητούνται στην επόμενη ενότητα), αυτά τα δεδομένα μπορούν να παράγουν συνεργιστικά την επιθυμητή επιβεβαίωση για το σχηματισμό μιας σαφούς εγκληματολογικής εικόνας. Τα οφέλη που προκύπτουν από την ανάλυση πολλαπλών συσκευών και διασταυρούμενων περιπτώσεων παρέχουν κίνητρο για την ανάπτυξη της έννοιας της εγκληματολογικής πληροφόρησης πολλαπλών επιπέδων που παρουσιάζεται στην τελευταία κύρια ενότητα της εργασίας. [12]

5.3.2.1.5. Lowest-layer physical

Πολλές από τις ψηφιακές τεχνικές υψηλότερου επιπέδου (higher-layer) που εξετάστηκαν προηγουμένως δεν αφορούν συγκεκριμένες εφαρμογές IIoT. Αυτή η ενότητα αναφέρεται σε φυσικές πληροφορίες χαμηλότερου επιπέδου(physical) που είναι διαθέσιμες για εγκληματολογική ανάλυση και έχουν άμεση εφαρμογή στην εγκληματολογία IIoT. Πολλές διεργασίες IIoT σε επίπεδο δικτύου και bit βασίζονται σε αισθητήρες για την παρακολούθηση και τον έλεγχο των φυσικών διεργασιών (πίεση, θερμοκρασία, ταχύτητα, κ.λπ.). Έτσι, ο τομέας IIoT PHY είναι πλούσιος σε εγκληματολογικές πληροφορίες που μπορεί να αξιοποιηθούν για έρευνα μετά την επίθεση. [12]

Εκτός των εγκληματολογικών εφαρμογών, υπήρξε σημαντική δραστηριότητα RDD σε μεθόδους RFF βασισμένες σε ένα επίπεδο PHY που αναπτύχθηκαν για την υποστήριξη της δικτυακής άμυνας τόσο των ενσύρματων όσο και των ασύρματων επικοινωνιών. Αυτές οι εργασίες έχουν κυρίως αντιμετωπίσει τη διάκριση διαφόρων στοιχείων υλικού που χρησιμοποιούνται για τη δημιουργία επικοινωνιών. Ενώ ορισμένες από αυτές τις εργασίες υποδηλώνουν ότι οι μέθοδοι που επιδεικνύονται υποστηρίζουν την εγκληματολογική ανάλυση, η έννοια της εγκληματολογικής υποστήριξης είναι περισσότερο ένα θέμα που χρησιμοποιείται για να παρακινήσει τους αναγνώστες και υπάρχουν ελάχιστες λεπτομέρειες σχετικά με την πραγματική εγκληματολογική εφαρμογή. [12]

Η χρήση μιας ψηφιακής ταυτότητας σε εγκληματολογικές εφαρμογές RFID δεν είναι μια πραγματική εγκληματολογική εκμετάλλευση βασισμένη σε PHY, αλλά μάλλον είναι πιο συνεπής με τις μεθόδους εγκληματολογικής εκμετάλλευσης υψηλότερου επιπέδου που εξετάστηκαν στην προηγούμενη ενότητα. [12]

Ενώ η μοναδικότητα των δακτυλικών αποτυπωμάτων ηλεκτρονικών συσκευών μπορεί να μην είναι απολύτως εφάμιλλη με τη μοναδικότητα των δακτυλικών αποτυπωμάτων μεταξύ των ανθρώπων, αποτελέσματα όπως παρέχονται από διάφορες έρευνες επιδεικνύουν τακτικά σχεδόν 100% διάκριση για επιλεγμένα σενάρια και είναι αρκετά υποσχόμενοι να διατηρήσουν την προοδευτική RDD τα τελευταία 10 χρόνια. Συλλογικά, αυτές και άλλες σχετικές εργασίες RFF έχουν αντιμετωπίσει σχεδόν όλα τα κοινά σχήματα σηματοδότησης επικοινωνίας, συμπεριλαμβανομένου του Bluetooth, του αυτοματισμού και του ZigBee Personal Area Networks (PANs); WiFi, Wireless Local Area Network (WLANs)

και WiMAX . Δίκτυα ευρείας περιοχής (WAN), για να αναφέρουμε μερικά. Για τις παραπομπές που παρέχονται, τα μοναδικά χαρακτηριστικά RFF έχουν εξαχθεί αξιόπιστα από διάφορους τομείς σήματος, συμπεριλαμβανομένου [12]

- χρόνου [12]
- συχνότητα [12]
- κοινή ώρα-συχνότητα [12]
- αστερισμός [12]

5.3.2.1.6 cross-layer forensic information

Εγγενής σε οποιαδήποτε έρευνα που περιλαμβάνει τη χρήση τεχνουργημάτων εγκληματολογίας στον κυβερνοχώρο είναι η ολοκληρωμένη ανάλυση όλων των τεχνουργημάτων υπό το φως των πραγματικών συνθηκών κατά τη στιγμή της επίθεσης. Μία εργασία που βασίζεται σε βιομετρικά στοιχεία περιγράφει αυτήν την έννοια ως «κυβερνοφυσική ενοποίηση» καθώς σχετίζεται με την υποστήριξη εγκληματικών ερευνών. Υπάρχει πληθώρα πληροφοριών για την εργασία πολλαπλών επιπέδων επίθεσης και άμυνας στο γνωστικό ραδιόφωνο (CR), δίκτυο μητροπολιτικών περιοχών (MANET) και ασύρματο δίκτυο αισθητήρων (WSN). Δεδομένων των πλεονεκτημάτων που πραγματοποιούνται σε αυτούς τους τομείς εφαρμογής, είναι εύλογο να συμπεράνουμε ότι ορισμένοι από τους αμυντικούς μηχανισμούς σε αυτές τις εργασίες μπορούν να υιοθετηθούν και να αξιοποιηθούν για όφελος εγκληματολογικής ανάλυσης και έρευνας IIoT. [12]

Το όφελος της εγκληματολογικής έρευνας πολλαπλών επιπέδων (cross-layer forensics) γίνεται πιο εμφανές λαμβάνοντας υπόψη το σχετικό παράδειγμα ICS/SCADA που βασίζεται σε PHY το οποίο παρέχει μια γενίκευση των αξιολογήσεων επιθέσεων IIoT με βάση αυτά που κατηγοριοποιούνται ως [12]

- Απομακρυσμένα στρατηγικές επίθεσης πρόσβασης (**RAA**) που στοχεύουν στην αλλαγή της κατάστασης της συσκευής ανίχνευσης/αναφοράς πεδίου που λαμβάνεται και ενεργείται από το PLC και [12]
- στρατηγικές επίθεσης φυσικής πρόσβασης (**PAA**) που στοχεύουν στην αλλαγή του υλικού της φυσικής συσκευής, του υλικολογισμικού κ.λπ. [12]

Οι αξιολογήσεις RAA και PAA έγιναν χρησιμοποιώντας διακριτικά χαρακτηριστικά που εξάγονται από συνδέσμους επικοινωνίας που χρησιμοποιούνται για την ανταλλαγή πληροφοριών ελέγχου και ανίχνευσης μεταξύ του PLC και των συσκευών πεδίου. Αξίζει να σημειωθεί σε αυτές τις αξιολογήσεις RAA και PAA ότι δεν εφαρμόστηκε ολοκληρωμένη επεξεργασία στρώματος cross-PERA και cross-SCADA. Αντίθετα, οι αξιολογήσεις βασίζονται σε μια εγγενή υπόθεση ότι οι μέθοδοι προστασίας σε επίπεδο bit μόνο μεταξύ επιπέδων και μόνο εντός ζώνης έχουν «ξεγελαστεί» και ότι είναι επιθυμητός ο προσδιορισμός ταυτότητας και κατάστασης της συσκευής 100% με βάση το PHY. Χρησιμοποιώντας μια στρατηγική ανίχνευσης κανονικής έναντι ανώμαλης (επίθεσης) και 12 σεναρίων αξιολόγησης (έξι αξιολογήσεις RAA και έξι αξιολογήσεις PAA χρησιμοποιώντας δύο συσκευές από τρεις κατασκευαστές με κάθε συσκευή να λειτουργεί σε δύο διαφορετικά σημεία ρύθμισης), η διαδικασία απέδωσε με επιτυχία ένα ποσοστό ανίχνευσης ανωμαλιών (ADR) ADR ≈ 91,3% και ADR ≈ 95,5% για τις αξιολογήσεις RAA και PAA, αντίστοιχα. Αυτή η απόδοση που βασίζεται μόνο στο PHY υποδηλώνει μεγάλη υπόσχεση για την επίτευξη ADR ≈ 100%, δηλαδή 100% ανίχνευσης επίθεσης ή/και απόδοσης μετά την επίθεση, σε εφαρμογές IIoT, συμπεριλαμβάνοντας μεθόδους cross-layer παρόμοιες με αυτές που σημειώθηκαν στην προηγούμενη παράγραφο. [12]

Όπως επιβεβαιώθηκε από τη βιβλιογραφική ανασκόπηση που διεξήχθη για την προετοιμασία αυτής της ανασκόπησης, το γενικό συμπέρασμα στην παλαιότερη αναφερόμενη εργασία παραμένει έγκυρο σήμερα, δηλαδή, «η πλειοψηφία της υπάρχουσας έρευνας για θέματα ασφάλειας στα ασύρματα δίκτυα επικεντρώνεται κυρίως στην επίθεση και την άμυνα σε επιμέρους επίπεδα δικτύου ». Αυτό περιλαμβάνει την πλειονότητα των προσεγγίσεων μεμονωμένων υψηλότερων επιπέδων που τείνουν να υποχρησιμοποιούν ή να αγνοούν πλήρως τις πληροφορίες του επιπέδου PHY. [12]

Ως αποτέλεσμα, αυτές οι προσεγγίσεις δεν επιτρέπουν την άμεση συσχέτιση της ανίχνευσης ανωμαλιών δικτύου σε επίπεδο bit (ψηφιακά εγκληματολογικά στοιχεία υψηλότερου επιπέδου) με τη συνδεσιμότητα PHY ή/και την κατάσταση της συσκευής υλικού (επιτέθηκε, ελαττωματικά, κ.λπ.). Αν και είναι πιθανός ένας περιορισμός στον ευρύτερο τομέα IIoT, η μεγαλύτερη ανησυχία για αυτό έχει επισημανθεί στην κοινότητα ICS/SCADA όπου ερευνητές και επαγγελματίες είναι η αιτία για τη βελτίωση της ασφάλειας και της ασφάλειας χρησιμοποιώντας πληροφορίες πολλαπλών επιπέδων. Το προβλεπόμενο όφελος πολλαπλών επιπέδων IIoT θα μπορούσε να αποδειχθεί χρησιμοποιώντας μια συγκριτική αξιολόγηση απόδοσης που βασίζεται σε ανάλυση χρησιμοποιώντας [12]

- μόνο Ψηφιακές Εγκληματολογικές Πληροφορίες για την ενότητα Ψηφιακών Εγκληματολογικών Πληροφοριών Ανώτερου Επιπέδου — συγκρίσιμο με τη διεξαγωγή ποινικής έρευνας χρησιμοποιώντας μόνο πληροφορίες μαρτύρων [12]
- μόνο πληροφορίες PHY ανά PHY χαμηλότερου επιπέδου—συγκρίσιμες με τη διεξαγωγή ποινικής έρευνας με χρήση μόνο φυσικών πληροφοριών δακτυλικών αποτυπωμάτων και [12]
- κυβερνοφυσική ενσωμάτωση τόσο του ψηφιακού όσο και του PHY—επιτρέποντας τη δημιουργία μιας πληρέστερης εικόνας των γεγονότων που συμβαίνουν κατά τη διάρκεια του εγκλήματος. [12]

Η ενοποίηση και η εκμετάλλευση του ψηφιακού και του PHY απεικονίζεται εννοιολογικά χρησιμοποιώντας την αρχιτεκτονική SCADA. Αυτό το σχήμα δείχνει ότι η εγκληματολογική ερευνητική επιφάνεια αποτελείται από πολλαπλές ζώνες SCADA που περιλαμβάνουν εκμεταλλεύσιμες ψηφιακές και φυσικές πληροφορίες. Η αρχιτεκτονική βασίζεται σε ένα πλαίσιο όπου η ζώνη ελέγχου επεκτείνεται σκόπιμα εδώ για να διακρίνει τα στοιχεία του επιπέδου του μοντέλου [12]

- PERA Basic Control και [12]
- Physical [12]

Όπως φαίνεται, υπάρχουν τείχη προστασίας μεταξύ ζώνης που επιτρέπουν την εγκληματολογική ανάλυση χρησιμοποιώντας τα τυπικά δεδομένα καταγραφής τείχους προστασίας, δεδομένα συμβάντων, διευθύνσεις πρωτοκόλλου Διαδικτύου (IP) και αρχεία καταγραφής θυρών. Επιπλέον, υπάρχει πληθώρα ιατροδικαστικών πληροφοριών διαθέσιμα σε όλες τις ζώνες SCADA που μπορούν να χρησιμοποιηθούν για την υποστήριξη της ανάλυσης. [12]

5.4 DF in XR/AR/VR

Στο άρθρο [2] μπορούμε να δούμε μία master thesis στην οποία αναφέρεται επακριβώς μία διαδικασία DF που ακολουθείται από τον ερευνητή ανάλογα το περιβάλλον VR/XR/AR που εξετάζει ανά περίπτωση. Βλέπουμε ότι χρησιμοποιούνται κυρίως τα παρακάτω εργαλεία ως μεθοδολογία:

➔ Forensic Artifact Analysis:

- Data Population
- Data Acquisition
- Artifact Identification
- Data Interpretation

➔ Network Traffic Analysis:
- Data Population (Emulating Network Communication)
- Packet Capture Analysis
- Wireshark Analysis
- NetworkMiner Analysis
- Interpretation of packets

Και μέσω των παραπάνω παρέχει εντατικά παραδείγματα για το πως μπορεί να γίνει DF στα ακόλουθα περιβάλλοντα:

- Oculus Go
- Meta Quest
- Meta Quest 2
- Social Community Applications .
- Alcove Application
- Bigscreen Application
- MeetinVR Application
- Meta Horizon Worlds Application
- Multiverse Application
- Rec Room Application
- VRChat Application
- vTime XR Application

Επειδή κάθε φορά αναφέρονται συγκεκριμένες διαφορές που εμπεριέχει το κάθε περιβάλλον δεν θα γίνει περισσότερη εκτενή παρουσίαση εδώ πέρα.

5.5 DF in 6G Environments

Είναι πάρα πολύ νωρίς ακόμα ώστε να υπάρξουν συγκεκριμένες μέθοδοι, οι οποίες να έχουν ήδη εφαρμοστεί σε δίκτυα 6g. Ως εκ τούτου η βιβλιογραφία που βρέθηκε [56], [59] είναι βιβλιογραφία η οποία προτείνει συγκεκριμένες προτάσεις ώστε να καλυφθούν κάποια από τα κενά των δικτύων 5G, τα οποία γνωρίζουμε ότι πρόκειται να αποτελέσουν πρόβλημα για μελλοντικά δίκτυα 6G και την DF ανάλυση τους.

Με την έλευση των εφαρμογών που βασίζονται στην τεχνητή νοημοσύνη (AI) και των δικτύων με δυνατότητα Internet-of-Things (IoT), όπως τα έξυπνα δίκτυα, η έξυπνη υγειονομική περίθαλψη και τα έξυπνα συστήματα μεταφοράς (ITS) κ.λπ., η επικοινωνία πέμπτης γενιάς (5G) οι αρχιτεκτονικές δεν μπορούν να ικανοποιήσουν τις προκλήσεις που θέτει η απαίτηση υπηρεσιών σε πραγματικό χρόνο, όπως η εξαιρετικά αξιόπιστη επικοινωνία χαμηλής καθυστέρησης (URLLC). Για παράδειγμα, μία από τις απαιτήσεις για την αποτροπή κυβερνο-φυσικών επιθέσεων σε έξυπνα δίκτυα είναι η επίτευξη ενός ελάχιστου λανθάνοντος χρόνου για την αντιμετώπιση των μεταβατικών φαινομένων για την ελαχιστοποίηση των πιθανοτήτων διαδοχικών αστοχιών. [56]

Μία από τις πιθανές λύσεις για την αποτροπή κυβερνοεπιθέσεων είναι η αποτελεσματική χρήση του SDIoT σε έξυπνα δίκτυα. Η δικτύωση που ορίζεται από λογισμικό (**SDN**) είναι μια προσέγγιση δικτύωσης που αποσυνδέει το επίπεδο ελέγχου από το επίπεδο δεδομένων για να απλοποιήσει τη διαχείριση ενός δικτύου. Στο SDIoT, το ευφυές επίπεδο ελέγχου μπορεί να παρακολουθεί τις καταστάσεις του δικτύου παγκοσμίως σε πραγματικό χρόνο και μπορούν να εφαρμοστούν τεχνικές ασφάλειας για τον εντοπισμό απειλών δικτύου. Τα δίκτυα 6G αναμένεται να δημιουργήσουν μαζική κίνηση με αυστηρές απαιτήσεις QoS. Οι υπάρχουσες τεχνικές ανάλυσης δεδομένων για την αξιολόγηση τρωτότητας των απειλών στον κυβερνοχώρο αντιμετωπίζουν ζητήματα επεκτασιμότητας και καθυστέρησης κατά την εκπαίδευση σε δεδομένα. Μια τέτοια προσέγγιση για την επίλυση του προβλήματος του χρόνου εκπαίδευσης προτείνεται σε ένα άρθρο, όπου οι συγγραφείς υιοθέτησαν ένα πλαίσιο με δυνατότητα SDN που προώθησε την εργασία υπολογισμού διαδρομής σε μια μονάδα επεξεργασίας γραφικών (GPU) για τη μείωση του χρόνου εκπαίδευσης των αλγορίθμων. Έτσι, η κεντρική φύση του επιπέδου ελέγχου SDN μπορεί να είναι αποτελεσματική για την υλοποίηση των εργασιών μηχανικής εκμάθησης σε μια GPU. [56]

Οι βασικές συνεισφορές αυτού του άρθρου είναι οι εξής: [56]

1) Πρόταση ενός προσαρμοστικού ισχυρού μοντέλου SE με δυνατότητα SDIoT, που υλοποιείται σε μια GPU για τον εντοπισμό και την πρόληψη κυβερνοεπιθέσεων σε έξυπνα δίκτυα.

2) Βελτίωση της αξιοπιστίας των οραματιζόμενων δικτύων 6G με την εκτέλεση δύο επιπέδων διαδικτυακής παραμετρικής SE για ασφαλή επικοινωνία και διαχείριση φορτίου.

3) Εισαγωγή πρόβλεψης χρονοσειρών βάσει LSTM που επιτρέπει σε έναν χειριστή κοινής ωφέλειας να παρατηρήσει απροσδόκητη μη γραμμικότητα στο προφίλ φορτίου που εισάγεται από έναν εισβολέα.

Το Automated ML (**AutoML**) έχει αναδειχθεί ως μια πολλά υποσχόμενη λύση για υπηρεσίες δικτύου που βασίζονται σε δεδομένα, αντιμετωπίζοντας τις προκλήσεις που σχετίζονται με τα παραδοσιακά μοντέλα ML και αυτοματοποιώντας την ανάλυση δεδομένων δικτύου. Το AutoML στοχεύει στην αυτοματοποίηση διαφόρων διαδικασιών ανάλυσης δεδομένων και ML, συμπεριλαμβανομένης της Αυτοματοποιημένης Προεπεξεργασίας Δεδομένων (**AutoDP**), της Μηχανικής Αυτοματοποιημένων Χαρακτηριστικών (**AutoFE**), της αυτοματοποιημένης επιλογής μοντέλου, της Βελτιστοποίησης Υπερπαραμέτρων (**HPO**) και της αυτοματοποιημένης ενημέρωσης μοντέλου. Το AutoDP και η μηχανική χαρακτηριστικών έχουν σχεδιαστεί για να βελτιώνουν την ποιότητα των δεδομένων δικτύου για καλύτερα αποτελέσματα ανάλυσης δεδομένων. Η αυτοματοποιημένη επιλογή μοντέλων και το HPO στοχεύουν στη δημιουργία βελτιστοποιημένων μοντέλων ML με βελτιωμένη απόδοση. Επιπλέον, η αυτοματοποιημένη ενημέρωση μοντέλων ή η προσαρμογή drift είναι μια πιθανή λύση για την αντιμετώπιση προβλημάτων μετατόπισης μοντέλων με αυτόματη ενημέρωση των μοντέλων ML για προσαρμογή σε δυναμικά περιβάλλοντα δικτύωσης. Οι τεχνικές AutoML υπόσχονται σημαντικά την υλοποίηση των ZTN με την αυτοματοποίηση των πολύπλοκων και επίπονων εργασιών που σχετίζονται με την ανάπτυξη και την ανάπτυξη μοντέλων ML. [59]

Για την προστασία των δικτύων από επιθέσεις στον κυβερνοχώρο, έχουν αναπτυχθεί πολλές λύσεις και μηχανισμοί κυβερνοασφάλειας, ιδιαίτερα συστήματα ελέγχου ταυτότητας συσκευών και ανίχνευσης εισβολής (IDS). Οι παραδοσιακές τεχνικές ελέγχου ταυτότητας που βασίζονται στην κρυπτογραφία που εφαρμόζονται στα ανώτερα επίπεδα έχουν υιοθετηθεί συνήθως για την επαλήθευση της ταυτότητας των χρηστών μέσω διαδικασιών

δημιουργίας και ανίχνευσης κλειδιών. Ωστόσο, σε δίκτυα που περιλαμβάνουν τεράστιο αριθμό κινητών και ετερογενών συσκευών, η διανομή και η διαχείριση των κρυπτογραφικών κλειδιών είναι μάλλον προκλητική. Επιπλέον, η υπολογιστική πολυπλοκότητα που σχετίζεται με τη δημιουργία και την ανίχνευση κλειδιών εισάγει ζητήματα καθυστέρησης που εξαντλούν τη διάρκεια ζωής της μπαταρίας συσκευών περιορισμένης ισχύος. [59]

Αυτοί οι περιορισμοί παρακίνησαν την ανάπτυξη καινοτόμων σχημάτων ελέγχου ταυτότητας φυσικού επιπέδου (PLA) για την επαλήθευση της αυθεντικότητας των συσκευών δικτύου με βάση τα χαρακτηριστικά του φυσικού επιπέδου τους, αποτρέποντας έτσι την πρόσβαση μη εξουσιοδοτημένων συσκευών στο δίκτυο. Αξίζει να σημειωθεί ότι, εκτός από το PLA, το φυσικό επίπεδο περιλαμβάνει και άλλες τεχνικές ασφάλειας, συμπεριλαμβανομένων των Physical Layer Security (PLS) και Physical Layer Key Generation (PLKG). Οι τεχνικές PLS διασφαλίζουν εμπιστευτική μετάδοση μεταξύ οντοτήτων αξιοποιώντας τα εγγενή χαρακτηριστικά του φυσικού επιπέδου, χωρίς την ανάγκη κοινής χρήσης μυστικών κλειδιών. Το PLKG εξάγει τυχαία κλειδιά με βάση τα χαρακτηριστικά του καναλιού μεταξύ νόμιμων οντοτήτων. Ωστόσο, το PLA έχει μεγαλύτερη σημασία καθώς χρησιμεύει ως η πρώτη γραμμή άμυνας για τον έλεγχο ταυτότητας της προέλευσης των λαμβανόμενων σημάτων. [59]

Από την άλλη πλευρά, τα IDS έχουν σχεδιαστεί για να ανιχνεύουν επιθέσεις στον κυβερνοχώρο σε ένα δίκτυο μέσω ανάλυσης δεδομένων δικτύου και τα Cross-Layer IDS (**CLIDS**) είναι ένας ειδικός τύπος IDS που ενσωματώνει πληροφορίες από πολλαπλά επίπεδα της στοίβας πρωτοκόλλων για τον εντοπισμό και τον μετριασμό των απειλών του κυβερνοχώρου. Για παράδειγμα, ένα CLIDS μπορεί να χρησιμοποιήσει την ικανότητα του φυσικού επιπέδου να ανιχνεύει ανωμαλίες σε ασύρματα σήματα, την ικανότητα του επιπέδου δικτύου να αναγνωρίζει ύποπτες συμπεριφορές πακέτων και την ικανότητα του επιπέδου εφαρμογής να αναγνωρίζει μοτίβα κακόβουλου λογισμικού. Σε γενικά δίκτυα, οι μηχανισμοί PLA αναπτύσσονται συνήθως ως το πρώτο επίπεδο άμυνας για τον έλεγχο ταυτότητας συσκευών, ενώ τα CLIDS μπορούν να χρησιμοποιηθούν ως το δεύτερο επίπεδο άμυνας για τον εντοπισμό κακόβουλων επιθέσεων που έχουν παραβιάσει το πρώτο επίπεδο άμυνας. Αν και αυτές οι λύσεις είναι ελπιδοφόρες, εξακολουθούν να βρίσκονται υπό ενεργό έρευνα και ανάπτυξη καθώς υπάρχουν πολλά περιθώρια βελτίωσης. Αντιπροσωπεύουν τις συνεχιζόμενες προσπάθειες στην κοινότητα της κυβερνοασφάλειας για την αντιμετώπιση των εξελισσόμενων προκλήσεων όσον αφορά την ασφάλεια των δικτύων 5G/6G. [59]

Οι αυτόνομες λύσεις κυβερνοασφάλειας, όπως τα αυτοματοποιημένα πλαίσια PLA και CLIDS, είναι ζωτικής σημασίας για τη βελτίωση της αυτοματοποίησης και της ασφάλειας του δικτύου στα δίκτυα ZTN/6G. Με την αυτοματοποίηση της διαδικασίας ελέγχου ταυτότητας και ανίχνευσης απειλών, οι αυτοματοποιημένοι μηχανισμοί ασφαλείας μπορούν να μειώσουν σημαντικά την ανθρώπινη εργασία και τον χρόνο για τον μετριασμό των επιθέσεων στον κυβερνοχώρο, ελαχιστοποιώντας έτσι τις πιθανές ζημιές που προκαλούνται από επιθέσεις. Σε αυτό το έγγραφο, προτείνεται ένα αυτόνομο πλαίσιο ασφάλειας στον κυβερνοχώρο που βασίζεται σε AuotoML για την επίλυση προβλημάτων τόσο PLA όσο και CLIDS για την προστασία των δικτύων ZTN/6G. Συγκεκριμένα, το προτεινόμενο πλαίσιο αποτελείται από τα ακόλουθα στοιχεία: την προσέγγιση υπερδειγματοληψίας Chebyshev για αυτοματοποιημένη εξισορρόπηση δεδομένων και AutoDP, τον συντελεστή συσχέτισης Pearson (PCC) βάσει Select-K- Best μέθοδος για AutoFE, Adaptive Random Forest (ARF) και Streaming Random Patches (SRP) για βασική ηλεκτρονική εκμάθηση μοντέλων, το βελτιωμένο μοντέλο διαδοχικής κατά το ήμισυ (SH) για βελτιστοποίηση συνδυασμένης επιλογής αλγορίθμου και υπερπαραμέτρων (CASH) και το ADaptive WINdowing (ADWIN) και η μέθοδος έγκαιρης ανίχνευσης μετατόπισης (EDDM) για την ανίχνευση μετατόπισης

μοντέλων και αυτοματοποιημένη ενημέρωση μοντέλου. Το προτεινόμενο πλαίσιο AutoML μπορεί να προσαρμοστεί αυτόματα σε οποιαδήποτε συγκεκριμένα σύνολα δεδομένων που σχετίζονται με προβλήματα ασφάλειας στον κυβερνοχώρο και να δημιουργήσει βελτιστοποιημένα μοντέλα ML με βέλτιστη απόδοση. [59]

5.6 Digital Forensics Tools

Τέλος δεδομένου ότι δεν είναι εφικτό να καλυφθούν όλα τα Digital Forensics Tools, ακόμα και εστιάζοντας ανα τομέα, όπως και κάναμε στο κεφάλαιο 5 μέχρι στιγμής, στη συνέχεια θα παρουσιάσουμε ένα πίνακα με διάφορα εργαλεία τα οποία συναντήσαμε στη βιβλιογραφία, παρουσιάζοντας μονάχα μία σύντομη περιγραφή τους. Ενδεικτικά αναφέρουμε ότι το Cellebrite ανήκει τόσο στα Computer Forensics, όσο και στο Mobile Device Forensics. Αντίστοιχα το Magnet Axiom υπάρχει στα Computer Forensics, Memory Forensics και Mobile Device Forensics και τέλος το Oxygen που υπάρχει στα Computer Forensics και Mobile Device Forensics.

Με βάση λοιπόν το [3] και έχοντας υπόψη αυτά που αναφέραμε στη προηγούμενη παράγραφο έχουμε ακόμα τα ακόλουθα εργαλεία:

Για **Computer Forensics** [3]:

Name	Platform	License	Version	Description
Autopsy	Windows, macOS, Linux	GPL	4.2	Μία digital forensics πλατφόρμα και GUI για το Sleuth Kit
Cellebrite Inspector	Windows/ macOS	proprietary	10.4	Αναλύει μεγάλους όγκους δεδομένων και μνήμης από υπολογιστές Windows και MAC για να βρει user actions και surface leads
COFEE	Windows	proprietary	n/a	Μια σειρά εργαλείων για Windows που αναπτύχθηκε από τη Microsoft
Digital Forensics Framework	Unix-like/Windows	GPL	1.3	Πλαίσιο και διεπαφές χρήστη αφιερωμένες στην ψηφιακή εγκληματολογία
Elcomsoft Premium Forensic Bundle	Windows, macOS	proprietary	1435	Σύνολο εργαλείων για κρυπτογραφημένα συστήματα με σκοπό την αποκρυπτογράφηση δεδομένων και την ανάκτηση κωδικού πρόσβασης
E3: Universal Software	Windows	proprietary	3.1	Το E3: Universal από την Paraben Corporation είναι μια ολοκληρωμένη λύση DFIR που μπορεί να λειτουργήσει μέσω ΟΛΩΝ των τύπων ψηφιακών δεδομένων: υπολογιστές, email,

				δεδομένα Διαδικτύου, smartphone και συσκευές IoT.
Forensic Explorer	Windows	proprietary	5.6.8	Το FEX είναι ένα προηγμένο ψηφιακό εγκληματολογικό πρόγραμμα για την ανάλυση δίσκων, εικόνων, τηλεφώνων και dvrs μέσω μιας εύκολης διεπαφής χρήστη.
FTK	Windows	proprietary	8	Εργαλείο πολλαπλών χρήσεων, το FTK είναι μια πλατφόρμα ψηφιακών ερευνών που αναφέρεται στο δικαστήριο, κατασκευασμένη για ταχύτητα, σταθερότητα και ευκολία στη χρήση.
IsoBuster	Windows	proprietary	5.3	Απαραίτητο εργαλείο μικρού βάρους για την επιθεώρηση οποιουδήποτε τύπου φορέα δεδομένων, που υποστηρίζει ένα ευρύ φάσμα συστημάτων αρχείων, με προηγμένη λειτουργία εξαγωγής.
LLIMAGER	macOS	proprietary	3.7	macOS forensic imager.
Magnet AXIOM	Windows	proprietary	6.X	Το Magnet AXIOM μπορεί να ανακτήσει και να αναλύσει ψηφιακά στοιχεία από τις περισσότερες πηγές, συμπεριλαμβανομένων συσκευών Windows και Mac, συστημάτων Linux και Chromebook, όλα σε ένα αρχείο υπόθεσης.
Netherlands Forensic Institute / Xiraf / HANSKEN	n/a	proprietary	n/a	Computer-forensic online service.
NTFSTool	Windows	MIT License	1.7	Πλήρες εργαλείο εγκληματολογίας για τόμους NTFS, Απεικόνιση, ανάλυση, εξαγωγή τεχνουργημάτων με υποστήριξη Bitlocker και Κρυπτογραφημένο Σύστημα Αρχείων (EFS).

Open Computer Forensics Architecture	Linux	LGPL/GPL	2.3.0	Πλαίσιο εγκληματολογίας υπολογιστών για περιβάλλον CF-Lab
OSForensics	Windows	proprietary	8	Multi-purpose forensic tool
Oxygen Forensic® Detective	Windows, macOs, Linux	proprietary	14.3	Το Oxygen Forensic® Detective μπορεί επίσης να βρει και να εξαγάγει μια τεράστια γκάμα τεχνουργημάτων, αρχείων συστήματος καθώς και διαπιστευτηρίων από μηχανήματα Windows, macOS και Linux.
PTK Forensics	LAMP	proprietary	2	GUI for The Sleuth Kit
SANS Investigative Forensics Toolkit - SIFT	Ubuntu		2.1	Multi-purpose forensic operating system
SPEKTOR Forensic Intelligence	Unix-like	proprietary	6.x	Εύκολο στη χρήση, ολοκληρωμένο εγκληματολογικό εργαλείο που χρησιμοποιείται παγκοσμίως από LE/Στρατιωτικά/Υπηρεσίες/Εταιρείες - περιλαμβάνει ταχεία απεικόνιση και πλήρως αυτοματοποιημένη ανάλυση.
The Coroner's Toolkit	Unix-like	IBM Public License	1.19	A suite of programs for Unix analysis
The Sleuth Kit	Unix-like/Windows	IPL, CPL, GPL	4.12.0	A library of tools for both Unix and Windows
Windows To Go	n/a	proprietary	n/a	Bootable operating system

Για **Memory Forensics** [3]:

Name	Vendor or sponsor	Platform	License
Magnet AXIOM	Magnet Forensics	Windows	proprietary
Volatility	Volatile Systems	Windows and Linux	free (GPL)
WindowsSCOPE	BlueRISC	Windows	proprietary

Για **Mobile Device Forensics** [3] :

Name	Platform	License	Version	Description
Cellebrite UFED	Windows	proprietary		Πακέτο υλικού/λογισμικού, που ειδικεύεται στην κινητή εγκληματολογική εξόρυξη
Magnet AXIOM	Windows	proprietary	6.X	Το Magnet AXIOM μπορεί να ανακτήσει και να αναλύσει ψηφιακά στοιχεία από τις περισσότερες πηγές, συμπεριλαμβανομένων των συσκευών iOS και Android, όλα σε ένα αρχείο υπόθεσης.
MicroSystemation XRY/XACT	Windows	proprietary		Πακέτο υλικού/λογισμικού, ειδικεύεται στα διαγραμμένα δεδομένα
Oxygen Forensic® Detective	Windows	proprietary	14.3	Το Oxygen Forensic® Detective είναι μια πλατφόρμα εγκληματολογικού λογισμικού all-in-one που έχει σχεδιαστεί για εξαγωγή, αποκωδικοποίηση και ανάλυση δεδομένων από πολλαπλές ψηφιακές πηγές: κινητές συσκευές και συσκευές IoT, αντίγραφα ασφαλείας συσκευών, κάρτες UICC και πολυμέσων, drones και υπηρεσίες cloud.

Για **Software Forensics** [3] :

Name	Platform	License	Version	Description
DECAF	Windows	free	n/a	Εργαλείο που εκτελεί αυτόματα ένα σύνολο ενεργειών που ορίζονται από το χρήστη για τον εντοπισμό του εργαλείου COFEE της Microsoft
Evidence Eliminator	Windows	proprietary	6.03	Λογισμικό κατά της εγκληματολογίας, ισχυρίζεται ότι διαγράφει αρχεία με ασφάλεια
HashKeeper	Windows	free	n/a	Εφαρμογή βάσης δεδομένων για την αποθήκευση υπογραφών κατακερματισμού αρχείων
MailXaminer	Windows	Perpetual	4.9.0	Specialized email forensics tool

5.7 Συγκεντρωτικός πίνακας όλων των εργαλείων και τεχνολογιών

Τέλος παρουσιάζουμε ένα συγκεντρωτικό πίνακα που περιέχει όλα τα Tools αυτού του κεφαλαίου για Digital Forensic Analysis :

Name	Κεφάλαιο	Περιγραφή
CAINE	3.8	είναι ένα διαδραστικό και ανοιχτού κώδικα εργαλείο εγκληματολογίας που υποστηρίζει πολλαπλές φάσεις εγκληματολογίας
EnCase	3.8	χρησιμοποιείται για την εκτέλεση αναλύσεων για εγκληματολογικές εικόνες, δεδομένα και αρχεία
Wireshark	3.8	χρησιμοποιείται ως επί το πλείστον για εγκληματολογική ανάλυση δικτύου
Bulk Extractor	3.8	βοηθά στη σάρωση και την εξαγωγή πληροφοριών, π.χ. αριθμών καρτών, διευθύνσεων email, διευθύνσεων ιστού και αριθμών τηλεφώνου από τις εικόνες του δίσκου και τα αρχεία καταλόγου
NUIX	3.8	χρησιμοποιείται για τη σάρωση ενός τεράστιου όγκου δεδομένων και διαδικασιών που οδηγεί στην εξαγωγή χρήσιμων πληροφοριών αργότερα που θα χρησιμοποιηθούν για σκοπούς ανάλυσης
RegRipper	3.8	χρησιμοποιείται κυρίως για τη σάρωση των αρχείων μητρώου των Windows

IEF	3.8	χρησιμοποιείται για τη σάρωση των εγκληματολογικών εικόνων και ενός ευρέος φάσματος δεδομένων που εξάγονται από το ιστορικό Διαδικτύου, το ιστορικό συνομιλιών και τα λειτουργικά συστήματα
NetAnalysis	3.8	βοηθά στη σάρωση των εγκληματολογικών εικόνων και δεδομένων που σχετίζονται με το ιστορικό του Διαδικτύου
Pajek64	3.8	βοηθά στην ανάλυση μεγάλου όγκου δεδομένων που σχετίζονται με το δίκτυο
CCAFM	5.2.1	ένα νέο ολοκληρωμένο εγκληματολογικό μοντέλο συλλογής και ανάλυσης (CCAFM) που εφαρμόζεται στον τομέα της εγκληματολογίας των drone
Dialog	5.2.2	συλλέγει εγκληματολογικά δεδομένα από το αυτοκίνητο και τα στέλνει σε ασφαλή αποθήκευση cloud χρησιμοποιώντας ένα ασφαλές πρωτόκολλο
Skyther	5.2.2	Το Scyther είναι ένα εργαλείο επαλήθευσης κρυπτογραφικού πρωτοκόλλου που χρησιμοποιείται για την ανάλυση και την αξιολόγηση της ασφάλειας των κρυπτογραφικών πρωτοκόλλων.
Casper FDR	5.2.2	Το εργαλείο Casper/FDR είναι ένας μεταγλωττιστής που ελέγχει την ορθότητα του πρωτοκόλλου με βάση τις καθορισμένες απαιτήσεις ασφαλείας
PushingBox	5.2.2	Πλατφόρμες, οι οποίες χρησιμοποιούν κλειδιά API για να πιστοποιήσουν ότι μία εφαρμογή μπορεί να έχει πρόσβαση για συγκεκριμένες πληροφορίες στο cloud
Xively	5.2.2	
Thingspeak	5.2.2	
SmartSat-IIOHT	5.2.3	Προτόκολλο για μεταφορά δεδομένων healthcare
HAS Forensic framework	5.3.1.	Framework για Smart Homes/Office το οποίο αποτελείται από 7 φάσεις: Preparation off-site, Search for a home automation system on-site, Preserve the HAS “as is”, wherever possible, Understanding the specific home automation system, Check security level, Locate and acquire evidential data, Process/analyse seized data
Almond+	5.3.1	Application μέσω terminal, cloud και κινητής συσκευής όπου καταγράφονται όλα τα στοιχεία για όλες τις smart συσκευές ενός smart home, με σκοπό τη καλύτερη DF analysis
Μέθοδος cross-layer	5.3.2	Πρόκειται για μία μέθοδο, η οποία μπορεί να χρησιμοποιηθεί γενικότερα για DF analysis σε IoT δίκτυα (αν και αναφέρεται στα πλαίσια του IIoT μέσα στην εργασία). Συγκεντρώνει στοιχεία από διάφορες βαθμίδες όπως το higher-layer, bit-level, network-level, user-level, physical level digital forensic information προκειμένου να διασταυρώσει αν έχει γίνει κάποιο έγκλημα και μέσω ποιάς βαθμίδας κατάφεραν οι εισβολείς να κάνουν το breach.

Forensic Artifact Analysis	5.4	Πρόκειται για μέθοδο η οποία (στην εργασία) χρησιμοποιείται για DF σε περιβάλλοντα XR/AR/VR. Αποτελείται από τα ακόλουθα 4 στάδια: Data Population, Data Aqcuisition, Artifact Identification, Data Interpretation
Network Traffic Analysis	5.4	Πρόκειται για μέθοδο η οποία (στην εργασία) χρησιμοποιείται για DF σε περιβάλλοντα XR/AR/VR. Αποτελείται από τα ακόλουθα 5 στάδια: Data Population, Packet Capture Analysis, Wireshark Analysis, NetworkMiner Analysis, Interpretation of Packets
AutoML	5.5	Το Automated ML (AutoML) έχει αναδειχθεί ως μια πολλά υποσχόμενη λύση για υπηρεσίες δικτύου που βασίζονται σε δεδομένα, αντιμετωπίζοντας τις προκλήσεις που σχετίζονται με τα παραδοσιακά μοντέλα ML και αυτοματοποιώντας την ανάλυση δεδομένων δικτύου
CLIDS	5.5	είναι ένας ειδικός τύπος IDS που ενσωματώνει πληροφορίες από πολλαπλά επίπεδα της στοίβας πρωτοκόλλων για τον εντοπισμό και τον μετριασμό των απειλών του κυβερνοχώρου
Autopsy	5.6	Μία digital forensics πλατφόρμα και GUI για το Sleuth Kit
Cellebrite Inspector	5.6	Αναλύει μεγάλους όγκους δεδομένων και μνήμης από υπολογιστές Windows και MAC για να βρει user actions και surface leads
COFEE	5.6	Μια σειρά εργαλείων για Windows που αναπτύχθηκε από τη Microsoft
Digital Forensics Framework	5.6	Πλαίσιο και διεπαφές χρήστη αφιερωμένες στην ψηφιακή εγκληματολογία
Elcomsoft Premium Forensic Bundle	5.6	Σύνολο εργαλείων για κρυπτογραφημένα συστήματα με σκοπό την αποκρυπτογράφηση δεδομένων και την ανάκτηση κωδικού πρόσβασης
E3: Universal Software	5.6	Το E3: Universal από την Paraben Corporation είναι μια ολοκληρωμένη λύση DFIR που μπορεί να λειτουργήσει μέσω ΟΛΩΝ των τύπων ψηφιακών δεδομένων: υπολογιστές, email, δεδομένα Διαδικτύου, smartphone και συσκευές IoT.
Forensic Explorer	5.6	Το FEX είναι ένα προηγμένο ψηφιακό εγκληματολογικό πρόγραμμα για την ανάλυση δίσκων, εικόνων, τηλεφώνων και dvrs μέσω μιας εύκολης διεπαφής χρήστη.
FTK	5.6	Εργαλείο πολλαπλών χρήσεων, το FTK είναι μια πλατφόρμα ψηφιακών ερευνών που αναφέρεται στο δικαστήριο, κατασκευασμένη για ταχύτητα, σταθερότητα και ευκολία στη χρήση.

IsoBuster	5.6	Απαραίτητο εργαλείο μικρού βάρους για την επιθεώρηση οποιουδήποτε τύπου φορέα δεδομένων, που υποστηρίζει ένα ευρύ φάσμα συστημάτων αρχείων, με προηγμένη λειτουργία εξαγωγής.
LLIMAGER	5.6	macOS forensic imager.
Magnet AXIOM	5.6	Το Magnet AXIOM μπορεί να ανακτήσει και να αναλύσει ψηφιακά στοιχεία από τις περισσότερες πηγές, συμπεριλαμβανομένων συσκευών Windows και Mac, συστημάτων Linux και Chromebook, όλα σε ένα αρχείο υπόθεσης.
Netherlands Forensic Institute / Xiraf / HANSKEN	5.6	Computer-forensic online service.
NTFSTool	5.6	Πλήρες εργαλείο εγκληματολογίας για τόμους NTFS, Απεικόνιση, ανάλυση, εξαγωγή τεχνουργημάτων με υποστήριξη Bitlocker και Κρυπτογραφημένο Σύστημα Αρχείων (EFS).
Open Computer Forensics Architecture	5.6	Πλαίσιο εγκληματολογίας υπολογιστών για περιβάλλον CF-Lab
OSForensics	5.6	Multi-purpose forensic tool
Oxygen Forensic® Detective	5.6	Το Oxygen Forensic® Detective μπορεί επίσης να βρει και να εξαγάγει μια τεράστια γκάμα τεχνουργημάτων, αρχείων συστήματος καθώς και διαπιστευτηρίων από μηχανήματα Windows, macOS και Linux.
PTK Forensics	5.6	GUI for The Sleuth Kit
SANS Investigative Forensics Toolkit - SIFT	5.6	Multi-purpose forensic operating system

6. Συζήτηση

Ο όρος Industry 4.0 προήλθε το 2011 από μια γερμανική πρωτοβουλία της ομοσπονδιακής κυβέρνησης με ακαδημαϊκές ενώσεις και εμπορικές επιχειρήσεις και ορίστηκε ως ένα μέσο για την επίτευξη ευέλικτης παραγωγής εξατομικευμένων προϊόντων υψηλής ποιότητας σε μαζική απόδοση μέσω της ενσωμάτωσης του CPS (Cyber–Physical Systems) στην παραγωγή. Σε παγκόσμιο επίπεδο, πολλές χώρες έχουν δημιουργήσει παρόμοιες πρωτοβουλίες τοπικής στρατηγικής, για παράδειγμα, Industrial Internet Consortium (ΗΠΑ), Made in China 2025 (Κίνα), La Nouvelle France Industrielle (Γαλλία), Society 5.0 (Ιαπωνία), Towards Industry 4.0 (Βραζιλία).). Ως εκ τούτου, το Industry 4.0 έγινε έκτοτε ένας όρος που υιοθετήθηκε παγκοσμίως και το επίκεντρο σημαντικών ερευνητικών προσπαθειών με τα Smart Factories να είναι μεταξύ των βασικών πρωτοβουλιών. Το Industry 4.0 αναγνωρίζεται ως τετραδιάστατη τεχνολογία front-end: Smart Manufacturing, Smart Products, Smart Supply Chain και Smart Working και βασίζεται σε τέσσερις βασικές τεχνολογίες: IoT, υπηρεσίες cloud, big data και analytics. Όσον αφορά τους οικονομικούς δείκτες, το Industry 4.0 έχει μειώσει το κόστος παραγωγής κατά 10-30%, το κόστος εφοδιαστικής κατά 10-30% και το κόστος διαχείρισης ποιότητας κατά 10-20%. Το Industry 4.0 βασίζεται στην τεχνολογία, παρέχοντας τεχνολογικές πιέσεις και λύσεις. [41]

Εν τω μεταξύ, το Industry 5.0, που θεωρείται η επόμενη βιομηχανική επανάσταση, στοχεύει να αξιοποιήσει τη δημιουργικότητα των ανθρώπινων ειδικών σε συνεργασία με έξυπνες μηχανές για την απόκτηση λύσεων κατασκευής που προτιμούν οι χρήστες. Το Industry 5.0 αναγνωρίζει τη δύναμη της βιομηχανίας να επιτυγχάνει κοινωνικούς στόχους και να υποστηρίζει τη μακροπρόθεσμη υπηρεσία στην ανθρωπότητα. Περιλαμβάνει τον συνδυασμό προηγμένων τεχνολογιών και ανθρώπινης κοινής ζωής, με την επιστροφή του ανθρώπου στο «Κέντρο του Σύμπαντος», εκμεταλλευόμενος την ικανότητα λήψης αποφάσεων των ανθρώπων για την εναρμόνιση των συνθηκών εργασίας και της αποτελεσματικότητας των ανθρώπων και των μηχανών. με συνεπή τρόπο [41].

Ο στόχος του Industry 4.0 είναι να μειώσει τη συμμετοχή των ανθρώπινων χειριστών και να τονίσει τα συστήματα αυτοματισμού, ενώ το Industry 5.0 στοχεύει να επιτύχει τα μέγιστα οφέλη μέσω του HMI. Επομένως, απαιτούνται προηγμένες λύσεις HMI μεταξύ πιο ευφυών μηχανημάτων και των παραγωγικών ικανοτήτων των ανθρώπων. Μεταξύ αυτών, το digital twin θεωρείται μία από τις βασικές τεχνολογίες για την ενίσχυση του HMI μέσω προηγμένων τεχνικών μοντελοποίησης. Παράλληλα, έφτασε η «Εποχή της Επαύξησης», στην οποία άνθρωποι και μηχανές εργάζονται συμβιωτικά για να αξιοποιήσουν τις τεχνολογίες XR, ενισχύοντας τις γνωστικές ικανότητες και τις ικανότητες αλληλεπίδρασης του χειριστή. [41]

Συνειδητοποιούμε λοιπόν ότι μια κοινή γραμμή μέσω ενός κοινού αποδεκτού framework και μίας γκάμας εργαλείων Digital Forensics είναι απαραίτητη ώστε οι επαγγελματίες Digital Forensics analysts να μη χρειάζεται να έχουν μία υπερβολικά εξιδανικευμένη γνώση των CPS και Digital Twin counterparts των συσκευών IoT που εξετάζουν και αναλύουν. Αυτό γίνεται ώστε να μπορούν να συνδυάσουν γνώσεις από πολλές διαφορετικές συσκευές IoT ξεχωριστά, με σκοπό να μαζέψουν στοιχεία τα οποία θα αλληλουποστηρίζονται από όλες τις συσκευές IoT που με κάποιο τρόπο συμμετείχαν στην εγκληματική πράξη προς εξέταση. Έτσι μόνο θα βρεθεί μία πλήρη εικόνα της κατάστασης.

7. Επίλογος

Μέσω των προηγουμενων αναφορών και όπως κρίνεται ακόμα πιο σαφές μέσα από τη διπλωματική αυτή εργασία, μπορούμε να δούμε ότι ενώ υπάρχουν frameworks για την Digital forensic analysis των δικτύων IoT απο το κεφάλαιο 3 (όπου έγινε μία ταξινόμηση και σύντομη ανάλυση τους), στη πραγματικότητα η βασική ετερογένεια της κάθε επιμέρους συσκευής (όπως είδαμε στο κεφάλαιο 4 με τα διαφορετικά CPS και Digital Twin ανά δίκτυο), σε συνδυασμό με τεχνολογίες ακμής όπως το ML ή δικτύωση 6G καθιστούν την υιοθέτηση μιας και μόνο γενικής μεθοδου ακόμα αδύνατη. Κρίνεται αναγκαίο ωστόσο να υιοθετηθεί ένα κοινό framework μέσω των οποίων στοιχεία από διάφορες IoT συσκευές θα μπορούν να χρησιμοποιηθούν συγκεντρωτικά στο μέλλον ακολουθώντας τα τελευταία τεχνολογικά trends, δηλαδή το δρόμο προς το Industry 5.0. Περισσότερη έρευνα λοιπόν θα πρέπει να δωθεί στην αυτοματοποίηση των τεχνολογιών CPS και digital Twin και καλύτερων εργαλείων χειρισμού τους, ώστε μέσω αυτών να βρεθούν κοινές πρακτικές και λύσεις για όλα τα δίκτυα IoT προκειμένου οι συνολικές πληροφορίες να μπορούν να συνδυαστούν συνολικά. Προτείνεται έτσι ουσιαστικά η υιοθέτηση κοινής πρακτικής για όλα τα δίκτυα IoT ώστε να αναφερόμαστε σε digital forensics μεθόδους για το Industry 5.0.

7.1 Παράρτημα

7.1.1 Ορολογίες

Amazon Web Services	(AWS)
Autonomous-Automated-Vehicles	(AAVs) τα λεγόμενα smart cars
Advanced Persistent Threats	(APTs)
Application Programming Interfaces	(APIs)
Body Area Network	(BAN)
Cloud Security Alliance	(CSA)
cloud service providers	(CSP)
Closed-circuit television	(CCTV)
Cross-Device Analysis	(CDA)
Crime-as-a-Service	(CaaS)
Contrast Limited Adaptive Histogram	(CLAHE)
Chain of Custody	(CoC)
Constrained Application Protocol	(CoAP)
Digital Chain of Custody	(DCoC)
Drone Disrupted Denial of Service	(3DOS)
Distributed Denial of Service	(DDoS)
Digital Forensics	(DF)
Digital Forensics-as-a-Service	(DFaaS)
Digital Forensics Readiness	(DFR)
Domain Name System	(DNS)
European Data Protection Board	(EDPB)
Electronically Signed Evidence	(ESE)
Forensics-as-a-Service	(FaaS)
Forensically Relevant Files	(FRF)
Forensically Irrelevant Files	(FIF)
Forensic Feature Extraction	(FFE)
General Data Privacy Regulation	(GDPR)
Google Compute Engine	(GCE)
High-Performance Computing	(HPC)
Internet-of-Things	(IoT)
Internet-of-Vehicle	(IoV)
Infrastructure-as-a-Service	(IaaS)
Internet Service Provider	(ISP)
International Data Corporation	(IDC)
Intrusion Prevention Systems	(IPSs)
Intrusion Detection systems	(IDSs)
Internet of Everything	(IoE)
Information Retrieval	(IR)
Internet of Things and Services	(IoT&S)
IPv6 over Low-Power Wireless Personal Area Network	(6IoWPAN)
Internet Protocol version 6	(IPv6)

In-Vehicle Infotainment	(IVI)
Machine-to-Machine Communication	(M2M)
Message Queuing Telemetry Transport	(MQTT)
National Institute of Standards and Technology	(NIST)
Near-Field Communication	(NFC)
On-board-unit	(OBU)
Personally Identifiable Information	(PII)
Platform-as-a-Service	(PaaS)
Potential Digital Evidence	(PDE)
Person-to-Machine Communication	(P2M)
Person-to-Person Communication	(P2P)
Personally Identifiable Information	(PII)
Quality-of-Service	(QoS)
RoadSite-unit	(RSU)
Real-Time Operating Systems	(RTOS)
Radio-Frequency Identification	(RFID)
Remote Health Monitoring System	(RHMS)
Software-as-a-Service	(SaaS)
Service Level Agreement	(SLA)
Transmission Control Protocol	(TCP)
Unmanned-Aerial-Vehicles	(UAVs) τα λεγόμενα drones του σήμερα ενισχυμένα με τις τεχνολογίες του αύριο (6G enabled drones) καλούνται και UAVs
User Datagram Protocol	(UDP)
Ultra-reliable Machine Type Communication	(u-MTC)
Vehicle-to-Vehicle	(V2V)
Vehicle-to-Infrastructure	(V2I)
Vehicle-to-Home	(V2H)
Vehicle-to-Pedestrian	(V2P)
Vehicle-to-X V2X = V2V + V2I + V2P + V2H	(V2X)
Vehicle-to-Consumer-Electronics	(V2CE)
Virtual Machines	(VMs)
Vehicular Ad-hoc NETwork	(VANET)
Voice over Internet Protocol	(VoIP)
Vehicle-Witness-as-a-Service	(VWaaS)
Wide Area Network.	(WAN)
massive Ultra-reliable Low Latency Communications	(mURLLC)
full-duplex (Terahertz) Communications	(THz)
non-orthogonal multiple access	(NOMA)
millimeter-wave Communications	(mmWave)
optical wireless communication	(OWC)
visible light communication	(VLC)

infrared radiation	(IR)
ultraviolet spectra	(UV)
radiofrequency based wireless communication systems	(RF)
optical camera communication	(OCC)
free-space optical communication	(FSO)
light-fidelity	(Li-Fi)
machine learning	(ML)
reconfigurable intelligent surfaces	(RISs)
multiple-input and multiple-output channel estimation and detection	(MIMO)
Intelligent reflecting surfaces	(IRS)
Screen-to-Camera	(S2C)
content delivery networks	(CDNs)
Industrial IoT	(IIoT)

8. Βιβλιογραφία

[1] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues.” In: IEEE Communications Surveys and Tutorials pp. 1191–1221. doi: 10.1109/COMST.2019.2962586. url: https://doi.org/10.1109/COMST.2019.2962586

[2] Li, S., Ho, F., Karabiyik, U., Rogers, M., Hands, N., & Laux, C. “DIGITAL TRAILS IN VIRTUAL WORLDS: A FORENSIC INVESTIGATION OF VIRTUAL REALITY SOCIAL COMMUNITY APPLICATIONS ON OCULUS PLATFORMS THE PURDUE UNIVERSITY GRADUATE SCHOOL STATEMENT OF COMMITTEE APPROVAL” In: Purdue University (2023)

[3] list of digital forensics tools. (n.d.). https://en.wikipedia.org/wiki/List_of_digital_forensics_tools. (accessed on June 25, 2024)

[4] Kebande, V. R., Karie, N. M., Michael, A., Malapane, S., Kigwana, I., Venter, H. S., & Wario, R. D. “Towards an integrated digital forensic investigation framework for an IoT-based ecosystem”. In: Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018 pp. 93–98. doi: 10.1109/SmartIoT.2018.00-19. url: https://doi.org/10.1109/SmartIoT.2018.00-19

[5] Al-Hawawreh, M., Moustafa, N., & Slay, J. “A threat intelligence framework for protecting smart satellite-based healthcare networks” In: Neural Computing and Applications pp. 15–35. doi: 10.1007/s00521-021-06441-5. url: https://doi.org/10.1007/s00521-021-06441-5

[6] Áine MacDermott, Thar Baker, Qi Shi. “IoT Forensics: Challenges For The IoA Era”. In: 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (2018)

[7] Dominik, O., Miljenko, M., & Marin, V. “Categorizing IoT Services According to Security Risks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering” In: LNICST pp. 154–166. doi: 10.1007/978-3-030-78459-1. url: https://doi.org/10.1007/978-3-030-78459-1_11

[8] Fischer, S., Neubauer, K., & Hackenberg, R. (n.d.). “A Study about the Different Categories of IoT in Scientific Publications” In: CLOUD COMPUTING (2020): The Eleventh International Conference on Cloud Computing, GRIDs, and Virtualization.

[9] Akinbi, A. O. “Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks” In: WIREs Forensic Science (2023). doi: 10.1002/wfs2.1496. url: https://doi.org/10.1002/wfs2.1496

[10] Pan, C., Ren, H., Wang, K., Kolb, J. F., Elkashlan, M., Chen, M., Di Renzo, M., Hao, Y., Wang, J., Swindlehurst, A. L., You, X., & Hanzo, L.. “Reconfigurable Intelligent Surfaces for 6G Systems: Principles, Applications, and Research Directions” In: Proceedings - 2021 IEEE

International Conference. doi: 2011.04300. url: http://arxiv.org/abs/2011.04300
[11] Qatawneh, M., Almobaideen, W., Alkhanafseh, M., al Qatawneh, I., Khanafseh, M., Qatawneh, I. AL, & Al Ain, P. “DFIM: A NEW DIGITAL FORENSICS INVESTIGATION MODEL FOR INTERNET OF THINGS” In: Journal of Theoretical and Applied Information Technology pp. 24-31. doi: 338991085. url: https://www.researchgate.net/publication/338991085
[12] Rondeau, C. M., Temple, M. A., & Lopez, J. “Industrial IoT cross-layer forensic investigation.” In: WIREs Forensic Science. doi: 10.1002/wfs2.1322. url: https://doi.org/10.1002/wfs2.1322
[13] Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. “The industrial internet of things (IIoT): An analysis framework” In: Computers in Industry pp. 1–12. doi: 10.1016/j.compind.2018.04.015. url: https://doi.org/10.1016/j.compind.2018.04.015
[14] Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (n.d.). “Internet of Things Forensics: Challenges and Approaches” In: 9th IEEE International Conference on Collaborative Computing: Networking, Application and Worksharing
[15] Zorić, P., Musa, M., & Kuljanić, T. M. “Smart Factory Environment: Review of Security Threats and Risks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering” In: LNICST pp. 203–214. doi: 10.1007/978-3-030-78459-1_15. url: https://doi.org/10.1007/978-3-030-78459-1_15
[16] OSI-TCP/IP model. (n.d.). https://developer.ibm.com/articles/iot-lp101-connectivity-network-protocols/ (accessed on June 25, 2024)
[17] Hutchinson, S., Yoon, Y. H., Shantaram, N., & Karabiyik, U. (n.d.). “Internet of Things Forensics in Smart Homes: Design, Implementation and Analysis of Smart Home Laboratory.” In: ASEE’S VIRTUAL CONFERENCE June 22-26 (2020)
[18] IoT definition. (n.d.). https://www.oracle.com/internet-of-things/what-is-iot/ (accessed on June 25, 2024)
[19] three and five layer architecture. (n.d.). https://onlinelibrary.wiley.com/doi/10.1155/2017/9324035 (accessed on June 25, 2024)
[20] 4 types of architecture. (n.d.). https://euristiq.com/types-of-iot-networks/#:~:text=IoT%20networks%20can%20be%20categorized,of%20IoT%20networks%20operate%20wirelessly (accessed on June 25, 2024)
[21] Uribe, F. (n.d.). “The classification of Internet of Things (IoT) devices Based on their impact on Living Things” In: 2017 Cybersecurity Predictions
[22] Muyideen AbdulRaheem, Idowu Dauda Oladipo, Alfonso González-Briones, Joseph Bamidele Awotunde, Adekola Rasheed Tomori, Rasheed Gbenga Jimoh. “Chapter 6 - An efficient lightweight speck technique for edge-IoT-based smart healthcare systems” In: 5G IoT and Smart Healthcare 2022

pp. 139-162. doi: 10.1016/B978-0-323-90548-0.00005-X url: https://doi.org/https://doi.org/10.1016/B978-0-323-90548-0.00005-X
[23] Jatin Sharma, Pawan Singh Mehra. “Secure communication in IOT-based UAV networks: A systematic survey” In: Internet of Things Volume 23, October 2023. doi: 10.1016/j.iot.2023.100883. url: https://doi.org/https://doi.org/10.1016/j.iot.2023.100883
[24] Liu, Y., Deng, Y., Elkashlan, M., Nallanathan, A., & Karagiannidis, G. K. “Optimization of Grant-Free NOMA with Multiple Configured-Grants for mURLLC” In: IEEE International Conference 2021. doi: 2111.09284. url: http://arxiv.org/abs/2111.09284
[25] Mahbub, M., & Shubair, R. M. “Analysis of IRS-Assisted NOMA for 6G Wireless Communications” In: Internet of Things 2022. doi: 2211.13045 url: http://arxiv.org/abs/2211.13045
[26] mmWave. (n.d.). https://www.celona.io/5g-lan/5g-mmwave (accessed on June 25, 2024)
[27] Wei Jiang, Fa-Long luo. “Optical and Visible Light Wireless Communications in 6G” In: 6G Key Technologies: A comprehensive Guide. doi: 10.1002/9781119847502.ch6. url: https://doi.org/https://doi.org/10.1002/9781119847502.ch6
[28] Ximenes, L. R., Larêdo, B. D. A., & Laˆredo, B. D. A. “A Tensor-Based Optical Camera Communication (OCC) System With Joint Data Detection and Video Restoration” In: IEEE TRANSACTIONS ON COMMUNICATIONS
[29] Aditi Malik, Preeti Singh. “Free Space Optics: Current Applications and Future Challenges” In: International Journal of Optics. doi: 10.1155/2015/945483. url: https://doi.org/https://doi.org/10.1155/2015/945483
[30] Li-Fi. (n.d.) https://www.symmetryelectronics.com/blog/li-fi-vs-wi-fi/#:~:text=Li%2DFi%20is%20more%20secure,well%20in%20high%2Ddensity%20regions (accessed on June 25, 2024)
[31] Jiaheng Wang, P. “6G Visible Light Communication Technology White Paper” In: China Mobile Research Institute
[32] smart city definition. https://www.ibm.com/topics/smart-city (accessed on June 25, 2024)
[33] wearables. https://www.techtarget.com/searchmobilecomputing/definition/wearable-technology (accessed on June 25, 2024)
[34] Smart Building and/or Facility. https://www.cognizant.com/us/en/glossary/smart-buildings#:~:text=Smart%20buildings%2C%20or%20smart%20facilities,to%20optimize%20the%20facility%27s%20performance (accessed on June 25, 2024)
[35] Jung-SuppUm. “Drones as Cyber-Physical Systems Concepts and Applications for the Fourth Industrial Revolution” In: Kyungpook National

University Daegu Korea Publications. doi: 10.1007/978-981-13-3741-3. url: https://doi.org/10.1007/978-981-13-3741-3

[36] Zhao, S., Li, S., Chen, L., Ding, Y., Zheng, Z., & Pan, G. “ICPS-Car: An intelligent cyber-physical system for smart automobiles” In: Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-IThings-CPSCom pp.818–825. doi: 10.1109/GreenCom-iThings-CPSCom.2013.145. url: https://doi.org/10.1109/GreenCom-iThings-CPSCom.2013.145

[37] Yan, W., & Sakairi, T. “Geo CPS: Spatial challenges and opportunities for CPS in the geographic dimension” In: Journal of Urban Management pp. 331–341. doi: 10.1016/j.jum.2019.09.005. url: https://doi.org/10.1016/j.jum.2019.09.005

[38] Criado, J., Asensio, J. A., Padilla, N., & Iribarne, L. “Integrating cyber-physical systems in a component-based approach for smart homes” In: Sensors (Switzerland). doi: 10.3390/s18072156. url: https://doi.org/10.3390/s18072156

[39] Jāmiʻat Qaṭar. “Cyber Physical Systems and Smart Homes in Healthcare: Current State and Challenges” In: Institute of Electrical and Electronics Engineers 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)

[40] Jóźwiak, L. “Advanced mobile and wearable systems. Microprocessors and Microsystems” In: Microprocessors and Microsystems 2017 pp. 202–221. doi: 10.1016/j.micpro.2017.03.008. url: https://doi.org/10.1016/j.micpro.2017.03.008

[41] Yang, C., Tu, X., Autiosalo, J., Ala-Laurinaho, R., Mattila, J., Salminen, P., & Tammi, K. “Extended Reality Application Framework for a Digital-Twin-Based Smart Crane” In: Applied Sciences (Switzerland). doi: 10.3390/app12126030. url: https://doi.org/10.3390/app12126030

[42] Cao, K., Hu, S., Shi, Y., Colombo, A. W., Karnouskos, S., & Li, X. “A Survey on Edge and Edge-Cloud Computing Assisted Cyber-Physical Systems” In: IEEE Transactions on Industrial Informatics pp. 7806–7819. doi: 10.1109/TII.2021.3073066. url: https://doi.org/10.1109/TII.2021.3073066

[43] Tristan, S., Sharma, S., & Gonzalez, R. “Alexa/Google Home Forensics” In: Studies in Big Data pp. 101–121. doi: 10.1007/978-3-030-23547-5_7. url: https://doi.org/10.1007/978-3-030-23547-5_7

[44] Awasthi, A., Read, H. O. L., Xynos, K., & Sutherland, I. “Welcome pwn: Almond smart home hub forensics” In: Proceedings of the Digital Forensic Research Conference. doi: 10.1016/j.diin.2018.04.014. url: https://doi.org/10.1016/j.diin.2018.04.014

[45] Nasos Grigoropoulos, Spyros Lalis “Simulation and Digital Twin Support for Managed Drone Applications” In: 2020 IEEE/ACM 24th International Symposium on Distributed Simulation and Real Time Applications (DS-RT). (2020).

[46] Bhatti, G., Mohan, H., & Raja Singh, R. “Towards the future of smart electric vehicles: Digital twin technology” In: Renewable and Sustainable Energy Reviews (Vol. 141) Elsevier Ltd. doi: 10.1016/j.rser.2021.110801. url: https://doi.org/10.1016/j.rser.2021.110801
[47] Sabatini, R., Gardi, A., Qiao, G., Zhuang, Y., Ye, T., & Qiao, Y. “A Digital-Twin-Based Detection and Protection Framework for SDC-Induced Sinkhole and Grayhole Nodes in Satellite Networks” In: Aerospace 2023. doi: 10.3390/aerospace. url: https://doi.org/10.3390/aerospace
[48] Bouchabou, D., Grosset, J., Nguyen, S. M., Lohr, C., & Puig, X. “A Smart Home Digital Twin to Support the Recognition of Activities of Daily Living” In Sensors, 23. doi: 10.3390/s23177586. url: https://doi.org/10.3390/s23177586
[49] Kim, T. “Cps modeling for smart factory implementation” In: ICIC Express Letters, Part B: Applications pp.1099–1105. doi: 10.24507/icicelb.10.12.1099. url: https://doi.org/10.24507/icicelb.10.12.1099
[50] Kamath, V., Morgan, J., & Ali, M. I. “Industrial IoT and Digital Twins for a Smart Factory : An open source toolkit for application design and benchmarking” In: GIoTS 2020 - Global Internet of Things Summit, Proceedings. doi: 10.1109/GIOTS49054.2020. 9119497. url: https://doi.org/10.1109/GIOTS49054.2020. 9119497
[51] Volkov, I., Radchenko, G., & Tchernykh, A. “Digital Twins, Internet of Things and Mobile Medicine: A Review of Current Platforms to Support Smart Healthcare” In: Programming and Computer Software pp. 578–590. doi: 10.1134/S0361768821080284. url: https://doi.org/10.1134/S0361768821080284
[52] Zhu, Z., & Zhong, R. Y. “A digital twin enabled wearable device for customized healthcare” In: Digital Twin, 2017. doi: 10.12688/digitaltwin.17717.1. url: https://doi.org/10.12688/digitaltwin.17717.1
[53] Stacchio, L., Angeli, A., & Marfia, G. “Empowering Digital Twins with eXtended Reality Collaborations” In: Virtual Reality and Intelligent Hardware pp. 487–505. doi: 10.1016/j.vrih.2022.06.004. url: https://doi.org/10.1016/j.vrih.2022.06.004
[54] Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. “Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks” In: IEEE Transactions on Industrial Informatics pp. 5098–5107. doi: 10.1109/TII.2020.3017668. url: https://doi.org/10.1109/TII.2020.3017668
[55] Nguyen, H. X., Trestian, R., To, D., & Tatipamula, M. “Digital Twin for 5G and beyond” In: IEEE Communications Magazine pp. 10–15. doi: 10.1109/MCOM.001.2000343. url: https://doi.org/10.1109/MCOM.001.2000343
[56] Tariq, M., Ali, M., Naeem, F., & Poor, H. V. “Vulnerability assessment of 6g-enabled smart grid cyber-physical systems” In: IEEE Internet of Things

Journal pp. 5468–5475. doi: 10.1109/JIOT.2020.3042090. url: https://doi.org/10.1109/JIOT.2020.3042090

[57] Goudbeek, A., Choo, K. K. R., & Le-Khac, N. A. “A Forensic Investigation Framework for Smart Home Environment. Proceedings” In: 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering pp.1446–1451. doi: 10.1109/TrustCom/BigDataSE.2018.00201. url: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00201

[58] Kebande, V. R. “Industrial internet of things (IIoT) forensics: The forgotten concept in the race towards industry 4.0” In: Forensic Science International: Reports. doi: 10.1016/j.fsir.2022.100257. url: https://doi.org/10.1016/j.fsir.2022.100257

[59] Yang, L., Naser, S., Shami, A., Muhaidat, S., Ong, L., Debbah, M., Member, S., & Debbah, M. “Towards Zero Touch Networks: Cross-Layer Automated Security Solutions for 6G Wireless Networks” In: IEEE Conferences 2021. doi: 10.36227/techrxiv.23971707.v1. url: https://doi.org/10.36227/techrxiv.23971707.v1

[60] Baig, Z., Khan, M. A., Mohammad, N., & Brahim, G. Ben. “Drone Forensics and Machine Learning: Sustaining the Investigation Process” In: Sustainability (Switzerland) (Vol. 14). MDPI. doi: 10.3390/su14084861. url: https://doi.org/10.3390/su14084861

[61] Alotaibi, F. M., Al-Dhaqm, A., Al-Otaibi, Y. D., & Alsewari, A. A. “A Comprehensive Collection and Analysis Model for the Drone Forensics Field” In: Sensors, 22(17). doi: 10.3390/s22176486. url: https://doi.org/10.3390/s22176486

[62] Feng, X., Dawam, E. S., & Amin, S. “A New Digital Forensics Model of Smart City Automated Vehicles” In: Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, IThings-GreenCom-CPSCom-SmartData 2017, 2018-January, pp. 274–279. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.47. url: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.47

[63] Feng, X., Dawam, E. S., & Li, D. “Autonomous vehicles’ forensics in smart cities. Proceedings” In: 2019 IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Internet of People and Smart City Innovation, SmartWorld/UIC/ATC/SCALCOM/IOP/SCI 2019 pp. 1688–1694. doi: 10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00301. url: https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00301

[64] Yaqoob, I., Hashem, I. A. T., Ahmed, A., Kazmi, S. M. A., & Hong, C. S. “Internet of things forensics: Recent advances, taxonomy, requirements,

and open challenges” In: Future Generation Computer Systems pp. 265–275. doi: 10.1016/j.future.2018.09.058. url: https://doi.org/10.1016/j.future.2018.09.058