ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη των απειλών και προκλήσεων σε θέματα ασφάλειας του Διαδικτύου των Πραγμάτων (IoT) στον τομέα της υγείας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΤΕΝΕΚΕΤΖΟΓΛΟΥ ΔΗΜΗΤΡΑΣ

(ΑΕΜ: 2222)

Επιβλέπων: **Νικολάου Σπυρίδων**

Λέκτορας

Καστοριά Δεκέμβριος - 2021

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη των απειλών και προκλήσεων σε θέματα ασφάλειας του Διαδικτύου των Πραγμάτων (IoT) στον τομέα της υγείας

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

της

ΤΕΝΕΚΕΤΖΟΓΛΟΥ ΔΗΜΗΤΡΑΣ

(ΑΕΜ: 2222)

Επιβλέπων: **Νικολάου Σπυρίδων**

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 17/12/2021

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδιότητα Μέλους	Ιδιότητα Μέλους	Ιδιότητα Μέλους

Καστοριά Δεκέμβριος - 2021

Ευχαριστίες

Θα ήθελα να εκφράσω τις ευχαριστίες μου σε όλους όσους συνέβαλαν στην πραγματοποίηση της παρούσας πτυχιακής εργασίας. Αρχικά, θέλω να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή μου, κύριο Νικολάου Σπυρίδωνα, για την πολύτιμη βοήθεια, τις συμβουλές του και την καθοδήγηση που μου παρείχε σε όλα τα στάδια συγγραφής αυτής της εργασίας. Επιπλέον, οφείλω να ευχαριστήσω την οικογένεια μου που με στήριξε με κάθε δυνατό τρόπο όλα αυτά τα χρόνια και ιδιαίτερα τον αδερφό μου Αλέξανδρο για την ηθική στήριξη και την αμέριστη συμπαράσταση του.

Περίληψη

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) εξελίσσεται συνεχώς και συγκεντρώνει αυξανόμενο ενδιαφέρον από την επιστημονική κοινότητα, καθώς είναι μια αναδυόμενη τεχνολογία η οποία αναμένεται να επιφέρει ριζικές αλλαγές στον σύγχρονο τρόπο ζωής. Η ραγδαία αυτή ανάπτυξή του έχει ως συνέπεια την επέκταση της εφαρμογής του σε ολοένα και περισσότερους τομείς της ανθρώπινης δραστηριότητας. Ανάμεσα στις διάφορες εφαρμογές του Διαδικτύου των Πραγμάτων, ενδιαφέρον παρουσιάζει αυτή στον τομέα της Υγειονομικής Περίθαλψης, εξαιτίας των καινοτόμων λύσεων που προσφέρει στα διαχρονικά προβλήματα του συμβατικού συστήματος υγείας, εκσυγχρονίζοντας και αυτοματοποιώντας πλήθος διαδικασιών.

Η ασφάλεια σε αυτά τα εξελιγμένα συστήματα ανάγεται σε μείζον θέμα, διότι διακινούνται ευαίσθητα ιατρικά δεδομένα και διακυβεύονται πολύτιμα αγαθά, όπως η ανθρώπινη υγεία και ζωή, ωστόσο η πολυπλοκότητα των συστημάτων αυτών οδηγεί κατά κανόνα σε σύνθετες ανάγκες ασφαλείας. Πλήθος ερευνών και μελετών έχουν αναδείξει ζητήματα τέτοιας φύσεως και τις προκλήσεις που πρέπει να ξεπεραστούν για την υιοθέτηση του Διαδικτύου των Πραγμάτων σε μεγάλη κλίμακα.

Στην παρούσα πτυχιακή εργασία επιχειρείται ο εντοπισμός και η ανάλυση των βασικότερων απειλών και προκλήσεων ασφαλείας που σχετίζονται με την ενσωμάτωση του Διαδικτύου των Πραγμάτων στον τομέα της υγείας και την εύρυθμη λειτουργία αυτού του περιβάλλοντος. Επίσης αναλύονται οι βασικότερες επιθέσεις ασφαλείας που μπορούν δυνητικά να πλήξουν αυτά τα συστήματα, ενώ γίνεται προσπάθεια ανάδειξης των πιθανών στόχων, των επιπτώσεων και των μεθόδων εξαπόλυσης της κάθε επίθεσης. Τέλος, γίνεται αναφορά σε πιθανά μέτρα αντιμετώπισης των απειλών ασφαλείας, με σημεία έμφασης την αποτελεσματικότητα, την καταλληλότητα και τη συνεισφορά του κάθε μέτρου.

Λέξεις κλειδιά: *Διαδίκτυο των Πραγμάτων, Υγειονομική Περίθαλψη, Ασφάλεια, Απειλές, Προκλήσεις, Επιθέσεις, Αντίμετρα*

Abstract

The internet of things (IoT) is constantly evolving and is gaining increasing interest among the scientific community, as it is an emerging technology that is expected to induce radical changes to the present-day way of life.

This rapid development has resulted in the expansion of its application to progressively more fields of human activity. Among the various applications of the internet of things, one particularly noteworthy is that in the field of Healthcare, due to the innovative solutions it offers to the long-standing problems of the conventional health system through the modernization and automation of a multitude of procedures.

Security in these advanced systems has emerged as a major issue, because of the sensitive medical data being handled and since values of paramount importance, such as human health and life, are at stake, however, the complexity of these systems typically leads to multiplex security needs. Numerous researches and studies have highlighted issues of this nature and the challenges that need to be overcome for the implementation of the internet of things on a large scale.

This thesis attempts to identify and analyze the principal security threats and challenges that pertain to the integration of the internet of things in the field of Healthcare and the proper functioning of this environment. Moreover, the main security attacks that can potentially impact these systems are analyzed as well, with the main focus being on highlighting the possible targets, repercussions and methods of launching each attack. Finally, a number of possible measures to address security threats are also examined, with emphasis on the effectiveness, suitability and contribution of each measure.

Key words: *Internet of Things (IoT), Healthcare, Security, Threats, Challenges, Attacks, Countermeasures*

Περιεχόμενα

Λίστα Εικόνων

Λίστα Πινάκων

Εισαγωγή

Το Διαδίκτυο των Πραγμάτων διεισδύει όλο και περισσότερο στον κλάδο της υγειονομικής περίθαλψης αναδεικνύοντας ως ζήτημα υψίστης σημασίας τη διαφύλαξη των ιατρικών δεδομένων των ασθενών. Στα πλαίσια αυτής της εργασίας μελετώνται και αναλύονται θέματα ασφάλειας του IoT σε αυτόν τον τομέα.

Το πρώτο κεφάλαιο έχει στόχο την εισαγωγή του αναγνώστη στο αντικείμενο της εργασίας και αποτελεί το γενικότερο θεωρητικό και τεχνικό υπόβαθρο στο οποίο στηρίζεται η υπόλοιπη εργασία. Αρχικά παρατίθενται κάποιοι από τους ορισμούς που έχουν αποδοθεί στο IoT διαχρονικά. Ακολουθεί μια σύντομη ανασκόπηση ορισμένων κρίσιμων γεγονότων και εξελίξεων που οδήγησαν στην ανάπτυξη του IoT τόσο ως ιδέα όσο και ως τεχνολογία. Στα πλαίσια του πρώτου κεφαλαίου επίσης περιγράφεται ο βασικός τρόπος λειτουργίας του IoT, ενώ γίνεται αναφορά στα δομικά του συστατικά και την αρχιτεκτονική του. Την εξοικείωση του αναγνώστη με την τεχνική διάσταση του αντικειμένου συμπληρώνει η συνοπτική παρουσίαση των πρωτοκόλλων και των προτύπων που διέπουν το IoT. Επιπλέον, σημειώνονται κάποια βασικά χαρακτηριστικά του IoT. Τέλος, για τη σφαιρική κατανόηση των πλεονεκτημάτων και των νέων δυνατοτήτων που προσφέρει η καινοτόμος αυτή τεχνολογία, επισημαίνονται οι διάφοροι τομείς της ανθρώπινης δραστηριότητας στους οποίους εφαρμόζεται.

Το επόμενο κεφάλαιο πραγματεύεται πιο συγκεκριμένα την εφαρμογή του IoT στον τομέα της υγείας (Internet of Health Things - IoHT). Στόχος σε αυτό το στάδιο της εργασίας είναι η ανάδειξη της ιδιάζουσας φύσης και σημασίας του IoHT. Μετά από μία σύντομη εισαγωγή στο IoHT, αναφέρονται οι αρχές λειτουργίας του και έπειτα παρουσιάζεται μία από τις βασικότερες αρχιτεκτονικές που χρησιμοποιούνται για την περιγραφή τέτοιων συστημάτων. Επιπροσθέτως, αναλύονται οι σημαντικότερες τεχνολογίες που απαρτίζουν το IoHT ή μπορούν να αξιοποιηθούν σε αυτό το περιβάλλον και αναφέρονται οι επιμέρους υπηρεσίες και εφαρμογές του. Η ενότητα ολοκληρώνεται με την υπογράμμιση των κυριότερων πλεονεκτημάτων που έχει να επιδείξει η χρήση του IoHT έναντι του συμβατικού συστήματος υγείας, αλλά και των προκλήσεων που χρήζουν άμεσης αντιμετώπισης.

Στο τρίτο κεφάλαιο μελετώνται ζητήματα που άπτονται του θέματος της εργασίας, δηλαδή ζητήματα ασφαλείας του IoHT. Εισαγωγικά επισημαίνεται η σημασία της ασφάλειας στα περιβάλλοντα του IoT γενικότερα και τεκμηριώνεται η θέση πως στην περίπτωση του IoHT η ασφάλεια αποκτά αυξημένη βαρύτητα. Στη συνέχεια παρατίθενται ενδεικτικά ορισμένες απαιτήσεις ή αρχές ασφαλείας, όπως η τριάδα CIA, τις οποίες οφείλει να πληροί ένα υπολογιστικό σύστημα και κατά επέκταση και το IoHT, ώστε να θεωρείται ασφαλές. Έχοντας λάβει γνώση περί των βασικών αυτών αρχών ο αναγνώστης είναι πλέον σε θέση να αντιληφθεί τη φύση και τη διάσταση των προκλήσεων ασφαλείας του IoHT, διεξοδική ανάλυση των οποίων ακολουθεί. Οι

απειλές και οι επιθέσεις αποτελούν το τελευταίο αντικείμενο μελέτης της συγκεκριμένης ενότητας, οι μεν απειλές διακρίνονται με βάση τις επιπτώσεις που μπορούν να επιφέρουν στους κύριους πόρους ενός υπολογιστικού συστήματος και οι δε επιθέσεις ομαδοποιούνται με γνώμονα το επίπεδο αρχιτεκτονικής όπου λαμβάνουν χώρα. Ταυτόχρονα, καταβάλλεται προσπάθεια εντοπισμού του στόχου, του κινήτρου και των πιθανών επιβλαβών συνεπειών της κάθε επίθεσης.

Στο τέταρτο και τελευταίο κεφάλαιο της εργασίας το ενδιαφέρον επικεντρώνεται στην αντιμετώπιση των απειλών και των επιθέσεων ασφαλείας. Αρχικά περιγράφονται τα διάφορα στάδια της διαδικασίας εκτίμησης κινδύνων (security risk assessment), μιας πρακτικής που διαδραματίζει σημαντικό ρόλο στη διάγνωση πιθανών κενών ασφαλείας, τον προσδιορισμό τρόπων αξιοποίησης τους και τις ενδεχόμενες επιπτώσεις αυτών. Επίσης, γίνεται αναφορά στη δοκιμή διείσδυσης (penetration testing) η οποία εφαρμόζεται συμπληρωματικά με την παραπάνω διαδικασία για τη λήψη εγκυρότερων αποτελεσμάτων. Στα πλαίσια του κεφαλαίου αυτού επιπλέον εξετάζεται η βιωσιμότητα συχνά προτεινόμενων λύσεων ασφαλείας (συστήματα IDS, IPS και SIEM), τα οποία χρησιμοποιούνται ευρέως στα συμβατικά συστήματα. Επιπροσθέτως, επιχειρείται μια μελέτη ορισμένων τεχνικών και μηχανισμών ασφαλείας που προτείνονται στη διεθνή βιβλιογραφία, εστιάζοντας στο κατά πόσο αυτά τα μέτρα αντιμετώπισης επαρκούν για τη διαφύλαξη συστημάτων IoHT.

Τέλος, διατυπώνονται τα συμπεράσματα της παρούσας εργασίας και κάποιες προτάσεις μελλοντικής επέκτασής της.

1. ΕΙΣΑΓΩΓΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (INTERNET OF THINGS - IOT)

1.1. Ορισμός IoT

Ο όρος Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) επινοήθηκε και χρησιμοποιήθηκε πρώτη φορά από τον Kevin Ashton το 1999 [1]. Στην προσπάθεια να αποδοθεί σαφής ορισμός του όρου, πολλές ομάδες επιστημόνων και ερευνητών κατά καιρούς έχουν δημοσιεύσει τους δικούς τους ορισμούς. Αλλά παρόλο που το IoT έχει αποκτήσει ιδιαίτερα μεγάλη φήμη δεν υφίσταται μέχρι τώρα ένας μοναδικός, κοινός ορισμός που να το περιγράφει. Μερικοί από τους πιο δημοφιλείς ορισμούς που του έχουν αποδοθεί είναι οι εξής:

- «Το Διαδίκτυο των Πραγμάτων αναφέρεται στη διασύνδεση έξυπνων αντικειμένων IP, όπως αισθητήρες και ενεργοποιητές.» [2]

- «Διαδίκτυο των Πραγμάτων (IoT): Μία παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που επιτρέπει προηγμένες υπηρεσίες διασυνδέοντας (φυσικά και εικονικά) πράγματα με βάση τις υπάρχουσες και εξελισσόμενες διαλειτουργικές τεχνολογίες πληροφοριών και επικοινωνιών.» [3]

- «Το IoT είναι ένα δίκτυο που συνδέει μοναδικός αναγνωρίσιμα “Πράγματα” στο Διαδίκτυο. Τα “Πράγματα” έχουν δυνατότητες αισθητήρα/ενεργοποιητή και παρέχουν τη δυνατότητα προγραμματισμού τους. Μέσω της αξιοποίησης της μοναδικής ταυτοποίησης και ανίχνευσης, μπορούν να συλλεχθούν πληροφορίες σχετικά με το “Πράγμα” και η κατάσταση αυτού μπορεί να αλλάξει από οπουδήποτε, οποτεδήποτε και από οτιδήποτε.» [4]

- «Διαδίκτυο των Πραγμάτων: Η διασύνδεση μέσω Διαδικτύου, υπολογιστικών συσκευών ενσωματωμένων σε καθημερινά αντικείμενα, που τους επιτρέπει να στέλνουν και να λαμβάνουν δεδομένα.» [5]

- «Το Διαδίκτυο των πραγμάτων (IoT) είναι το δίκτυο φυσικών αντικειμένων που περιέχουν ενσωματωμένη τεχνολογία για να επικοινωνούν και να αισθάνονται ή να αλληλεπιδρούν με τις εσωτερικές τους καταστάσεις ή το εξωτερικό περιβάλλον.» [6]

Οι ορισμοί οι οποίοι αναφέρθηκαν παραπάνω δεν παρουσιάζουν σημαντική απόκλιση σχετικά με την έννοια του IoT, απλώς την εξετάζουν υπό διαφορετικό πρίσμα τονίζοντας κάποια βασικά χαρακτηριστικά της αντίστοιχης τεχνολογίας,

χρησιμοποιώντας όμως εμφανώς διαφορετική διατύπωση. Αυτό έχει ως αποτέλεσμα είτε τη γενίκευση είτε σε διαφορετική περίπτωση την εξειδίκευση του όρου.

1.2. Ιστορική Αναδρομή IoT

Σήμερα πια το IoT αποτελεί ένα τεχνολογικό άλμα το οποίο βρίσκεται σε διαρκή εξέλιξη, ωστόσο η ανάπτυξή του, τόσο ως ιδέα, όσο και σε πρακτικό επίπεδο, έχει τις ρίζες της αρκετά χρόνια πριν, στο παρελθόν. Στα πλαίσια αυτής της μελέτης θεωρείται σκόπιμο να αναφερθούν συνοπτικά τα ορόσημα-σταθμοί που κατέστησαν την ιδέα του IoT πραγματοποιήσιμη.

1.2.1. Η δημιουργία του Διαδικτύου (Internet)

Ένα θεμελιώδες συστατικό στοιχείο του IoT όπως γίνεται εύκολα αντιληπτό από τον τίτλο του είναι το Διαδίκτυο (Internet) το οποίο οφείλει την ύπαρξή του στη δημιουργία του δικτύου ARPANET (Advanced Research Projects Agency Network) το 1969, από το Υπουργείο Άμυνας των ΗΠΑ. Αυτό το δίκτυο ARPANET αποτέλεσε την πρώιμη μορφή του Διαδικτύου και διατέθηκε αποκλειστικά για ακαδημαϊκή και ερευνητική χρήση. Ακολούθησαν διάφορες τεχνολογικές εξελίξεις στον τομέα της πληροφορικής οι οποίες συνεισέφεραν στο να λάβει το Διαδίκτυο τη σημερινή του μορφή και να εξαπλωθεί με ταχείς ρυθμούς σε όλο τον κόσμο.

Μία καθοριστική εξέλιξη ήταν η καθιέρωση της οικογένειας πρωτοκόλλων TCP/IP (Transmission Control Protocol/Internet Protocol) ως βασικό πρότυπο που διέπει τα πρωτόκολλα διασύνδεσης, διευθυνσιοδότησης και μεταφοράς δεδομένων στο ARPANET. Η 1^{η} Ιανουαρίου του 1983 ορίστηκε ως η ημέρα κατάργησης του προγενέστερου πρωτοκόλλου NCP (Network Control Protocol) και σήμανε την ολοκλήρωση της μετάβασης στο νέο πρωτόκολλο TCP/IP. Ένα από τα κύρια πλεονεκτήματα της χρήσης της οικογένειας πρωτοκόλλων TCP/IP ήταν ότι πρόσφερε συμβατότητα μεταξύ διαφορετικών δικτύων.

Σημαντική εξέλιξη επίσης αποτέλεσε η δημιουργία του δικτύου NSFNET το 1985, το οποίο βασίστηκε στο TCP/IP και χάρη στη ραγδαία εξάπλωσή του σε πολλές χώρες οδήγησε στην απόσυρση του ARPANET το 1990. Τότε άρχισε να χρησιμοποιείται πιο εντατικά ο όρος Διαδίκτυο. Η εμπορική του χρήση γινόταν προοδευτικά διαθέσιμη με την άρση κάποιων περιορισμών και με τη δημιουργία των Παρόχων Υπηρεσιών Διαδικτύου (Internet Service Providers - ISPs), οι οποίοι πρόσφεραν στους χρήστες τους τη δυνατότητα να συνδέονται στο Διαδίκτυο έναντι κάποιου χρηματικού ποσού. Κάθε περιορισμός χρήσης του Διαδικτύου έπαψε τελικά να ισχύει το 1995 με την κατάργηση του NSFNET και τη μετατροπή του για εμπορική χρήση.

Το Διαδίκτυο παρόλα αυτά γνώρισε μεγαλύτερη δημοτικότητα μετά τη δημιουργία της υπηρεσίας του Παγκόσμιου Ιστού WWW (World Wide Web) το 1989 από τον

επιστήμονα Tim Berners-Lee στο CERN της Ελβετίας. Η υπηρεσία αυτή διατέθηκε δωρεάν για γενική χρήση το 1993 και αποτελεί την πιο δημοφιλή υπηρεσία του Διαδικτύου μέχρι σήμερα.

1.2.2. Η γέννηση του IoT

Μπορεί ο όρος Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) να πρωτοεμφανίστηκε το 1999, ωστόσο η ιδέα της διασύνδεσης κάποιας συσκευής πέραν των υπολογιστών με το Διαδίκτυο, που μπορεί να χαρακτηριστεί ως η απαρχή της ιδέας του IoT, υπήρχε ήδη δεκαετίες πριν την επινόηση του όρου. Στη συνέχεια παρουσιάζονται κάποια από τα πιο αξιοσημείωτα επιτεύγματα και γεγονότα, τα οποία έθεσαν τη βάση για τη γέννηση και εξέλιξη του IoT.

Ένα χαρακτηριστικό παράδειγμα εφαρμογής αυτής της πρωταρχικής ιδέας αποτελεί η σύνδεση ενός αυτόματου πωλητή αναψυκτικών με το ARPANET. Πιο συγκεκριμένα το 1982 μια ομάδα φοιτητών του Πανεπιστημίου Carnegie Mellon που εδρεύει στο Πίτσμπουργκ της Πενσυλβάνια, θέλησε να συνδέσει το μηχάνημα αυτόματης πώλησης αναψυκτικών που υπήρχε στο πανεπιστήμιο, με τον κεντρικό υπολογιστή του Τμήματός τους, έτσι ώστε να μπορούν να ελέγχονται τα περιεχόμενα του μηχανήματος εξ' αποστάσεως. Αυτή η ιδέα επιτεύχθηκε με τη χρήση κατάλληλου λογισμικού, με την τοποθέτηση μικροαισθητήρων στο μηχάνημα καθώς και με τη σύνδεσή του στο τοπικό δίκτυο του Πανεπιστημίου. Έτσι όποιος μπορούσε να συνδεθεί στο ARPANET ή στο τοπικό δίκτυο του Πανεπιστήμιου μπορούσε επίσης να έχει πρόσβαση σε πληροφορίες σχετικά με το εν λόγω μηχάνημα και να ενημερωθεί για τη διαθεσιμότητα κρύων αναψυκτικών. Θεωρείται ως η πρώτη συσκευή που συνδέθηκε στο Διαδίκτυο και από αυτήν εμπνεύστηκαν πολλοί εφευρέτες, ώστε να δημιουργήσουν τις δικές τους συνδεδεμένες συσκευές.

Το 1988 ο Mark Weiser, που εργαζόταν στο ερευνητικό κέντρο της εταιρείας Xerox στο Palo Alto της Καλιφόρνια, εισήγαγε τον όρο πανταχού παρούσα υπολογιστική (ubiquitous computing) για να περιγράψει ένα μέλλον στο οποίο οι ηλεκτρονικοί υπολογιστές θα ενσωματώνονται σε αντικείμενα καθημερινής χρήσης και θα γίνονται αόρατοι για τον άνθρωπο. Επίσης το 1991 σε ένα άρθρο του [7] που δημοσιεύθηκε στο επιστημονικό περιοδικό Scientific American με τίτλο "The Computer for the 21st Century" ο ίδιος αναφέρει πως:

«Εξειδικευμένα στοιχεία υλικού και λογισμικού, που συνδέονται με καλώδια, ραδιοκύματα και υπέρυθρες, θα είναι τόσο πανταχού παρόντα που κανείς δεν θα παρατηρήσει την παρουσία τους.»

Σύμφωνα με μια διαδεδομένη άποψη η πρώτη συσκευή IoT κατασκευάστηκε μόλις το 1990. Ο John Romkey σε συνεργασία με τον Simon Hackett δημιούργησαν την πρώτη φρυγανιέρα που μπορούσε να τεθεί σε λειτουργία ή να απενεργοποιηθεί μέσω της σύνδεσής της στο Διαδίκτυο. Πρόκειται για την Sunbeam Deluxe Automatic Radiant

Control Toaster στην οποία πρόσθεσαν δυνατότητα δικτύωσης. Η συσκευή υποστήριζε σύνδεση στο Διαδίκτυο με βάση το μοντέλο δικτύωσης TCP/IP. Παρόλα αυτά ήταν απαραίτητο ο χρήστης να εισάγει τις φέτες ψωμιού στις ειδικές θέσεις κάτι το οποίο οι δημιουργοί θέλησαν να αλλάξουν. Έτσι λοιπόν έναν χρόνο αργότερα το 1991 προστέθηκε στη συσκευή ένας ρομποτικός γερανός ο οποίος ήταν διαχειρίσιμος χάρη στη σύνδεσή του στο Διαδίκτυο και τοποθετούσε τις φέτες ψωμιού στις κατάλληλες υποδοχές. Με αυτήν την προσθήκη επιτεύχθηκε η από άκρη-σε-άκρη αυτοματοποίηση του συστήματος.

Το 1993 στο εργαστήριο υπολογιστών Trojan Room του Πανεπιστημίου του Cambridge της Αγγλίας, ο Quentin Stafford-Fraser και ο Paul Jardetzky δημιούργησαν το Trojan Room Coffee Pot [8], μια καφετιέρα που παρακολουθούνταν από μια κάμερα συνδεδεμένη με το τοπικό δίκτυο. Αυτή η κάμερα ελεγχόταν από μία εφαρμογή διακομιστή που παρατηρούσε το δοχείο καφέ και λάμβανε εικόνες του αρκετές φορές το λεπτό. Στη συνέχεια, οι εικόνες αυτές στέλνονταν στην εφαρμογή πελάτη, ώστε να ενημερώνεται ο χρήστης σχετικά με το εάν το δοχείο της καφετιέρας ήταν γεμάτο ή όχι [9].

Το 1995 στο Πανεπιστήμιο της Νότιας Καλιφόρνιας κατασκευάζεται το Telegarden, μια εγκατάσταση που περιλάμβανε έναν κήπο μικρών διαστάσεων και έναν ρομποτικό βραχίονα εξοπλισμένο με μια κάμερα, ο οποίος με βάση τις εντολές που λάμβανε μπορούσε να εκτελέσει κάποιες συγκεκριμένες ενέργειες για την ανάπτυξη φυτών και τη διαμόρφωση του κήπου. Οι χρήστες του Διαδικτύου, μέσω της πρόσβασης στην αντίστοιχη ιστοσελίδα που είχε σχεδιαστεί για αυτήν την εγκατάσταση, μπορούσαν να χειριστούν εξ’ αποστάσεως τον ρομποτικό βραχίονα, ώστε να φυτέψουν σπόρους, να τους ποτίσουν και να παρακολουθήσουν την εξέλιξη των φυτών. Το 1996 το Telegarden μεταφέρθηκε στο Κέντρο Ars Electronica στην Αυστρία όπου παρέμεινε συνδεδεμένο στο Διαδίκτυο μέχρι την απενεργοποίησή του τον Αύγουστο του 2004.

Όπως προαναφέρθηκε, ο Kevin Ashton επινόησε τον όρο «Internet of Things» το 1999 και τον χρησιμοποίησε ως τίτλο σε μία παρουσίασή του στην εταιρία Procter&Gamble (P&G) [1]. Στα πλαίσια της παρουσίασης αυτής συνδύασε την τεχνολογία ταυτοποίησης μέσω ραδιοσυχνοτήτων RFID (Radio Frequency Identification), που χρησιμοποιούνταν στην εφοδιαστική αλυσίδα της εταιρίας, με το εξαιρετικά επίκαιρο θέμα εκείνης της εποχής, το Διαδίκτυο. Η τεχνολογία RFID έμελλε να γίνει μία από τις σημαντικότερες τεχνολογίες στις οποίες θα βασιζόταν το IoT.

Ως τώρα οι εφευρέσεις οι οποίες αναφέρθηκαν δεν απευθύνονταν στο καταναλωτικό κοινό και είχαν πειραματικό χαρακτήρα. Ωστόσο η μαζική παραγωγή συσκευών IoT δεν άργησε να έρθει. Από τα τέλη της δεκαετίας του 1990 με αρχές του 2000 ξεκίνησε η κατασκευή και η εμπορική διάθεση έξυπνων συστημάτων και συσκευών, που έβρισκαν χρήση στο περιβάλλον ενός σπιτιού και είχαν στόχο τη βελτίωση του τρόπου ζωής.

Σημείο αναφοράς είναι η παρουσίαση του LG Internet Digital DIOS, του πρώτου Ψυγείου στον κόσμο με δυνατότητα σύνδεσης στο Διαδίκτυο που κατασκεύασε η εταιρία LG το 2000. Υποστήριζε σύνδεση τοπικού δικτύου μέσω θύρας LAN και πρόσφερε πλήθος υπηρεσιών όπως, ενημέρωση σχετικά με την κατάσταση των αποθηκευμένων τροφίμων, μέχρι βιντεοκλήσεις και πλοήγηση στο Διαδίκτυο. Όμως δεν είχε απήχηση στο αγοραστικό κοινό, κυρίως λόγω της υψηλής του τιμής και έτσι οι χαμηλές πωλήσεις που κατέγραψε οδήγησαν στην παύση της παραγωγής του. Στη συνέχεια αναπτύχθηκαν προϊόντα πιο προσιτά στον καταναλωτή και η ιδέα του έξυπνου σπιτιού άνοιξε τον δρόμο για τη διάδοση και εφαρμογή του IoT στην καθημερινότητα των ανθρώπων.

Από το 2004 και ύστερα ο όρος IoT αποκτά πιο ευρεία χρήση, καθώς κάνει την εμφάνισή του σε άρθρα γνωστών εφημερίδων, σε επιστημονικά περιοδικά αλλά και σε τίτλους βιβλίων. Η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union - ITU) δημοσίευσε το 2005 μία από τις πρώτες αναφορές σχετικά με το IoT με τίτλο “The Internet of Things” [10], στην οποία παρουσιάζονται οι τεχνολογίες οι οποίες επιτρέπουν τη δημιουργία του, ο τρόπος που αυτές διαμορφώνουν την αγορά, τα οφέλη και οι ευκαιρίες που προσφέρουν, καθώς και ορισμένες αναδυόμενες προκλήσεις.

Το πρώτο διεθνές συνέδριο για το Διαδίκτυο των Πραγμάτων πραγματοποιήθηκε το 2008 στη Ζυρίχη με τίτλο «IOT 2008» και σημείωσε μεγάλη επιτυχία. Επίσης, το ίδιο έτος συγκροτήθηκε η IPSO Alliance, μια μη κερδοσκοπική οργάνωση στην οποία συμμετείχαν εταιρίες, επιστήμονες και ερευνητές από τον χώρο της τεχνολογίας και των επικοινωνιών και είχε ως στόχο τη διάδοση της χρήσης του Πρωτοκόλλου Διαδικτύου (IP) στην επικοινωνία μεταξύ των έξυπνων αντικειμένων (Smart Objects). Επιπλέον, με την υλοποίηση καινοτόμων ιδεών σχετικά με το πεδίο του IoT, προσέφερε σημαντικά στην προώθηση της χρήσης του.

Ένα σημαντικό βήμα για τη μετάβαση στην εποχή του IoT συντελέστηκε όταν ο αριθμός των συνδεδεμένων συσκευών στο Διαδίκτυο ξεπέρασε τον ανθρώπινο πληθυσμό της γης. Σύμφωνα με την ομάδα IBSG της Cisco [11] αυτό έλαβε χώρα κατά τη χρονική περίοδο 2008-2009.

Το 2010 το IoT αρχίζει να γίνεται περισσότερο γνωστό, καθώς κερδίζει αναγνώριση από τις μεγάλες εταιρίες πληροφορικής αλλά και από κυβερνήσεις κρατών. Ο πρωθυπουργός της Κίνας Wen Jiabao σε κάποιες δηλώσεις του αποκάλεσε το IoT ως τη βασική βιομηχανία και ανακοίνωσε πως υπάρχουν σχέδια για σημαντικές επενδύσεις σε αυτό το πεδίο έρευνας στη χώρα του. Την ίδια χρονιά, η εταιρία Nest κυκλοφορεί τον Nest Thermostat, ένα θερμοστάτη με δυνατότητα αυτό-μάθησης και ασύρματης δικτύωσης για χρήση στο περιβάλλον ενός έξυπνου σπιτιού. Ήταν ο πρώτος παγκοσμίως IoT θερμοστάτης που βασιζόταν στη μηχανική μάθηση, και καταγράφοντας

τη συμπεριφορά των χρηστών του ρύθμιζε κατάλληλα τη θερμοκρασία του χώρου, έτσι ώστε να προσφέρει εξοικονόμηση ενέργειας.

Με τη συνεχόμενη αύξηση των συσκευών που συνδέονται στο Διαδίκτυο ανέκυψε ένα πολύ σημαντικό ζήτημα, αυτό της εξάντλησης των διαθέσιμων διευθύνσεων IPv4. Η επιστημονική κοινότητα βέβαια μελετούσε και έψαχνε λύσεις για αυτό το ζήτημα ήδη από τη δεκαετία του 1990 προετοιμάζοντας την επόμενη έκδοση του Πρωτοκόλλου Διαδικτύου, το IPv6, το οποίο τελικά κατέστη διαθέσιμο μετά την παγκόσμια ημέρα έναρξής του (World IPv6 Launch Day) στις 6 Ιουνίου 2012. Είχε σκοπό να αντικαταστήσει σταδιακά την προγενέστερη έκδοση IPv4 και να επιλύσει το ζήτημα εξάντλησης του χώρου IP διευθύνσεων. Το γεγονός ότι το IPv6 προσφέρει 2^{128} διαθέσιμες διευθύνσεις προς ανάθεση, έπαιξε καθοριστικό ρόλο στην ανάπτυξη των συστημάτων IoT, καθώς έπαψε να ισχύει ο περιορισμός του πλήθους των συνδεδεμένων συσκευών που όριζε το IPv4.

Τέλος από τα μέσα της προηγούμενης δεκαετίας αρχίζει η δημιουργία πλατφορμών υπολογιστικού νέφους (cloud computing platforms) για το IoT, από μεγάλες εταιρίες πληροφορικής. Η τεχνολογία του υπολογιστικού νέφους, η οποία επιτρέπει την παροχή υπολογιστικών πόρων από απομακρυσμένα κέντρα δεδομένων μέσω της χρήσης του Διαδικτύου, προσέδωσε στο IoT σημαντικά πλεονεκτήματα και έγινε αναπόσπαστο κομμάτι του. Πρώτη η Amazon Web Services (AWS) το 2015 παρουσίασε το AWS IoT, μια διαχειρίσιμη πλατφόρμα υπολογιστικού νέφους που επιτρέπει την εύκολη και ασφαλή αλληλεπίδραση των συνδεδεμένων συσκευών με εφαρμογές της πλατφόρμας, αλλά και με άλλες συσκευές. Την περίοδο 2016-2018 ακολούθησαν εταιρείες όπως η Microsoft και η Google που ανέπτυξαν τις δικές τους πλατφόρμες υπολογιστικής νέφους για το IoT, το Microsoft Azure IoT Suite και το Google Cloud IoT Platform αντίστοιχα.

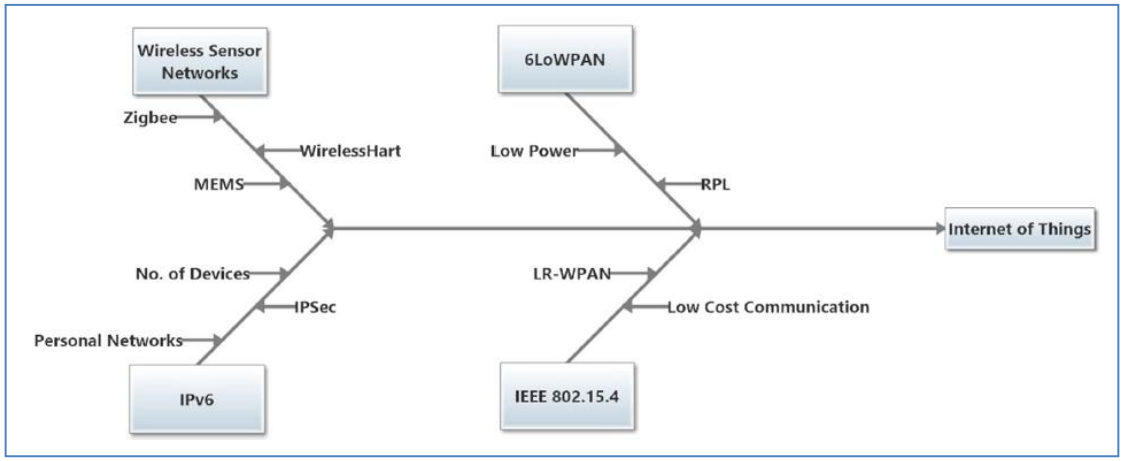
Οι συνεχείς μελέτες και έρευνες στο πεδίο του IoT, σε συνδυασμό με την αδιάκοπη τεχνολογική πρόοδο, συνέβαλαν και συμβάλλουν στην ανάπτυξη βελτιωμένων συστημάτων IoT, που βρίσκουν εφαρμογή σε μεγάλο αριθμό διαφορετικών κλάδων, όπως μεταξύ άλλων στη βιομηχανία, στην υγεία, στον περιβάλλον, κλπ. Αυτή η επέκταση του πεδίου χρήσης του IoT ενίσχυσε την παγκόσμια εξάπλωσή του.

1.3. Δομή και Αρχιτεκτονική του IoT

Στη σημερινή εποχή το Διαδίκτυο έχει εισχωρήσει σε τόσο μεγάλο βαθμό στη καθημερινότητα, ώστε να θεωρείται ως αναπόσπαστο κομμάτι του σύγχρονου τρόπου ζωής. Προς την ίδια κατεύθυνση βαδίζει και το IoT, το οποίο έχει να επιδείξει πολλά πλεονεκτήματα ως προς τη χρήση του. Στα πλαίσια του IoT, φυσικά αντικείμενα του πραγματικού κόσμου, όπως οικιακές συσκευές, οχήματα κα., καθίστανται πλέον έξυπνα, διότι ενσωματώνεται σε αυτά κατάλληλο υλικό και λογισμικό, που επιτρέπει τη διασύνδεση και αλληλεπίδραση αυτών με άλλες συσκευές σε ένα δίκτυο. Αυτά τα

αντικείμενα βρίσκονται σε θέση να επικοινωνήσουν με συσκευές του δικτύου και να διαμοιραστούν πληροφορίες σχετικά με την κατάσταση τους και το περιβάλλον στο οποίο λειτουργούν. Κατά αυτόν τον τρόπο οι έξυπνες συσκευές υποστηρίζουν την αυτοματοποίηση διαδικασιών, όπως η συλλογή και διαχείριση δεδομένων/πληροφοριών.

Η ανάπτυξη των ασύρματων δικτύων και της τεχνολογίας RFID ήταν καθοριστική για την εφαρμογή του IoT. Εξελίξεις στα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Network - WSN) επέτρεψαν τη διαδικτύωση διαφορετικών τύπων συσκευών, όπως συσκευές με περιορισμένες δυνατότητες όσον αφορά τη μνήμη, την υπολογιστική ισχύ και την ενεργειακή αυτονομία τους (constrained devices). Επιπροσθέτως, το πρωτόκολλο IPv6 και το πρότυπο IEEE 802.15.4 βοήθησαν στη διασύνδεση πλήθους συσκευών και διαφορετικών δικτύων μεταξύ τους, με αποτέλεσμα την επέκταση του IoT και την ενίσχυση της αποδοτικότητας του. Οι εν λόγω τεχνολογίες θεωρούνται θεμελιώδεις για τη δημιουργία του IoT [12] και αποτελούν το τεχνολογικό υπόβαθρο πάνω στο οποίο βασίστηκε, όπως φαίνεται στην Εικόνα 1.



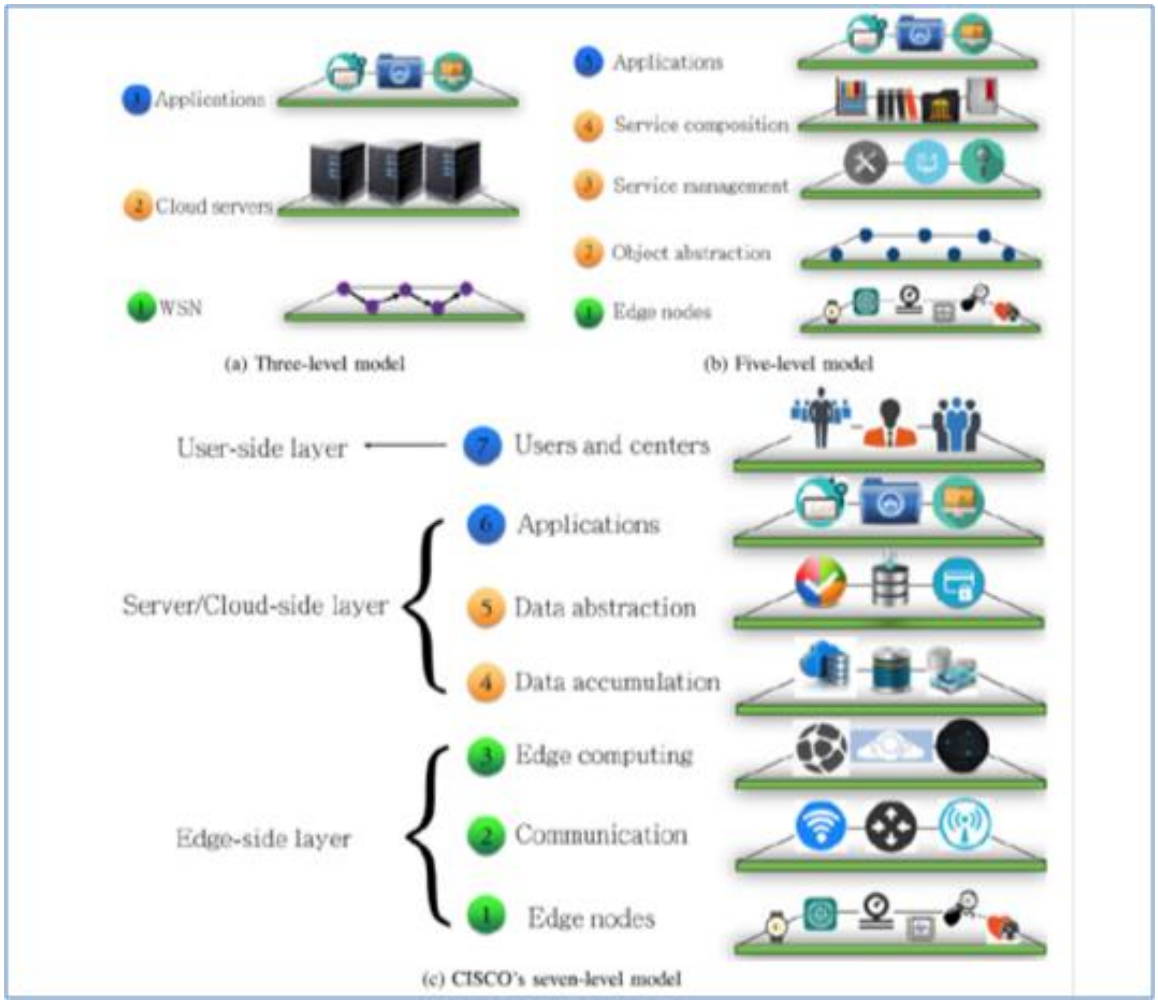
Εικόνα 1. Τεχνολογίες, Πρότυπα και Πρωτόκολλα Δικτύωσης για το IoT.

Πηγή: [12]

Το γεγονός ότι το IoT εφαρμόζεται σε πλήθος διαφορετικών κλάδων συνεπάγεται την ύπαρξη διαφορετικών απαιτήσεων που θα πρέπει να πληρούνται σε κάθε ξεχωριστό περιβάλλον (ή σε κάθε ξεχωριστή περίπτωση χρήσης), αυτό έχει ως αποτέλεσμα την ανάπτυξη εξειδικευμένων συστημάτων IoT. Όπως γίνεται εύκολα αντιληπτό, κάθε σύστημα IoT παρουσιάζει ιδιαιτερότητες στη λειτουργία του οι οποίες ενδεχομένως το διαφοροποιούν σε κάποιο βαθμό. Ωστόσο παρά τις όποιες ιδιαιτερότητες, οποιοδήποτε σύστημα IoT άσχετα με το πεδίο χρήσης του απαιτεί την ύπαρξη κάποιων συγκεκριμένων στοιχείων όπως συσκευές και αισθητήρες, συνδεσιμότητα, επεξεργασία δεδομένων και τη διεπαφή χρήστη [13].

Για τη μελέτη της βασικής λειτουργίας του IoT γενικότερα σαν σύστημα έχουν προταθεί διάφορες αρχιτεκτονικές, χωρίς ωστόσο καμία να έχει προτυποποιηθεί. Κατά

κανόνα όσα περισσότερα είναι τα επίπεδα μιας αρχιτεκτονικής τόσο πιο εξειδικευμένες λειτουργίες επιτελούν και τόσο ακριβέστερα περιγράφουν τη συνολική λειτουργία του συστήματος. Το γεγονός ότι δεν έχει προτυποποιηθεί κάποια αρχιτεκτονική για το IoT έχει οδηγήσει σε μία σχετική ευελιξία. Ανάλογα με την οπτική γωνία υπό την οποία εξετάζεται ένα σύστημα IoT και το σκοπό της κάθε μελέτης υπάρχει η δυνατότητα να επιλεγεί η αρχιτεκτονική που εξυπηρετεί καλύτερα τους ερευνητικούς στόχους. Μερικές από τις προτεινόμενες αρχιτεκτονικές για το IoT παρουσιάζονται στην Εικόνα 2.



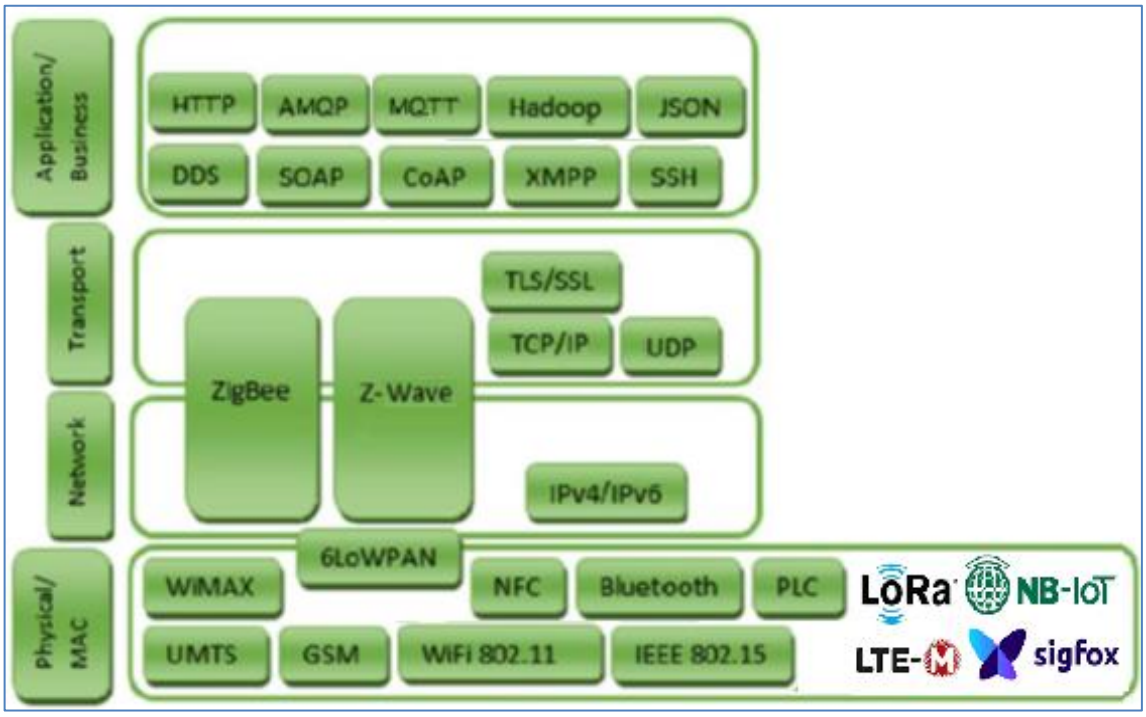
Εικόνα 2. Τρία χαρακτηριστικά Μοντέλα Αναφοράς για την Αρχιτεκτονική του IoT

Πηγή: **[14]**

Μελετώντας τις διάφορες προτεινόμενες αρχιτεκτονικές για το IoT παρατηρείται ότι συνήθως τα κατώτερα επίπεδα κάθε αρχιτεκτονικής αναφέρονται στη συλλογή δεδομένων μέσω αισθητήρων που είναι τοποθετημένοι στο φυσικό περιβάλλον, τα ενδιάμεσα επίπεδα αντιστοιχούν στη μεταφορά και επεξεργασία αυτών των δεδομένων και τέλος τα ανώτερα επίπεδα στην παρουσίαση και αξιοποίηση των πληροφοριών που έχουν εξαχθεί.

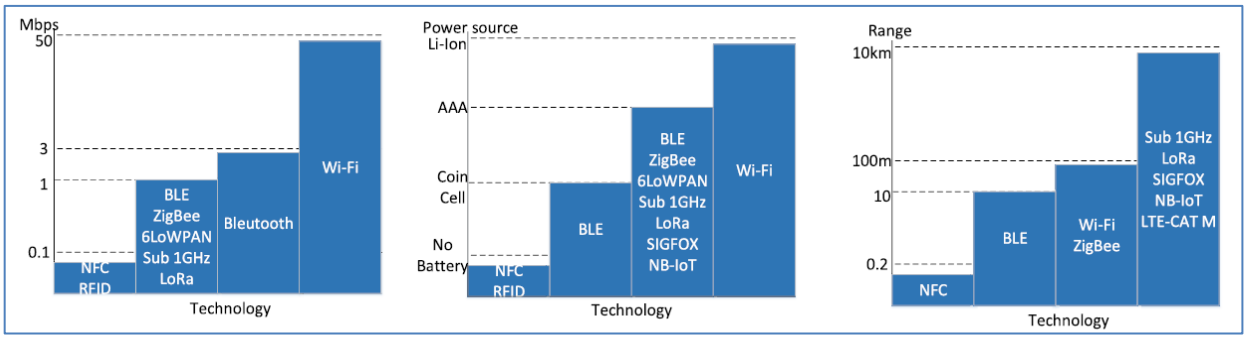
1.4. Πρότυπα και Πρωτόκολλα του IoT

Πολλά από τα πρωτόκολλα που χρησιμοποιούνται στα συμβατικά δίκτυα υπολογιστών καταναλώνουν μεγάλο πλήθος πόρων. Συνεπώς δεν είναι ικανά να ανταποκριθούν στις ιδιαίτερες απαιτήσεις του IoT και ειδικότερα στην περίπτωση των συσκευών με περιορισμένες δυνατότητες. Επομένως είναι αναγκαίο να καθοριστούν εξειδικευμένα πρωτόκολλα για το IoT που θα προσφέρουν την απαιτούμενη λειτουργικότητα παραμένοντας όμως αποδοτικά ως προς την κατανάλωση πόρων.



Εικόνα 3. Τα κυριότερα πρότυπα και πρωτόκολλα που χρησιμοποιούνται σε κάθε ένα επίπεδο του IoT.

Πηγή: [15]



Εικόνα 4. Throughput, Power source, Range of main IoT protocols.

Πηγή: [16]

Κάποια από τα πιο γνωστά πρωτόκολλα και πρότυπα που χρησιμοποιούνται συχνά στο IoT είναι:

- CoAP
- MQTT
- AMQP
- XMPP
- ZigBee
- Z-Wave
- BLE
- 6LoWPAN
- Wi-Fi
- LoRa
- LTE-M
- NB-IoT
- SigFox

1.4.1. Constrained Application Protocol – COAP

Το πρωτόκολλο CoAP (Constrained Application Protocol) είναι ένα πρωτόκολλο επιπέδου εφαρμογής εξειδικευμένο για χρήση σε κόμβους και δίκτυα περιορισμένων δυνατοτήτων. Σχεδιάστηκε για εφαρμογές που στηρίζονται στην επικοινωνία μηχανής-με-μηχανή (Machine-to-Machine, M2M) και καθορίζεται στο πρότυπο RFC 7252 [17], που έχει εκδώσει ο οργανισμός IETF (Internet Engineering Task Force).

Κύρια χαρακτηριστικά αυτού του πρωτοκόλλου, όπως μεταξύ άλλων η υποστήριξη πολλαπλής εκπομπής (multicast), η μικρότερη πολυπλοκότητα του καθώς και η εξοικονόμηση πόρων του δικτύου, το καθιστούν κατάλληλο για χρήση σε περιβάλλοντα όπως το IoT όπου υπάρχουν διάφοροι περιορισμοί.

Το CoAP βασίζεται στην αρχιτεκτονική REST (Representational State Transfer) και ενσωματώνει λειτουργίες του Πρωτοκόλλου Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol - HTTP). Πιο συγκεκριμένα, το μοντέλο αλληλεπίδρασης που χρησιμοποιεί το CoAP είναι παρόμοιο με το μοντέλο πελάτη/εξυπηρετητή (client/server) του HTTP [17]. Σύμφωνα με αυτό το μοντέλο, ένα αίτημα CoAP, το οποίο είναι ισοδύναμο με ένα αίτημα HTTP, αποστέλλεται από τον πελάτη, για να ζητηθεί πρόσβαση σε κάποιον πόρο που στεγάζεται στον εξυπηρετητή και έπειτα ο εξυπηρετητής στέλνει πίσω μία απόκριση (response). Σε κάθε πόρο αντιστοιχεί ένα Ενιαίο Αναγνωριστικό Πόρου (Uniform Resource Identifier - URI) που του προσδίδει μία μοναδική ταυτότητα και παρέχει τα μέσα για τον ακριβή εντοπισμό του. Κάθε αίτημα περιλαμβάνει έναν Κωδικό Μεθόδου (Method Code) ο οποίος μπορεί να είναι GET, PUT, POST ή DELETE και προσδιορίζει την ενέργεια που θα υποστούν οι πόροι. Επίσης, στην απόκριση που αποστέλλει ο εξυπηρετητής περιέχεται ένας Κωδικός Απόκρισης

(Response Code) και σε πολλές περιπτώσεις ενδέχεται να περιλαμβάνεται η αναπαράσταση του πόρου που έχει ζητηθεί [17].

Παρόλο που το πρωτόκολλο CoAP υιοθετεί κάποια χαρακτηριστικά του HTTP, έχει σχεδιαστεί για να λειτουργεί με το πρωτόκολλο UDP (User Datagram Protocol) του επιπέδου μεταφοράς. Το UDP είναι εγγενώς ένα ελαφρύ πρωτόκολλο και δεν εγγυάται αξιόπιστη μετάδοση πακέτων. Για αυτό το λόγο το CoAP χρησιμοποιεί κάποια συγκεκριμένα μηνύματα, ώστε να συγκροτήσει τον δικό του μηχανισμό αξιοπιστίας. Τα είδη μηνυμάτων που ορίζει το CoAP είναι:

- Επιβεβαιώσιμο Μήνυμα (Confirmable, CON)
- Μη-Επιβεβαιώσιμο Μήνυμα (Non-confirmable, NON)
- Μήνυμα Αναγνώρισης (Acknowledgement, ACK)
- Μήνυμα Επαναφοράς (Reset, RST)

Τέλος, αξίζει να σημειωθεί πως το πρωτόκολλο CoAP έχει τη δυνατότητα να συνδυαστεί με το πρωτόκολλο DTLS (Datagram Transport Layer Security), με σκοπό την αναβάθμιση του παρεχόμενου επιπέδου ασφάλειας στην επικοινωνία.

1.4.2. Message Queue Telemetry Transport – MQTT

Το πρωτόκολλο MQTT (Message Queue Telemetry Transport) είναι ένα ελαφρύ πρωτόκολλο ανταλλαγής μηνυμάτων, το οποίο βρίσκει ευρεία χρήση σε M2M και IoT εφαρμογές. Αναπτύχθηκε αρχικά από την εταιρία IBM το 1999, ενώ εκδόθηκε ως ανοιχτό πρότυπο από τον οργανισμό OASIS το 2014. Επίσης, το εν λόγω πρωτόκολλο χρησιμοποιεί τα πρωτόκολλα TCP και TLS (Transport Layer Security) τα οποία προσφέρουν αξιόπιστη και ασφαλή επικοινωνία μεταξύ συσκευών.

Το MQTT βασίζεται στο μοντέλο δημοσίευσης/εγγραφής (publish/subscribe), στο οποίο ορίζονται τρείς οντότητες:

- Συνδρομητής (Subscriber): Πελάτης που είναι εγγεγραμμένος σε κάποιο συγκεκριμένο θέμα (topic) και περιμένει να λάβει αντίστοιχα μηνύματα.
- Εκδότης (Publisher): Πελάτης που στέλνει μηνύματα στον διαμεσολαβητή.
- Διαμεσολαβητής (Broker): Ενδιάμεσος εξυπηρετητής που διανέμει τα μηνύματα στους συνδρομητές.

Στα πλαίσια του IoT, εκδότες είναι οι ενσωματωμένες συσκευές (πχ. αισθητήρες) που στέλνουν τα καταγραφόμενα δεδομένα στον διαμεσολαβητή και συνδρομητές είναι οι εφαρμογές οι οποίες ενδιαφέρονται για ένα συγκεκριμένο θέμα (πχ. καταγραφές θερμοκρασίας). Ο διαμεσολαβητής είναι ένας κεντρικός εξυπηρετητής, ο οποίος είναι υπεύθυνος για την κατηγοριοποίηση των ληφθέντων μηνυμάτων με βάση το θέμα τους και τη διανομή αυτών στους ενδιαφερόμενους συνδρομητές.

Το MQTT υποστηρίζει τρία επίπεδα ποιότητας υπηρεσίας (Quality of Service - QoS) για να εγγυηθεί την αξιόπιστη παράδοση των μηνυμάτων [18]:

- QoS 0 (Το πολύ μία φορά): Ένα μήνυμα μεταδίδεται μία φορά ή και καθόλου. Επίσης δεν αποστέλλεται καμία απάντηση από τον παραλήπτη, ούτε γίνεται προσπάθεια επαναμετάδοσης από τον αποστολέα.
- QoS 1 (Τουλάχιστον μία φορά): Εξασφαλίζεται ότι ένα μήνυμα θα σταλθεί τουλάχιστον μία φορά. Ο παραλήπτης πρέπει να απαντήσει στο μήνυμα που θα λάβει με ένα μήνυμα επιβεβαίωσης. Στην περίπτωση, όμως, που ο παραλήπτης καθυστερήσει να απαντήσει, ενδεχομένως να ληφθούν διπλότυπα μηνύματα.
- QoS 2 (Ακριβώς μία φορά): Χρησιμοποιείται για περιπτώσεις όπου δεν πρέπει να υπάρξει καμία απώλεια μηνυμάτων, ούτε όμως και διπλότυπα μηνύματα. Ο παραλήπτης αναγνωρίζει τη λήψη του μηνύματος με μια διαδικασία επιβεβαίωσης δύο βημάτων. Αυτό το επίπεδο QoS είναι αναμφισβήτητα το πιο αξιόπιστο, ωστόσο προκαλεί αυξημένη επιβάρυνση στο δίκτυο.

Το πρωτόκολλο MQTT χαρακτηρίζεται από χρήση μικρού εύρους ζώνης και χαμηλή κατανάλωση ενέργειας. Επιπλέον, προσφέρει αξιοπιστία, όταν είναι απαραίτητο, και έχει τη δυνατότητα να λειτουργεί με μειωμένους επεξεργαστικούς και αποθηκευτικούς πόρους. Παρά το γεγονός ότι το MQTT είναι κατάλληλο για περιβάλλοντα IoT, δεν είναι συμβατό με τις απαιτήσεις συσκευών πολύ μικρών δυνατοτήτων. Για αυτό το λόγο έχει σχεδιαστεί μία παραλλαγή αυτού, το πρωτόκολλο MQTT-SN (MQTT for Sensor Networks), το οποίο χρησιμοποιεί ως πρωτόκολλο μεταφοράς το UDP αντί για TCP.

1.4.3. Advanced Message Queuing Protocol – AMQP

Το πρωτόκολλο AMQP (Advanced Message Queuing Protocol) [19] είναι ένα ανοιχτό πρότυπο του οργανισμού OASIS το οποίο αρχικά προοριζόταν για τη χρηματοπιστωτική βιομηχανία, αλλά η χρήση του δεν άργησε να επεκταθεί και στο IoT. Όπως το MQTT, έτσι και το AMQP χρησιμοποιεί το πρωτόκολλο TCP για τη μετάδοση των δεδομένων και βασίζεται στο μοντέλο δημοσίευσης/εγγραφής (publish/subscribe). Η κυρία διαφορά μεταξύ αυτών των πρωτοκόλλων είναι πως στο AMQP ο διαμεσολαβητής (broker) χωρίζεται σε δύο κύρια μέρη, σε αυτό της ανταλλαγής (exchange) και αυτό των ουρών (queues). Το πρώτο μέρος είναι υπεύθυνο για τη λήψη των μηνυμάτων που αποστέλλουν οι εκδότες και τη διανομή αυτών στις ουρές ακολουθώντας προκαθορισμένους κανόνες. Οι ουρές είναι ουσιαστικά τα διάφορα θέματα (topics) που δημιουργούνται, στα οποία συνδέονται οι συνδρομητές για να λάβουν μηνύματα αντίστοιχου περιεχομένου.

Τέλος, αξίζει να αναφερθεί πως οι εξελιγμένες λειτουργίες που επιτελεί το AMQP αυξάνουν τις απαιτήσεις σε πόρους συστήματος. Επομένως, το AMQP δεν προτείνεται για χρήση σε συσκευές περιορισμένων πόρων.

1.4.4. eXtensible Messaging and Presence Protocol - XMPP

Το πρωτόκολλο XMPP (e**X**tensible **M**essaging and **P**resence **P**rotocol) είναι ένα ανοιχτό και ελεύθερο προς χρήση πρωτόκολλο για επικοινωνία πραγματικού χρόνου. Αρχικά σχεδιάστηκε για εφαρμογές ανταλλαγής άμεσων μηνυμάτων (instant messaging) και σταδιακά επεκτάθηκε σε πλήθος εφαρμογών όπως και στο IoT. Χρησιμοποιεί δύο μοντέλα επικοινωνίας, το μοντέλο αιτήματος/απάντησης και το μοντέλο δημοσίευσης/εγγραφής. Επίσης βασίζεται στη γλώσσα XML (eXtensible Markup Language) και επιτρέπει την ανταλλαγή δομημένων αλλά και επεκτάσιμων δεδομένων σε σχεδόν πραγματικό χρόνο μεταξύ οποιωνδήποτε δύο ή περισσοτέρων οντοτήτων δικτύου [20].

1.4.5. ZigBee

Το ZigBee πρόκειται για μια τεχνολογία ασύρματης επικοινωνίας, η οποία βασίζεται στο πρότυπο IEEE 802.15.4 και προορίζεται για ασύρματα δίκτυα χαμηλής ισχύος και χαμηλού κόστους. Υποστηρίζει τρείς τοπολογίες δικτύου, την τοπολογία αστέρα (star), πλέγματος (mesh) και δέντρου (tree). Επίσης λειτουργεί στη ζώνη συχνοτήτων 2.4 GHz, η εμβέλεια του φτάνει στα 10 έως 100 μέτρα και έχει ρυθμό μετάδοσης δεδομένων 250 Kbits/sec. Αυτά τα χαρακτηριστικά του ZigBee σε συνδυασμό με τη χαμηλή κατανάλωση ενέργειας που αυτό επιτρέπει, το καθιστούν εφαρμόσιμο σε δίκτυα όπου υπάρχουν συσκευές τροφοδοτούμενες από μπαταρίες.

1.4.6. Z-Wave

Το Z-Wave [21] είναι ένα πρωτόκολλο ασύρματης επικοινωνίας το οποίο βασίζεται στην τεχνολογία ραδιοσυχνοτήτων χαμηλής ισχύος. Χρησιμοποιείται κυρίως σε συστήματα οικιακού αυτοματισμού και συστήματα ασφαλείας. Σε αντίθεση με το ZigBee που εκπέμπει στη ζώνη συχνοτήτων 2.4 GHz, οι συχνότητες στις οποίες λειτουργεί το Z-Wave διαφοροποιούνται από χώρα σε χώρα, για παράδειγμα στις ΗΠΑ χρησιμοποιεί τη συχνότητα 908.42 MHz.

1.4.7. Bluetooth Low Energy – BLE

Το Bluetooth Low Energy (BLE) που αναφέρεται και ως Bluetooth Smart είναι ένα πρότυπο ασύρματης επικοινωνίας μικρής εμβέλειας, το οποίο τυγχάνει ευρείας χρήσης σε περιβάλλοντα IoT. Όπως υποδεικνύει η ονομασία του χαρακτηρίζεται από σημαντικά χαμηλή κατανάλωση ενέργειας γεγονός που το κάνει να διαφέρει από το κλασσικό πρότυπο Bluetooth. Αυτό το χαρακτηριστικό ενσωματώθηκε αρχικά στην έκδοση Bluetooth 4.0 και περιλαμβάνεται σε όλες τις μεταγενέστερες εκδόσεις με πιο πρόσφατη την Bluetooth 5.3 η οποία διατέθηκε το 2021.

Το Bluetooth Low Energy είναι ιδανικό για συσκευές που τροφοδοτούνται από μπαταρίες και επικοινωνούν περιοδικά αποστέλλοντας μικρής ποσότητας δεδομένα.

Αυτό οφείλεται στο γεγονός πως έχει την ικανότητα να παραμένει ανενεργό (sleep mode) και να ενεργοποιείται μόνο όταν πρόκειται να πραγματοποιηθεί κάποια σύνδεση, με άμεσο αποτέλεσμα την επιμήκυνση της διάρκειας ζωής της μπαταρίας.

1.4.8. IPv6 Low Power Wireless Personal Area Networks – 6LoWPAN

Ο όρος 6LoWPAN αναφέρεται σε ασύρματα προσωπικά δίκτυα χαμηλής ισχύος (Low Power Wireless Personal Area Networks - LoWPANs) που λειτουργούν με το πρωτόκολλο IPv6. Είναι ένα πρότυπο [22] που έχει στόχο να προσφέρει τη δυνατότητα σε συσκευές IoT, οι οποίες λειτουργούν με περιορισμένους πόρους, να επικοινωνούν χρησιμοποιώντας πακέτα IPv6. Με την αξιοποίηση μηχανισμών συμπίεσης κεφαλίδων (header compression) και ενθυλάκωσης (encapsulation) καθώς και άλλων τεχνολογιών εξοικονόμησης ενέργειας, το 6LoWPAN επιτρέπει σε συσκευές να ανταλλάσσουν δεδομένα μέσω δικτύων IEEE 802.15.4, τα οποία υποστηρίζουν επικοινωνία χαμηλής ταχύτητας και χαμηλού κόστους.

1.4.9. Wi-Fi

Το Wi-Fi (**Wi**reless **Fi**delity) είναι μία οικογένεια πρωτοκόλλων ασύρματης δικτύωσης βασισμένη στην οικογένεια προτύπων IEEE 802.11. Χρησιμοποιείται σε ασύρματα τοπικά δίκτυα (WLANs) διότι η μέγιστη εμβέλεια του προσεγγίζει τα 100 μέτρα. Συγκριτικά με το ZigBee που και αυτό καλύπτει την ίδια έκταση, το Wi-Fi καταναλώνει περισσότερη ενέργεια με αποτέλεσμα να θεωρείται μη κατάλληλο για ορισμένες εφαρμογές IoT και πιο συγκεκριμένα για την περίπτωση συσκευών περιορισμένων πόρων.

1.4.10. LoRa

Το LoRa (**Lo**ng **Ra**nge) είναι μία τεχνολογία διαμόρφωσης δικτύων ευρείας περιοχής χαμηλής ισχύος (LPWANs), η οποία βασίζεται στην τεχνική CSS (Chirp Spread Spectrum) για την κωδικοποίηση των δεδομένων. Η τεχνολογία LoRa ενσωματώνεται στο φυσικό επίπεδο της αρχιτεκτονικής IoT και επιτρέπει την επικοινωνία μεγάλης εμβέλειας και χαμηλής ενεργειακής κατανάλωσης. Η εμβέλεια που καλύπτει δύναται να υπερβεί τα 10 χιλιόμετρα υπό ιδανικές συνθήκες.

1.4.11. LTE-M

Το LTE-M [23] γνωστό και ως LTE Cat-M1 είναι μια τεχνολογία που χρησιμοποιείται για την απευθείας σύνδεση συσκευών IoT σε κυψελωτά δίκτυα τέταρτης γενιάς (4G) χωρίς την απαίτηση πρόσβασης σε οποιαδήποτε ενδιάμεση πύλη δικτύου (gateway). Παρέχει ρυθμό μετάδοσης δεδομένων περίπου 100 kbps και εφόσον μεταδίδει μικρότερη ποσότητα δεδομένων, είναι ικανό να αυξήσει τη διάρκεια ζωής της μπαταρίας των συσκευών.

1.4.12. NB-IoT

Το NB-IoT (Narrow Band Internet of Things) [23] πρόκειται για ακόμα μία τεχνολογία που χρησιμοποιείται σε δίκτυα LPWAN και απευθύνεται σε εφαρμογές που απαιτούν χαμηλή κατανάλωση ενέργειας και επικοινωνία σε μεγάλες αποστάσεις. Το πλεονέκτημα της εν λόγω τεχνολογίας είναι πως έχει καλή ικανότητα κάλυψης, δηλαδή το σήμα μπορεί να μεταδοθεί μέσω τοίχων ή σε υπόγειες περιοχές όπου δεν φτάνουν τα κανονικά κυψελοειδή σήματα. Η μέγιστη εμβέλεια του είναι τα 10 χιλιόμετρα.

1.4.13. SigFox

Το SigFox [24] είναι ένα είδος ασύρματης επικοινωνίας κυψελοειδούς μορφής που χαρακτηρίζεται από μεγάλη εμβέλεια, χαμηλή ισχύ και χαμηλό ρυθμό μετάδοσης δεδομένων. Έχει αναπτυχθεί με σκοπό να παρέχει ασύρματη συνδεσιμότητα σε συσκευές όπως απομακρυσμένους αισθητήρες, ενεργοποιητές και άλλες M2M και IoT συσκευές.

1.5. Χαρακτηριστικά του IoT

Παρακάτω αναφέρονται κάποια βασικά χαρακτηριστικά του IoT [25]:

- ✓ **Διασυνδεσιμότητα**: Οποιαδήποτε συσκευή μπορεί να διασυνδεθεί με την παγκόσμια υποδομή τεχνολογιών πληροφόρησης και επικοινωνίας (ΤΠΕ).

- ✓ **Συνδεσιμότητα**: Επιτρέπει την προσβασιμότητα και τη συμβατότητα του δικτύου. Η προσβασιμότητα αφορά την πρόσβαση σε ένα δίκτυο, ενώ η συμβατότητα παρέχει την κοινή ικανότητα δημιουργίας και χρήσης των δεδομένων του δικτύου.

- ✓ **Ετερογένεια**: Οι συσκευές στο IoT παρουσιάζουν ετερογένεια, καθώς βασίζονται σε διαφορετικές πλατφόρμες υλικού και σε διαφορετικά δίκτυα. Μπορούν να αλληλεπιδρούν με άλλες συσκευές ή πλατφόρμες υπηρεσιών μέσω διαφορετικών δικτύων.

- ✓ **Δυναμικές Αλλαγές**: Η κατάσταση των συσκευών αλλάζει δυναμικά, για παράδειγμα, όταν είναι απενεργοποιημένες ή ενεργές, συνδεδεμένες ή αποσυνδεμένες, αλλά και με βάση τη θέση και την ταχύτητά τους. Επιπλέον ο αριθμός των συσκευών μπορεί να αλλάξει δυναμικά.

- ✓ **Τεράστια κλίμακα**: Ο αριθμός των συσκευών IoT, που πρέπει να διαχειρίζονται και να επικοινωνούν μεταξύ τους, θα είναι αρκετά μεγαλύτερος από το πλήθος των συσκευών που είναι συνδεδεμένες στο τρέχον Διαδίκτυο. Ακόμη πιο κρίσιμη

θα είναι η διαχείριση των παραγόμενων δεδομένων (Big Data) και η ερμηνεία αυτών για σκοπούς διαφόρων εφαρμογών τους. Αυτό σχετίζεται με τη σημασιολογία των δεδομένων, καθώς και τον αποτελεσματικό χειρισμό του τεράστιου όγκου δεδομένων.

- ✓ **Ασφάλεια**: Το IoT και οι συσκευές που περιλαμβάνονται σε αυτό χαρακτηρίζονται από ευπάθειες, και κενά ασφάλειας, παρουσιάζοντας αδυναμίες στην αντιμετώπιση διαφόρων απειλών. Έτσι, ο σχεδιασμός τους πρέπει να επικεντρώνεται στην ασφάλεια των προσωπικών δεδομένων και της φυσικής ευεξίας των χρηστών. Για αυτό το λόγο, κρίνεται αναγκαία η επίτευξη ασφάλειας σε κάθε δομικό στοιχείο του δικτύου, όπως στα τερματικά σημεία, αλλά και στα δεδομένα τα οποία διακινούνται μέσα σε αυτό.

- ✓ **Τεχνολογία Αισθητήρων:** Οι αισθητήρες αποτελούν βασικό συστατικό του IoT. Εντοπίζουν, ανιχνεύουν, παρακολουθούν αλλαγές στο περιβάλλον και έπειτα παράγουν αντιπροσωπευτικά δεδομένα σχετικά με τις συνθήκες που επικρατούν. Αυτή η τεχνολογία είναι πολύ σημαντική, γιατί επιτυγχάνει τη μετατροπή απλών αναλογικών δεδομένων του πραγματικού κόσμου σε ψηφιακή πληροφορία στον εικονικό κόσμο. Επομένως, οι αισθητήρες είναι απαραίτητοι για την αλληλεπίδραση των έξυπνων αντικειμένων μεταξύ τους, αλλά και με τον φυσικό κόσμο, καθώς και με τους ανθρώπους μέσα σε αυτόν.

1.6. Τομείς Εφαρμογής του IoT

Οι απαιτητικοί ρυθμοί της καθημερινότητας έχουν αυξήσει την ανάγκη ύπαρξης τεχνολογιών IoT που θα είναι σε θέση να διευκολύνουν την εκτέλεση διάφορων διαδικασιών στα πλαίσια ενός σύγχρονου τρόπου ζωής. Αυτό έχει ως αποτέλεσμα να εφαρμόζεται το διαδίκτυο των πραγμάτων σε πολλούς τομείς της καθημερινής ζωής. Παρακάτω θα δούμε εν συντομία μερικές από τις κύριες εφαρμογές του IoT.

1.6.1. Έξυπνη Υγεία (Smart Health)

Η βιομηχανία της υγειονομικής περίθαλψης χρησιμοποιεί εκτενώς τεχνολογίες IoT με σκοπό τη δημιουργία ενός βελτιωμένου και πιο αποδοτικού συστήματος υγείας, το οποίο θα είναι σε θέση να προσφέρει εξελιγμένες υπηρεσίες για την προάσπιση και προαγωγή της υγείας των ανθρώπων. Προς αυτή την κατεύθυνση, συνδυαστικά με το IoT, εφαρμόζονται και άλλες τεχνολογίες αιχμής, όπως η τεχνητή νοημοσύνη, cloud computing, Big Data και 5G.

Η κεντρική ιδέα είναι η διασύνδεση και αλληλεπίδραση μεταξύ των οντοτήτων, των συστημάτων και των ανθρώπων που απαρτίζουν ένα σύστημα υγείας και η πρόσβαση σε ένα σύνολο πληροφοριών αμιγώς ιατρικών ή μη το οποίο θα είναι συνεχώς διαθέσιμο. Με τη χρήση σύγχρονων τεχνολογικών υποδομών, επιτρέπεται η αμεσότερη

επικοινωνία μεταξύ των ασθενών και των επαγγελματιών υγείας. Κατά αυτόν τον τρόπο επιτυγχάνεται η βελτίωση των προσφερόμενων υπηρεσιών υγείας και η ελαχιστοποίηση του χρόνου αναμονής των ασθενών.

Μια πτυχή της έξυπνης υγείας είναι το έξυπνο νοσοκομείο. Στα πλαίσια ενός έξυπνου νοσοκομείου παρέχεται η υπηρεσία απομακρυσμένης παρακολούθησης των ασθενών (Remote Patient Monitoring - RPM) σε πραγματικό χρόνο με χρήση αισθητήρων και φορέσιμων συσκευών (wearables). Οι πληροφορίες που αντλούν αυτές οι συσκευές σχετικά με την κατάσταση της υγείας των ασθενών, αποθηκεύονται στο νέφος (cloud) και γίνονται άμεσα διαθέσιμες τόσο στο ιατρονοσηλευτικό προσωπικό όσο και στους ίδιους τους ασθενείς. Επομένως, οι ασθενείς μπορούν πλέον να διαμένουν στην οικία τους επωφελούμενοι της απομακρυσμένης ιατρικής φροντίδας. Αυτό έχει ως αποτέλεσμα την εξοικονόμηση νοσοκομειακών πόρων και τη μείωση του κόστους περίθαλψης γενικότερα.

1.6.2. Έξυπνα Σπίτια (Smart Homes)

Στο περιβάλλον των έξυπνων σπιτιών υποστηρίζονται λειτουργίες όπως:

- Προσαρμογή και παραμετροποίηση του περιβάλλοντος του σπιτιού σύμφωνα με τις ανάγκες και τις προτιμήσεις των κατοίκων του.
- Ενίσχυση της ασφάλειας των κατοίκων μέσω συστημάτων ασφαλείας, όπως σύστημα παρακολούθησης εισόδων και παραθύρων για την ανίχνευση και αποτροπή ενδεχόμενης εισβολής, σύστημα πυρανίχνευσης και άλλα.
- Εξ’ αποστάσεως έλεγχος και χειρισμός οικιακών συσκευών και λοιπών συστημάτων. Ο εξ’ αποστάσεως έλεγχος και χειρισμός των οικιακών συσκευών επιτυγχάνεται μέσω της χρήσης κατάλληλων εφαρμογών στο smartphone (έξυπνο κινητό τηλέφωνο) του χρήστη. Έτσι δίνεται η δυνατότητα στον χρήστη να χειριστεί οικιακές συσκευές όπως ψυγεία, πλυντήρια, κλιματιστικά, κλπ. ακόμα και αν δεν βρίσκεται στο σπίτι του, χρησιμοποιώντας απλώς τις κατάλληλες εφαρμογές στο smartphone του. Για παράδειγμα το έξυπνο κλιματιστικό δίνει τη δυνατότητα στον χρήστη να το θέσει σε λειτουργία εξ’ αποστάσεως και να επιλέξει την επιθυμητή θερμοκρασία, με αποτέλεσμα όταν γυρίσει στο σπίτι του, η θερμοκρασία του χώρου να έχει προσαρμοστεί κατάλληλα. Όσο για το έξυπνο ψυγείο, μια λειτουργία που δύναται να υποστηρίξει είναι η ενημέρωση για τα περιεχόμενά του και για την ημερομηνία λήξης αυτών, ή ακόμα και η υπενθύμιση στον χρήστη, για να προμηθευτεί κάποια τρόφιμα που λείπουν.
- Παρακολούθηση κατανάλωσης ηλεκτρικής ενέργειας και νερού. Οι πληροφορίες σχετικά με την κατανάλωση των πόρων, όπως το νερό και το ηλεκτρικό ρεύμα, σε ένα έξυπνο σπίτι, βοηθούν στην ελάττωση της υπέρμετρης

χρήσης και σπατάλης τους από τον άνθρωπο, οδηγώντας στην εξοικονόμηση των πόρων αυτών, αλλά και στη μείωση του κόστους.

Όπως γίνεται εύκολα αντιληπτό, η ζωή των ανθρώπων που διαμένουν σε έξυπνα σπίτια καθίσταται πιο εύκολη και βολική, διότι προσφέρεται μεγαλύτερη άνεση καθώς και ασφάλεια. Οι άνθρωποι έχουν την ευκαιρία να αποκτήσουν περισσότερο ελεύθερο χρόνο, επειδή πολλές ενέργειες μέσα στο σπίτι θα είναι προγραμματισμένες και αυτοματοποιημένες.

Εικόνα 5. Έξυπνο Σπίτι

Πηγή: https://www.energymatters.com.au/energy-efficiency/smart-home-automation/

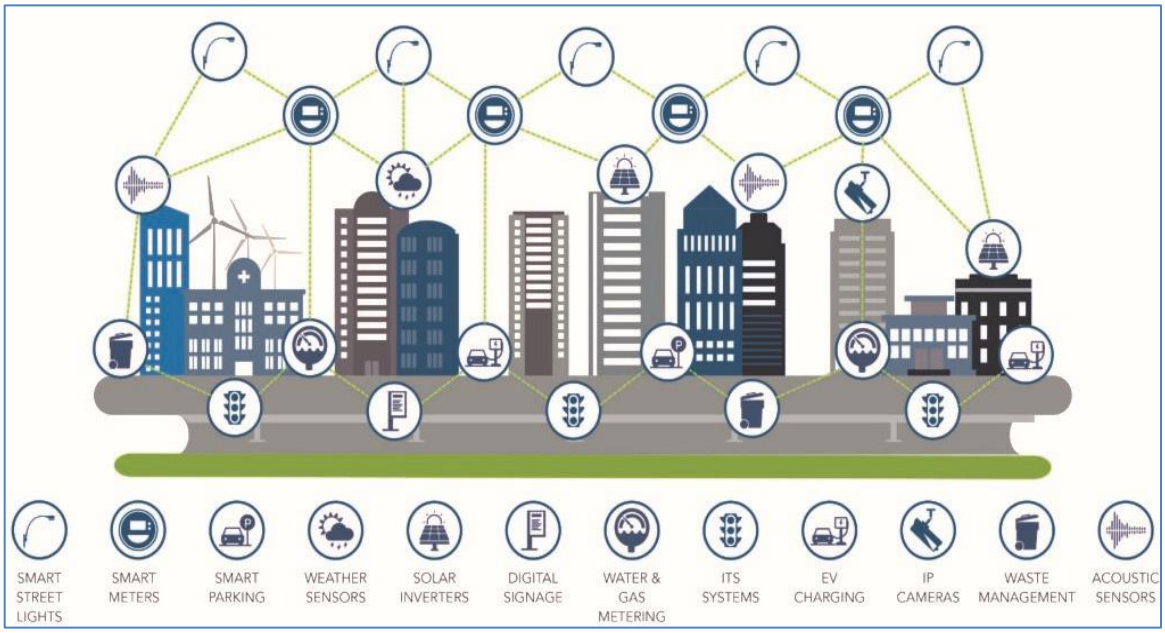
1.6.3. Έξυπνες Πόλεις (Smart Cities)

Το οικοσύστημα μιας έξυπνης πόλης προσφέρει πληθώρα υπηρεσιών, όπως:

- Αποτελεσματικός έλεγχος και διαχείριση της κίνησης των οχημάτων στην πόλη, ώστε να αποφευχθεί η κυκλοφοριακή συμφόρηση στο οδικό δίκτυο. Αποστέλλονται πληροφορίες στους οδηγούς σχετικά με την κίνηση, τις καιρικές συνθήκες που επικρατούν, αλλά και για ενδεχόμενα ατυχήματα. Επίσης υπάρχει η δυνατότητα ενημέρωσης των οδηγών για υπάρχουσες ελεύθερες θέσεις στάθμευσης.
- Αποδοτικό σύστημα διανομής νερού το οποίο έχει ως στόχο τον έλεγχο και την εξασφάλιση της ποιότητας του νερού που προσφέρεται στους κατοίκους, αλλά και τον περιορισμό της κατανάλωσης σε περίπτωση μη επαρκούς αποθέματος.
- Καλύτερη διαχείριση των απορριμμάτων. Η τοποθέτηση αισθητήρων σε κάδους απορριμμάτων βοηθάει στην ανίχνευση της πληρότητας αυτών, ώστε να

αποφεύγονται οι άσκοπες διαδρομές των απορριμματοφόρων και έτσι να ελαχιστοποιούνται τα λειτουργικά έξοδα.

- Βελτιωμένη αστική ασφάλεια. Το γεγονός της ύπαρξης καμερών παρακολούθησης και αισθητήρων σε διάφορα σημεία της πόλης οδηγεί στη βελτίωση της αστικής ασφάλειας. Αυτά τα συστήματα μπορούν να έχουν μεγάλη χρησιμότητα ως προς την αντιμετώπιση της εγκληματικότητας, καθώς οι αστυνομικές αρχές θα ειδοποιούνται εγκαίρως, κατά την εξέλιξη κάποιας βίαιης πράξης, ώστε να προβούν στις κατάλληλες ενέργειες.
- Αποτελεσματική παρακολούθηση του περιβάλλοντος. Με τη χρήση κατάλληλης τεχνολογικής υποδομής επιτυγχάνεται η ακριβής παρακολούθηση των καιρικών συνθηκών, της ατμοσφαιρικής ρύπανσης, της κατανάλωσης πόρων και άλλων περιβαλλοντικών δεδομένων.



Εικόνα 6. Έξυπνη Πόλη

Πηγή: www.polisnetwork.eu/topic/smart-cities/

1.6.4. Έξυπνο Δίκτυο Διανομής Ηλεκτρικής Ενέργειας (Smart Grid)

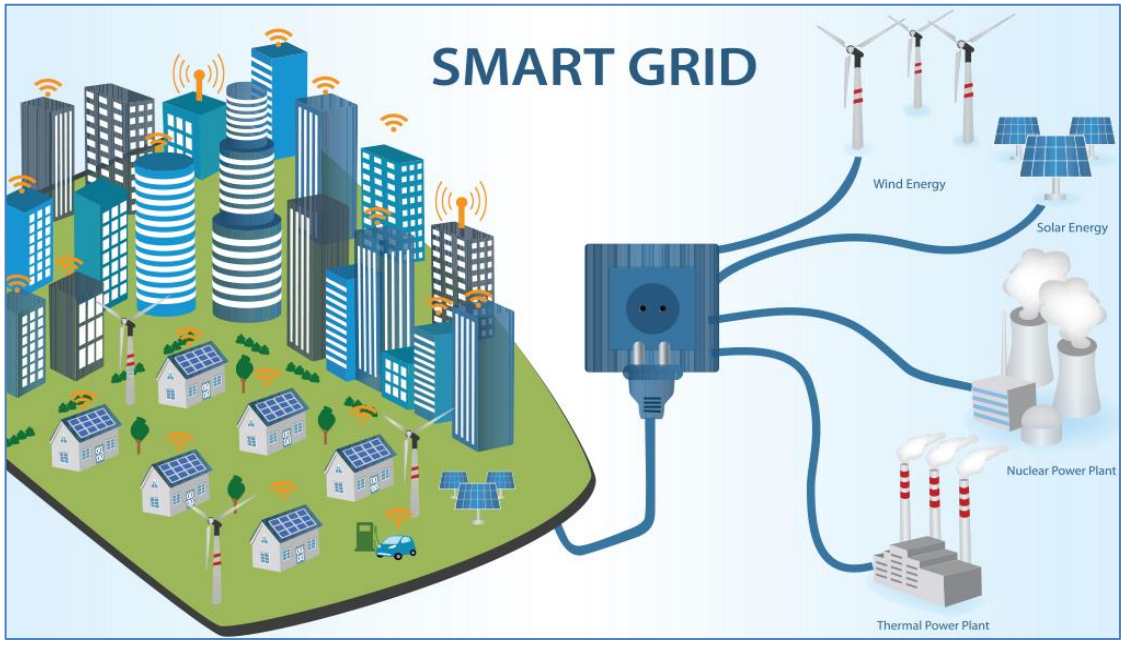
Η ραγδαία επιδείνωση του ενεργειακού προβλήματος εξαιτίας της αύξησης του πληθυσμού αλλά και της ολοένα αυξανόμενης κατά κεφαλήν ενεργειακής κατανάλωσης, έχει οδηγήσει στο ζήτημα διαχείρισης της ενέργειας, στο οποίο θα δώσει λύση το IoT.

Κύριος στόχος είναι ο σχεδιασμός και η ανάπτυξη ενός βιώσιμου και ευέλικτου συστήματος έξυπνης διαχείρισης της ενέργειας, το οποίο θα βασίζεται στο IoT και θα αποσκοπεί στον περιορισμό των απωλειών και τη βελτιστοποίηση της παραγωγής, της

παροχής και της κατανάλωσης ηλεκτρικής ενέργειας και στην ελαχιστοποίηση του λειτουργικού κόστους.

Το σύστημα αυτό, γνωστό ως έξυπνο δίκτυο διανομής ηλεκτρικής ενέργειας (“smart grid”), εκτιμάται πως στο μέλλον θα αντικαταστήσει σταδιακά τα συμβατικά κοστοβόρα δίκτυα ηλεκτροδότησης.

Θεμελιώδης αρχή του smart grid είναι η αυτοματοποιημένη συλλογή και επεξεργασία πληροφοριών σχετικά με τις συμπεριφορές των χρηστών του, δηλαδή των παρόχων, των καταναλωτών και αυτών που εμπίπτουν και στις δυο κατηγορίες. Έξυπνοι μετρητές (“smart meters”) και ένα δίκτυο αισθητήρων θα διαμοιράζουν πληροφορίες αμφίδρομα και σε πραγματικό χρόνο στους χρήστες. Δομείται κατά αυτόν τον τρόπο ένα νέο “οικοσύστημα” που προσφέρει πληθώρα εφαρμογών και διευκολύνσεων.



Εικόνα 7. Έξυπνο Δίκτυο Διανομής Ηλεκτρικής Ενέργειας (Smart Grid)

Πηγή: https://innovationatwork.ieee.org/smart-grid-transforming-renewable-energy/

Αρχικά, με την παροχή πληροφοριών σε πραγματικό χρόνο, η σχέση μεταξύ προσφοράς και ζήτησης καθίσταται πλέον άμεση, επιτρέποντας την προσαρμογή της συμπεριφοράς τόσο του καταναλωτή (κατανάλωση σε περιόδους χαμηλότερου κόστους, ακριβής έλεγχος της κατανάλωσης), όσο και του παρόχου (πρόβλεψη υψηλής ζήτησης, προσαρμογή παραγωγής με βάση τη ζήτηση).

Επιπλέον ένα έξυπνο δίκτυο διανομής ηλεκτρικής ενέργειας θα μπορεί να δέχεται με ακρίβεια όση ενέργεια χρειάζεται από εναλλακτικές ανανεώσιμες πηγές, όπως φωτοβολταϊκά ή ανεμογεννήτριες. Κατά αυτόν τον τρόπο ενισχύεται η αξιοπιστία του δικτύου, αφού σε αντίθεση με τα συμβατικά συστήματα διανομής ενέργειας, θα έχει

επιπρόσθετους πόρους πέραν της κεντρικής μονάδας παραγωγής ενέργειας. Τέλος αξίζει να αναφερθεί η διευκόλυνση που προσφέρεται αναφορικά με την άμεση διάγνωση και την επιδιόρθωση βλαβών, διότι, όπως είναι ευνόητο, η εποπτεία ενός τέτοιου δικτύου θα τελείται αυτόματα, σε σχεδόν πραγματικό χρόνο.

1.6.5. Έξυπνο Περιβάλλον (Smart Environment)

Το IoT παρέχει την κατάλληλη τεχνολογία για την παρακολούθηση του περιβάλλοντος. Η ύπαρξη αισθητήρων βοηθάει στην καταγραφή φυσικών φαινομένων και μεταβολών στο περιβάλλον, καθώς και πιθανών ανωμαλιών που μπορούν να οδηγήσουν σε καταστροφές. Μέσω των αισθητήρων μπορεί να προβλεφθεί ο καιρός και μπορούν να ανιχνευθούν δονήσεις σε σεισμογενείς περιοχές, ή και πυρκαγιές σε δασικές περιοχές. Επίσης παρακολουθείται η ατμοσφαιρική ρύπανση και η στάθμη των υδάτων.

Καταστροφές, οι οποίες είναι δυνατό να προκληθούν από ακραία φυσικά φαινόμενα, θα μπορούν να αποφευχθούν με τη χρήση συστημάτων λήψης αποφάσεων μέσω πλατφόρμας IoT. Για παράδειγμα, αν οι αισθητήρες παρατηρήσουν μεταβολή της θερμοκρασίας και προβλέψουν ότι υπάρχει πιθανότητα να εκδηλωθεί πυρκαγιά, τότε θα ενημερώσουν το πυροσβεστικό σώμα, για να παρέμβει.

Είναι προφανές ότι η χρήση των τεχνολογιών IoT για την παρακολούθηση του περιβάλλοντος μπορεί να συμβάλλει στην πρόληψη και αποφυγή οικολογικών καταστροφών. Με άμεσο αποτέλεσμα να προστατεύεται τόσο η ανθρώπινη ζωή όσο και το περιβάλλον.

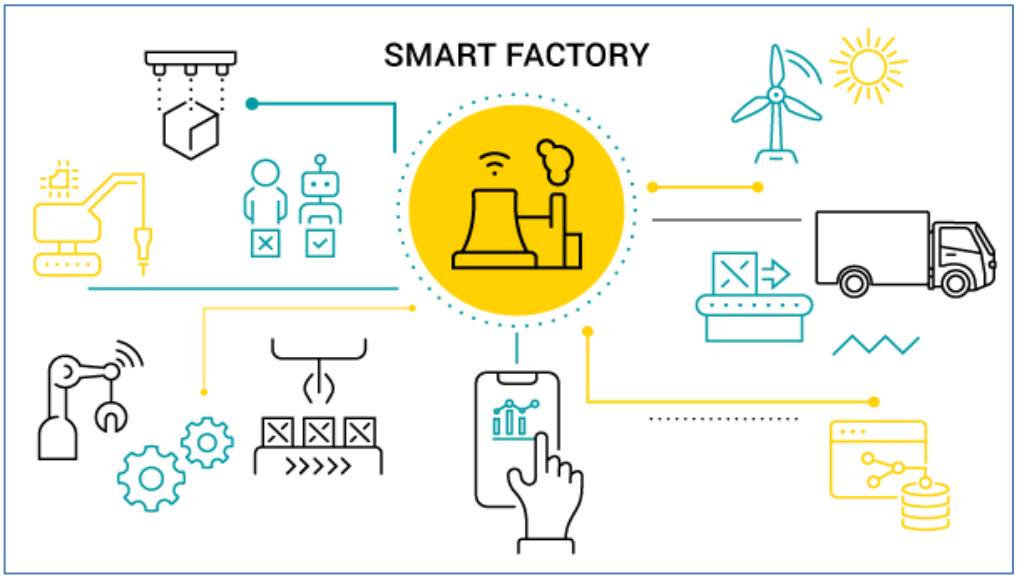
1.6.6. Έξυπνη Βιομηχανία (Smart Industry)

Ένα ακόμα σημαντικό πεδίο εφαρμογής του IoT είναι η Έξυπνη Βιομηχανία. Με την εφαρμογή τεχνολογιών IoT στη βιομηχανία γεννάται η έννοια του «έξυπνου εργοστασίου», το οποίο επικεντρώνεται στο σύστημα παραγωγής, κάνοντας το πιο έξυπνο και αποδοτικό, βελτιώνοντας την παραγωγικότητα και μειώνοντας τα λειτουργικά έξοδα. Οι συνδεδεμένοι αισθητήρες προσφέρουν διευκόλυνση στη συντήρηση των μηχανημάτων, καθώς θα είναι δυνατή η παρακολούθηση του εξοπλισμού του εργοστασίου σε πραγματικό χρόνο, ώστε να ελέγχεται η σωστή λειτουργία και απόδοσή του. Με αυτόν τον τρόπο θα είναι εφικτή η πρόληψη και αποφυγή ενδεχόμενων κινδύνων.

Στο έξυπνο εργοστάσιο μπορούν να εφαρμοστούν διάφορες βασικές τεχνολογίες όπως:

- Δίκτυα αισθητήρων
- Τεχνολογία RFID
- GPS

- M2M
- Cloud computing
- Big data analytics, business analytics
- Τεχνητή νοημοσύνη και μηχανική μάθηση



Εικόνα 8. Έξυπνο Εργοστάσιο

Πηγή: https://www.avsystem.com/blog/smart-factory/

2. Το IoT στον Τομέα της Υγείας - Internet of Health Things (IoHT)

2.1. Εισαγωγή στο IoHT

Η υγεία είναι μία ιδιαίτερα σημαντική παράμετρος στη ζωή των ανθρώπων και θεωρείται ευρέως ως το πολυτιμότερο αγαθό. Ο χώρος της υγειονομικής περίθαλψης αναζητεί διαχρονικά λύσεις για τη βελτίωση των παρεχόμενων υπηρεσιών με απώτερο σκοπό την πιο αποτελεσματική λειτουργία του υγειονομικού συστήματος.

Ήδη από τα μέσα του προηγούμενου αιώνα, άρχισε να αναπτύσσεται η ιδέα της τηλεϊατρικής (telemedicine) που αφορά την παροχή κλινικών υπηρεσιών σε ασθενείς από απόσταση. Επίσης την ίδια χρονική περίοδο υλοποιήθηκε μία πρώιμη μορφή πληροφοριακού συστήματος υγείας (Health Information System - HIS) με χαρακτηριστικά παραδείγματα τον ηλεκτρονικό ιατρικό φάκελο (Electronic Medical Record - EMR) και τον ηλεκτρονικό φάκελο υγείας (Electronic Health Record - EHR). Ωστόσο υπήρχαν εμπόδια που δυσχέραιναν την ενσωμάτωση και την αξιοποίηση των παραπάνω εφαρμογών στον τομέα της υγειονομικής περίθαλψης, μερικά από τα οποία παρακάμφθηκαν με την εδραίωση της χρήσης των προσωπικών υπολογιστών και του Διαδικτύου.

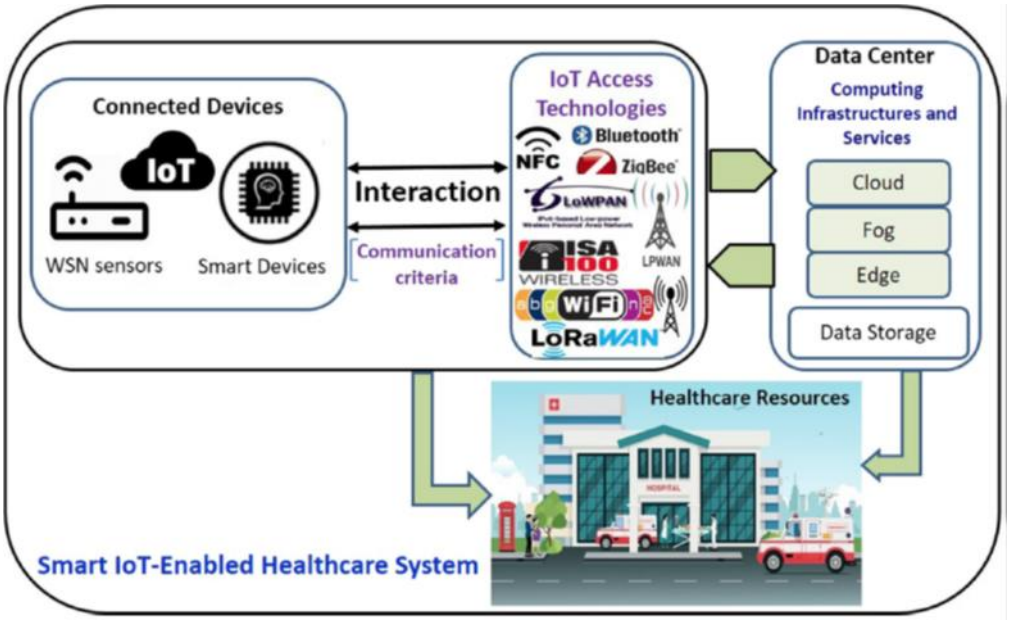
Αυτές οι τεχνολογικές εφαρμογές μεταξύ άλλων έφεραν πιο κοντά την εποχή της ψηφιοποίησης και του εκσυγχρονισμού των υποδομών υγείας. Κατά αυτόν τον τρόπο προετοιμάστηκε το έδαφος για την εφαρμογή των τεχνολογιών IoT σε αυτόν τον τομέα.

Ο όρος Internet of Health Things (IoHT) χρησιμοποιείται για να περιγράψει ένα υποσύνολο του IoT με πεδίο εφαρμογής τον χώρο της υγείας. Στην υπάρχουσα διαθέσιμη βιβλιογραφία απαντάται επίσης ο ισοδύναμος όρος Internet of Medical Things (IoMT). Στα πλαίσια της εργασίας θα χρησιμοποιηθεί ο πρώτος όρος που αναφέρθηκε.

Ιδιαίτερο χαρακτηριστικό του IoHT είναι το ότι συνδέονται μεταξύ τους αλλά και με το Διαδίκτυο, συσκευές και συστήματα που χρησιμοποιούνται για ιατρικούς σκοπούς. Το IoHT διατηρεί την ίδια βασική αρχή λειτουργίας με το IoT και στοχεύει στη δημιουργία ενός εξελιγμένου περιβάλλοντος παροχής υγειονομικών υπηρεσιών με τη συμβολή έξυπνων συσκευών, τεχνολογιών επικοινωνίας και υπολογιστικής υποδομής, στο οποίο η προσβασιμότητα των ιατρικών δεδομένων κατέχει καθοριστικό ρόλο. Μέσω του IoHT επιτυγχάνεται η έγκαιρη ανίχνευση συμπτωμάτων στους ασθενείς και κατά συνέπεια η έγκαιρη διάγνωση και αποτελεσματική θεραπεία μιας νόσου.

Έναντι του συμβατικού συστήματος υγείας, το IoHT παρέχει πλήθος πλεονεκτημάτων και αναβαθμίσεων και έτσι η υιοθέτηση αυτής της τεχνολογίας θεωρείται από πολλούς επιτακτική. Συνεπώς, το IoHT ως ερευνητικό πεδίο γνωρίζει

άνθιση το τελευταίο χρονικό διάστημα με τις σχετικές αναφορές στη διεθνή βιβλιογραφία ολοένα να αυξάνονται.



Εικόνα 9. Το έξυπνο περιβάλλον παροχής υγειονομικών υπηρεσιών που επιχειρεί να δημιουργήσει το IoT

Πηγή: [26]

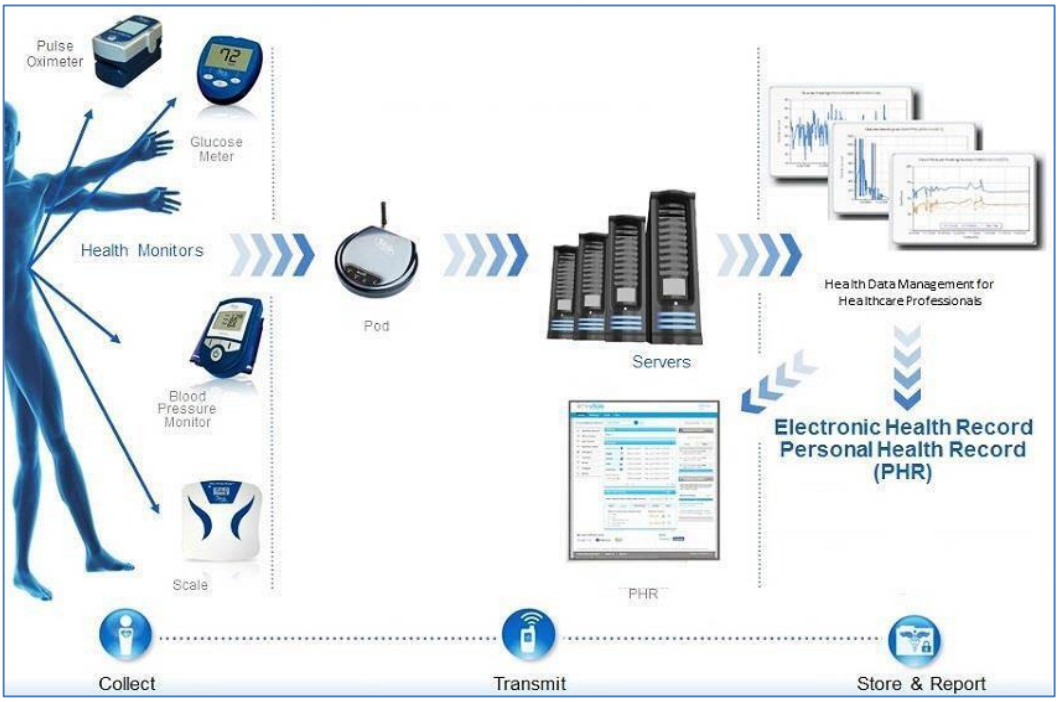
2.2. Αρχές Λειτουργίας του IoHT

Το IoHT, όπως προαναφέρθηκε, βασίζεται στην αρχή λειτουργίας του IoT. Στην Εικόνα 10 παρουσιάζονται τα κυριότερα στάδια της διαδικασίας που ακολουθεί το IoHT.

Αρχικά, ένα σύνολο έξυπνων ιατρικών αισθητήρων συλλέγει πληροφορίες σχετικές με την υγεία του ασθενή και τις προωθεί μέσω Διαδικτύου σε απομακρυσμένους εξυπηρετητές (servers). Εκεί, πραγματοποιείται η ανάλυσή τους και τα εξαγόμενα αποτελέσματα αποθηκεύονται στο EHR του ασθενή και καθίστανται προσβάσιμα σε εξουσιοδοτημένους χρήστες όπως τους θεράποντες ιατρούς, τον ίδιο τον ασθενή ή και τους οικείους του. Οι έξυπνοι αισθητήρες οι οποίοι χρησιμοποιούνται στο IoHT διακρίνονται σε αυτούς που ενσωματώνονται σε φορέσιμες συσκευές (wearables), σε εμφυτεύσιμους αισθητήρες (implantables) και σε εξωτερικούς αισθητήρες στο περιβάλλον του ασθενή.

Συστήματα IoHT βρίσκουν εφαρμογή σε τρία βασικά πεδία: σε νοσοκομεία, σε σπίτια ασθενών και στο ανθρώπινο σώμα. Στο περιβάλλον του νοσοκομείου υποστηρίζεται η δυνατότητα της ανίχνευσης των ασθενών μέσω μοναδικών αναγνωριστικών, η δυνατότητα εξ' αποστάσεως παρακολούθησης της υγείας τους και η ύπαρξη έξυπνων κρεβατιών που προσαρμόζονται στις ανάγκες τους. Αναφορικά με το περιβάλλον του σπιτιού, η δυνατότητα της εξ' αποστάσεως παρακολούθησης της

υγείας των ασθενών αποκτά ιδιαίτερη βαρύτητα, καθώς γίνεται δυνατή η έγκαιρη αντιμετώπιση έκτακτων καταστάσεων. Όσο για το ανθρώπινο σώμα, η εφαρμογή των εμφυτεύσιμων και φορέσιμων αισθητήρων εμφανίζει αύξηση ενδιαφέροντος για το ευρύ κοινό, διότι παρέχεται πλήθος πλεονεκτημάτων χωρίς όμως να περιορίζεται η κινητικότητα των χρηστών.



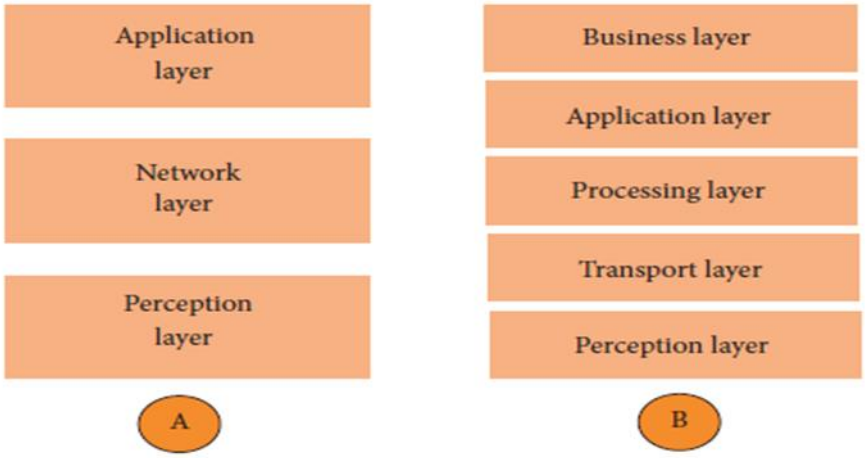
Εικόνα 10. Απλοποιημένη περιγραφή της λειτουργίας ενός συστήματος IoHT

Πηγή: [27]

2.3. Αρχιτεκτονική IoHT

Όπως αναλύθηκε σε προηγούμενο κεφάλαιο, έως τώρα δεν έχει προκύψει μία κοινή, αποκλειστική αρχιτεκτονική για συστήματα IoT η οποία να είναι ευρέως αποδεκτή. Πλήθος διαφορετικών αρχιτεκτονικών έχει διατυπωθεί, με πιο θεμελιώδη την αρχιτεκτονική τριών επιπέδων που απαρτίζεται από τα επίπεδα αντίληψης, δικτύου, και εφαρμογής (Εικόνα 11). Εισήχθη κατά τα αρχικά στάδια της έρευνας και περιγράφει την κύρια ιδέα και λειτουργία του IoT. Παρόλα αυτά, δεν είναι πλέον επαρκής, διότι δεν μπορεί να ικανοποιήσει τις αυξανόμενες απαιτήσεις των εφαρμογών, δεδομένης της συνεχούς επέκτασης και ανάπτυξης του IoT.

Όπως είναι ευνόητο, ανάλογα με το πεδίο εφαρμογής ενός συστήματος IoT είναι αναγκαία μια αρχιτεκτονική που να καλύπτει τις αντίστοιχες απαιτήσεις που προκύπτουν. Για αυτό το λόγο έχουν προταθεί διάφορες αρχιτεκτονικές που απαρτίζονται από περισσότερα επίπεδα, ανάμεσα στις οποίες η αρχιτεκτονική τεσσάρων επιπέδων, η αρχιτεκτονική πέντε επιπέδων μέχρι και αρχιτεκτονικές με οκτώ επίπεδα.



Εικόνα 11. Αρχιτεκτονική IoT (A: τριών επιπέδων, B: πέντε επιπέδων)

Πηγή: [28]

Για τις ανάγκες της παρούσας εργασίας θα χρησιμοποιηθεί η αρχιτεκτονική πέντε επιπέδων, η οποία απαντάται εξαιρετικά συχνά σε μελέτες και εμπεριέχει τα επίπεδα αντίληψης, μεταφοράς, επεξεργασίας, εφαρμογής και επιχείρησης (Εικόνα 11). Στη συνέχεια παρουσιάζεται συνοπτικά η λειτουργικότητα κάθε επιπέδου.

2.3.1. Επίπεδο Αντίληψης (Perception Layer)

Πρόκειται για το κατώτερο επίπεδο της αρχιτεκτονικής το οποίο είναι γνωστό αλλιώς και ως επίπεδο αισθητήρα (sensor layer) ή επίπεδο συσκευής (device layer) και περιλαμβάνει τα έξυπνα αντικείμενα και τους αισθητήρες που έχουν ενσωματωθεί σε αυτά. Επιπλέον είναι υπεύθυνο για τη συλλογή πληροφοριών σχετικά με το περιβάλλον και την κατάσταση των έξυπνων αντικειμένων, οι οποίες ανιχνεύονται μέσω αισθητήρων. Οι πληροφορίες που συλλέγονται, προωθούνται στα υψηλότερα επίπεδα για την περαιτέρω επεξεργασία τους. Αξίζει να αναφερθεί ότι το κυριότερο πρωτόκολλο που υποστηρίζεται στο επίπεδο αντίληψης είναι το IEEE 802.15.4.

2.3.2. Επίπεδο Μεταφοράς (Transport Layer)

Ο ρόλος του επιπέδου μεταφοράς, το οποίο ονομάζεται αλλιώς και ως επίπεδο δικτύου, είναι να διαβιβάζει τα δεδομένα από το επίπεδο αντίληψης στο επίπεδο επεξεργασίας και αντίστροφα μέσω ενσύρματων ή ασύρματων δικτύων. Επίσης, είναι υπεύθυνο για τη δρομολόγηση των προς μετάδοση πακέτων και τη διευθυνσιοδότηση των συσκευών του δικτύου. Περιέχει διάφορες τεχνολογίες όπως Wi-Fi, Bluetooth, Zigbee, RFID, κλπ. που υποστηρίζουν την ασύρματη επικοινωνία και χρησιμοποιεί τα πρωτόκολλα UDP, TCP, IPv4/IPv6, 6LoWPAN.

2.3.3. Επίπεδο Επεξεργασίας (Processing Layer)

Αναφέρεται και ως επίπεδο ενδιάμεσου λογισμικού (middleware layer) [28] και καθήκον του είναι η αποθήκευση, ανάλυση και επεξεργασία των δεδομένων που λαμβάνει από το επίπεδο μεταφοράς. Για να επιτευχθεί αυτό, χρησιμοποιεί βάσεις δεδομένων, πλατφόρμες υπολογιστικού νέφους και εργαλεία για την επεξεργασία μεγάλου όγκου δεδομένων (big data).

2.3.4. Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής είναι η διεπαφή μέσω της οποίας ο χρήστης μπορεί να συνδεθεί και να αλληλεπιδράσει με τις συσκευές IoHT [27], [29]. Αρμοδιότητα αυτού του επιπέδου είναι να παρέχει στους χρήστες συγκεκριμένες υπηρεσίες εφαρμογών. Οι υπηρεσίες ποικίλουν ανάλογα τον τύπο της εκάστοτε εφαρμογής και το περιεχόμενο των δεδομένων που έχουν παραληφθεί από το προηγούμενο επίπεδο. Κάποια από τα πρωτόκολλα του επιπέδου εφαρμογής είναι τα CoAP, MQTT, AMQP και XMPP.

2.3.5. Επίπεδο Επιχείρησης (Business Layer)

Κύρια λειτουργία του επιπέδου επιχείρησης, που είναι και το υψηλότερο αυτής της αρχιτεκτονικής, είναι η συνολική διαχείριση ενός συστήματος IoT και των εφαρμογών και υπηρεσιών που το απαρτίζουν. Το συγκεκριμένο επίπεδο είναι υπεύθυνο [27], [29] για τον χειρισμό της επιχειρηματικής λογικής του παρόχου υγειονομικής περίθαλψης και την υποστήριξη του κύκλου ζωής της επιχειρηματικής διαδικασίας. Πιο συγκεκριμένα, οι αρμοδιότητές του συμπεριλαμβάνουν την παρακολούθηση, τη διαχείριση, και τη βελτιστοποίηση των επιχειρηματικών διαδικασιών.

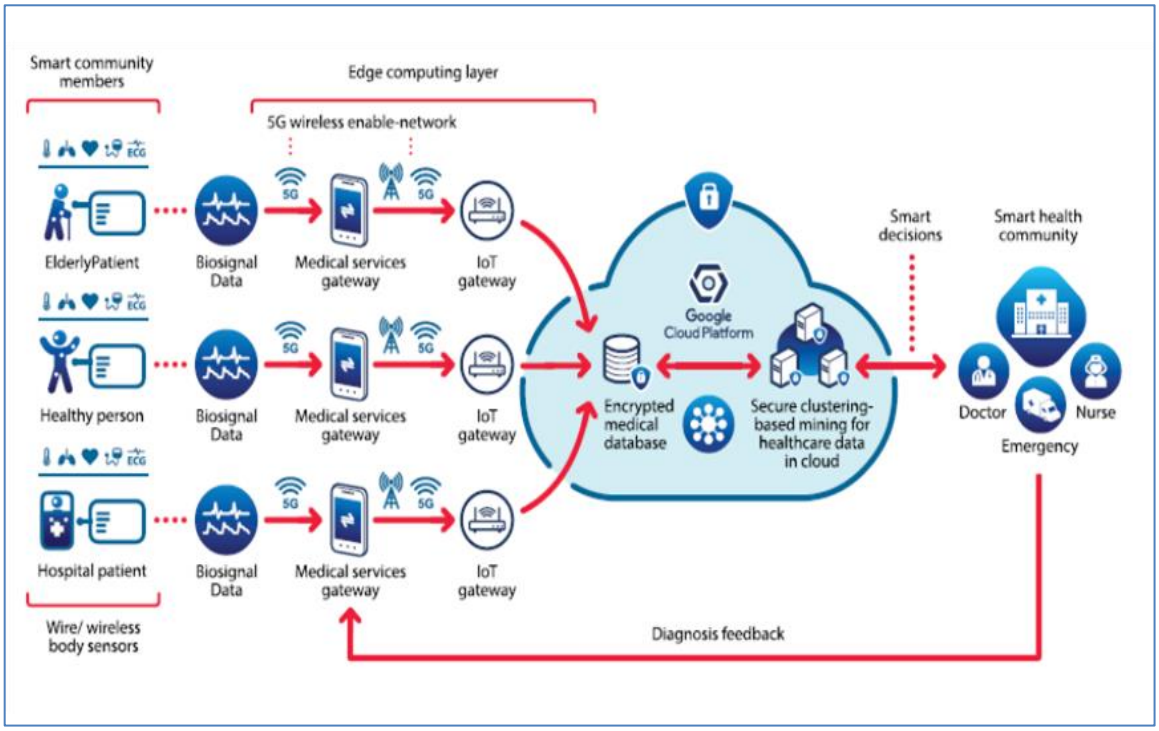
Με βάση τα δεδομένα που λαμβάνονται από το επίπεδο εφαρμογής, δημιουργούνται επιχειρηματικά μοντέλα, μοντέλα κέρδους, γραφήματα, διαγράμματα ροής κλπ. τα οποία βοηθούν στο να προσδιοριστούν μελλοντικές ενέργειες και επιχειρηματικές στρατηγικές που θα είναι ωφέλιμο να ακολουθηθούν [30].

2.4. Τεχνολογίες

Κομβικό ρόλο στη λειτουργία του IoHT έχει η υπολογιστική νέφους (Cloud Computing). Μέσω της τεχνολογίας αυτής εξυπηρετείται η ευρεία πρόσβαση σε παρεχόμενους πόρους και προσφέρονται υπηρεσίες κατόπιν αιτήματος στους εξουσιοδοτημένους χρήστες. Η ενσωμάτωση του cloud computing στο IoHT καθίσταται απαραίτητη εξαιτίας του μεγάλου όγκου δεδομένων που παράγονται από τους διάφορους αισθητήρες, η αποθήκευση και η ανάλυση των οποίων λαμβάνει χώρα σε απομακρυσμένα κέντρα δεδομένων. Παρά τα αναμφισβήτητα οφέλη της τεχνολογίας

δεν παύει να παρατηρείται σημαντική καθυστέρηση, ή οποία είναι αποτρεπτική ιδιαιτέρως σχετικά με την παροχή υπηρεσιών έκτακτης ανάγκης. Πιθανοί τρόποι μείωσης αυτής της καθυστέρησης είναι η χρήση της υπολογιστικής ομίχλης (fog computing) ή υπολογιστικής άκρων (edge computing).

Η υπολογιστική άκρων χαρακτηρίζεται από μια αποκεντρωμένη αρχιτεκτονική που επιτρέπει την επεξεργασία και την ανάλυση μεγάλου ποσοστού των δεδομένων να λαμβάνει χώρα πιο κοντά στην πηγή των δεδομένων, δηλαδή πλησιέστερα στις συσκευές IoT στα όρια του δικτύου. Πιο συγκεκριμένα, συσκευές του δικτύου με τις κατάλληλες υπολογιστικές και αποθηκευτικές ικανότητες λειτουργούν ως αποκεντροποιημένα μικρά κέντρα δεδομένων, αναλαμβάνοντας την ανάλυση δεδομένων και την εκτέλεση διαδικασιών λήψης αποφάσεων, ώστε να εξυπηρετήσουν αποδοτικότερα εφαρμογές που απαιτούν απόκριση πραγματικού χρόνου. Συνεπώς, κάποιες διεργασίες μπορούν να γίνουν τοπικά, ενώ διεργασίες που χρειάζονται μεγαλύτερη υπολογιστική ισχύ παραπέμπονται στο νέφος, γεγονός που συνεισφέρει στην καλύτερη διαχείριση της κίνησης του δικτύου. Αναμφίβολα η υπολογιστική άκρων παρουσιάζει καίρια πλεονεκτήματα αναφορικά με την απόκριση και την κατανάλωση του εύρους ζώνης του δικτύου, ωστόσο το κόστος της απαιτούμενης φυσικής υποδομής καθώς και οι ενδεχόμενοι κίνδυνοι ασφαλείας δεν παύουν να συνιστούν εστία προβληματισμού.



Εικόνα 12. Σχηματική αναπαράσταση ενός μοντέλου συστήματος IoHT όπου φαίνεται η συναρμογή των επιμέρους τεχνολογιών.

Πηγή: [31]

Ο όγκος των πληροφοριών που συλλέγονται είναι τόσο μεγάλος, με αποτέλεσμα οι συμβατικές εφαρμογές λογισμικού για την επεξεργασία δεδομένων να μην επαρκούν. Στο σημείο αυτό είναι κρίσιμη η συμβολή των τεχνικών ανάλυσης μεγάλου όγκου δεδομένων (Big Data Analytics), με σκοπό την εξαγωγή κρυφών μοτίβων και την εύρεση συσχετισμών. Κατά συνέπεια ενισχύεται η εγκυρότητα των ιατρικών διαγνώσεων και αναβαθμίζεται η ποιότητα των υπηρεσιών υγείας.

Ένα από τα δομικά στοιχεία του IoHT όσον αφορά τη συλλογή δεδομένων των ασθενών, είναι οι ιατρικοί αισθητήρες (medical sensors). Μία κατηγορία αυτών που έχει μονοπωλήσει το ενδιαφέρον τα τελευταία χρόνια λόγω της αυξημένης χρήσης τους, είναι οι αισθητήρες ενσωματωμένοι σε φορέσιμες συσκευές (wearables). Μεταξύ των καταγραφόμενων δεδομένων είναι η θερμοκρασία σώματος, η τοποθεσία, η αρτηριακή πίεση και οι καρδιακοί παλμοί του ασθενή. Επίσης, ιδιαίτερα σημαντική είναι και η ύπαρξη των εμφυτεύσιμων αισθητήρων (implantables), οι οποίοι είναι δυνατόν να τοποθετηθούν στο εσωτερικό του ανθρώπινου σώματος ώστε να καταγράφουν μεγαλύτερης ακρίβειας δεδομένα αναφορικά με τις βιολογικές λειτουργίες του οργανισμού.

Για τη μετάδοση των πληροφοριών αυτών όπως είναι προφανές, απαιτείται κάποιου είδους δικτύωση, είτε ενσύρματη, είτε ασύρματη. Πληθώρα δικτύων μπορούν να χρησιμοποιηθούν για να επιτελέσουν αυτόν τον ρόλο, από δίκτυα επικοινωνίας μικρής εμβέλειας (πχ. Ασύρματα Προσωπικά Δίκτυα Υπολογιστών - WPANs, Ασύρματα Τοπικά Δίκτυα Υπολογιστών - WLANs, Ασύρματα Δίκτυα Αισθητήρων - WSNs), μέχρι και δίκτυα επικοινωνίας μεγάλης εμβέλειας (πχ. κάθε είδους κυψελοειδή δίκτυα) [32].

Η ύπαρξη των τεχνολογιών Bluetooth, Επικοινωνίας Κοντινού Πεδίου (Near Field Communication - NFC) και του RFID επιτρέπει την κατασκευή ιατρικών αισθητήρων χαμηλής ισχύος και τον ορισμό αντίστοιχων πρωτοκόλλων επικοινωνίας.

Μια ακόμη πολλά υποσχόμενη τεχνολογία που μπορεί να βρει εφαρμογή στον τομέα του IoHT είναι η Επαυξημένη Πραγματικότητα (Augmented Reality - AR) η οποία επιτρέπει τη θέαση του φυσικού περιβάλλοντος με την προσθήκη σχετικών ψηφιακών πληροφοριών. Μέσω αυτής μπορεί να διευκολυνθεί η εκπαίδευση του ιατρικού προσωπικού, να κατατοπιστούν οι ασθενείς σχετικά με την κατάσταση της υγείας τους ακόμα και να τους δοθούν οδηγίες σε περιπτώσεις έκτακτης ανάγκης (πχ. παροχή πρώτων βοηθειών).

Τέλος, δεν θα μπορούσαμε να μην αναφέρουμε σε αυτό το σημείο και την τεχνολογία της περιβάλλουσας νοημοσύνης (Ambient Intelligence - AmI). Πρόκειται για την εφαρμογή της τεχνητής νοημοσύνης (Artificial Intelligence – AI) στο φυσικό περιβάλλον του ανθρώπου. Με την ενσωμάτωση αισθητήρων και επεξεργαστών σε αντικείμενα καθημερινής χρήσης, το περιβάλλον αποκτά την ικανότητα αλληλεπίδρασης με τον άνθρωπο, με κύριο στόχο να εντοπίζονται ανά πάσα στιγμή οι απαιτήσεις και οι ανάγκες και το περιβάλλον να προσαρμόζεται σε αυτές και, σε

δεύτερο επίπεδο, να προβλέπονται οι ανθρώπινες συμπεριφορές. Αναφορικά με τον τομέα της υγείας το AmI μπορεί να χρησιμοποιηθεί σε περιβάλλοντα όπως σπίτια ασθενών, κλινικές ή νοσοκομεία βελτιώνοντας σε σημαντικό βαθμό τις συνθήκες διαβίωσης των ασθενών.

2.5. Υπηρεσίες IoHT

Στα πλαίσια της υγειονομικής περίθαλψης [32], δεν υπάρχει αυστηρό ορισμός των υπηρεσιών IoT. Με αποτέλεσμα, την ύπαρξη περιπτώσεων όπου μια υπηρεσία δεν μπορεί να διαφοροποιηθεί αντικειμενικά από μια συγκεκριμένη προτεινόμενη λύση ή εφαρμογή.

Μεταξύ των υπηρεσιών που αναφέρονται παρακάτω μερικές έχουν πιο ευρεία έννοια, όπως για παράδειγμα η Διαβίωση Υποβοηθούμενη από το Περιβάλλον (Ambient Assisted Living – AAL) και η Κινητή Υγεία (Mobile Health - mHealth), δηλαδή μπορούν να περιλαμβάνουν αρκετές άλλες υπηρεσίες και εφαρμογές. Σε αντιδιαστολή, υπάρχουν και πιο εξειδικευμένες υπηρεσίες, όπως η Υγειονομική Περίθαλψη Κοινότητας (Community Healthcare) και η Πληροφόρηση σχετικά με την Υγεία των Παιδιών (Children Health Information - CHI).

2.5.1. Διαβίωση Υποβοηθούμενη από το Περιβάλλον (Ambient Assisted Living – AAL)

Είναι μία υπηρεσία η οποία βασίζεται στο IoT και αφορά την παροχή ιατρικής φροντίδας κυρίως σε ηλικιωμένα άτομα και σε άτομα με κινητικά προβλήματα που έχουν ανάγκη από υποστήριξη στον χώρο διαβίωσής τους. Σκοπός της υπηρεσίας AAL είναι να βελτιώσει την ποιότητα ζωής αυτών των ατόμων επιτρέποντάς τους να είναι πιο αυτόνομοι, ασφαλείς και ανεξάρτητοι στην καθημερινότητά τους.

Σε ένα σύστημα AAL περιλαμβάνονται έξυπνες συσκευές, ιατρικοί αισθητήρες, υπολογιστές, ασύρματα δίκτυα, και εφαρμογές λογισμικού, που συντελούν στη δημιουργία ενός ευφυούς περιβάλλοντος διαβίωσης. Σε αυτό το περιβάλλον με χρήση της προαναφερθείσας τεχνολογίας επιτυγχάνεται η συνεχής εξ’ αποστάσεως παρακολούθηση των ανθρώπων από τα μέλη της οικογένειάς τους ή και από κάποια ομάδα επαγγελματιών υγείας, που έχουν τη δυνατότητα να παρέμβουν σε περίπτωση όπου παραστεί ανάγκη.

2.5.2. Κινητή Υγεία (Mobile Health - mHealth)

Η Κινητή Υγεία αναφέρεται στη χρήση κινητών συσκευών όπως κινητά τηλέφωνα, φορέσιμες συσκευές, και άλλες ασύρματες συσκευές για τη συλλογή πληροφοριών υγείας σε πραγματικό χρόνο. Με την τεχνολογική πρόοδο αυξάνεται η διαθεσιμότητα

των συσκευών αυτών και συνεπώς προοδευτικά μεγαλύτερο μέρος του πληθυσμού αποκτά πρόσβαση στην υπηρεσία αυτή.

2.5.3. Ανεπιθύμητη Αντίδραση Φαρμάκου (Adverse Drug Reaction - ADR)

Οι ανεπιθύμητες αντιδράσεις που μπορούν να προκληθούν μετά τη λήψη κάποιου φαρμάκου ή συνδυασμού αυτών και έχουν συνήθως επιβλαβείς επιδράσεις στον οργανισμό των ασθενών αποτελούν ένα ζήτημα εξέχουσας σημασίας για την επιστημονική κοινότητα. Στις ανεπιθύμητες αντιδράσεις συγκαταλέγονται οι αλλεργικές αντιδράσεις, οι παρενέργειες, και η αλληλεπίδραση μεταξύ φαρμάκων. Σε μερικές περιπτώσεις ανάλογα με το είδος της ανεπιθύμητης αντίδρασης είναι δυνατόν να εμφανιστούν στον ασθενή ήπια έως και πολύ σοβαρά συμπτώματα.

Το IoT είναι ικανό να προσφέρει λύσεις για την πρόληψη και αντιμετώπιση ανεπιθύμητων αντιδράσεων. Ένα από τα συστήματα IoT που έχουν προταθεί [33], περιλαμβάνει προσωπικές συσκευές οι οποίες με τη χρήση τεχνολογιών ταυτοποίησης όπως RFID, Επικοινωνία Κοντινού πεδίου (Near Field Communication - NFC) και barcode συμβάλλουν στην ταυτοποίηση των φαρμάκων και στην παρακολούθηση της φαρμακευτικής αγωγής σε έναν ασθενή.

Μετά το στάδιο της ταυτοποίησης ενός φαρμάκου [33], ακολουθεί η πιστοποίηση της συμβατότητας του φαρμάκου από το ευφυές φαρμακευτικό υπολογιστικό σύστημα (Pharmaceutical Intelligent Information System - PIIS), το οποίο ελέγχει αν το συγκεκριμένο φάρμακο είναι κατάλληλο αναφορικά με το αλλεργικό προφίλ και το ιατρικό ιστορικό του ασθενή.

2.5.4. Υγειονομική Περίθαλψη Κοινότητας (Community Healthcare)

Ακόμα μία σημαντική υπηρεσία που μπορεί να προσφέρει το IoT σχετικά με τον τομέα της υγείας είναι η υποστήριξη της υγειονομικής περίθαλψης μιας συγκεκριμένης κοινότητας. Πρόκειται για ένα δίκτυο [32], [34] το οποίο βασίζεται στο IoT περιλαμβάνοντας έξυπνες συσκευές και αισθητήρες και καλύπτει την έκταση μιας τοπικής κοινότητας, όπως μια κατοικημένη περιοχή ή ένας αγροτικός οικισμός. Αυτό το δίκτυο συνδέεται σε ένα κεντρικοποιημένο σύστημα υγειονομικής περίθαλψης με συνέπεια να ικανοποιούνται αποτελεσματικά οι ιατρικές ανάγκες της κοινότητας και πιθανές καταστάσεις έκτακτης ανάγκης, και να διαμοιράζονται πληροφορίες σχετικά με την υγεία.

2.5.5. Πληροφόρηση σχετικά με την Υγεία των Παιδιών (Children Health Information - CHI)

Τα πρώτα χρόνια της ζωής ενός παιδιού είναι ιδιαίτερα κρίσιμα για την υγιή ανάπτυξή του. Η χρήση νέων τεχνολογιών όπως το IoT μπορεί να βοηθήσει στην υποστήριξη και στη διατήρηση της ευεξίας (wellbeing) των παιδιών μέσω της

παρακολούθησης της κατάστασης της υγείας τους. Για αυτόν τον λόγο έχει αναπτυχθεί μία εξειδικευμένη υπηρεσία του IoHT, το CHI, για την παρακολούθηση της υγείας των παιδιών που έχουν ψυχικά, συμπεριφορικά ή συναισθηματικά προβλήματα [34]. Επιπροσθέτως, έχουν σχεδιαστεί ειδικές συσκευές και εφαρμογές βασισμένες στο IoT για να αναδείξουν τη σημασία της ευεξίας, της διατροφής και του υγιεινού τρόπου ζωής στα μικρά παιδιά.

2.5.6. Σημασιολογική Ιατρική Πρόσβαση (Semantic Medical Access - SMA)

Η σημασιολογία και οι οντολογίες χρησιμοποιούνται ευρέως στον διαμοιρασμό μεγάλου όγκου ιατρικών πληροφοριών και γνώσεων. Οι δυνατότητες που παρέχει η αξιοποίηση της σημασιολογίας και της οντολογίας με την ενσωμάτωσή της στην αρχιτεκτονική IoT συστημάτων υγειονομικής περίθαλψης έχουν αποτελέσει το επίκεντρο της προσοχής και το σημείο πραγμάτευσης πληθώρας μελετών. Ως αποτέλεσμα των παραπάνω, έχει γίνει δυνατή η υποστήριξη της υπηρεσίας SMA που βοηθά στην επεξεργασία πανταχού διαθέσιμων δεδομένων (ubiquitous data) τα οποία διατίθενται στο ιατρικό νέφος [35].

2.5.7. Πρόσβαση Φορέσιμης Συσκευής (Wearable Device Access)

Η τεχνολογική εξέλιξη έχει οδηγήσει στην ανάπτυξη διαφόρων ειδών αισθητήρων για ποικίλο εύρος ιατρικών εφαρμογών. Σε πολλές περιπτώσεις, οι αισθητήρες αυτοί ενσωματώνονται σε φορέσιμες συσκευές καθιστώντας τες κατάλληλες να παρέχουν υπηρεσίες υγειονομικής περίθαλψης μέσω του IoT. Η ετερογενής φύση των φορέσιμων αυτών προϊόντων και των ιατρικών αισθητήρων αποκαλύπτει πολυάριθμες προκλήσεις σχετικά με την εν λόγω ενσωμάτωσή τους [32]. Σε αυτό το πλαίσιο, απαιτείται μια ειδική υπηρεσία που ονομάζεται πρόσβαση φορέσιμης συσκευής.

2.5.8. Έμμεση Υγειονομική Περίθαλψη Έκτακτης Ανάγκης (Indirect Emergency Healthcare - IEH)

Σε καταστάσεις έκτακτης ανάγκης όπως ακραία καιρικά φαινόμενα, φυσικές καταστροφές και ατυχήματα, η ζωή των ανθρώπων μπορεί να βρεθεί σε κίνδυνο. Σε μερικές από αυτές τις καταστάσεις είναι αναγκαία η έγκαιρη και αποτελεσματική απόκριση ενός επαγγελματία υγείας. Για αυτό το λόγο, αναπτύχθηκε μια ειδική υπηρεσία βασισμένη στο IoT που μπορεί να προσφέρει λύσεις όπως διαθεσιμότητα πληροφοριών, τροποποίηση ειδοποιήσεων, δράση μετά το ατύχημα και τήρηση αρχείων [32], [34].

2.6. Εφαρμογές IoHT

2.6.1. Παρακολούθηση της γλυκόζης αίματος (Blood Glucose Monitoring)

Ο σακχαρώδης διαβήτης είναι μία χρόνια μεταβολική νόσος η οποία χαρακτηρίζεται από αυξημένα επίπεδα γλυκόζης στο αίμα. Οι επιπλοκές που είναι δυνατόν να προκληθούν από αυτήν τη νόσο περιλαμβάνουν σοβαρά περιστατικά τα οποία αν δεν αντιμετωπιστούν εγκαίρως μπορεί να οδηγήσουν ακόμη και σε θάνατο.

Επομένως, η παρακολούθηση της γλυκόζης στο αίμα μέσω συσκευών IoT είναι ιδιαιτέρως χρήσιμη για τους διαβητικούς ασθενείς, διότι οι σημαντικές πληροφορίες που συλλέγονται σχετικά με την υγεία τους μπορούν να βοηθήσουν στη διαχείριση της νόσου και στην αποφυγή κινδύνων [36].

Επιπροσθέτως, οι συσκευές IoT που χρησιμοποιούνται για αυτόν τον σκοπό, έχουν τη δυνατότητα να υπενθυμίζουν τη λήψη φαρμάκων, να προτείνουν υγιεινές διατροφικές συνήθειες, ακόμα και να προειδοποιούν τον ασθενή σε περίπτωση κινδύνου.

Πιο συγκεκριμένα με την τακτική παρακολούθηση της γλυκόζης στο αίμα εξάγονται αντιπροσωπευτικά μοτίβα των διακυμάνσεων του επιπέδου γλυκόζης στο αίμα τα οποία βοηθούν τους ασθενείς να προγραμματίσουν με τον βέλτιστο τρόπο, τη φαρμακευτική τους αγωγή, τα γεύματα και τις δραστηριότητές τους [32].

2.6.2. Παρακολούθηση Αρτηριακής Πίεσης (Blood Pressure Monitoring)

Η υψηλή αρτηριακή πίεση (υπέρταση) επηρεάζει ένα μεγάλο ποσοστό ανθρώπων παγκοσμίως και αποτελεί σημαντικό πρόβλημα υγείας, το οποίο συνήθως διαγιγνώσκεται σε προχωρημένο στάδιο. Η συχνή παρακολούθηση της αρτηριακής πίεσης μέσω του IoT είναι πολύτιμη και συμβάλλει στην πρώιμη διάγνωση της υπέρτασης.

Προς αυτήν την κατεύθυνση, έχουν σχεδιαστεί και ήδη βρίσκονται σε χρήση, συστήματα και συσκευές IoT για την παρακολούθηση της αρτηριακής πίεσης, τα οποία πραγματοποιούν ακριβείς μετρήσεις στους ασθενείς, οποιαδήποτε στιγμή και σε οποιαδήποτε τοποθεσία και αν βρίσκονται. Επίσης, οι συγκεκριμένες μετρήσεις γίνονται διαθέσιμες σε εξειδικευμένο ιατρό μέσω διαδικτυακής εφαρμογής ή εφαρμογής κινητού.

2.6.3. Παρακολούθηση Ηλεκτροκαρδιογραφήματος (Electrocardiogram Monitoring - ECG)

Η ηλεκτροκαρδιογραφία είναι μια διαγνωστική εξέταση κατά την οποία καταγράφεται η ηλεκτρική δραστηριότητα της καρδιάς και τυπώνεται ένα ηλεκτροκαρδιογράφημα. Η ανάλυσή του δίνει πληροφορίες για τον καρδιακό ρυθμό

του ασθενή, οι οποίες συμβάλλουν στη διάγνωση ποικίλων καρδιαγγειακών νοσημάτων.

Συστήματα παρακολούθησης ηλεκτροκαρδιογραφήματος βασισμένα στο IoT προσφέρουν τη δυνατότητα εξατομικευμένης παρακολούθησης σε πραγματικό χρόνο, ώστε η καρδιακή λειτουργία του ασθενή να καταγράφεται συνεχώς χωρίς καμία διακοπή.

Τα δεδομένα που συλλέγονται, παρέχονται εξ' αποστάσεως στο ιατρικό προσωπικό μέσω εφαρμογών κινητού με άμεσο αποτέλεσμα να μην χρειάζεται ο ασθενής να επισκέπτεται το νοσοκομείο εκτός αν βρεθεί σε έκτακτη ανάγκη [37].

2.6.4. Παρακολούθηση Θερμοκρασίας Σώματος (Body Temperature Monitoring)

Η ομοιόσταση αναφέρεται ως η ικανότητα ενός οργανισμού να διατηρεί σταθερή την εσωτερική του κατάσταση ανεξάρτητα από τις εξωτερικές περιβαλλοντικές συνθήκες. Ένας από τους ομοιοστατικούς μηχανισμούς είναι η ρύθμιση και διατήρηση της θερμοκρασίας του ανθρώπινου σώματος σε ένα συγκεκριμένο επίπεδο. Η θερμοκρασία σώματος αποτελεί βασικό ζωτικό σημείο και είναι ένα από τα στοιχεία που εξετάζονται πρωταρχικά σε έναν ασθενή για τη λήψη μιας γενικής εικόνας της κατάστασής του. Σε διάφορες παθήσεις κρίνεται απαραίτητη η συνεχής παρακολούθηση της θερμοκρασίας σώματος του ασθενή, παρέχοντας πληροφορίες σχετικά με τη λειτουργία της ομοιόστασης του οργανισμού του.

Συστήματα για την παρακολούθηση της θερμοκρασίας σώματος, που αναπτύσσονται με βάση το IoT, περιλαμβάνουν κατάλληλους αισθητήρες για την ανίχνευση της θερμοκρασίας του ασθενή, αντίστοιχες διαδικτυακές εφαρμογές και το νέφος IoT όπου γίνεται η επεξεργασία των δεδομένων. Ο χρήστης μπορεί να έχει πρόσβαση οποιαδήποτε στιγμή στις καταγραφές του με χρήση smartphone και να προειδοποιείται, όταν παρατηρηθεί κάποια ασυνήθιστη κατάσταση.

2.6.5. Παρακολούθηση Κορεσμού του Οξυγόνου (Oxygen Saturation Monitoring)

Η παλμική οξυμετρία είναι μία μέθοδος για την μη επεμβατική και ανώδυνη παρακολούθηση του κορεσμού οξυγόνου στο αίμα. Με τη συμβολή τεχνολογιών IoT, η παρακολούθηση αυτή καθίσταται αδιάλειπτη, καθώς φορέσιμα παλμικά οξύμετρα μπορούν να χρησιμοποιηθούν σε εφαρμογές συνεχούς και απομακρυσμένης παρακολούθησης ασθενών.

2.6.6. Σύστημα Αποκατάστασης (Rehabilitation System)

Ένα μεγάλο εύρος παθήσεων ή ατυχημάτων οδηγεί τους ασθενείς σε κέντρα αποκατάστασης για την αποθεραπεία τους. Η φυσική ιατρική και η αποκατάσταση αντιπροσωπεύουν έναν ζωτικό κλάδο της ιατρικής, διότι μπορούν να βελτιώσουν και να αποκαταστήσουν τη λειτουργική ικανότητα και ποιότητα ζωής ατόμων με κάποια σωματική δυσλειτουργία ή αναπηρία [32].

Το IoT έχει τη δυνατότητα να βελτιώσει τα συστήματα αποκατάστασης όσον αφορά τον περιορισμό των προβλημάτων που σχετίζονται με τη γήρανση του πληθυσμού, την έλλειψη υγειονομικών εγκαταστάσεων και τον ανεπαρκή αριθμό επαγγελματιών υγείας [32].

Έχουν προταθεί εξειδικευμένα συστήματα αποκατάστασης IoT για χρήση σε πολλά και διαφορετικά περιβάλλοντα και για μεγάλο εύρος παθήσεων. Αυτά τα συστήματα παρέχουν την κατάλληλη υποδομή, ώστε να υποστηρίζονται αποτελεσματικά οι απομακρυσμένες συνεδρίες μεταξύ ιατρών και ασθενών.

2.6.7. Διαχείριση Φαρμακευτικής Αγωγής (Medication Management)

Η φαρμακευτική συμμόρφωση των ασθενών είναι ένα ζήτημα ιδιαίτερης βαρύτητας για την ασφάλειά τους και η μη τήρηση των ιατρικών συστάσεων μπορεί να αποβεί επικίνδυνη. Μια εφαρμογή του IoHT που είναι ικανή να προσφέρει λύσεις στο παραπάνω ζήτημα, είναι η διαχείριση της φαρμακευτικής αγωγής των ασθενών.

Για την υποστήριξη της συγκεκριμένης εφαρμογής έχουν σχεδιαστεί διάφορα προϊόντα IoT, με πιο χαρακτηριστικά τα έξυπνα κουτιά για χάπια, κατάλληλα για την οργάνωση φαρμάκων. Στα έξυπνα κουτιά υπάρχει ένας αισθητήρας σε κάθε ξεχωριστή θήκη στην οποία τοποθετείται κάποιο χάπι και καταγράφει αν υπάρχει ή όχι περιεχόμενο. Αυτοί οι αισθητήρες συνδέονται ασύρματα με το smartphone του χρήστη και μέσω της αντίστοιχης εφαρμογής ουσιαστικά τον ενημερώνουν αν ακολουθεί σωστά τη φαρμακευτική του αγωγή. Επιπλέον, δίνεται η δυνατότητα στον χρήστη να ορίσει τις ώρες που πρέπει να λάβει τα φάρμακά του και έπειτα το σύστημα υπενθύμισης λήψης φαρμάκου θα τον ειδοποιεί, ώστε να μην παραληφθεί καμία δόση.

2.6.8. Διαχείριση Αναπηρικών Αμαξιδίων (Wheelchair Management)

Έξυπνα αναπηρικά αμαξίδια που είναι πλήρως αυτοματοποιημένα και βασίζονται στο IoT έχουν αναπτυχθεί για να βελτιώσουν την κινητικότητα και την ποιότητα ζωής ανθρώπων με κινητικά προβλήματα [32], [37]. Σε αυτά ενσωματώνονται διαφόρων ειδών αισθητήρες για την παρακολούθηση της κατάστασης του αμαξιδίου, τον εντοπισμό της τοποθεσίας του καθώς και για την ανίχνευση εμποδίων στον περιβάλλοντα χώρο του χρήστη. Επιπροσθέτως, υποστηρίζεται η παρακολούθηση των ζωτικών δεδομένων των χρηστών τα οποία καθίστανται προσβάσιμα στο ιατρικό

προσωπικό, το οποίο θα μπορεί να σπεύσει προς βοήθεια του χρήστη σε περίπτωση έκτακτης ανάγκης.

2.7. Πλεονεκτήματα

Το IoHT φέρει ένα πλήθος υπηρεσιών και εφαρμογών, κάθε μια εκ των οποίων προσφέρει επιμέρους οφέλη τόσο για τους ασθενείς όσο και για το ιατρονοσηλευτικό προσωπικό. Στην προσπάθεια εντοπισμού σημείων σύγκλισης μεταξύ των πλεονεκτημάτων παρατηρούνται οι εξής τέσσερις γενικές κατευθύνσεις:

1) **Μείωση του κόστους περίθαλψης:** Η κατάσταση της υγείας των ασθενών παρακολουθείται εξ' αποστάσεως σε πραγματικό χρόνο, ακόμα και όταν αυτοί βρίσκονται στο σπίτι τους. Συνεπώς ελαχιστοποιούνται έως και εξαλείφονται τα έξοδα που αφορούν την παραμονή του ασθενή στις νοσοκομειακές δομές και αποτρέπονται οι άσκοπες επισκέψεις σε γιατρούς οι οποίοι μπορούν να έχουν συνεχή και εύκολη πρόσβαση στα δεδομένα των ασθενών.

2) **Απομακρυσμένη παρακολούθηση των ασθενών σε πραγματικό χρόνο:** Η απομακρυσμένη παρακολούθηση των ασθενών σε πραγματικό χρόνο αποτελεί μεγάλο πλεονέκτημα για τον τομέα της Υγειονομικής Περίθαλψης. Η αξιοποίηση αυτής της λειτουργίας εκτός των άλλων οδηγεί επίσης στη βελτίωση της διαχείρισης της νόσου του ασθενή, καθώς και στη διαχείριση και αντιμετώπιση κάποιου έκτακτου περιστατικού ή επιπλοκής της νόσου.

3) **Πρόβλεψη και διάγνωση ασθενειών:** Η χρήση τεχνικών ανάλυσης μεγάλου όγκου δεδομένων (big data analytics) βοηθάει στην εξαγωγή, συλλογή και ανάλυση πληροφοριών σχετικά με την υγεία του ασθενή επιτρέποντας την έγκαιρη πρόβλεψη και διάγνωση προβλημάτων υγείας, ώστε αυτά να μπορούν να αντιμετωπιστούν σε πρώιμο στάδιο και να θεραπευτούν.

4) **Ευχρηστία:** Οι χρήστες μπορούν με ευχέρεια να χρησιμοποιούν τις συσκευές IoHT, αφού αυτές σχεδιάζονται με τέτοιο τρόπο, ώστε να παρέχουν μία φιλική διεπαφή χρήστη. Επίσης δίνεται η δυνατότητα στους χρήστες να έχουν πρόσβαση στα δεδομένα της υγείας τους οποιαδήποτε στιγμή επιθυμούν και μάλιστα με απλό τρόπο όπως με τη χρήση κατάλληλης εφαρμογής στο smartphone.

2.8. Προκλήσεις

Παρά τα αναμφισβήτητα οφέλη της υιοθέτησης της τεχνολογίας IoHT για το σύστημα υγείας, δεν παύει να υπάρχει πλήθος πρακτικών ζητημάτων, που πιθανώς να αποτελέσουν τροχοπέδη για την ομαλή μετάβαση στη νέα τεχνολογία και την

αποδοτικότητα του αναβαθμισμένου υγειονομικού συστήματος. Η διευθέτηση των ζητημάτων αυτών και η εύρεση εφαρμόσιμων λύσεων αποτελούν τις βασικότερες προκλήσεις, τις οποίες η επιστημονική κοινότητα καλείται να αντιμετωπίσει. Οι προαναφερθείσες αντιξοότητες και κατ' επέκταση οι αντίστοιχες προκλήσεις που ανακύπτουν μπορούν να ομαδοποιηθούν σε διακριτές κατηγορίες με βάση τις θεμελιώδεις λειτουργίες του IoHT, οι οποίες πλήττονται.

1) **Διαχείριση δεδομένων:** Η αποτελεσματική διαχείριση δεδομένων διαδραματίζει κυρίαρχο ρόλο στα συστήματα IoHT και αποτελεί προϋπόθεση για τη βέλτιστη λειτουργία τους. Η ανάγκη για άμεση απόκριση των συστημάτων IoHT και διαχείριση μεγάλων δεδομένων εισάγει όπως είναι φυσικό διάφορες προκλήσεις. Τα δεδομένα που καλείται να διαχειριστεί ένα σύστημα IoHT είναι τεράστιου όγκου και αδόμητα, συνεπώς ο χρόνος επεξεργασίας τους είναι μεγάλος. Η επεξεργασία αυτών απαιτεί υπολογιστικά συστήματα υψηλής απόδοσης (High Performance Computing - HPC). Σε σχέση με το μειούμενο κόστος των ιατρικών αισθητήρων, το κόστος αγοράς και συντήρησης συστημάτων HPC είναι σημαντικά μεγαλύτερο και η κάλυψή του συνιστά πρόκληση για την εφαρμογή του IoHT σε μεγάλη κλίμακα. Μια επιπλέον πρόκληση, λόγω της ιδιαίτερης φύσης της παροχής υπηρεσιών υγειονομικής περίθαλψης, που μπορεί να έχει και έκτακτο χαρακτήρα, είναι η άμεση επεξεργασία δεδομένων και ελαχιστοποίηση του χρόνου απόκρισης.

2) **Διαλειτουργικότητα:** Ο όρος «διαλειτουργικότητα» αναφέρεται στην ικανότητα διαφορετικών συστημάτων να επικοινωνούν μεταξύ τους και θεωρείται παράγοντας-κλειδί για την αξιοποίηση των πλήρων δυνατοτήτων του IoHT. Οι αισθητήρες που χρησιμοποιούνται μπορεί να ανήκουν σε διαφορετικό κατασκευαστή, το οποίο συνήθως συνεπάγεται την υποστήριξη διαφορετικών πρωτοκόλλων επικοινωνίας. Το γεγονός αυτό καθιστά την επικοινωνία δύσκολη. Η ετερογένεια των συσκευών και των συστημάτων στο IoHT σε συνδυασμό με τη χρήση ανομοιογενών πρωτοκόλλων επικοινωνίας και υλικολογισμικού από τους κατασκευαστές, έχουν αναδείξει την ανάγκη για θέσπιση ενός ανοιχτού προτύπου (open standard) που θα ακολουθείται από την πλειοψηφία τους. Προς αυτήν την κατεύθυνση μολονότι έχουν γίνει σχετικές προσπάθειες, τίποτα δεν έχει ακόμα οριστικοποιηθεί ή επισημοποιηθεί.

3) **Συνεργασία των ενδιαφερόμενων μερών και εξοικείωση:** Στο πεδίο της υγειονομικής περίθαλψης, εμπλέκονται πολλά ενδιαφερόμενα μέρη όπως ασθενείς, πάροχοι υπηρεσιών υγείας, ιατρονοσηλευτικό προσωπικό, ερευνητικά εργαστήρια και σχεδιαστές εφαρμογών IoHT. Η διαρκής συνεργασία μεταξύ αυτών των μερών είναι επιβεβλημένη για την επιτυχή μετάβαση στο IoHT.

Οι ιατροί, το νοσηλευτικό προσωπικό και οι ασθενείς έχουν εξειδικευμένες ανάγκες, οι οποίες είναι κρίσιμο να αναγνωριστούν και να κατανοηθούν ώστε να επιτευχθεί η βέλτιστη παροχή υπηρεσιών. Σε πρώτο στάδιο είναι επιτακτική η συλλογή πληροφοριών μέσω ερευνών και εργαστηριακών μελετών και στη συνέχεια η ανάλυσή τους για τον προσδιορισμό αυτών των αναγκών. Κατά αυτόν τον τρόπο, είναι δυνατή η ανάλογη προσαρμογή των παρεχόμενων υπηρεσιών. Ο κλάδος της υγείας έχει συγκεκριμένες ιδιαιτερότητες που δεν επιτρέπουν πλήρως αυτοματοποιημένες διαδικασίες. Η συμβολή του ανθρώπινου παράγοντα είναι καίρια για το IoHT και δεν καταργείται η προσωπική σχέση ασθενή-ιατρού. Ωστόσο η υιοθέτηση της νέας τεχνολογίας προϋποθέτει την εκπαίδευση των επαγγελματιών υγείας σχετικά με τη χρήση της, ενώ και οι ασθενείς πρέπει με τη σειρά τους να εξοικειωθούν με αυτήν. Όπως είναι ευνόητο αυτή η διαδικασία απαιτεί ανθρώπινους και οικονομικούς πόρους και είναι χρονοβόρα.

4) **Ασφάλεια και Ιδιωτικότητα:** Η ασφάλεια και ιδιωτικότητα αποτελούν σημαντικά πεδία για το IoT, καθώς σε αυτά εντοπίζονται ευπάθειες που χρήζουν ιδιαίτερης προσοχής. Στην περίπτωση του IoHT εξαιτίας των ευαίσθητων δεδομένων (π.χ. ιατρικές εκθέσεις, ιστορικό του ασθενή, αριθμός κοινωνικής ασφάλισης κ.α.) που χειρίζεται το σύστημα, η ασφάλεια και η ιδιωτικότητα ανάγονται πλέον σε κυρίαρχα ζητήματα.
   Στο σημείο αυτό αξίζει να σημειωθεί πως τα συστήματα IoT δεν είχαν σχεδιαστεί εξαρχής με γνώμονα την ασφάλεια, αλλά με επίκεντρο προσοχής τη λειτουργικότητά τους. Σήμερα η ασφάλεια θεωρείται ευρέως ως ο κυριότερος παράγοντας που εμποδίζει την υιοθέτηση τέτοιων συστημάτων σε μεγάλη κλίμακα. Οι προκλήσεις στον τομέα της ασφάλειας, ως αντικείμενο της παρούσας εργασίας, θα αναλυθούν διεξοδικά σε επόμενο κεφάλαιο.

3. Ασφάλεια στο IoHT

3.1. Εισαγωγή στην Ασφάλειας στο IoHT

Η ασφάλεια στον τομέα της Πληροφορικής αποτελεί μείζον ζήτημα στη σημερινή εποχή, αλλά η αξία και η σημασία της αναδείχθηκε ήδη από τα πρώιμα χρόνια του Διαδικτύου. Το IoT όντας μια καινοτόμος τεχνολογία εξελίσσεται και διεισδύει βαθμιαία σε ολοένα και περισσότερους τομείς της καθημερινής ζωής. Εντούτοις, ζητήματα ασφάλειας συνεχίζουν να συνιστούν εστίες προβληματισμού και βασικότερα πεδία έρευνας. Οι πρώτες εφαρμογές του IoT αναπτύχθηκαν με κεντρικό άξονα την πραγμάτωση του τεχνολογικού οράματος, στο οποίο φυσικά αντικείμενα στην καθημερινή ζωή των ανθρώπων θα διασυνδέονται και θα αλληλεπιδρούν με τον άνθρωπο, με σκοπό την αυτοματοποίηση διαφόρων διαδικασιών. Ωστόσο η ασφάλεια ως ποιοτικό χαρακτηριστικό των παρεχόμενων υπηρεσιών IoT παραγκωνίστηκε για ένα διόλου αμελητέο χρονικό διάστημα, ώσπου αναδύθηκε εκ νέου, όταν τέθηκε επί τάπητος η υιοθέτηση από το ευρύ κοινό και η υλοποίηση συστημάτων IoT σε μεγάλη κλίμακα.

Συγκριτικά με τις υπόλοιπες εφαρμογές του IoT, στο IoHT η ασφάλεια αποκτά αυξημένη βαρύτητα, καθώς το σύστημα διαχειρίζεται ευαίσθητα προσωπικά ιατρικά δεδομένα. Η προσπέλαση δεδομένων αυτής της φύσης αποδεικνύεται ιδιαίτερα επικερδής για τους κυβερνοεγκληματίες και, κατά συνέπεια, τα υπολογιστικά συστήματα που επεξεργάζονται πληροφορίες υγείας αποτελούν πόλο έλξης κυβερνοεπιθέσεων. Αυτές οι πληροφορίες, λόγω του προσωπικού τους χαρακτήρα, μπορούν μεταξύ άλλων να χρησιμοποιηθούν είτε για εκβιασμό του θύματος είτε για να υποδυθεί ο επιτιθέμενος την ταυτότητά του. Η προσφορά και η ζήτηση ιατρικών πληροφοριών έχει οδηγήσει στην άνθιση μιας εξαιρετικά προσοδοφόρας παράνομης αγοράς στο σκοτεινό διαδίκτυο (dark web). Ενδεικτικά, αξίζει να αναφερθεί, πως οι πληροφορίες που εμπεριέχονται σε έναν ηλεκτρονικό φάκελο υγείας (EHR) κοστολογούνται έως και δέκα φορές ακριβότερα σε σχέση με τις πληροφορίες μιας πιστωτικής κάρτας, ανάλογα πάντα με το πόσο πλήρης είναι ο φάκελος [38].

Κοινό τόπο μεταξύ των ερευνητών αποτελεί η άποψη πως κανένα σύστημα IoHT, όπως και κανένα άλλο πληροφοριακό σύστημα, δεν μπορεί να είναι πλήρως θωρακισμένο εναντίον εσωτερικών και εξωτερικών κινδύνων. Η ανάδειξη κάποιου κενού ασφαλείας, το οποίο δεν λήφθηκε υπόψη κατά τη μελέτη, το σχεδιασμό, την υλοποίηση ή την εγκατάσταση του συστήματος, δεν είναι παρά ζήτημα χρόνου. Επιπλέον ποτέ δεν μπορεί να αποκλειστεί, σε θεωρητικό τουλάχιστον επίπεδο, το ενδεχόμενο επιτυχίας μιας επίθεσης, ακόμα και αν αυτή προϋποθέτει μη αναμενόμενα γεγονότα ή δυσεύρετους πόρους και φαντάζει αρχικά σαν μη ρεαλιστικό σενάριο. Παρότι η πιθανότητα παραβίασης δεν είναι δυνατόν να εκμηδενιστεί, είναι εφικτή η σημαντική ελάττωσή της. Προς την κατεύθυνση αυτή είναι αναγκαία σε πρώτο στάδιο η

ανάλυση των υπαρχόντων απειλών και των επιθέσεων, η αναγνώριση των προκλήσεων ασφαλείας και η κατανόηση των αρχών και των απαιτήσεων, τις οποίες ένα σύστημα ασφαλείας καλείται να εξυπηρετήσει.

3.2. Απαιτήσεις Ασφάλειας στο IoHT

Κάθε υπολογιστικό σύστημα και κατά επέκταση το IoHT οφείλει να τηρεί κάποιες αρχές για να υποστηρίζει την ασφάλεια. Μολονότι σχετικά με αυτές τις αρχές δεν υφίσταται καθολική επιστημονική συναίνεση, στα πλαίσια αυτής της εργασίας αξίζουν να επισημανθούν οι ακόλουθες.

- **Εμπιστευτικότητα και Ιδιωτικότητα (Confidentiality and Privacy):** Η ικανότητα να παραμένουν τα δεδομένα ιδιωτικά κατά τα στάδια της συγκέντρωσης, μετάδοσης και αποθήκευσής τους. Η εμπιστευτικότητα στο IoHT εξασφαλίζει το απροσπέλαστο των ιατρικών δεδομένων των ασθενών από μη εξουσιοδοτημένους χρήστες.

- **Ακεραιότητα (Integrity):** Σκοπός της ακεραιότητας είναι η διασφάλιση ότι τα δεδομένα δεν θα υποστούν καμία παραποίηση/αλλοίωση κατά την ασύρματη μετάδοσή τους εξαιτίας μη εξουσιοδοτημένης παρέμβασης ή τυχαίου σφάλματος επικοινωνίας. Εξίσου σημαντική είναι η ακεραιότητα των δεδομένων και κατά το στάδιο της αποθήκευσής τους.

- **Διαθεσιμότητα (Availability):** Ο όρος αναφέρεται στη δυνατότητα των υπηρεσιών IoHT να παραμένουν διαθέσιμες σε εξουσιοδοτημένα μέρη του συστήματος ακόμα και υπό συνθήκες κάποιας επίθεσης Άρνησης Υπηρεσίας (Denial-of-service attack, DoS).

- **Αυθεντικοποίηση (Authentication):** Η αυθεντικοποίηση πιστοποιεί ως ένα βαθμό ότι οι οντότητες (όπως χρήστες και συσκευές) είναι όντως αυτές που υποδεικνύει η ταυτότητά τους. Αυτό εξυπηρετείται μέσω της επαλήθευσης ταυτότητας των οντοτήτων που είναι σε θέση να επικοινωνήσουν, η οποία μπορεί να επιτευχθεί με την ανταλλαγή κλειδιών αυθεντικοποίησης, ψηφιακών πιστοποιητικών, ή ψηφιακών υπογραφών. Η διαδικασία αυθεντικοποίησης είναι απαραίτητο να λαμβάνει χώρα πριν την οποιαδήποτε μετάδοση πληροφοριών.

- **Εξουσιοδότηση (Authorization):** Η εξουσιοδότηση διασφαλίζει ότι μόνο οι εξουσιοδοτημένες οντότητες μπορούν να έχουν πρόσβαση σε υπηρεσίες και πόρους του δικτύου.

- **Μη Αποποίηση (Non Repudiation):** Η ικανότητα κάθε εξουσιοδοτημένος χρήστης ή κόμβος του συστήματος να καθίσταται υπεύθυνος για τις ενέργειές του. Με άλλα λόγια, αυτή η απαίτηση εγγυάται ότι οποιαδήποτε αλληλεπίδραση στο σύστημα δεν μπορεί να αμφισβητηθεί [39].

- **Ενημερωμένα Δεδομένα (Data Freshness):** Ο όρος ενημερωμένα δεδομένα περιγράφει την ανάγκη τα δεδομένα να είναι πρόσφατα, χρονικά ταξινομημένα και μη διπλότυπα. Αυτή η ανάγκη συνήθως εξυπηρετείται μέσω της χρήσης αριθμών ακολουθίας και χρονοσφραγίδων (timestamps).
- **Αυτοΐαση/Αυτοθεραπεία (Self - Healing):** Ο όρος αναφέρεται στην ικανότητα ενός συστήματος να συνεχίσει να παρέχει υπηρεσίες ακόμα και μετά την ενδεχόμενη προσβολή κάποιας συσκευής από μία επίθεση, την παρουσίαση σφάλματος λογισμικού ή εμφάνιση βλάβης. Βασική προϋπόθεση είναι οι εναπομείναντες ή οι συνεργαζόμενες συσκευές να επιτρέπουν ένα ελάχιστο επίπεδο ασφάλειας [32]. Για την επίτευξη αυτοθεραπείας είναι αναγκαίο ένα υψηλό επίπεδο αυτοματοποίησης που να απαιτεί την ελάχιστη δυνατή ανθρώπινη παρέμβαση.

Στο σημείο αυτό αξίζει να παρατηρηθεί πως η Εμπιστευτικότητα, Ακεραιότητα και Διαθεσιμότητα θεωρούνται ευρέως ως οι πιο θεμελιώδεις αρχές ασφάλειας και απαντώνται στη βιβλιογραφία ως τριάδα CIA (CIA triad). Συχνή επίσης στη βιβλιογραφία είναι η χρήση του όρου «CIANA» , ο οποίος διαμορφώνεται με την προσθήκη των αρχών της Μη Αποποίησης και της Αυθεντικοποίησης.

3.3. Προκλήσεις Ασφάλειας στο IoHT

Το IoT και κατ' επέκταση το IoHT προϋποθέτουν για την υλοποίησή τους ένα πολύπλοκο, τεραστίου μεγέθους, δίκτυο όπου ενσωματώνονται αρμονικά επιμέρους καινοτόμες τεχνολογίες. Το μέγεθος και η πολυπλοκότητα του δικτύου, οι αρχές λειτουργίας των μερών του, οι απαιτούμενες προδιαγραφές, οι περιορισμοί καθώς και το ευρύ φάσμα των διασυνδεδεμένων συσκευών που χαρακτηρίζουν το IoT διαφέρουν παρασάγγας από τα συμβατικά συστήματα.

Ως φυσικό ακόλουθο, η υλοποίηση τέτοιων συστημάτων αναπόφευκτα εγείρει ερωτήματα σχετικά με τους τρόπους κάλυψης των σύνθετων αναγκών ασφαλείας τους και το επίπεδο της παρεχόμενης ασφάλειας που είναι αναγκαίο και επιτεύξιμο, χωρίς εκπτώσεις στο αρχικό όραμα. Οι πολυάριθμες προκλήσεις που εντοπίζονται ειδικότερα για την περίπτωση του IoHT χρήζουν μελέτης και άμεσων, τελεσφόρων, μα συνάμα εφαρμόσιμων λύσεων, εξαιτίας της κρισιμότητας της ασφάλειας στον τομέα της υγείας, όπως αυτή υπογραμμίστηκε παραπάνω.

- **Περιορισμοί Υπολογιστικής Ισχύος και Μνήμης Συσκευών**
  Οι περισσότερες συσκευές IoHT έχουν ενσωματωμένους επεξεργαστές χαμηλής ταχύτητας, οι οποίοι δεν μπορούν να υποστηρίξουν λειτουργίες και διαδικασίες που απαιτούν αυξημένη επεξεργαστική ισχύ. Παρομοίως οι περισσότερες

συσκευές στο IoHT έχουν περιορισμένο αποθηκευτικό χώρο που δεν επαρκεί για την εκτέλεση περίπλοκων πρωτοκόλλων ασφαλείας. Τη δεδομένη χρονική στιγμή οι υπάρχουσες εφαρμογές δεν είναι σχεδιασμένες, ώστε να συμπεριλαμβάνουν τους περιορισμούς στις υπολογιστικές δυνατότητες και τη διαθέσιμη μνήμη όλων των συσκευών. Πρόκληση συνιστά η εύρεση λύσης που να μεγιστοποιεί το επίπεδο της παρεχομένης ασφάλειας, ενώ παράλληλα ελαχιστοποιεί τους χρησιμοποιούμενους πόρους.

- **Περιορισμοί Ενεργειακής Αυτονομίας Συσκευών**
  Η φορητότητα ως χαρακτηριστικό πολλών συσκευών IoHT είναι εξέχουσας σημασίας. Η υποστήριξη αυτής της δυνατότητας έχει ως επακόλουθο την αναγκαστική τροφοδοσία αυτών των συσκευών από μπαταρίες, γεγονός που εισάγει περιορισμούς στην ενεργειακή κατανάλωση. Για την επίτευξη της μέγιστης δυνατής αυτονομίας και της ελάχιστης κατανάλωσης, μία τέτοια συσκευή οφείλει να τίθεται αυτομάτως σε κατάσταση εξοικονόμησης ενέργειας, όταν δεν υπάρχει κάποια σημαντική λειτουργία να επιτελέσει. Αυτό συνεπάγεται τη λειτουργία της συσκευής με χαμηλότερη ταχύτητα επεξεργαστή, η οποία δεν πρέπει όμως να είναι επιζήμια για την ασφάλειά της. Συμπερασματικά, είναι αναγκαίο ένα σύστημα ασφαλείας να λαμβάνει υπόψη τους περιορισμούς στην ενέργεια και την ιδιαίτερη λειτουργία των συσκευών που αυτοί επιτάσσουν.

- **Επεκτασιμότητα και Ετερογένεια**
  Η συνεχής ανάπτυξη του IoHT έχει ως άμεσο αποτέλεσμα την κατασκευή πληθώρας συσκευών διαφορετικού είδους, η κάθε μία εκ των οποίων φέρει ιδιαίτερα χαρακτηριστικά. Η δημιουργία ενός σχεδίου ασφάλειας (security plan) που εξυπηρετεί όλες τις συσκευές ακόμα και αυτές με τις χαμηλότερες δυνατότητες (υπολογιστικές, ενεργειακές και μνήμης) αποτελεί σπουδαία πρόκληση.

- **Ενημερώσεις ασφάλειας**
  Για την εξάλειψη πιθανών ευπαθειών, τα πρωτόκολλα ασφαλείας πρέπει να είναι συνεχώς επικαιροποιημένα, ανάγκη που εξυπηρετείται με τη λήψη και εγκατάσταση λογισμικών επιδιόρθωσης ασφάλειας (security patches). Είναι απαραίτητος ο σχεδιασμός ενός μηχανισμού που θα εξασφαλίζει την άμεση ενημέρωση όλων των συσκευών σε ένα σύστημα IoHT.

- **Κινητικότητα**
  Σε ένα σύστημα IoHT περιλαμβάνεται πλήθος κινητών συσκευών που μπορούν να εξέρχονται από ένα τοπικό δίκτυο και να εισέρχονται σε ένα άλλο προκαλώντας δυναμικές αλλαγές στην τοπολογία των δικτύων. Για παράδειγμα, μία συσκευή που παρακολουθεί την αρτηριακή πίεση του ασθενή συνδέεται στο τοπικό δίκτυο της οικίας του, όταν αυτός είναι παρόν, ενώ όταν αυτός εργάζεται,

η συσκευή θα συνδεθεί στο δίκτυο του χώρου εργασίας του. Αυτή η μετάβαση παρότι στη θεωρία φαντάζει εύκολη, στην πράξη εμφανίζει προβλήματα. Διαφορετικά δίκτυα χαρακτηρίζονται από διαφορετικές παραμετροποιήσεις ασφάλειας και ρυθμίσεις και κατά συνέπεια ο σχεδιασμός ενός συστήματος ασφαλείας που ικανοποιεί την προϋπόθεση φορητότητας, παρότι αναγκαίος, δεν είναι εύκολη υπόθεση.

- **Υποστήριξη πολλαπλών πρωτοκόλλων δικτύωσης**
  Σε ένα σύστημα IoHT μια συσκευή καλείται να επικοινωνήσει τόσο με άλλες συσκευές που ανήκουν στο ίδιο τοπικό δίκτυο, όσο και με απομακρυσμένα κέντρα δεδομένων μέσω Διαδικτύου. Η παραπάνω απαίτηση, καθιστά απαραίτητη τη χρήση μεγάλου αριθμού πρωτοκόλλων επικοινωνίας, το καθένα από τα οποία ενδεχομένως έχει τις δικές του ευπάθειες και κενά ασφαλείας. Μια σχετική πρόκληση είναι ο σχεδιασμός ενός συστήματος ασφαλείας ο οποίος να λαμβάνει υπόψη την ποικιλομορφία των πρωτοκόλλων επικοινωνίας.

- **Φυσική Ασφάλεια**
  Ένα ζήτημα που συχνά παραλείπεται αλλά είναι εξίσου σημαντικό είναι η φυσική ασφάλεια, καθώς και το υλικό (hardware) μπορεί να είναι ευάλωτο σε απειλές. Οι συσκευές πρέπει να έχουν την κατάλληλη ποιότητα κατασκευής και να εφαρμόζουν δικλείδες ασφαλείας, που να ενισχύουν την ανθεκτικότητα στις παραβιάσεις και να μην επιτρέπουν την παραμετροποίησή τους και την εξαγωγή κρυπτογραφημένων πληροφοριών.

3.4. Απειλές και Επιθέσεις στο IoHT

Δύο διακριτές έννοιες που συχνά όμως συγχέονται σε θέματα ασφάλειας των πληροφοριών είναι οι **απειλές** και οι **επιθέσεις**. Στα πλαίσια αυτής της εργασίας θεωρείται σκόπιμο να επισημανθούν οι κυριότερες διαφορές τους, για την καλύτερη κατανόηση αυτών των εννοιών.

Απειλή ασφαλείας (security threat) ορίζεται ως μία **κατάσταση** ή **συμβάν**, όπου μπορούν να προκληθούν ζημιές και απώλειες σε ένα υπολογιστικό σύστημα, δεδομένων των κενών ασφαλείας του. Απειλές μπορεί να προκύψουν από διάφορες καταστάσεις, όπως μία πυρκαγιά, ένα λάθος στον χειρισμό ενός συστήματος ή μία επίθεση.

Επίθεση ασφαλείας (security attack) ορίζεται αντίστοιχα ως η εκούσια μη εξουσιοδοτημένη **ενέργεια** που στοχεύει σε ένα υπολογιστικό σύστημα με σκοπό την παραβίασή του.

Όπως απορρέει από τους παραπάνω ορισμούς, οι απειλές και οι επιθέσεις έχουν όντως σημαντικές διαφορές. Μια ειδοποιός διαφορά είναι ότι μια απειλή μπορεί να έχει ή να μην έχει κάποιο κίνητρο, ενώ στην περίπτωση των επιθέσεων υπάρχει πάντα

κίνητρο και μάλιστα κακόβουλο. Αναφορικά με τις επιπτώσεις τους, οι απειλές μπορούν να προκαλέσουν από μικρή έως πολύ μεγάλη ζημιά, αντιθέτως οι επιθέσεις στοχεύουν αποκλειστικά στην πρόκληση μεγάλων ζημιών. Τέλος, σχετικά με τη δυνατότητα αντιμετώπισης, οι απειλές είναι εν γένει δυσκολότερο να αντιμετωπιστούν συγκριτικά με τις επιθέσεις, διότι συμπεριλαμβάνουν καταστάσεις ή συνθήκες δύσκολα προβλέψιμες και αποτρέψιμες.

3.4.1. Απειλές στο IoHT

Μία απειλή μπορεί να έχει πολλές πηγές προέλευσης. Πιθανή πηγή προέλευσης είναι τα έντονα καιρικά φαινόμενα και οι καταστροφές από ατυχήματα. Τέτοιες καταστροφές είναι δύσκολο να προβλεφθούν και κατά συνέπεια να αποτραπούν εγκαίρως. Τακτικά αντίγραφα ασφαλείας των δεδομένων και η κατασκευή πιο ανθεκτικού υλικού (hardware) είναι κάποια από τα περιορισμένα αντίμετρα που μπορούν να εφαρμοστούν για να μετριάσουν τις πιθανές επιπτώσεις.

Σε δεύτερο επίπεδο απειλές μπορούν να προκύψουν από δυσλειτουργίες υλικού ή λογισμικού ή από ακούσια ανθρώπινα λάθη. Αποτελούν μία από τις κυριότερες ομάδες απειλών και ο βασικότερος τρόπος αντιμετώπισής τους είναι η εκπαίδευση του ιατρονοσηλευτικού προσωπικού και η εξοικείωση των χρηστών με τη νέα τεχνολογία. Από την άλλη, η σχεδίαση και η υλοποίηση συσκευών και συστημάτων IoHT θα πρέπει να γίνεται με γνώμονα την ευχρηστία τους και να εφαρμόζεται εντατικά ποιοτικός έλεγχος.

Δεν προκαλούνται όμως όλες οι απειλές από καταστροφές, ατυχήματα ή παραβλέψεις, αλλά υπάρχουν και αυτές που έχουν ως πηγή προέλευσης την κακόβουλη ανθρώπινη παρέμβαση. Οι συγκεκριμένες απειλές μονοπωλούν το ενδιαφέρον των ερευνών σχετικά με την ασφάλεια στο IoHT εξαιτίας της αυξημένης επικινδυνότητάς τους. Οι στοχευμένες ενέργειες για την πραγματοποίηση των απειλών αυτών αναφέρονται ως επιθέσεις ασφαλείας και θα περιγραφούν εκτενέστερα παρακάτω.

Παρά τις ιδιαιτερότητες του IoHT, οι απειλές που εμφανίζονται δεν αποκλίνουν ιδιαίτερα από αυτές που χαρακτηρίζουν οποιοδήποτε συμβατικό πληροφοριακό σύστημα. Αυτές μπορούν να διακριθούν με βάση τις επιπτώσεις που επιφέρονται στους κύριους πόρους ενός πληροφοριακού συστήματος δηλαδή το υλικό, το λογισμικό και τα δεδομένα [40].

- **Υποκλοπή (Interception):** Πρόκειται για την μη εξουσιοδοτημένη πρόσβαση σε εφαρμογές και συσκευές του συστήματος ή σε δεδομένα που διακινούνται ή είναι αποθηκευμένα σε ένα σύστημα. Ένας μη εξουσιοδοτημένος χρήστης δύναται να προσπελάσει ευαίσθητα αρχεία και να δημιουργήσει αντίγραφα αυτών. Αποτελεί απειλή κατά της Εμπιστευτικότητας και εφόσον διενεργηθεί

σωστά με την απαραίτητη τεχνογνωσία, η ανίχνευσή της καθίσταται εξαιρετικά δύσκολη.

- **Διακοπή (Interruption):** Είναι η περίπτωση αχρήστευσης ή μη διαθεσιμότητας μέρους του συστήματος. Η διακοπή λειτουργίας μπορεί να είναι προσωρινή ή μακροπρόθεσμη και μπορεί να προκύψει ως αποτέλεσμα φυσικών καταστροφών, ανθρώπινης αμέλειας ή επιθέσεων. Θεωρείται κατά κύριο λόγο απειλή κατά της Διαθεσιμότητας του συστήματος, αλλά εξαιτίας της πιθανής απώλειας και αλλοίωσης των δεδομένων μπορεί να θεωρηθεί σε δεύτερο επίπεδο και ως απειλή κατά της Ακεραιότητας.
- **Πλαστογραφία (Fabrication):** Είναι η περίπτωση κατά την οποία ένας μη εξουσιοδοτημένος χρήστης εισάγει στο σύστημα παραποιημένα δεδομένα τα οποία αντιμετωπίζονται σαν δεδομένα ενός πιστοποιημένου χρήστη. Συνιστά απειλή αποκλειστικά για τα δεδομένα ενός συστήματος και προσβάλει πρωτίστως την Ακεραιότητα του συστήματος.
- **Τροποποίηση (Modification):** Η μεταβολή των δεδομένων ή του λογισμικού αναφέρεται στην περίπτωση όπου ένας μη εξουσιοδοτημένος χρήστης, αφού πρώτα έχει αποκτήσει πρόσβαση στο σύστημα, προβαίνει στην παραποίησή τους. Λογίζεται ως απειλή για την Ακεραιότητα, παρόλα αυτά, ανάλογα το είδος των δεδομένων και το μέρος του λογισμικού που προσβάλλονται, η απειλή επεκτείνεται και σε άλλες αρχές ασφάλειας.

3.4.2. Επιθέσεις στο IoHT

Όπως αναφέρθηκε παραπάνω, οι επιθέσεις αποτελούν κακόβουλες παραβιάσεις της ασφάλειας ενός υπολογιστικού συστήματος. Ο ενυπάρχων αυτός δόλος ανάγει τις ενέργειες αυτές σε ένα μείζον ζήτημα που χρήζει άμεσης και αποτελεσματικής αντιμετώπισης, ιδιαίτερα για την περίπτωση του IoHT στο οποίο διακινούνται ευαίσθητες πληροφορίες.

Κύριος στόχος των περισσότερων επιθέσεων στο IoHT είναι τα ιατρικά δεδομένα και κατά επέκταση άλλες ιδιωτικές πληροφορίες των ασθενών. Πιο συγκεκριμένα, για την επίτευξη αυτού του απώτερου στόχου, την απόκτηση δηλαδή μη εξουσιοδοτημένης πρόσβασης στα δεδομένα, ειδικότεροι στόχοι μπορούν να θεωρηθούν τα φυσικά μέρη (πχ. ιατρικοί αισθητήρες), τα μέρη του λογισμικού (πχ. το λειτουργικό σύστημα μιας συσκευής) και η επικοινωνία μεταξύ των συσκευών σε ένα σύστημα.

Ανάλογα με το μέγεθος της περιοχής του συστήματος που προσβάλλεται από μια επίθεση, αυτή μπορεί να χαρακτηριστεί ως μικρής, μεσαίας ή μεγάλης κλίμακας. Παρότι οι στόχοι και τα κίνητρα των επιθέσεων μπορεί να διαφέρουν, στη γενική περίπτωση οι επιτιθέμενοι επιδιώκουν, όσο είναι εφικτό, τη μεγαλύτερης κλίμακας προσβολή και συνεπώς τη μέγιστη δυνατή ζημιά.

Οι επιθέσεις στο IoHT μπορούν να κατηγοριοποιηθούν με πολλούς τρόπους με κριτήριο διάκρισης τα χαρακτηριστικά των επιτιθέμενων, των επιθέσεων και των συνεπειών τους.

3.4.2.1. Χαρακτηριστικά των επιτιθέμενων

Σε σχέση με τον τρόπο οργάνωσής τους, οι επιτιθέμενοι μπορεί να είναι μεμονωμένα άτομα, οργανωμένες ομάδες και ομάδες χορηγούμενες από κρατικές οντότητες ή μεγάλους επιχειρηματικούς ομίλους, που αποσκοπούν σε κάποιο πολιτικό και οικονομικό όφελος. Όσον αφορά τα μεμονωμένα άτομα, αυτοί σχετικά δεν αποτελούν σημαντικό κίνδυνο, καθώς συνήθως δεν έχουν τους απαραίτητους πόρους για να επιτύχουν αξιόλογη ζημιά. Αντιθέτως, στην περίπτωση των οργανωμένων ομάδων και πόσο μάλλον των υποβοηθούμενων ομάδων, ο κίνδυνος αυξάνεται εκθετικά.

Δεν έχουν όλες οι επιθέσεις εξωτερική πηγή προέλευσης, αλλά υπάρχει και η περίπτωση εξουσιοδοτημένοι χρήστες του συστήματος (πχ. ιατρονοσηλευτικό προσωπικό) να δράσουν με κακή πρόθεση. Πιθανοί στόχοι τέτοιων ενεργειών μπορεί να είναι η παραποίηση και υποκλοπή δεδομένων των ασθενών, ή πλήξη της φήμης του παρόχου υγειονομικής περίθαλψης κ.α. Αυτοί οι «εσωτερικοί» επιτιθέμενοι μπορούν να δημιουργήσουν τις κατάλληλες συνθήκες για την εισβολή άλλων «εξωτερικών» επιτιθέμενων στο σύστημα.

Ο τρόπος δράσης μπορεί να ποικίλει μεταξύ των διαφόρων επιτιθέμενων. Με βάση αυτόν, οι επιτιθέμενοι μπορούν να διακριθούν σε δύο κατηγορίες, τους παθητικούς και τους ενεργητικούς. Βασικός σκοπός των παθητικών επιτιθέμενων είναι να παραμένουν μη ανιχνεύσιμοι από το σύστημα, χωρίς να προκαλούν εμφανή δυσλειτουργία του, ενώ παράλληλα συλλέγουν διακινούμενες πληροφορίες. Αυτές οι πληροφορίες μπορούν να αξιοποιηθούν σε δεύτερο χρόνο για το σχεδιασμό μιας επίθεσης μεγαλύτερης κλίμακας. Σε αντιδιαστολή, οι ενεργητικοί επιτιθέμενοι αποσκοπούν στην παρεμπόδιση της εύρυθμης λειτουργίας του συστήματος, υποκλέπτοντας, παραποιώντας ή διαγράφοντας δεδομένα. Εξαιρετικά επίφοβη είναι η πιθανότητα συνεργασίας ενεργητικών και παθητικών επιτιθέμενων καθώς σε μια τέτοια περίπτωση, όπως είναι ευνόητο, οι κίνδυνοι πολλαπλασιάζονται.

Ένα καθοριστικό στοιχείο για τη φύση των επιτιθέμενων, είναι ο στόχος της δράσης τους. Ορισμένοι επιτιθέμενοι δεν έχουν κάποιον ειδικό στόχο, ούτε κινούνται προς την επίτευξη συγκεκριμένου αποτελέσματος, αλλά αρκούνται γενικά στην πρόκληση δυσλειτουργιών. Στον αντίποδα, άλλοι επιτιθέμενοι έχουν ως στόχο την προσβολή συγκεκριμένων πόρων ή χρηστών του συστήματος, για παράδειγμα την αχρήστευση ιατρικού εξοπλισμού ή την υποκλοπή ιατρικών δεδομένων μιας συγκεκριμένης ομάδας ασθενών. Κατά κανόνα οι τελευταίοι συνιστούν συγκριτικά μεγαλύτερο κίνδυνο, εξαιτίας του οργανωμένου και στοχευμένου τρόπου δράσης.

3.4.2.2. Μέθοδοι Επίθεσης

Οι μέθοδοι επίθεσης [29] κατηγοριοποιούν τις επιθέσεις IoHT με βάση την τεχνική που χρησιμοποιείται για την παραβίαση ενός συστήματος. Η σημασία αυτής της ταξινόμησης έγκειται στο ότι βοηθά στην κατανόηση των κινήτρων ενός κακόβουλου εισβολέα και των εργαλείων που έχει στο οπλοστάσιό του, προκειμένου να εφαρμοστούν οι κατάλληλες πολιτικές και διαδικασίες ασφαλείας. Οι μέθοδοι επίθεσης περιλαμβάνουν τα ακόλουθα:

1. Κοινωνική μηχανική: Οι επιτιθέμενοι χρησιμοποιούν αυτές τις τακτικές, για να εξαπατήσουν άτομα, ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες. Πρόκειται για ένα σύνολο μεθόδων που συνήθως δεν απαιτεί από τον επιτιθέμενο εξειδικευμένες γνώσεις προγραμματισμού. Η κοινωνική μηχανική αποτελεί πτυχή που συχνά παραβλέπεται στον σχεδιασμό μιας στρατηγικής ασφάλειας.
2. Εκμετάλλευση σφαλμάτων στη ρύθμιση παραμέτρων ή στην εφαρμογή: Συχνά μπορεί να εξαπολυθούν επιθέσεις μέσω εκμετάλλευσης πιθανής εσφαλμένης διαμόρφωσης ή σφάλματος εφαρμογής που διέφυγε της προσοχής κατά την υλοποίηση ενός συστήματος IoHT. Για παράδειγμα, η μη κατάλληλη ρύθμιση ενός τείχους προστασίας στη σύνδεση μεταξύ των συσκευών IoHT και του υπολογιστικού νέφους καθιστά τη διακίνηση πληροφοριών ευάλωτη.
3. Εκμετάλλευση σφαλμάτων (bugs) λογισμικού/υλικού: Η εκμετάλλευση σφαλμάτων, όπως η υπερχείλιση μνήμης, είναι ένας ακόμη τρόπος επίθεσης εναντίον των έξυπνων ιατρικών συσκευών.
4. Κακόβουλο λογισμικό: Επιθέσεις επίσης μπορούν να εξαπολυθούν από κακόβουλο λογισμικό (ιός, Trojan horse, worm κ.λπ.), με σκοπό να μολύνουν τα συστήματα IoHT και να παρεμποδίσουν τις υπηρεσίες τους.

3.4.2.3. Πιθανές επιπτώσεις Επίθεσης

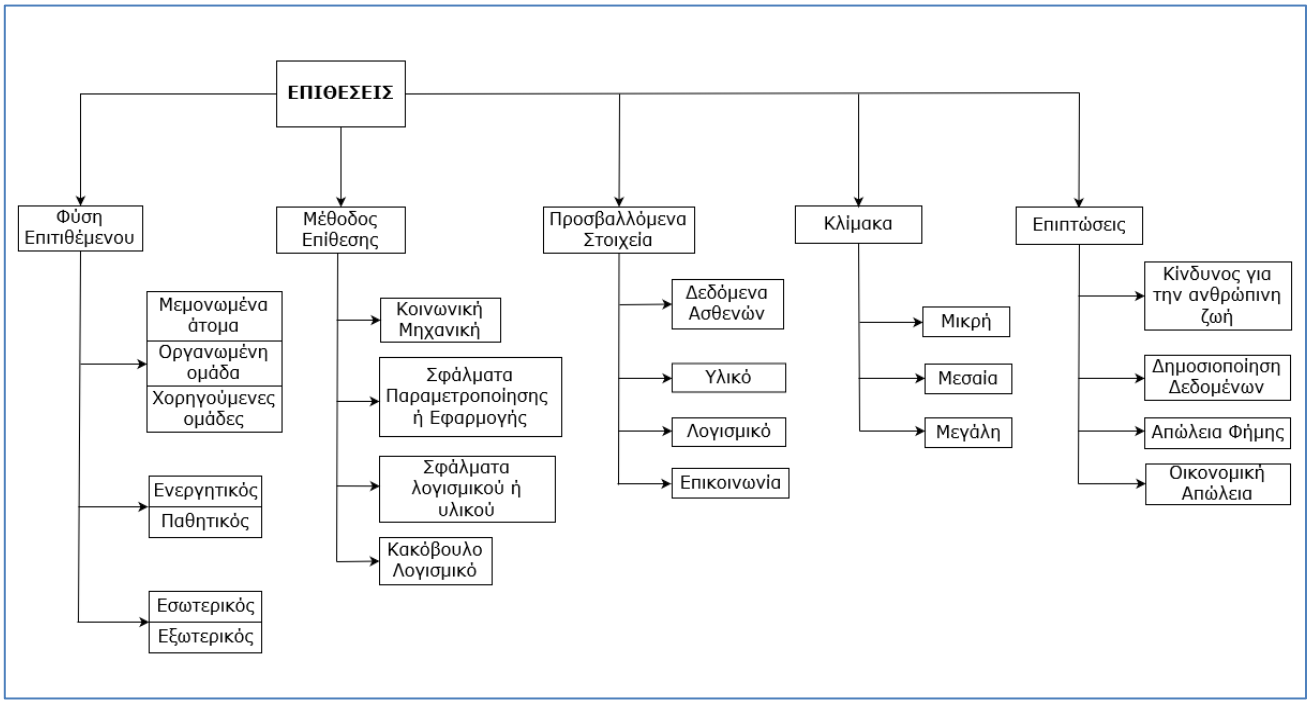
Η διαφοροποίηση όσον αφορά τα κίνητρα, τα μέσα και τους στόχους των επιτιθέμενων οδηγεί σε πληθώρα διαφορετικών κινδύνων, οι οποίοι σχετίζονται με τις πιθανές επιπτώσεις των επιθέσεων. Η ταυτοποίηση, η κατανόηση και η ιεράρχηση αυτών των κινδύνων είναι επιτακτική για τη σχεδίαση μιας αποτελεσματικής στρατηγικής ασφαλείας. Με βάση τα παραπάνω, οι επιθέσεις στο IoHT κατηγοριοποιούνται ως εξής:

1. Κίνδυνος για την ανθρώπινη ζωή
   Οι επιπτώσεις στην υγεία ενός ασθενή κυμαίνονται από αμελητέες, οι οποίες δεν απαιτούν καν την επέμβαση κάποιου επαγγελματία υγείας, έως και επικίνδυνες για τη σωματική ακεραιότητα του ασθενή, μέχρι και την απώλεια της ζωής του. Για παράδειγμα, στην περίπτωση που ένας επιτιθέμενος αποκτήσει πρόσβαση στην εμφυτευμένη αντλία έγχυσης ινσουλίνης ενός

ασθενή, μπορεί να προκληθεί λήψης υπερβολικής δόσης που πιθανώς να αποβεί μοιραία.

2. Δημοσιοποίηση Δεδομένων
   Ένας επιτιθέμενος είναι σε θέση να εκμεταλλευτεί κενά ασφαλείας του συστήματος, ώστε να προσπελάσει απόρρητες ιατρικές πληροφορίες, τις οποίες δύναται να κοινοποιήσει σε τρίτους, παραβιάζοντας την ιδιωτικότητα και το ιατρικό απόρρητο.
3. Απώλεια Φήμης
   Ως συνέπεια μιας επίθεσης η αξιοπιστία των εμπλεκόμενων μερών, όπως ένα εθνικό σύστημα υγείας, ένας ιδιώτης πάροχος υπηρεσιών υγείας ή οι κατασκευαστές υλικού και λογισμικού, μπορεί να πληγεί ανεπανόρθωτα.
4. Οικονομική Απώλεια
   Η απώλεια φήμης συνήθως συνεπάγεται σημαντικές οικονομικές απώλειες. Εντούτοις, δεν είναι αυτή η μόνη αιτία οικονομικής επιβάρυνσης των εμπλεκόμενων μερών. Μετά το πέρας μιας επίθεσης απαιτείται να διενεργηθεί έλεγχος ζημιών και να καταρτιστεί ένα σχέδιο αποκατάστασης, διαδικασίες που είναι επίσης κοστοβόρες.

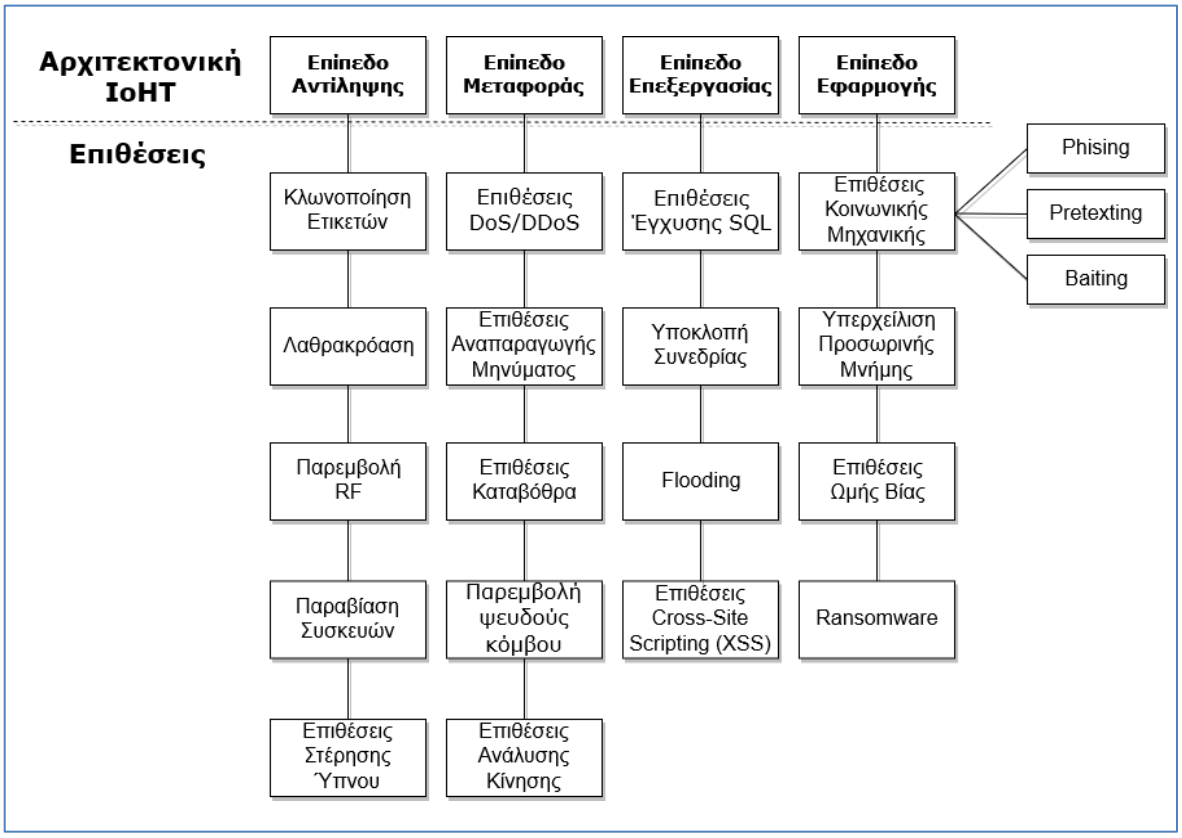
Όσα αναφέρθηκαν παραπάνω σχετικά με την κατηγοριοποίηση των επιθέσεων, παρουσιάζονται συνοπτικά στην Εικόνα 13.



Εικόνα 13. Κατηγοριοποίηση επιθέσεων στο IoHT

3.5. Επιθέσεις στα Επίπεδα της Αρχιτεκτονικής του IoHT

Η αρχιτεκτονική των πέντε επιπέδων, όπως αναλύθηκε στο προηγούμενο κεφάλαιο, παρουσιάζει ένα σύστημα IoHT ως αλληλουχία επιπέδων, το καθένα από τα οποία επιτελεί διακριτές λειτουργίες. Κάθε λειτουργία και κατά επέκταση κάθε επίπεδο φέρει τις δικές του ευπάθειες και κενά ασφαλείας. Η αντιστοίχηση των επιθέσεων στα επίπεδα αρχιτεκτονικής, όπου μπορούν να εμφανιστούν, συνεισφέρει σε μεγάλο βαθμό στην πληρέστερη κατανόηση των στόχων και των επικείμενων κινδύνων μιας επίθεσης. Η εν λόγω αντιστοίχηση απεικονίζεται στο σχήμα που ακολουθεί και επικεντρώνεται στις επιθέσεις που επηρεάζουν τα τέσσερα επίπεδα της αρχιτεκτονικής.



Εικόνα 14. Κυριότερες επιθέσεις στα αντίστοιχα επίπεδα αρχιτεκτονικής του IoHT

3.5.1. Επίπεδο Αντίληψης

Ακολούθως παρατίθενται ορισμένες επιθέσεις που μπορούν να πλήξουν τις έξυπνες συσκευές και τους αισθητήρες που εμπεριέχονται στο επίπεδο αντίληψης.

- **Κλωνοποίηση Ετικετών (Tag Cloning)**
  Ένας επιτιθέμενος, αφού σε πρώτο στάδιο αποκτήσει πρόσβαση στις πληροφορίες μιας RFID ετικέτας μέσω άλλων επιθέσεων και τεχνολογιών, είναι σε θέση να προβεί στην κλωνοποίησή της. Το αποτέλεσμα μιας τέτοιου είδους επίθεσης είναι η δημιουργία μιας κλωνοποιημένης RFID ετικέτας, η οποία φέρει

τα ίδια χαρακτηριστικά με την αυθεντική σε βαθμό που ένας αναγνώστης RFID δεν μπορεί να διακρίνει τις όποιες διαφορές τους. Αυτό έχει ως συνέπεια, ένας επιτιθέμενος χρησιμοποιώντας την πλαστή ετικέτα να αποκτά τη δυνατότητα μη εξουσιοδοτημένης προσπέλασης ιδιωτικών πληροφοριών, όπως ο ηλεκτρονικός ιατρικός φάκελος (EMR) ενός ασθενή. Αξίζει να σημειωθεί πως τα απαιτούμενα εργαλεία για την κατασκευή μιας πλαστής ετικέτας δεν έχουν σχετικά μεγάλο κόστος.

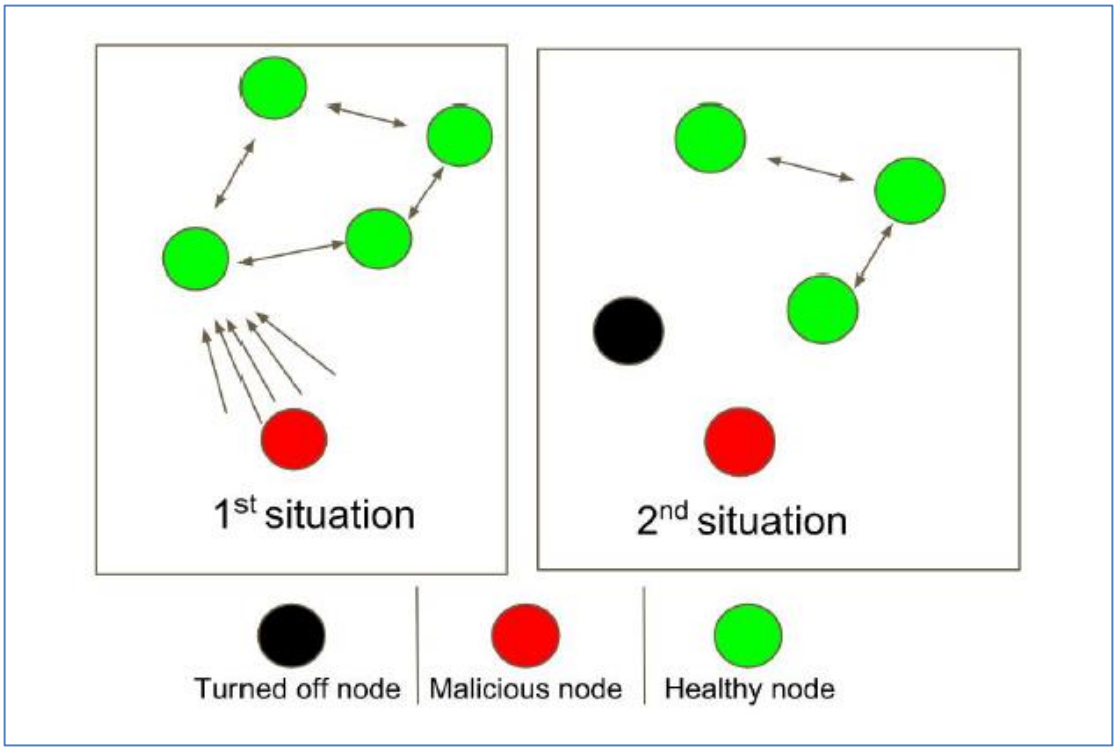
- **Λαθρακρόαση (Eavesdropping)**
  Πρόκειται για μία ομάδα επιθέσεων στις οποίες οι επιτιθέμενοι παραβιάζουν την επικοινωνία μεταξύ συσκευών IoHT, ώστε να παρακολουθούν, να παραποιήσουν ή και να διαγράψουν τις μεταδιδόμενες πληροφορίες. Η λαθρακρόαση αποκτά ιδιαίτερη βαρύτητα σε συστήματα όπως το IoHT, όπου λαμβάνει χώρα συνεχής διακίνηση πληροφοριών, και ως απόρροια εμφανίζεται με διαφορετικές μορφές, στοχεύοντας σε διάφορα επίπεδα της αρχιτεκτονικής. Πιο συγκεκριμένα στο επίπεδο Αντίληψης, κατά την επικοινωνία μεταξύ των RFID συσκευών ένας επιτιθέμενος μπορεί με χρήση δέκτη ραδιοσυχνοτήτων, να υποκλέψει τα δεδομένα που ανταλλάσσουν πιστοποιημένες συσκευές.

  Αυτή η εκδοχή της επίθεσης αποτελεί παθητική μορφή λαθρακρόασης, διότι ο επιτιθέμενος απλά υποκλέπτει τα δεδομένα χωρίς να τα παραποιεί. Περιπτώσεις λαθρακρόασης και ιδιαίτερα παθητικής μορφής είναι δύσκολα ανιχνεύσιμες.

- **Παρεμβολές Ραδιοσυχνοτήτων (RF Jamming)**
  Στην ασύρματη επικοινωνία μεταξύ των συσκευών στο IoHT η τεχνολογία RFID κατέχει δεσπόζουσα θέση. Ένας επιτιθέμενος εκμεταλλευόμενος τις ευπάθειες αυτής της τεχνολογίας έχει τη δυνατότητα με χρήση ενός ειδικού πομπού ραδιοσυχνοτήτων (RF Jammer) να προκαλέσει παρεμβολές στις συχνότητες που χρησιμοποιούν οι πιστοποιημένες συσκευές RFID. Πιο συγκεκριμένα, εκπέμπονται ραδιοκύματα στο ίδιο φάσμα συχνοτήτων αλλά υψηλότερης έντασης συγκριτικά με τα ραδιοκύματα των ετικετών RFID, με συνέπεια ένας αναγνώστης RFID να λαμβάνει πλήθος μη αναγνώσιμων σημάτων. Οι παρεμβολές ραδιοσυχνοτήτων μπορούν να παρεμποδίσουν την επικοινωνία των συσκευών ή σε ορισμένες περιπτώσεις να οδηγήσουν ακόμη και στη διακοπή της, δυσχεραίνοντας έτσι σημαντικά τη διαδικασία συλλογής πληροφοριών του επιπέδου Αντίληψης.

- **Επίθεση Στέρησης Ύπνου (Sleep Deprivation Attack)**
  Οι έξυπνες συσκευές του IoHT, όπως αναλύθηκε παραπάνω, είναι σε μεγάλο βαθμό τροφοδοτούμενες από μπαταρίες και η δυνατότητα λειτουργίας τους σε κατάσταση εξοικονόμησης ενέργειας είναι βασική απαίτηση. Η επίθεση στέρησης ύπνου στοχεύει στην εξάντληση της μπαταρίας των συσκευών, μέσω

της διατήρησής τους σε μόνιμη επαγρύπνηση. Αυτό επιτυγχάνεται με την αδιάκοπη αποστολή αιτημάτων στις συσκευές, η επεξεργασία των οποίων αποτρέπει τη λειτουργία τους υπό καθεστώς μειωμένης κατανάλωσης.



Εικόνα 15. Επίθεση Στέρησης Ύπνου. (Αριστερά παρουσιάζεται η διεξαγωγή της επίθεσης και δεξιά το αποτέλεσμα της με τον κόμβο-στόχο να έχει τεθεί εκτός λειτουργίας).

Πηγή: [41]

- **Παραβίαση Συσκευών (Tampering)**

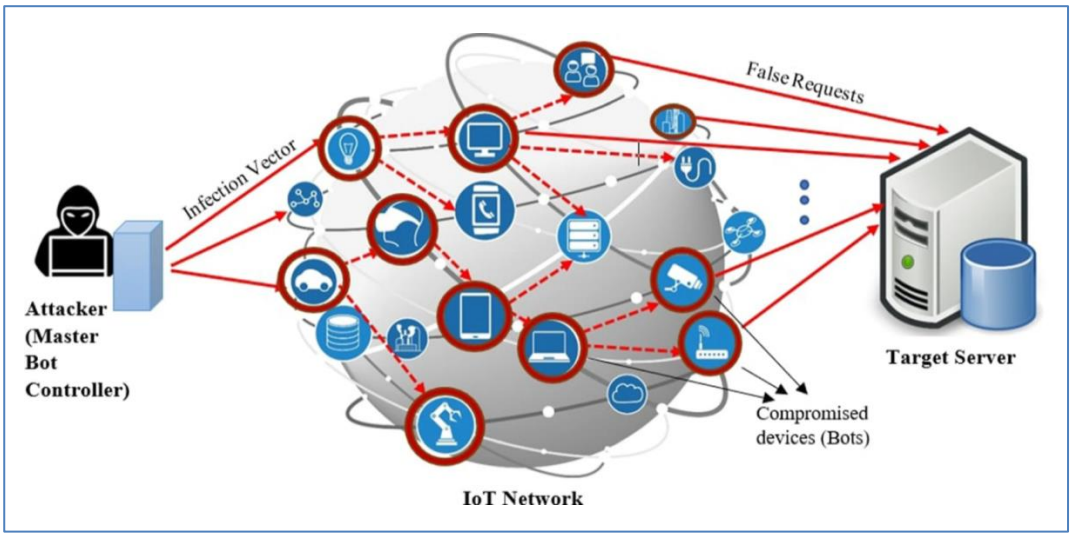
  Οι συσκευές του επιπέδου Αντίληψης έχουν φυσική υπόσταση, γεγονός που προφανώς τις καθιστά πιθανούς στόχους φυσικών επιθέσεων, όπως η σύνδεση καλωδίων στην ηλεκτρονική πλακέτα μιας συσκευής ή η σύνδεση άλλων συσκευών στη θύρα USB της. Ο στόχος των επιτιθέμενων στην περίπτωση αυτή είναι η μη εξουσιοδοτημένη προσπέλαση αποθηκευμένων και διακινούμενων δεδομένων, ενώ και η λειτουργικότητα των συσκευών μπορεί να πληγεί ανεπανόρθωτα. Επιπροσθέτως, οι επιτιθέμενοι μέσω της παραβίασης συσκευών μπορούν να μεταβάλουν την αρχική συνδεσμολογία της ηλεκτρονικής πλακέτας ή να αλλάξουν το περιεχόμενο της μνήμης των συσκευών και να τις χρησιμοποιήσουν με οποιονδήποτε τρόπο [42].

  Ο βασικότερος λόγος ανησυχίας που συντρέχει αναφορικά με αυτές τις επιθέσεις είναι η πιθανότητα εξαγωγής κλειδιών κρυπτογράφησης, η οποία τις ανάγει σε απειλή, όχι μόνο για το συγκεκριμένο επίπεδο αρχιτεκτονικής, αλλά και για ολόκληρο το σύστημα IoHT.

3.5.2. Επίπεδο Μεταφοράς

Κάποιες από τις πιο δημοφιλείς επιθέσεις στο επίπεδο μεταφοράς είναι οι παρακάτω:

- **Επίθεση Άρνησης Υπηρεσίας (Denial of Service - DoS)**
  Οι επιθέσεις DoS έχουν στόχο την προσβολή της διαθεσιμότητας ενός συστήματος IoHT μέσω του κατακλυσμού του δικτύου με πληθώρα αιτημάτων, τα οποία αυξάνουν την κίνηση στο δίκτυο σε βαθμό που δεν είναι διαχειρίσιμη. Κατά συνέπεια οι πιστοποιημένοι χρήστες παύουν να απολαμβάνουν τις υπηρεσίες του δικτύου και στερούνται τη δυνατότητα χρήσης των πόρων του. Μολονότι αυτή η επίθεση είναι γενικά εύκολα αντιμετωπίσιμη, δεν ισχύει το ίδιο για την κυριότερη παραλλαγή της, την Κατανεμημένη Επίθεση Άρνησης Υπηρεσίας (Distributed Denial of Service - DDoS). Αυτός ο τύπος επίθεσης προϋποθέτει τη χρήση πλήθους συσκευών για την αύξηση της κίνησης του δικτύου, στις οποίες ο επιτιθέμενος έχει προηγουμένως εγκαταστήσει κακόβουλο λογισμικό. Συγκριτικά, λοιπόν, με την επίθεση DoS, στην περίπτωση επίθεσης DDoS ο ιθύνων νους είναι σαφώς δυσκολότερα ιχνηλάσιμος, αλλά παράλληλα για τη διενέργειά της απαιτούνται δυσεύρετοι πόροι.



Εικόνα 16. Εξαπόλυση επίθεσης Κατανεμημένης Άρνησης Υπηρεσίας σε δίκτυο IoT.

Πηγή: [43]

Οι προσβεβλημένες συσκευές κατά τη διάρκεια μιας επίθεσης DDoS εκτελούν αυτοματοποιημένες εργασίες (scripts) και για τον λόγο αυτόν έχει καθιερωθεί ο όρος «διαδικτυακά ρομπότ» (internet bots ή bots) για την περιγραφή τους, ενώ ένα σύνολο διασυνδεδεμένων bots ονομάζεται botnet. Το 2016 botnets αποτελούμενα από συσκευές IoT που είχαν μολυνθεί από το κακόβουλο λογισμικό Mirai χρησιμοποιήθηκαν για την εξαπόλυση πρωτοφανούς κλίμακας επιθέσεων DDoS. Οι επιθέσεις αυτές είχαν σοβαρό οικονομικό αντίκτυπο και, ως εκ τούτου, θορύβησαν την επιστημονική κοινότητα και επανέφεραν στο

προσκήνιο το θέμα της ασφάλειας του IoT. Βασικός πυλώνας για μερικές από τις πιο θεμελιώδεις υπηρεσίες του IoHT είναι η άμεση και αδιάλειπτη απόκριση του συστήματος. Συμπερασματικά, κακόβουλες ενέργειες που προσβάλλουν τη Διαθεσιμότητα συνεπάγονται άμεσο κίνδυνο για την υγεία των ασθενών.

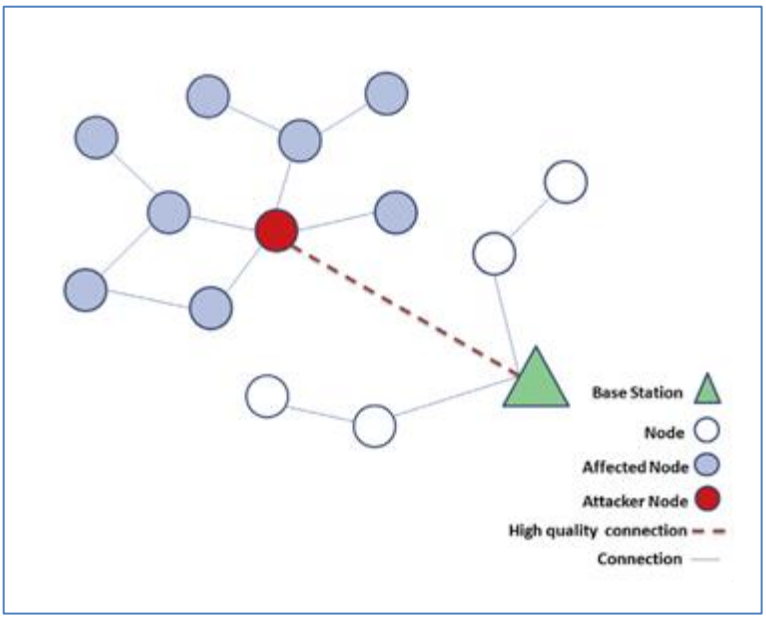
- **Επίθεση Αναπαραγωγής Μηνύματος (Replay Attack)**
  Μετά από επιτυχημένη επίθεση λαθρακρόασης, ένα μήνυμα που έχει μεταδοθεί μεταξύ πιστοποιημένων κόμβων του δικτύου μπορεί να περιέλθει στην κατοχή του επιτιθέμενου. Η επίθεση Replay περιλαμβάνει τη συνεχή επαναμετάδοση του μηνύματος, χωρίς να έχει υποστεί κάποια μεταβολή, προς τον νόμιμο αποδέκτη, προξενώντας αυξημένη κίνηση και καταναλώνοντας τους διαθέσιμους πόρους του δικτύου επικοινωνίας. Οι εξαντλούμενοι πόροι συμπεριλαμβάνουν τόσο τους υπολογιστικούς πόρους των εμπλεκόμενων συσκευών, αλλά και τον αποθηκευτικό χώρο στη βάση δεδομένων. Με επανάληψη της διαδικασίας αυτής, η επίθεση αναπαραγωγής μηνύματος πιθανώς να οδηγήσει σε μία επίθεση DoS/DDoS [39].

- **Παρεμβολή Ψευδούς Κόμβου (Malicious node injection)**
  Πρόκειται για την περίπτωση όπου ένας επιτιθέμενος παρενθέτει έναν ψευδεπίγραφο κόμβο μεταξύ των εξουσιοδοτημένων κόμβων του συστήματος. Ο κόμβος αυτός καταφέρνει να παραμείνει μη ανιχνεύσιμος κατά τη διαδικασία επαλήθευσης και ως αποτέλεσμα να λογίζεται πλέον σαν ένα πιστοποιημένο μέρος του συστήματος. Μέσω αυτού του κόμβου ο επιτιθέμενος δύναται να προβεί σε πληθώρα επιβλαβών ενεργειών, όπως για παράδειγμα την εισαγωγή όγκου ψευδών πληροφοριών στο σύστημα, την υπερκατανάλωση πόρων του συστήματος ή την παραποίηση των διακινούμενων δεδομένων.
  Παρόλα αυτά, η παρεμβολή ψευδούς κόμβου είναι δυνατόν να έχει παθητικό χαρακτήρα, όταν ο επιτιθέμενος περιορίζεται απλά στην ανάγνωση των μηνυμάτων, χωρίς να προξενεί κάποια εμφανή δυσλειτουργία στο σύστημα. Αυτή η επίθεση, είτε με την ενεργητική είτε με την παθητική της μορφή, είναι γνωστή και ως Man-in-the-Middle (MITM). Προϋπόθεση για την εξαπόλυση μιας τέτοιας επίθεσης είναι η κατοχή εκτεταμένης γνώσης αναφορικά με τα πρωτόκολλα και τις διαδικασίες αυθεντικοποίησης, που χρησιμοποιούνται στο σύστημα. Αυτές οι απόρρητες πληροφορίες είναι πιθανό να έχουν διαρρεύσει από άλλες επιθέσεις που έχουν προηγηθεί.
  Στην περίπτωση του IoHT, οι επιπτώσεις, οι οποίες επιφέρονται ιδιαίτερα από την ενεργητική μορφή των εν λόγω επιθέσεων, είναι εξαιρετικά επιζήμιες για την υγεία του ασθενή. Με την εισροή ψευδών πληροφοριών ή την απόκρυψη των πραγματικών βιομετρικών δεδομένων, ενδέχεται να προκύψουν εσφαλμένες ιατρικές διαγνώσεις και να ακολουθηθούν ακατάλληλες θεραπευτικές μέθοδοι.

- **Επίθεση Καταβόθρα (Sinkhole Attack)**

  Ένας κακόβουλος κόμβος δύναται να προσελκύσει κίνηση από τους γειτονικούς του κόμβους ισχυριζόμενος ότι παρέχει το βέλτιστο μονοπάτι δρομολόγησης των δεδομένων προς τον τελικό τους προορισμό. Αυτός ο κόμβος ο οποίος λειτουργεί σαν καταβόθρα, έχει τη δυνατότητα να επηρεάσει τη σύνδεση των γειτονικών του κόμβων στο δίκτυο ή και να αποκλείσει ορισμένους από αυτούς μέσω της επιλεκτικής προώθησης των πακέτων δεδομένων που λαμβάνει.

  Ωστόσο, αξίζει να σημειωθεί πως ένας κόμβος-καταβόθρα μπορεί να χρησιμοποιηθεί απλά σαν μέσο για την παθητική λαθρακρόαση των πληροφοριών που δέχεται. Στην περίπτωση αυτή, προκειμένου να παραμείνει μη ανιχνεύσιμος, επιτελεί τη λειτουργία ενός κανονικού κόμβου, προωθώντας όλα τα πακέτα δεδομένων που λαμβάνει, ώστε να αξιοποιηθεί σε δεύτερο χρόνο ως εφαλτήριο για άλλες επιθέσεις.



Εικόνα 17. Σχηματική αναπαράσταση επίθεσης Sinkhole.

Πηγή: [45]

- **Επίθεση Ανάλυσης Κίνησης (Traffic Analysis)**

  Πρόκειται για μία παθητική και δύσκολα ανιχνεύσιμη μορφή επίθεσης, όπου ο επιτιθέμενος παρατηρώντας τα εκπεμπόμενα σήματα σε ένα ασύρματο δίκτυο είναι σε θέση να εξάγει συμπεράσματα για τον τρόπο επικοινωνίας των συσκευών και την τοπολογία του δικτύου.

  Πιο συγκεκριμένα, με τη συγκέντρωση και την ανάλυση πληροφοριών σχετικά με τον αριθμό των πακέτων δεδομένων και το μέγεθός τους μπορούν να προσδιοριστούν τα μοτίβα επικοινωνίας που ακολουθούνται σε ένα δίκτυο, ακόμα και όταν τα πακέτα αυτά είναι κρυπτογραφημένα. Με την επίθεση ανάλυσης κίνησης είναι εφικτή η απόκτηση πληροφοριών σχετικά με τη δραστηριότητα που εμφανίζεται στο δίκτυο, τη φυσική θέση των ασύρματων

σημείων πρόσβασης και τον τύπο των πρωτοκόλλων, που χρησιμοποιούνται στη διαδικασία μετάδοσης δεδομένων [44].

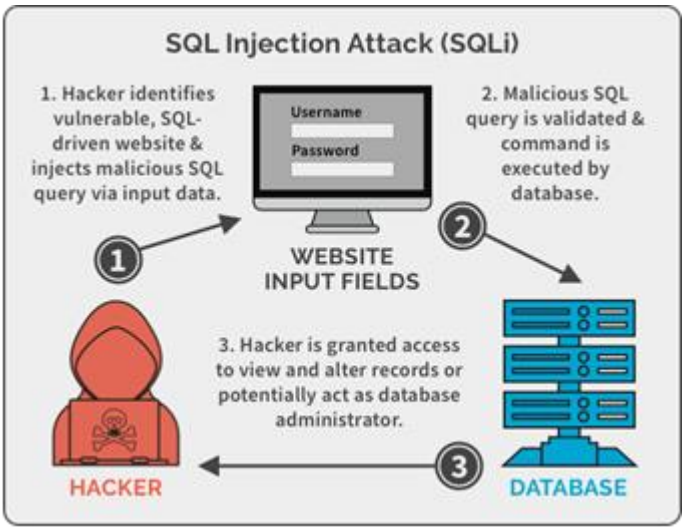
Τέλος, μπορούν να εξαχθούν συμπεράσματα για το είδος και τα χαρακτηριστικά των συσκευών ενός δικτύου και να εντοπιστούν πιθανές ευπάθειές τους, στοιχεία που είναι δυνατόν να αξιοποιηθούν για την εξαπόλυση διαφορετικών επιθέσεων σε δεύτερο χρόνο. Για παράδειγμα, όσον αφορά το IoHT, η ανάλυση πληροφοριών σχετικά με τον τρόπο επικοινωνίας μιας συσκευής μπορεί να οδηγήσει στην ταυτοποίησή της ως φορέσιμη και, εκμεταλλευόμενος τους περιορισμούς της στην ενεργειακή κατανάλωση, ένας επιτιθέμενος μπορεί να προβεί σε μια επίθεση στέρησης ύπνου.

3.5.3. Επίπεδο Επεξεργασίας

Στη συνέχεια αναφέρονται επιθέσεις οι οποίες αντιστοιχούν στο επίπεδο επεξεργασίας:

- **Επίθεση Έγχυσης SQL (SQL Injection Attack)**

  Επιθέσεις έγχυσης SQL αποτελούν απειλή για διάφορα είδη συστημάτων ανάμεσά τους και για το IoT [47]. Στόχος της επίθεσης είναι η προσβολή της βάσης δεδομένων όπου αποθηκεύονται δεδομένα μιας εφαρμογής. Ο επιτιθέμενος ενσωματώνει ερωτήματα SQL στα δεδομένα που εισάγει στην εφαρμογή, εκμεταλλευόμενος την απουσία ειδικού περιορισμού, ο οποίος απαγορεύει την εξυπηρέτηση τέτοιων αιτημάτων. Αυτό έχει ως αποτέλεσμα την εκχώρηση δικαιωμάτων διαχειριστή στον επιτιθέμενο και έτσι αυτός αποκτά τη δυνατότητα μεταξύ άλλων να προσπελάσει, να παραποιήσει και να διαγράψει ευαίσθητα ιατρικά δεδομένα ή ακόμα και να προσθέσει ψευδείς πληροφορίες στη βάση δεδομένων.



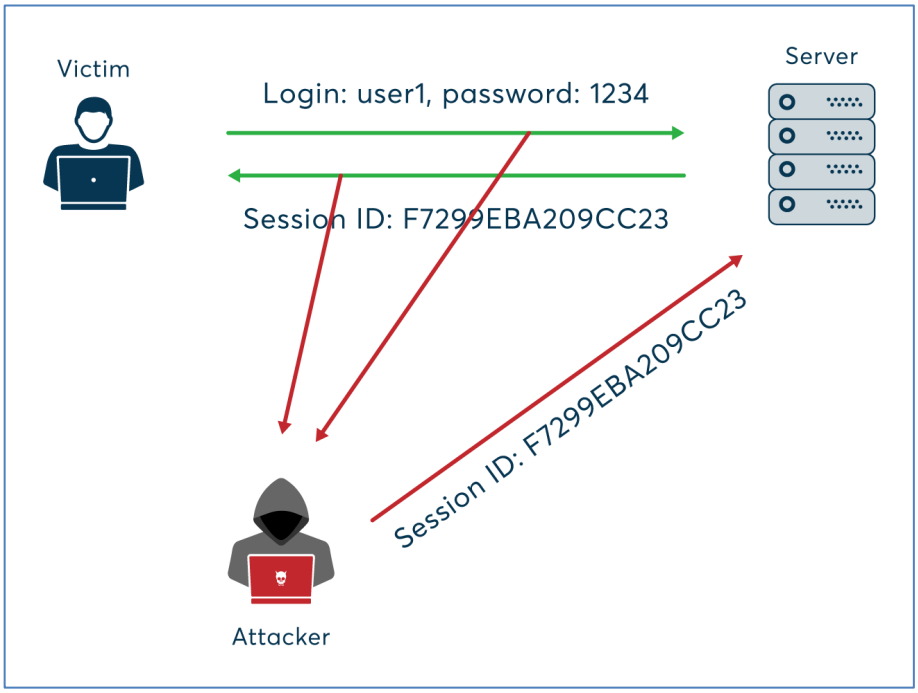
Εικόνα 18. Τα επιμέρους στάδια μιας επίθεσης Έγχυσης SQL.

Πηγή: https://securityboulevard.com/2019/07/sql-injection-attacks-sqli-web-based-application-security-part-4/

- **Επίθεση Υποκλοπής Συνεδρίας (Session Hijacking Attack)**

  Στην περίπτωση επίθεσης υποκλοπής συνεδρίας [48], ο επιτιθέμενος, αφού πρώτα υποκλέψει το αναγνωριστικό συνεδρίας (Session ID) ενός πιστοποιημένου χρήστη, μπορεί να «μεταμφιεστεί» σε αυτόν. Κατά αυτόν τον τρόπο ο επιτιθέμενος απολαμβάνει τα ίδια δικαιώματα και εξουσιοδοτείται σαν εγκεκριμένος χρήστης του δικτύου. Κατά τη διάρκεια της συνεδρίας, ο επιτιθέμενος δεν απαιτείται να περάσει από διαδικασία αυθεντικοποίησης, καθώς η υποκλοπή του αναγνωριστικού συνεδρίας ισοδυναμεί ουσιαστικά με την παράκαμψή της.

  Κατά κανόνα, τα αναγνωριστικά συνεδρίας είναι τυχαία δημιουργημένα, ωστόσο οι αλγόριθμοι που χρησιμοποιούνται για τη δημιουργία τους συχνά εισάγουν ευκόλως προβλέψιμες μεταβλητές (πχ. ο χρόνος ή η διεύθυνση IP) [48]. Στις περιπτώσεις που χρησιμοποιούνται προβλέψιμα αναγνωριστικά συνεδρίας, ο κίνδυνος εμφάνισης τέτοιων επιθέσεων προφανώς αυξάνει σημαντικά. Στο πλαίσιο IoHT, όπου υπάρχει ταυτόχρονα ένας μεγάλος αριθμός συνεδριών, η επίθεση υποκλοπής συνεδρίας είναι δύσκολο να ανιχνευτεί.



Εικόνα 19. Επίθεση Υποκλοπής Συνεδρίας

Πηγή: https://www.netsparker.com/blog/web-security/session-hijacking/

- **Επίθεση Flooding**

  Η επίθεση flooding είναι μια μορφή επίθεσης DoS που στοχεύει το υπολογιστικό νέφος [44]. Αναφορικά με την εκτέλεση της επίθεσης, ο επιτιθέμενος αποστέλλει τεράστιο όγκο αιτημάτων προς μία συγκεκριμένη υπηρεσία του υπολογιστικού νέφους. Δεδομένου ότι αυτά τα αιτήματα πρέπει να εξεταστούν ως προς την εγκυρότητά τους, αυξάνεται σημαντικά ο φόρτος εργασίας του

εξυπηρετητή [46] και ως εκ τούτου δεν είναι πλέον σε θέση να υποστηρίξει άλλες υπηρεσίες. Όταν οι διαθέσιμοι πόροι ενός εξυπηρετητή εξαντληθούν, αυτός ενδέχεται να σταματήσει ή να επανεκκινήσει τη λειτουργία του είτε να διαμοιράσει τον φόρτο εργασίας του σε άλλους εξυπηρετητές με συνέπεια να υποβαθμιστεί συνολικά η λειτουργικότητα του υπολογιστικού νέφους [44]. Πλήθος εργαλείων που συμβάλλουν στην εξαπόλυση επιθέσεων flooding είναι ευρέως διαθέσιμα και ταυτόχρονα οι συνέπειές τους είναι εξαιρετικά επιβλαβείς, γεγονός που αναδεικνύει την αναγκαιότητα εφαρμογής εξειδικευμένων αντίμετρων για την αναχαίτισή τους.

- **Επίθεση Δέσμης Ενεργειών μεταξύ Τοποθεσιών (Cross-site scripting (XSS) Attack)**
  Η δέσμη ενεργειών μεταξύ τοποθεσιών, ή XSS, είναι μια ευπάθεια βασισμένη στα πρωτόκολλα του παγκόσμιου ιστού, που μπορεί να χρησιμοποιήσει ένας επιτιθέμενος για να προσθέσει επικίνδυνο κώδικα σε έναν σύνδεσμο (URL link) που κατά τα άλλα είναι νομότυπος. Κάνοντας κλικ στον σύνδεσμο στέλνεται στον νόμιμο ιστότοπο τόσο το αβλαβές αίτημα όσο και το κακόβουλο σενάριο. Ο ιστότοπος δίνει μια απάντηση στο αρχικό αίτημα και περιλαμβάνει το σενάριο του επιτιθέμενου, το οποίο εκτελείται από το τοπικό πρόγραμμα περιήγησης Ιστού επειδή προέρχεται από μια αξιόπιστη πηγή. Μια επιτυχημένη επίθεση XSS δεν προκαλεί κανένα συναγερμό στον χρήστη και θα μπορούσε να οδηγήσει σε παραβιάσεις λογαριασμών Ιστού, κλοπή περιόδων σύνδεσης ιστού, έλεγχο του προγράμματος περιήγησης από απόσταση ή ανακατεύθυνση σε κακόβουλες τοποθεσίες.

3.5.4. Επίπεδο Εφαρμογής

Στο επίπεδο εφαρμογής αντιστοιχούν οι εξής επιθέσεις:

- **Επίθεση Ransomware**
  Αυτού του είδους οι επιθέσεις έχουν κάνει την εμφάνισή τους ήδη από το 1989 (AIDS Trojan) και παραμένουν επίκαιρες μέχρι και σήμερα. Η επίθεση τυπικά περιλαμβάνει κρυπτογράφηση αρχείων στον προσωπικό υπολογιστή ενός χρήστη, ο οποίος καλείται έπειτα να πληρώσει το χρηματικό ποσό, που ορίζει ο επιτιθέμενος, ώστε να επανακτήσει πρόσβαση. Στην περίπτωση του IoT και κατά επέκταση του IoHT συχνά υποτιμούνται οι επιπτώσεις που μπορούν να επιφέρουν αυτές οι επιθέσεις, εξαιτίας δύο κυρίων παραγόντων. Αρχικά, στο IoT το συντριπτικό πλήθος των δεδομένων αποθηκεύονται στο υπολογιστικό νέφος γεγονός που καθιστά την προσβολή μιας συσκευής IoT με Ransomware ασύμφορη [49]. Τα δεδομένα που βρίσκονται αποθηκευμένα στις συσκευές είναι επί το πλείστον χαμηλής ή μηδαμινής αξίας, συνεπώς το θύμα δεν έχει ικανό κίνητρο για να ανταποκριθεί στις οικονομικές απαιτήσεις του επιτιθέμενου. Σε δεύτερο επίπεδο, η ετερογένεια των συσκευών IoT επιτάσσει,

για την εξαπόλυση μιας τέτοιας επίθεσης, διαφορετικό τρόπο προσέγγισης για κάθε είδος συσκευής [49]. Συμπερασματικά, το IoT δεν παρέχει, φαινομενικά τουλάχιστον, πρόσφορο έδαφος για να λάβουν χώρα επιθέσεις Ransomware.

Παρά τα όσα αναφέρθηκαν, επιθέσεις Ransomware είναι πιθανό να συμβούν στο περιβάλλον του IoT και μάλιστα με καταστροφικές συνέπειες. Οι επιτιθέμενοι, λαμβάνοντας υπόψη πως η κρυπτογράφηση των δεδομένων του στόχου δεν είναι επικερδής θα στραφούν σε μια παλαιότερη εκδοχή της επίθεσης [49], η οποία παρότι ανατρέψιμη (με μια απλή επαναφορά συσκευής) είναι υπό συνθήκες εξίσου αποτελεσματική. Αυτή διενεργείται με το «κλείδωμα» της συσκευής, ενώ τα λύτρα ζητούνται πλέον για την αποκατάσταση της λειτουργικότητάς της. Παράγοντας-κλειδί για την επιτυχία της επίθεσης είναι η προσβολή μιας συσκευής σε κατάλληλο χώρο και χρόνο που καθιστούν την επαναφορά της αδύνατη [49]. Συγκεκριμένα για το IoHT, όπου η διαθεσιμότητα των συσκευών είναι ζωτικής σημασίας, επιθέσεις Ransomware, εκτός από τις συνήθεις οικονομικές επιπτώσεις, έχουν και ολέθριες συνέπειες για την υγεία και τη ζωή των ασθενών.

- **Επίθεση Υπερχείλισης Προσωρινής Μνήμης (Buffer Overflow Attack)**

  Οι επιθέσεις υπερχείλισης προσωρινής μνήμης είναι από τις πιο συχνά παρατηρούμενες μορφές επιθέσεων στο λογισμικό και τις εφαρμογές. Η υπερχείλιση προσωρινής μνήμης είναι μία αδυναμία του συστήματος που επιτρέπει την εγγραφή ή την αντικατάσταση δεδομένων σε θέσεις μνήμης του. Τα δεδομένα αυτά προέρχονται από «υπερχείλιση» ενός γειτονικού buffer μνήμης, του οποίου η χωρητικότητα έχει εξαντληθεί. Τέτοιες αδυναμίες είναι εύκολα εκμεταλλεύσιμες από επιτιθέμενους που αποσκοπούν στην τροποποίηση της μνήμης ενός συστήματος [50], ώστε να υπονομεύσουν ή γενικότερα να ελέγξουν την εκτέλεση προγραμμάτων. Ο επιτιθέμενος μπορεί να εισάγει προσεκτικά διαμορφωμένα δεδομένα εισόδου σε ένα πρόγραμμα, το οποίο εν συνεχεία θα επιχειρήσει να τα αποθηκεύσει σε ένα buffer μνήμης ανεπαρκούς χωρητικότητας [50].

  Τα αποτελέσματα αυτής της επίθεσης ποικίλουν και συμπεριλαμβάνουν την τροποποίηση προϋπαρχόντων δεδομένων (πχ. όταν τα δεδομένα υπερχειλίζουν προς μία περιοχή δεδομένων διαφορετικού buffer), την εκτέλεση κακόβουλου κώδικα (πχ. όταν τα δεδομένα παρεισδύουν στο τμήμα κώδικα ενός προγράμματος και εμπεριέχουν κακόβουλο εκτελέσιμο κώδικα) και τη διατάραξη του ελέγχου ροής σε ένα πρόγραμμα [44].

- **Επιθέσεις Ωμής Βίας (Brute Force Attacks)**

  Μία μέθοδος για την απόκτηση των διαπιστευτηρίων (credentials) ενός εγκεκριμένου χρήστη είναι η επίθεση ωμής βίας. Όπως υποδηλώνει η ονομασία της, η επίθεση αυτή δεν βασίζεται σε κάποια εξεζητημένη στρατηγική, μα περιλαμβάνει επαναλαμβανόμενες δοκιμές συνδυασμών (χαρακτήρων, αριθμών

και συμβόλων), ώσπου να βρεθεί ο σωστός κωδικός (password). Για τη διενέργεια επιθέσεων ωμής βίας μέσω του διαδικτύου, συχνά επιστρατεύονται αυτοματοποιημένες εργασίες (scripts) ή διαδικτυακά ρομπότ (bots) που στοχεύουν στη σελίδα εισόδου ενός ιστοτόπου [51]. Κυριότερο πλεονέκτημα αυτής της τεχνικής αποτελεί η σχετική απλότητά της και το γεγονός ότι, αν δεν υπάρχει περιορισμός στον χρόνο και δεν εφαρμόζεται κάποιος μηχανισμός αποτροπής της, μπορεί, σε θεωρητικό τουλάχιστον επίπεδο, να ανακαλύψει οποιονδήποτε κωδικό [51]. Σε πρακτικό όμως επίπεδο, οι επιθέσεις αυτές είναι χρονοβόρες ιδιαίτερα για την περίπτωση πολύπλοκων κωδικών μεγάλου μήκους. Μάλιστα ο απαιτούμενος χρόνος αυξάνεται εκθετικά με το μέγεθος του συνδυασμού, διότι απαιτείται εξέταση πολύ περισσότερων συνδυασμών.

Μια ακόμη χρήση της επίθεσης στο IoT, που αξίζει να σημειωθεί και δεν απαιτεί σύνδεση στο διαδίκτυο, αφορά την αποκρυπτογράφηση πακέτων που έχουν περιέλθει στην κατοχή του επιτιθέμενου από κάποια άλλη επίθεση [39].

- **Επιθέσεις Κοινωνικής Μηχανικής (Social Engineering Attacks)**

  Η κοινωνική μηχανική αποτελεί ένα ευρύ σύνολο μεθόδων και τεχνικών, κοινή συνισταμένη των οποίων είναι η εξαπάτηση των θυμάτων (χρηστών ή οργανισμών), με απώτερο στόχο οι επιτιθέμενοι να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες ή να εξαναγκάσουν τα θύματα να προβούν σε ενέργειες που θα αποδυναμώσουν την ασφάλεια του συστήματος.

  Στη δεύτερη περίπτωση, οι επιτιθέμενοι μπορούν να αξιοποιήσουν τα δημιουργούμενα κενά ασφαλείας, ώστε να εξαπολύσουν στη συνέχεια επιθέσεις μεγαλύτερης κλίμακας. Η επικινδυνότητα τέτοιων επιθέσεων έγκειται στο γεγονός ότι δεν εκμεταλλεύονται τεχνικές ευπάθειες του συστήματος, αλλά σύμφυτες ανθρώπινες αδυναμίες, όπως η περιέργεια, η αφέλεια και η πλεονεξία. Ως αποτέλεσμα της ολοένα αυξανόμενης ευρηματικότητας των επιτιθέμενων, διαρκώς παρατηρούνται νέες μορφές επιθέσεων κοινωνικής μηχανικής, πέρα από τις γνωστές υπάρχουσες μορφές.

  Τέλος, αξίζει να σημειωθεί πως η ανάπτυξη και η διάδοση συσκευών IoT αυξάνει δραματικά το βελησνεκές των εν λόγω επιθέσεων, διότι εκτός του προσωπικού υπολογιστή είναι δυνατή η προσβολή πλήθους έξυπνων συσκευών. Στη συνέχεια παρατίθενται τρείς βασικές μέθοδοι κοινωνικής μηχανικής.

- **Phishing**

  Πρόκειται για την πιο διαδεδομένη μέθοδο κοινωνικής μηχανικής, όπου το θύμα προσεγγίζεται κυρίως μέσω μηνύματος ηλεκτρονικού ταχυδρομείου (e-mail), αλλά και μέσω διαφορετικών τρόπων επικοινωνίας. Τα μηνύματα αυτά έχουν συνταχθεί και σχεδιαστεί με τέτοιον τρόπο, ώστε το θύμα να πειστεί πως προέρχονται από έναν αξιόπιστο αποστολέα, ενώ στην πραγματικότητα εμπεριέχουν συχνά κακόβουλα επισυναπτόμενα αρχεία ή συνδέσμους, οι οποίοι παραπέμπουν σε ψευδείς ιστοσελίδες. Τα ανύποπτα θύματα καλούνται να

συμπληρώσουν διαπιστευτήρια εισόδου και άλλες προσωπικές πληροφορίες, οι οποίες καταλήγουν στην κατοχή του επιτιθέμενου.

Αρκεί μία μόνο επιτυχημένη επίθεση Phishing [52] για να αποκτήσει ο επιτιθέμενος πρόσβαση σε διαδικτυακούς λογαριασμούς του χρήστη, καθώς και την άδεια να τροποποιήσει ή να παραποιήσει συνδεδεμένα συστήματα, όπως συσκευές IoHT.

- **Pretexting**

  Ένα από τα πρώτα παραδείγματα κοινωνικής μηχανικής είναι η μέθοδος του Pretexting κατά την οποία ο επιτιθέμενος, υιοθετώντας μια ψεύτικη ταυτότητα, παρουσιάζει στο θύμα μια πλαστή, προσεγμένα δομημένη ιστορία. Καταλυτικό ρόλο σε αυτή την τεχνική έχει η οικοδόμηση μιας σχέσης εμπιστοσύνης με το θύμα, την οποία ο θύτης σε επόμενο στάδιο εκμεταλλεύεται για να αποσπάσει ευαίσθητες πληροφορίες, υπό κάποιο πρόσχημα. Στην πλειοψηφία των περιπτώσεων ο επιτιθέμενος επιλέγει να υποδυθεί πρόσωπα κύρους, όπως τον προϊστάμενο μιας τράπεζας, κάποιον εργαζόμενο στο αστυνομικό σώμα ή στο τμήμα τεχνικής υποστήριξης διάσημης εταιρείας. Σε αντίθεση με την περίπτωση του Phishing, οι επιθέσεις Pretexting μπορούν να λάβουν χώρα, χωρίς να είναι απαραίτητη η χρήση της τεχνολογίας.

- **Baiting**

  Οι επιθέσεις Baiting έχουν πολλά κοινά στοιχεία με τις επιθέσεις Phishing. Η πιο ουσιαστική διαφορά μεταξύ τους είναι ότι οι πρώτες βασίζονται στην υπόσχεση ενός δωρεάν προϊόντος ή αγαθού για να παραπλανήσουν το θύμα τους, ευελπιστώντας πως το θύμα θα υποκύψει στην περιέργεια η την απληστία του. Πέρα από τη χρήση διαδικτυακών μεθόδων τέτοιες επιθέσεις μπορούν να γίνουν πραγματικότητα με τη χρήση φυσικών μέσων (DVD, USB), τα οποία παρά τις δελεαστικές τους ετικέτες, περιέχουν κακόβουλο λογισμικό.

4. Αντιμετώπιση Απειλών Ασφαλείας στο IoHT

Η ασφάλεια στα πλαίσια του IoHT, όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, αποτελεί μείζον ζήτημα, ενώ συντρέχουν ποικίλες απειλές για τα διάφορα περιουσιακά στοιχεία (assets) του συστήματος. Το πλήθος και η διαφορετική φύση των απειλών ασφαλείας, παρότι ενίοτε φαντάζει ανυπέρβλητος ανασταλτικός παράγοντας για την υιοθέτηση συστημάτων IoHT σε μεγάλη κλίμακα, έχει ταυτόχρονα κινητροδοτήσει την έρευνα για την εύρεση εξειδικευμένων μέτρων αποτροπής τους.

Η διεθνής βιβλιογραφία εμπεριέχει πληθώρα νέων καινοτόμων ιδεών για την ασφάλεια του IoT, ενώ παράλληλα έχουν εκπονηθεί μελέτες για την προσαρμογή συμβατικών μεθόδων και μηχανισμών στις πολύπλοκες ανάγκες των νέων συστημάτων. Η αποτελεσματικότητα κάθε αντιμέτρου είναι συνάρτηση του κόστους του σε σχέση με οικονομικούς, υπολογιστικούς και ενεργειακούς πόρους και της επικινδυνότητας της αντίστοιχης απειλής, για την εκτίμηση της οποίας έχουν αναπτυχθεί εξειδικευμένες μέθοδοι.

4.1. Μεθοδολογία Διαχείρισης Κινδύνων

4.1.1. Εκτίμηση κινδύνων ασφαλείας (Security Risk Assessment)

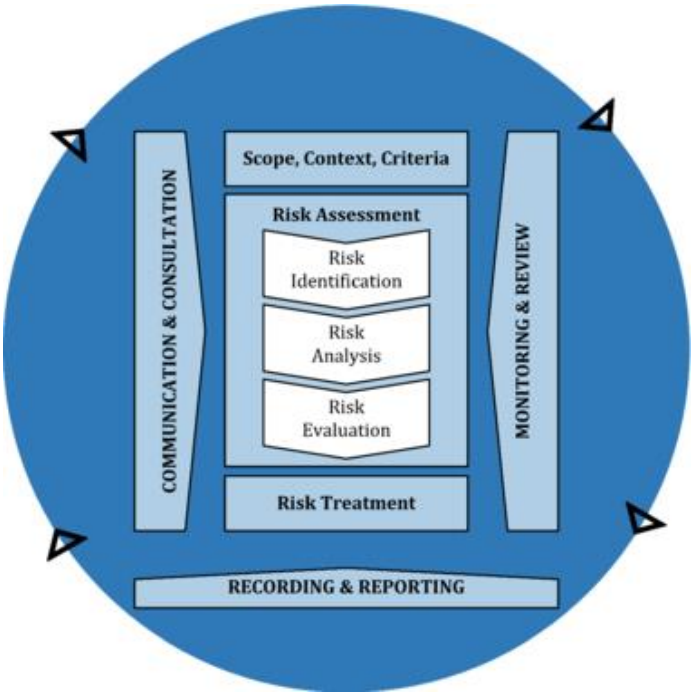
Οι επιθέσεις που παρουσιάστηκαν στο προηγούμενο κεφάλαιο, παρότι όλες είναι σε θέση να επιφέρουν δυσμενείς συνέπειες, δεν αντιπροσωπεύουν τον ίδιο κίνδυνο για την ασφάλεια των διαφόρων συστημάτων IoHT, ούτε και έχουν την ίδια πιθανότητα εμφάνισης. Για παράδειγμα η εξαπόλυση επίθεση DDoS προφανώς έχει αυξημένες απαιτήσεις σε ζητήματα χρόνου, τεχνογνωσίας και μέσων συγκριτικά με μια επίθεση κοινωνικής μηχανικής, παράλληλα όμως φέρει, στη γενική περίπτωση, πιο επιζήμιες συνέπειες. Επιπλέον μια επίθεση ωμής βίας μπορεί σε συστήματα χωρίς ισχυρούς κωδικούς πρόσβασης και σχετικές δικλείδες ασφαλείας να συνιστά άμεσο κίνδυνο, εντούτοις σε δίκτυα όπου αυτές οι αρχές στοιχειωδώς πληρούνται, η επικινδυνότητα τους μειώνεται αισθητά. Από τα παραπάνω γίνεται αντιληπτή η αναγκαιότητα της κατάλληλης προσαρμογής της ασφάλειας ενός συστήματος IoHT με γνώμονα την πρόληψη, τον εντοπισμό και την αποτροπή των επιβλαβέστερων και συνηθέστερων επιθέσεων για το **συγκεκριμένο** περιβάλλον.

Καθοριστικό ρόλο στην αντιμετώπιση των κίνδυνων και στην οικοδόμηση ενός αποδοτικού και ευέλικτου συστήματος ασφαλείας διαδραματίζει η διαδικασία εκτίμησης κινδύνων ασφαλείας (Security Risk Assessment). Πρόκειται για μια πρακτική, η οποία ανήκει στη γενικότερη διαδικασία διαχείρισης κινδύνων ασφαλείας (Security Risk Management) και περιλαμβάνει την αναγνώριση, την ανάλυση και τέλος την αξιολόγηση και προτεραιοποίηση των κινδύνων [53], με κριτήρια τη βαρύτητα των επιπτώσεων τους και την πιθανότητα εμφάνισης τους. Η διαδικασία αυτή παρέχει τα απαραίτητα εφόδια για την αντιμετώπιση υπαρχόντων και νέων απειλών και οφείλει να

εκτελείται περιοδικά καθ' όλη τη διάρκεια ζωής του συστήματος, ιδίως όταν έχουν συντελεστεί δομικές αλλαγές ή αφότου εντοπιστούν κενά ασφαλείας.

Τα επιμέρους στάδια της διαδικασίας [54] όπως απεικονίζονται στην Εικόνα 20, είναι τα εξής:

- **Αναγνώριση των κινδύνων (Risk Identification):**
  Η αναγνώριση των κινδύνων είναι κατ' ουσίαν ο προσδιορισμός των ενδεχόμενων επιθέσεων για το κάθε περιουσιακό στοιχείο (asset) του συστήματος, η εύρεση των ευπαθειών και των ακριβών τρόπων εκμετάλλευσής τους και στη συνέχεια η εξαγωγή συμπερασμάτων για την έκταση της ζημίας.



Εικόνα 20. Τα στάδια της διαδικασίας εκτίμησης κινδύνων μέσα στο γενικότερο πλαίσιο της διαχείρισης κινδύνων.

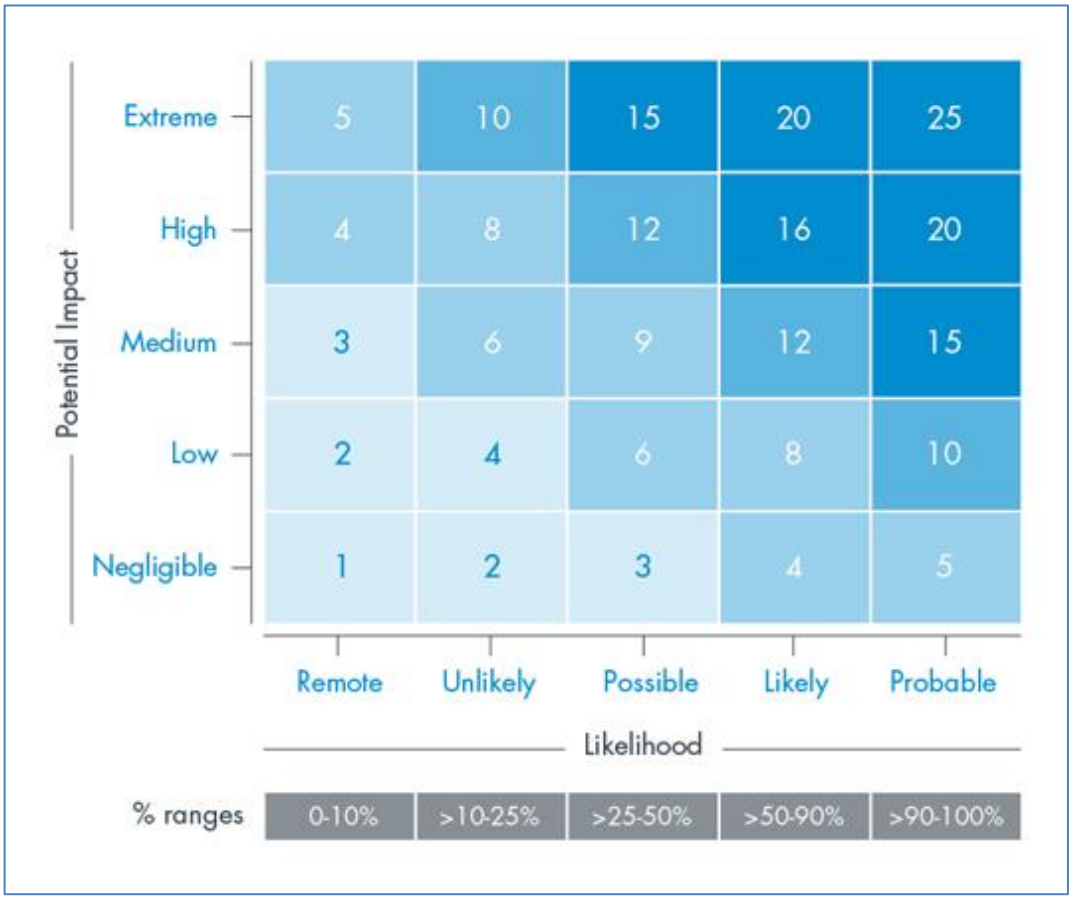
Πηγή: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

- **Ανάλυση των κινδύνων (Risk Analysis):**
  Σε αυτό το στάδιο με βάση τα δεδομένα του προηγούμενο σταδίου επιχειρείται μια «μέτρηση» της επικινδυνότητας της εκάστοτε απειλής. Οι προσεγγίσεις που χρησιμοποιούνται για το σκοπό αυτό μπορούν να διακριθούν σε δυο κατηγορίες, τις ποιοτικές και τις ποσοτικές. Η πρώτη κατηγορία εμπεριέχει τρόπους μέτρησης που χρησιμοποιούνται στις πιο διαδεδομένες προτάσεις (π.χ. NIST SP800-30, ISO/IEC 27001), οι οποίοι στηρίζονται σε προσεγγιστικούς χαρακτηρισμούς της επικινδυνότητας [55], όπως για παράδειγμα σε υψηλή, μεσαία ή χαμηλή. Μολονότι η χρήση αυτής της μεθόδου παρουσιάζει σημαντικά πλεονεκτήματα αναφορικά με την απλότητα της και τη δυνατότητα κατανόησης

του επιπέδου επικινδυνότητας από τρίτους, πάσχει, όπως είναι φυσικό, εξαιτίας της εισαγωγής του υποκειμενικού παράγοντα και της ανακρίβειάς της. Οι ποσοτικές προσεγγίσεις από την άλλη βασίζονται σε μαθηματικά μοντέλα πιθανοτήτων και, ενώ επιλύουν αρκετά από τα προβλήματα των ποιοτικών προσεγγίσεων, εγείρουν εξίσου σημαντικά ερωτήματα όσον αφορά την ακρίβεια, την ευχρηστία και την πολυπλοκότητα των μοντέλων [55].

- **Αξιολόγηση των κινδύνων (Risk Evaluation):**
  Στο τελευταίο αυτό στάδιο της διαδικασίας οι απειλές ιεραρχούνται με βάση την επικινδυνότητα τους, ώστε να δρομολογηθούν στη συνέχεια διαδικασίες αντιμετώπισης για όσες εξ αυτών κρίνεται απαραίτητο.

Πρέπει να διευκρινιστεί πως αναφορικά με το IoT, παρά τις προσπάθειες προτυποποίησης και παρότι η θεμελιώδης λειτουργία της διαδικασίας εκτίμησης κινδύνων, όπως αυτή αναλύθηκε παραπάνω, σε γενικές γραμμές έχει καθοριστεί, τα ειδικότερα εργαλεία και οι επιμέρους διεργασίες που χρησιμοποιούνται στα διάφορα στάδια συνεχίζουν να αποτελούν ανοιχτά θέματα προς συζήτηση [55], [56].



Εικόνα 21. Τυπικό παράδειγμα πίνακα επικινδυνότητας (risk matrix/risk heat mat). Τέτοιου είδους πίνακες χρησιμοποιούνται ευρέως στην ποιοτική αξιολόγηση κινδύνων.

Πηγή: https://www.cgma.org/resources/tools/essential-tools/risk-heat-maps.html

Μετά το πέρας της διαδικασίας εκτίμησης κινδύνων, οι διαχειριστές του συστήματος μπορούν να προβούν σε στοχευμένες ενέργειες για την αντιμετώπιση τους, αξιοποιώντας τις πληροφορίες που έχουν συγκεντρωθεί. Ανάλογα με το βαθμό επικινδυνότητας μιας απειλής, τα διαθέσιμα μέσα αντιμετώπισης της, τους οικονομικούς πόρους και τα ιδιαίτερα χαρακτηριστικά του δικτύου, προσφέρονται διαφορετικές επιλογές για τη διαχείριση του αντίστοιχου κινδύνου, μεταξύ των οποίων ξεχωρίζουν οι παρακάτω [54], [55]:

- **Μετρίαση κινδύνου:** Η προσπάθεια περιορισμού είτε του αντικτύπου είτε της πιθανότητας εμφάνισης μιας επίθεσης, με τη χρήση μηχανισμών ασφαλείας και αντιμέτρων.
- **Αποδοχή κινδύνου:** Η τήρηση παθητικής στάσης απέναντι στην απειλή, χωρίς τη λήψη οποιουδήποτε μέτρου αποτροπής η ελάττωσης των επιπτώσεων της. Πρόκειται για επιλογή εναντίον απειλών μικρής επικινδυνότητας, η οποία κυμαίνεται εντός των αποδεκτών ορίων του συστήματος.
- **Αποφυγή κινδύνου:** Η αποφυγή χρήσης ή απόσυρση ενός ευάλωτου asset, όταν οι υπόλοιπες μέθοδοι είναι ασύμφορες.

Στα πλαίσια της παρούσας εργασίας και αναφορικά με τον τομέα της ασφάλειας του IoHT, όπως είναι ευνόητο, το ενδιαφέρον μονοπωλεί η πρώτη κατηγορία, αφού ουσιαστικά περιγράφει τον αυτοσκοπό της ασφάλειας ενός συστήματος.

4.1.2. Δοκιμή Διείσδυσης (Penetration Testing/Pentest)

Ανεξάρτητα από τις τεχνικές που εφαρμόζονται στα πλαίσια της διαδικασίας εκτίμησης κινδύνου, δεν μπορεί να αποκλειστεί το ενδεχόμενο εσφαλμένης αξιολόγησης της επικινδυνότητας μιας απειλής ή η πιθανότητα παράβλεψης κάποιων σημαντικών παραμέτρων. Είναι συνεπώς αναγκαίος ο έλεγχος των ισχυρισμών που διατυπώνονται στην παραπάνω διαδικασία σε πρακτικό επίπεδο, ώστε να διαπιστωθεί κατά πόσο ευσταθούν. Ειδικότερα για την περίπτωση των εφαρμογών του IoT, όπου, εξαιτίας της πολυπλοκότητας των συστημάτων, η θεωρητική ανάλυση των κινδύνων δεν επαρκεί, η διεξαγωγή πρακτικών δοκιμών κρίνεται απαραίτητη.

Μία ευρέως διαδεδομένη μέθοδος που έχει προτυποποιηθεί είναι η δοκιμή διείσδυσης (Penetration Testing). Πρόκειται για μία εξουσιοδοτημένη προσομοίωση κυβερνοεπίθεσης στα επιμέρους τμήματα και πολύτιμα περιεχόμενα (assets) του συστήματος υπό ελεγχόμενες συνθήκες. Σκοπός της μεθόδου είναι η ανάδειξη κενών ασφαλείας και ευπαθειών, τις οποίες ένας επιτιθέμενος θα ήταν σε θέση να εκμεταλλευτεί, και η εξακρίβωση της έκτασης της ζημίας που συνδέεται με αυτή την εκμετάλλευση. Ιδανικά το αντικείμενο μελέτης μιας δοκιμής διείσδυσης πρέπει να είναι ολόκληρο το σύστημα IoT και η συνολική υποδομή του, ωστόσο, λόγω του κόστους και των τεχνικών περιορισμών ο έλεγχος μονό ενός υποσυνόλου του συστήματος αποτελεί

συνήθη πρακτική [57]. Η δοκιμή διείσδυσης λειτουργεί συμπληρωματικά ως προς τη διαδικασία της εκτίμησης κινδύνων, επιτρέποντας την εξαγωγή εγκυρότερων συμπερασμάτων και τη λήψη πιο εξειδικευμένων και αποτελεσματικότερων μέτρων αντιμετώπισης.

4.2. Τρόποι Αντιμετώπισης Απειλών

Στη διεθνή βιβλιογραφία υπάρχει πλήθος προτάσεων μέτρων ασφαλείας που μπορούν να αξιοποιηθούν στα πλαίσια των διαφόρων εφαρμογών του IoT. Σε αυτήν την ενότητα, παρουσιάζονται μερικές από τις βασικότερες μεθόδους και μηχανισμοί, άλλοι ευρέως χρησιμοποιούμενοι στα συμβατικά δίκτυα και άλλοι πιο καινοτόμοι, η υιοθέτηση των οποίων δύναται να ενισχύσει την ασφάλεια των συστημάτων. Για την κάθε τεχνολογία αναλύεται η βασική αρχή λειτουργίας της καθώς και τα οφέλη και οι προκλήσεις που συνδέονται με την ενσωμάτωση της στο IoT και κατά επέκταση στο IoHT. Επίσης, αξίζει να επισημανθεί πως αυτά τα μέτρα ασφαλείας δεν επαρκούν για την **πλήρη** κάλυψη των σύνθετων αναγκών του IoT παρά μόνο προσφέρουν ένα ελάχιστο επίπεδο ασφάλειας.

4.2.1. Σύστημα Ανίχνευσης Εισβολής (Intrusion Detection System - IDS)

Για την ανίχνευση πιθανών παραβιάσεων και ύποπτων ή ασυνήθιστων δραστηριοτήτων σε ένα υπολογιστικό σύστημα ή δίκτυο, είναι διαδεδομένη η χρήση συσκευών ή εφαρμογών λογισμικού, οι οποίες είναι επιφορτισμένες με τη διαρκή παρακολούθηση των συνθηκών λειτουργίας. Αυτές οι συσκευές ή εφαρμογές είναι γνωστές ως συστήματα ανίχνευσης εισβολών (Intrusion Detection System - IDS). Η βασική λειτουργία ενός τέτοιου συστήματος περιορίζεται, όπως υποδηλώνει και το όνομά τους, αποκλειστικά στην ανίχνευση εισβολών, τη σύνταξη δηλαδή αναφορών σχετικά με ύποπτα περιστατικά, χωρίς να προβαίνει σε δράσεις μετρίασης των επιπτώσεών τους.

Διαχρονικά σε συστήματα IDS έχουν χρησιμοποιηθεί διάφοροι μέθοδοι ανίχνευσης εισβολών, με κυριότερες την ανίχνευση με βάση την απόκλιση της συμπεριφοράς ενός κόμβου του δικτύου από την προβλεπόμενη (anomaly-based detection) και την ανίχνευση με βάση τις αλλαγές που προκαλούν τα κακόβουλα λογισμικά σε αρχεία που προσβάλλουν (signature-based detection). Αυτές οι αλλαγές, το λεγόμενο «αποτύπωμα» ενός κακόβουλου λογισμικού, είναι μια χαρακτηριστική ακολουθία bytes που έχει προστεθεί σε ένα αρχείο ή πακέτο δεδομένων. Οι δυο μέθοδοι έχουν έκαστη τα δικά της πλεονεκτήματα και μειονεκτήματα. Στην περίπτωση της πρώτης υπάρχει μεγάλη πιθανότητα λανθασμένης αναφοράς μιας νόμιμης δραστηριότητας ως κακόβουλης (false positive). Από την άλλη, στην περίπτωση του «αποτυπώματος» ενός κακόβουλου λογισμικού, το ενδεχόμενο λανθασμένης εκτίμησης είναι σπάνιο,

εντούτοις απαιτείται η εξέταση των αρχείων για ένα μεγάλο και συνεχώς αυξανόμενο σύνολο γνωστών «αποτυπωμάτων». Όπως γίνεται εύκολα αντιληπτό, μια τέτοια διαδικασία δεν μπορεί παρά να έχει υψηλό κόστος για τους υπολογιστικούς πόρους και να επιβαρύνει δραστικά την απόδοση του συστήματος.

Μολονότι συστήματα IDS χρησιμοποιούνται ευρέως σε συμβατικά δίκτυα και συστήματα ήδη από το 1983, η ενσωμάτωσή τους σε περιβάλλοντα IoT και IoHT, εξαιτίας της πολυπλοκότητάς τους, παρουσιάζει αξιοσημείωτες προκλήσεις.

Αρχικά, ο αριθμός των συνδεδεμένων συσκευών είναι τάξεις μεγέθους μεγαλύτερος από αυτόν στα συμβατικά δίκτυα. Το μεγάλο πλήθος συσκευών έχει ως πιθανή συνέπεια την εμφάνιση πρωτόγνωρων μοτίβων συμπεριφοράς μιας ομάδας κόμβων, των οποίων η αξιολόγηση είναι περίπλοκη διαδικασία [58]. Αντιθέτως, στην περίπτωση των δικτύων στα οποία σήμερα βρίσκουν εφαρμογή IDS, η συμπεριφορά μπορεί εύκολα να εκτιμηθεί και να αποφασιστεί εάν εμπίπτει σε κάποιο ύποπτο μοτίβο. Μοτίβα ομαδικής συμπεριφοράς των κόμβων είναι δύσκολο να προβλεφθούν σε θεωρητικό επίπεδο, πριν την εγκατάσταση συστημάτων IoHT σε μεγάλη κλίμακα.

Επιπροσθέτως, η επικοινωνία στο IoT δεν ακολουθεί μια συγκεκριμένη κατεύθυνση προς ένα σημείο, όπου θα μπορούσε εύκολα να υποστεί έλεγχο, αλλά προϋποθέτει τη διακίνηση πληροφοριών μεταξύ των διαφόρων έξυπνων συσκευών [58]. Το πλήθος των καναλιών επικοινωνίας, το οποίο πρέπει να βρίσκεται υπό την αδιάκοπη εποπτεία ενός συστήματος IDS, καθώς και τα διαφορετικά πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στα κανάλια αυτά, αποτελούν εξίσου σημαντική πρόκληση.

Τέλος, τόσο η ευπάθεια των έξυπνων συσκευών σε φυσικές επιθέσεις, οι περιορισμοί τους αναφορικά με την κατανάλωση ενέργειας, τη μνήμη και την υπολογιστική ισχύ, όσο και η ετερογένειά τους πρέπει να εξεταστούν ενδελεχώς για το σχεδιασμό ενός αποτελεσματικού συστήματος IDS. Οι έξυπνες συσκευές αποτελούν, όπως αναλύθηκε παραπάνω, τους πιο ευάλωτους στόχους σε ένα σύστημα IoHT, για τον λόγο αυτό απαιτείται συνεχής και προσεκτικός έλεγχος της συμπεριφοράς τους καθώς και η έγκαιρη αναγνώριση των μοτίβων που υποδεικνύουν ύποπτη συμπεριφορά. Τα μοτίβα αυτά ωστόσο, χωρίς την απαραίτητη προτυποποίηση, ενδέχεται να διαφέρουν μεταξύ συσκευών, κατασκευαστών ή ακόμα και διαφορετικών εκδόσεων λογισμικού, γεγονός που καθιστά αδήριτη την ανάγκη για αδιάλειπτη έρευνα στον τομέα αυτό και τη συνεχή ενημέρωση των συστημάτων IDS.

4.2.2. Σύστημα Αποτροπής Εισβολής (Intrusion Prevention System - IPS)

Η λειτουργία των συστημάτων IDS προϋποθέτει τη συμβολή του ανθρώπινου παράγοντα, αφού οι συντασσόμενες αναφορές πρέπει αρχικά να προωθηθούν σε μια ομάδα διαχειριστών, οι οποίοι έπειτα καλούνται να αποφασίσουν και να προβούν στις αναγκαίες ενέργειες. Αυτή η διαδικασία είναι χρονοβόρα και κατά τη διάρκειά της το σύστημα παραμένει ευάλωτο και οι επιπτώσεις της εισβολής αυξάνονται. Για την

αμεσότερη αντιμετώπιση των απειλών, τα συστήματα IDS σταδιακά απέκτησαν τη δυνατότητα, πέρα από την ανίχνευση εισβολών, να επιτελούν αυτοματοποιημένες λειτουργίες για την αποτροπή τους. Τα εξελιγμένα αυτά συστήματα είναι γνωστά ως συστήματα αποτροπής εισβολής (IPS) ή ως συστήματα ανίχνευσης και αποτροπής εισβολής (IDPS).

Ένα σύστημα IPS εξετάζει σε πραγματικό χρόνο την εισερχόμενη και εξερχόμενη κίνηση σε ένα δίκτυο ή υπολογιστικό σύστημα και, στην περίπτωση ανίχνευσης συμβάντων που δυνητικά συνιστούν απειλή, μπορεί να προχωρήσει στις εξής ενέργειες [59]:

- Τερματισμός της TCP συνεδρίας, την οποία έχουν εκμεταλλευτεί οι εισβολείς, αποκλεισμός και στέρηση πρόσβασης της IP διεύθυνσης πηγής ή του λογαριασμού χρήστη σε οποιαδήποτε εφαρμογή ή άλλους πόρους του συστήματος.
- Επαναπρογραμματισμός ή επαναπαραμετροποίηση του τείχους προστασίας για την αποτροπή παρόμοιων επιθέσεων μελλοντικά.
- Αφαίρεση ή αντικατάσταση οποιουδήποτε κακόβουλου περιεχομένου που έχει παραμείνει στο δίκτυο, μετά το πέρας μιας επίθεσης.

Παρόλο που η ενσωμάτωση συστημάτων IPS και IDS σε περιβάλλοντα IoHT παρουσιάζει ιδιαίτερες δυσκολίες, αυτή θα ήταν αναμφίβολα ευεργετική, διότι έτσι θα παρεχόταν η δυνατότητα ανίχνευσης (ή και αποτροπής) πλήθους επιθέσεων. Μεταξύ άλλων οι επιθέσεις αυτές περιλαμβάνουν [59]:

- Επιθέσεις DDoS
- Επιθέσεις DoS
- Κακόβουλο λογισμικό (ιούς, worms κ.α.)
- Επιθέσεις Brute Force

4.2.3. Διαχείριση Πληροφοριών και Συμβάντων Ασφαλείας (Security Information and Event Management - SIEM)

Η κοινή αδυναμία των συστημάτων IDS και IPS έγκειται στην αντιμετώπιση νέων απειλών, οι οποίες δεν έχουν ακόμη μελετηθεί, ώστε να είναι εφικτή η ανίχνευση και αποτροπή τους. Την ανάγκη αυτή εξυπηρετούν τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM). Πρόκειται για ένα σύνολο εργαλείων, τα οποία προσφέρουν παρακολούθηση και ανάλυση συμβάντων σε πραγματικό χρόνο, καθώς και ανίχνευση και καταγραφή δεδομένων ασφαλείας [60].

Η λειτουργία των συστημάτων SIEM στηρίζεται στην πρόσληψη πληροφοριών από ένα μεγάλο εύρος πηγών, το οποίο περιλαμβάνει χρήστες, εφαρμογές λογισμικού, συσκευές και συστήματα IDS και IPS. Οι συλλεγόμενες πληροφορίες στη συνέχεια αποθηκεύονται και αναλύονται σε πραγματικό χρόνο. Οι προηγμένες μέθοδοι

ανάλυσης, που εφαρμόζονται, επιτρέπουν τη συσχέτιση συμβάντων και την αναγνώριση πολύπλοκων μοτίβων δεδομένων, ενισχύοντας έτσι την ικανότητα και την ταχύτητα εντοπισμού και αντιμετώπισης απειλών [60]. Μία ακόμη δυνατότητα των συστημάτων αυτών είναι η αναπαράσταση παρελθοντικών συμβάντων, για την εμπεριστατωμένη εξέταση των υπαίτιων ενεργειών και, μετά τον προσδιορισμό των σχετικών εγγενών ευπαθειών, η πρόταση κατάλληλων μέτρων αντιμετώπισής τους [60].

Τα πιο εξελιγμένα συστήματα SIEM ενσωματώνουν τεχνολογίες τεχνητής νοημοσύνης και πιο συγκεκριμένα τεχνολογίες deep learning (βαθιά μηχανική μάθηση). Κατά αυτόν τον τρόπο, διευκολύνεται η αυτοματοποίηση διαδικασιών σχετικών με την ανίχνευση και την εξουδετέρωση απειλών και τη διαχείριση συμβάντων και, συνεπακόλουθα, περιορίζονται σημαντικά τα καθήκοντα των διαχειριστών. Επιπροσθέτως, μέσω του deep learning, τα συστήματα βαθμιαία αποκτούν την ικανότητα να διακρίνουν πρωτοεμφανιζόμενα μοτίβα συμπεριφοράς, πέρα από αυτά που τους έχουν κατασταθεί γνωστά. Αυτή η ικανότητα αναδεικνύει τα συστήματα SIEM ως αποτελεσματικά μέσα ασφάλειας ενάντια σε καινοφανείς απειλές.

Παρότι οι αυτοματοποιημένες διαδικασίες διαδραματίζουν κομβικό ρόλο στη λειτουργία των SIEM, σε ορισμένες καταστάσεις η συνεισφορά του ανθρώπινου παράγοντα δεν παύει να είναι απαραίτητη. Ειδικότερα, όταν παρατηρούνται συμβάντα ασφαλείας, όπου ένα σύστημα SIEM δεν μπορεί να προσδιορίσει με ακρίβεια τον βαθμό επικινδυνότητάς τους, τότε είναι σε θέση να αποστείλει άμεσα ειδοποιήσεις στους διαχειριστές του συστήματος, οι οποίοι θα κινητοποιηθούν ανάλογα.

Από τα παραπάνω εύκολα συνάγονται τα πιθανά οφέλη της υιοθέτησης συστημάτων SIEM στο περιβάλλον του IoHT, όπως και για οποιοδήποτε άλλο πληροφοριακό σύστημα. Η υιοθέτηση αυτή παρουσιάζει παρόμοιας φύσης προκλήσεις με την περίπτωση των συστημάτων IDS και IPS, καθώς τα συμβατικά δίκτυα, για τα οποία έχουν σχεδιαστεί, δεν χαρακτηρίζονται από την ίδια πολυπλοκότητα και όγκο διακινούμενων πληροφοριών, όπως τα δίκτυα IoT, συνεπώς απαιτούνται προσαρμογές. Προτάσεις συστημάτων SIEM για χρήση σε περιβάλλοντα IoT αναλύονται στα [61], [62] και [63].

4.2.4. Παγίδες Εισβολέων (Honeypot)

Τα honeypot αποτελούν ένα διαθέσιμο μέτρο ασφαλείας για τα συμβατικά συστήματα και η πρώτη εφαρμογή τους εντοπίζεται δεκαετίες πριν. Η χρήση τους μπορεί να συνεισφέρει σημαντικά στην ανίχνευση μη εξουσιοδοτημένων ενεργειών και στην άντληση πληροφοριών σχετικά με τις συγκεκριμένες δράσεις και τη συμπεριφορά των επιτιθέμενων. Η υιοθέτηση τους σε συστήματα IoT αποτελεί πεδίο έρευνας, ενώ υπάρχει πλήθος προτεινόμενων λύσεων honeypot για τις διάφορες εφαρμογές του IoT [64].

Ο όρος honeypot χρησιμοποιείται για την περιγραφή ενός συνόλου μηχανισμών ασφαλείας, κοινός παρονομαστής των οποίων είναι η προσέλκυση και στη συνέχεια η παγίδευση επίδοξων εισβολέων, παρέχοντας πρόσφορο έδαφος για μια επίθεση. Τα honeypot παριστάνουν γνήσιες οντότητες του δικτύου, οι οποίες στεγάζουν πολύτιμα δεδομένα ή πόρους. Στην πραγματικότητα ωστόσο, αποτελούν μέρη του δικτύου που δεν διαχειρίζονται σημαντικές πληροφορίες, δεν επιτελούν κρίσιμες λειτουργίες και δεν προσφέρουν δίοδο προς άλλα μέρη του δικτύου, συνεπώς ενδεχόμενη προσβολή τους δεν συνιστά κανένα κίνδυνο για το δίκτυο. Απεναντίας ο σκοπός της ύπαρξης τους είναι να γίνουν στόχοι των επιτιθέμενων και στη συνέχεια να συγκεντρώσουν πληροφορίες για τον ακριβή τρόπο δράσης τους και τις ευπάθειες του συστήματος, ώστε να αποτραπούν παρόμοια περιστατικά στο μέλλον. Τέλος, αξίζει να σημειωθεί, πως η συμβολή τους είναι κρίσιμη κυρίως αναφορικά με την εξιχνίαση και τη μελέτη επιθέσεων οι οποίες διαγράφουν τα ίχνη τους [64].

Όπως είναι ευνόητο, ένας εξουσιοδοτημένος ή μη εξουσιοδοτημένος χρήστης του δικτύου δεν θα είχε παρά κακόβουλο κίνητρο παραβίασης ενός honeypot, κατά συνέπεια οι εν λόγω μηχανισμοί ασφαλείας αποδεικνύονται τελεσφόροι στην ανίχνευση τόσο εξωτερικών, όσο και εσωτερικών απειλών. Οποιαδήποτε προσπάθεια προσπέλασης των δεδομένων συνεπάγεται άμεση ειδοποίηση προς τους διαχειριστές για την ύπαρξη κινδύνου.

Τα honeypot μπορούν να χρησιμοποιηθούν συνδυαστικά με συστήματα IDS ενισχύοντας την αποτελεσματικότητα τους. Πλεονεκτήματα αποτελούν επίσης οι χαμηλές ανάγκες τους σε υπολογιστικούς πόρους και το σχετικά μικρό χρηματικό κόστος τους, καθώς δεν απαιτείται να είναι φυσικές συσκευές, αλλά μπορούν να είναι και εικονικές (virtual machines) [64].

4.2.5. Τείχος Προστασίας (Firewall)

Τα τείχη προστασίας (firewalls) είναι συσκευές ή εφαρμογές λογισμικού που περιλαμβάνονται στη συντριπτική πλειονότητα των σύγχρονων συστημάτων ασφαλείας δικτύων. Βασική αρχή λειτουργίας τους είναι η παρακολούθηση της εισερχόμενης και εξερχόμενης κίνησης και η απόρριψη πακέτων δεδομένων που δεν συμμορφώνονται με ένα προκαθορισμένο σύνολο κανόνων ασφαλείας [65]. Υπάρχουν firewalls τόσο για την προστασία ενός ολοκλήρου δικτύου (network-based), όσο και προσωπικά (host-based) για την προστασία συγκεκριμένης συσκευής-κόμβου του δικτύου. Στην πρώτη περίπτωση τα firewalls συνήθως εφαρμόζονται με τη χρήση ανεξάρτητου υπολογιστικού συστήματος, ενώ στη δεύτερη, όπου ο όγκος των δεδομένων είναι αισθητά μικρότερος, μπορούν να έχουν τη μορφή εφαρμογής λογισμικού που είναι εγκατεστημένη στον κόμβο.

Ένα κατάλληλα παραμετροποιημένο firewall έχει τη δυνατότητα καταστολής πλήθους εξωτερικών απειλών, όπως επιθέσεις DDoS και προσβολές από κακόβουλο

λογισμικό, πριν ακόμη εγκαθιδρυθεί η σύνδεση με τη συσκευή-στόχο. Εντούτοις, η συμβολή τους στην αποσόβηση εσωτερικών απειλών είναι μηδαμινή, καθώς δεν έχει την ικανότητα αποκλεισμού ενός εξουσιοδοτημένου χρήστη του δικτύου, ανεξαρτήτως αν αυτός δρα κακόβουλα. Επιπροσθέτως, το παρεχόμενο επίπεδο ασφάλειας υποβαθμίζεται σημαντικά, τη στιγμή που ένα κακόβουλο λογισμικό διαπεράσει το τείχος προστασίας, γεγονός το οποίο καταδεικνύει την ανάγκη συνεχούς ενημέρωσής του.

Μολονότι η χρήση τειχών προστασίας φαντάζει αναπόσπαστο στοιχείο της ασφάλειας στα συμβατικά δίκτυα, η επέκταση της τεχνολογίας αυτής στις διάφορες εφαρμογές του IoT δεν είναι εύκολα πραγματοποιήσιμη. Πιο συγκεκριμένα, ενώ η υιοθέτηση network-based firewalls είναι εφικτή, μετά από απαραίτητες προσαρμογές στις ανάγκες του IoT, στην προσπάθεια ενσωμάτωσης host-based firewalls ανακύπτουν σημαντικά προβλήματα. Όσον αφορά τις έξυπνες συσκευές, τις περισσότερες φορές δεν απαιτούνται σύνθετα τείχη προστασίας με προηγμένα χαρακτηριστικά, όμως δεν παύει να υφίσταται ανάγκη για τις θεμελιώδεις λειτουργίες τους [66]. Ανεξαρτήτως με το χαμηλό κόστος σε πόρους της συσκευής, η εξεύρεση αυτών των πόρων αποτελεί τροχοπέδη, δεδομένου πως οι συσκευές αυτές υπόκεινται σε περιορισμούς υπολογιστικής ισχύος, μνήμης και ενεργειακής αυτονομίας. Επιπλέον δεν πρέπει να παραβλέπεται το σημαντικό οικονομικό κόστος, που συνδέεται με την εφαρμογή host-based firewalls, καθώς και το γεγονός πως η διαδικασία σχεδιασμού και υλοποίησης εξειδικευμένων firewalls για τις διάφορες έξυπνες συσκευές είναι πολύπλοκη [67].

4.2.6. Κρυπτογράφηση

Στα σύγχρονα συμβατικά συστήματα είναι πλέον σχεδόν αυτονόητη η χρήση κάποιου είδους κρυπτογράφησης, για τη διαφύλαξη της εμπιστευτικότητας των πληροφοριών. Πρόκειται για μία διαδικασία, κατά την οποία ένα μήνυμα καθίσταται μη αναγνώσιμο από οποιονδήποτε πέρα από τον προκαθορισμένο παραλήπτη του, με τη βοήθεια ειδικών αλγορίθμων κρυπτογράφησης. Η κρυπτογράφηση θεωρείται ευρέως ως το πιο αποτελεσματικό αντίμετρο εναντίον των διαφόρων μορφών επιθέσεων Λαθρακρόασης και η εφαρμογή της σε περιβάλλοντα IoT έχει αποτελέσει σημαντικό πεδίο έρευνας.

Για την πληρέστερη κατανόηση των όσων ακολουθούν, θεωρείται σκόπιμο αρχικά να αναφερθούν κάποιες βασικές σχετικές έννοιες.

- Αρχικό ή απλό κείμενο (plaintext): Είναι τα δεδομένα σε αναγνώσιμη μορφή που χρησιμοποιούνται ως είσοδος σε μία διεργασία κρυπτογράφησης.
- Κλειδί κρυπτογράφησης: μία ακολουθία bit βάσει της οποίας γίνεται ο μετασχηματισμός.

- Αλγόριθμος κρυπτογράφησης (cipher): Μία σύνθετη μαθηματική συνάρτηση, η οποία μετασχηματίζει το αρχικό κείμενο, ώστε αυτό να λάβει μία ακατανόητη μορφή.
- Κρυπτογραφημένο κείμενο ή κρυπτογράφημα (ciphertext): Η έξοδος της διεργασίας κρυπτογράφησης.
- Αποκρυπτογράφηση: Η αντίστροφη διαδικασία εξαγωγής του αρχικού κειμένου από το κρυπτογράφημα.
- Κλειδί αποκρυπτογράφησης: Μία ακολουθία bit βάσει της οποία γίνεται ο αντίστροφος μετασχηματισμός.

Ανάλογα με τη σχέση κλειδιού κρυπτογράφησης και κλειδιού αποκρυπτογράφησης διακρίνονται δύο είδη κρυπτογράφησης, η Συμμετρική και η Ασύμμετρη. Στην περίπτωση της πρώτης τα δύο κλειδιά είναι ίδια. Αυτό προϋποθέτει ότι ο αποστολέας έχει γνωστοποιήσει, μέσω ασφαλούς καναλιού επικοινωνίας, το μυστικό κλειδί του στον παραλήπτη, ώστε αυτός να το χρησιμοποιήσει για την αποκρυπτογράφηση. Όπως γίνεται αντιληπτό, θεμελιώδης απαίτηση της Συμμετρικής κρυπτογράφησης είναι η διασφάλιση της μυστικότητας του κλειδιού.

Από την άλλη, στην Ασύμμετρη κρυπτογράφηση κάθε χρήστης έχει στη κατοχή του ένα ζεύγος κλειδιών, το δημόσιο κλειδί, το οποίο κοινοποιείται και με βάση αυτού κρυπτογραφούνται τα μηνύματα που του αποστέλλονται, και το ιδιωτικό κλειδί, με βάση το οποίο τα μηνύματα αποκρυπτογραφούνται. Με τη μέθοδο αυτή εξαλείφεται η ανάγκη διαμοιρασμού των κλειδιών και συνεπώς η πιθανότητα υποκλοπής τους. Παρόλα αυτά οι ανάγκες για υπολογιστικούς πόρους τείνουν να είναι αρκετά μεγαλύτερες συγκριτικά με τη Συμμετρική κρυπτογράφηση.

Οι πιο διαδεδομένοι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται σήμερα σε tablets, smartphones, σε υπολογιστικά συστήματα κλπ. έχουν υψηλές απαιτήσεις σε υπολογιστικούς πόρους και, ως απόρροια, η χρήση τους δεν μπορεί να επεκταθεί σε έξυπνες συσκευές IoT. Λαμβάνοντας υπόψη τους περιορισμένους πόρους των συσκευών αυτών, έχουν προταθεί αλγόριθμοι κρυπτογράφησης, των οποίων η εφαρμογή δεν επιβαρύνει τη λειτουργικότητα τους (Lightweight Cryptographic Algorithms). Αυτό επιτυγχάνεται με την αξιοποίηση μόνο ορισμένων διεργασιών κρυπτογράφησης σε συνδυασμό με τη χρήση παραμέτρων ασφάλειας μικρότερου μεγέθους (όπως μικρότερο μέγεθος κλειδιού κρυπτογράφησης και μικρότερο μέγεθος κρυπτογραφημένου μηνύματος) [68].

Ένα μειονέκτημα αυτών των αλγορίθμων είναι πως το παρεχόμενο επίπεδο ασφάλειας είναι αισθητά υποδεέστερο σε σχέση με τους συμβατικούς αλγόριθμους. Η κύρια πρόκληση αναφορικά με το σχεδιασμό του κατάλληλου Lightweight αλγορίθμου είναι η εύρεση χρυσής τομής μεταξύ της ελάχιστης δυνατής κατανάλωσης και της μέγιστης δυνατής παρεχόμενης ασφάλειας. Τέλος, είναι αναγκαίο να επισημανθεί ότι για την κρυπτογράφηση δεδομένων σε συσκευές περιορισμένων δυνατοτήτων, έχουν

επίσης αναπτυχθεί αλγόριθμοι ultra-lightweight. Πρόκειται για αλγόριθμους, η εκτέλεση των οποίων είναι ταχύτατη και ο αντίκτυπος στη λειτουργία των συσκευών αμελητέος, ωστόσο η χρήση του στις εφαρμογές του IoT αντενδείκνυται εξαιτίας της υπερβολικής απλότητας τους.

Εξαιτίας της ανάγκης για χαμηλή κατανάλωση πόρων, η συντριπτική πλειοψηφία των Lightweight αλγορίθμων αφορούν τη Συμμετρική κρυπτογράφηση. Παραδείγματα τέτοιων αλγορίθμων που έχουν προταθεί για χρήση σε έξυπνες συσκευές IoT είναι οι αλγόριθμοι AES, PRESENT, DESL, DESX, DESLX, TEA, LEA, HIGHT, Simon, SPECK και TWINE [69], [70]. Αντίστοιχα στην περίπτωση της ασύμμετρης κρυπτογράφησης προτείνεται ο αλγόριθμος ECC, που θεωρείται από πολλούς ως η καλύτερη λύση αναφορικά με αυτό το είδος κρυπτογράφησης.

Στα ασύρματα δίκτυα αισθητήρων (WSN) η διανομή των κλειδιών (key distribution) ανάγεται σε μείζον πρόβλημα λόγω της εγγενούς ευπάθειας σε επιθέσεις Λαθρακρόασης. Η ευρέως θεωρούμενη ως αποτελεσματικότερη τεχνική για την υπέρβαση αυτού του προβλήματος είναι η προδιανομή των κλειδιών (key predistribution), όπου τα μυστικά κλειδιά ενσωματώνονται στις συσκευές πριν την υλοποίηση του δικτύου.

4.2.7. Πιστοποίηση Ταυτότητας Χρηστών

Πιστοποίηση Ταυτότητας ή Αυθεντικοποίηση ενός χρήστη είναι η διαδικασία, η οποία κατά κανόνα απαιτείται να λαμβάνει χώρα, πριν την οποιαδήποτε παροχή πρόσβασης σε εμπιστευτικά δεδομένα. Στην περίπτωση του IoHT, η κρισιμότητα και η προσωπική φύση των δεδομένων καθιστούν την ανάγκη για ασφαλείς μεθόδους αυθεντικοποίησης επιτακτική.

Στα πλαίσια της διαδικασίας Πιστοποίησης Ταυτότητας ζητείται από τον χρήστη η εισαγωγή προσωπικών στοιχείων ή η χρήση κάποιας ιδιόκτητης συσκευής. Αυτοί οι τρόποι επαλήθευσης ταυτότητας, γνωστοί ως παράγοντες αυθεντικοποίησης, κατηγοριοποιούνται σε τρείς διακριτές ομάδες [71].

- Παράγοντες σχετικοί με τη γνώση (Knowledge Factors): Πρόκειται για πληροφορίες που είναι γνωστές αποκλειστικά στον χρήστη.
- Παράγοντες σχετικοί με την ιδιοκτησία (Ownership Factors): Η χρήση, ως τεκμήρια ασφαλείας, αντικειμένων ή συσκευών που βρίσκονται υπό την κατοχή του χρήστη.
- Παράγοντες σχετικοί με τα προσωπικά γνωρίσματα του χρήστη (Inference Factors): Πληροφορίες οι οποίες προσδιορίζουν τη φυσική υπόσταση ή τη συμπεριφορά του χρήστη.

Η πρώτη και μέχρι σήμερα πιο διαδεδομένη μέθοδος αυθεντικοποίησης, είναι αυτή που χρησιμοποιεί έναν παράγοντα για την πιστοποίηση (Single Factor

Authentication - SFA), ο οποίος συνήθως είναι παράγοντας σχετικός με τη γνώση. Αυτή η μέθοδος κρίνεται ανεπαρκής, καθώς δεν παρέχει ικανοποιητικό επίπεδο ασφάλειας, ιδιαίτερα όσον αφορά την εφαρμογή της σε ηλεκτρονικές τραπεζικές συναλλαγές και σε περιβάλλοντα IoT.

Για την επίτευξη αυτού του αναγκαίου επιπέδου ασφάλειας, συνιστάται η χρήση μεθόδων αυθεντικοποίησης που αξιοποιούν δύο η περισσότερους παράγοντες (Multi Factor Authentication - MFA). Η απαίτηση εισαγωγής επιπρόσθετων πληροφοριών λειτουργεί αποτρεπτικά ενάντια σε επιθέσεις κοινωνικής μηχανικής και επιθέσεις ωμής βίας, διότι ακόμα και αν τα διαπιστευτήρια του χρήστη (π.χ. κωδικός πρόσβασης) περιέλθουν στην κατοχή του επιτιθέμενου, αυτό δεν συνεπάγεται την απόκτηση πιστοποίησης.

Σε συστήματα IoHT για την εφαρμογή της μεθόδου MFA, είναι ιδανική η χρήση βιομετρικών στοιχείων ως παράγοντα αυθεντικοποίησης, καθώς, ως γνωστόν, τα συστήματα αυτά ήδη διαχειρίζονται τέτοιας φύσης πληροφορίες, οι οποίες μάλιστα αντλούνται μέσω έξυπνων ιατρικών συσκευών σε πραγματικό χρόνο [72].

Πίνακας 1. Τρόποι Πιστοποίησης Ταυτότητας Χρηστών

Knowledge Factors:	Όνομα Χρήστη (Username)
	Κωδικός Πρόσβασης (Password)
Πληροφορία που γνωρίζει το άτομο	Κωδική φράση Πρόσβασης (Passphrase)
	Προσωπικός Αριθμός Αναγνώρισης (PIN)
	Ερώτηση Ασφαλείας (Security Question)
	Απαντήσεις σε προκαθορισμένες ερωτήσεις
Ownership Factors:	Έξυπνες Κάρτες (Smart Cards)
	Κλειδί USB (USB Key fob)
Αντικείμενο που βρίσκεται στην κατοχή του ατόμου (τεκμήριο ασφαλείας)	Συσκευή Κωδικών Μιας Χρήσης (Hardware Token)
	Έξυπνα κινητά τηλέφωνα (Smartphones)
	Φορέσιμες Συσκευές (Wearables)
	Εμφυτευμένες Συσκευές (Implantables)
Inference Factors:	Δακτυλικά Αποτυπώματα (Fingerprints)
	Αμφιβληστροειδής Χιτώνας (Retina Scan)
Στατικό βιομετρικό χαρακτηριστικό	Αναγνώριση Προσώπου (Face Recognition)
	Αναγνώριση Φωνής (Voice Recognition)
Δυναμικό βιομετρικό χαρακτηριστικό	Γραφικός Χαρακτήρας
	Ρυθμός πληκτρολόγησης
	Έλεγχος Καρδιακής Λειτουργίας
	Σωματικό βάρος

4.2.8. Αυθεντικοποίηση Συσκευών με τη χρήση PUFs (Physical Unclonable Functions)

Εκτός από την αυθεντικοποίηση χρηστών, η αυθεντικοποίηση των συσκευών αποτελεί ένα εξίσου σημαντικό ζήτημα σε περιβάλλοντα IoT. Οι συμβατικές λύσεις για την αυθεντικοποίηση συσκευών στηρίζονται στη χρήση εργαλείων κρυπτογράφησης και στις περισσότερες των περιπτώσεων δεν μπορούν να υιοθετηθούν από συσκευές IoT, εξαιτίας των περιορισμών τους. Μία πολλά υποσχόμενη εναλλακτική λύση προς την κατεύθυνση αυτή είναι η αξιοποίηση μηχανισμών PUF (Physical Unclonable Function).

Κάθε ολοκληρωμένο κύκλωμα (chip) εμφανίζει μικροσκοπικές δομικές διαφορές και, κατά συνέπεια, διαφορές στις ηλεκτρικές του ιδιότητες, οι οποίες προκύπτουν κατά τη διαδικασία κατασκευής του. Τα PUFs είναι κυκλώματα, αυτόνομα ή ενσωματωμένα στο chip, που, όταν λαμβάνουν μια ακολουθία bit, τον λεγόμενο έλεγχο (challenge), παράγουν μια χαρακτηριστική απόκριση (response), αξιοποιώντας αυτά τα μοναδικά γνωρίσματα του chip. Ο συνδυασμός ενός ελέγχου και της αντίστοιχης απόκρισης σχηματίζουν το Ζεύγος Ελέγχου-Απόκρισης (Challenge Response Pair – CRP). Όπως είναι φυσικό, δυο PUFs δεν μπορούν να παράγουν την ίδια απόκριση για ένα συγκεκριμένο έλεγχο, ακόμα και όταν πρόκειται για φαινομενικά ίδια κυκλώματα και συσκευές ίδιου μοντέλου, γεγονός που καθιστά αυτό το μηχανισμό ιδανικό για χρήση σε διαδικασίες αυθεντικοποίησης [73].

Η αυθεντικοποίηση μέσω PUFs περιλαμβάνει δύο στάδια, το στάδιο της εγγραφής και το στάδιο της επικύρωσης. Αρχικά, μία συσκευή IoT με ενσωματωμένο PUF πρέπει να υποβληθεί σε ένα μεγάλο πλήθος ελέγχων και στη συνέχεια τα CRP που θα προκύψουν αποθηκεύονται σε μία ασφαλή βάση δεδομένων υπό μορφή πίνακα (στάδιο εγγραφής). Κατόπιν στο στάδιο επικύρωσης ο εξυπηρετητής, όποτε κρίνεται αναγκαίο, μπορεί να υποβάλλει τη συσκευή σε ελέγχους και να διασταυρώσει τις παραγόμενες αποκρίσεις με αυτές που έχουν καταγραφεί στο προηγούμενο στάδιο. Είναι αναγκαία για λόγους ασφαλείας η χρήση διαφορετικών ελέγχων κάθε φορά, ώστε να αποτραπούν περιπτώσεις υποκλοπής των αποκρίσεων και η αυθεντικοποίηση συσκευών οι οποίες μπορούν να χρησιμοποιηθούν με κακόβουλο κίνητρο.

Το κύριο πλεονέκτημα της χρήσης μηχανισμών PUF έγκειται στη χαμηλή κατανάλωση πόρων που απαιτούν, στην απλότητα του σχεδιασμού τους και στο ικανοποιητικό επίπεδο ασφάλειας που παρέχουν, γεγονός το οποίο επιτρέπει την εφαρμογή τους σε συσκευές περιορισμένων δυνατοτήτων. Παρόλα αυτά το θέμα της αξιοπιστίας τους παραμένει εστία προβληματισμών, καθώς, με την πάροδο του χρόνου και την αλλαγή των περιβαλλοντικών συνθηκών (π.χ. θερμοκρασία), είναι δυνατόν να συντελεστούν αλλαγές στο κύκλωμα και, επομένως, οι αποκρίσεις σε έναν συγκεκριμένο έλεγχο να διαφοροποιηθούν. Επιπροσθέτως, αναφορικά με την ασφάλεια, ανησυχία εμπνέει η ευπάθεια τους απέναντι σε επιθέσεις μοντελοποίησης (modeling attacks). Στόχος των επιθέσεων αυτών είναι η εξαγωγή του πίνακα CRP μέσω

ενός μοντέλου, που μπορεί να κατασκευαστεί με τη χρήση μαθηματικών μεθόδων ή μεθόδων μηχανικής εκμάθησης. Κατά αυτόν τον τρόπο, ένας επιτιθέμενος που θα καταφέρει να υποκλέψει πληροφορίες για κάποια από τα CRP είναι σε θέση να εξάγει ολόκληρο τον πίνακα CRP και να προβλέψει τη συμπεριφορά των συσκευών σε οποιοδήποτε έλεγχο. [73], [74]

Ενδιαφέρον παρουσιάζει το γεγονός πως υπάρχουν προτάσεις για επέκταση της χρήσης των PUFs και στην κρυπτογράφηση. Οι τεχνικές και ο ακριβής τρόπος εφαρμογής τους ωστόσο δεν ανήκουν στα πλαίσια της παρούσας εργασίας.

4.2.9. Ασφαλή Πρωτόκολλα Δρομολόγησης

Δρομολόγηση σε ένα δίκτυο ονομάζεται η διαδικασία εντοπισμού της βέλτιστης διαδρομής μεταξύ των κόμβων του, για τη μετάδοση των πακέτων δεδομένων. Στα πλαίσια του IoT και πιο συγκεκριμένα σε ασύρματα δίκτυα αισθητήρων (WSN) εφαρμόζονται διαδικασίες δυναμικής δρομολόγησης. Οι διαδικασίες αυτές περιλαμβάνουν τη συλλογή πληροφοριών του δικτύου με τη χρήση πρωτοκόλλου δρομολόγησης, κατόπιν τη σύνταξη πίνακα δρομολόγησης με τις πιθανές διαδρομές (routing table) και την εύρεση της βέλτιστης, με χρήση κατάλληλου αλγορίθμου. Στις συλλεγόμενες πληροφορίες συγκαταλέγονται μεταβλητές σχετικές με τον αριθμό των παρεμβαλλόμενων κόμβων, την αξιοπιστία του μονοπατιού και τον χρόνο που απαιτείται, για τη μετάδοση των δεδομένων στον τελικό προορισμό τους.

Η ανάπτυξη εφαρμόσιμων πρωτοκόλλων δρομολόγησης για το WSN και για μία ευρύτερη κατηγορία δικτύων, τα επονομαζόμενα **LLN** (Low-Power and Lossy Networks), συνιστά πρόκληση, αφενός εξαιτίας των λειτουργικών χαρακτηριστικών των κόμβων και αφετέρου λόγω των σύνθετων αναγκών επικοινωνίας που πρέπει να εξυπηρετούνται. Ειδικότερα ο σχεδιασμός και η εφαρμογή πρωτοκόλλων δρομολόγησης σε αυτά τα δίκτυα, εκτός από τους εγγενείς περιορισμούς των συσκευών, οφείλουν να λαμβάνουν υπόψη και να συμμορφώνονται με θεμελιώδεις απαιτήσεις όπως [75], [76]:

- **Ποικιλομορφία των εφαρμογών:** Σε δίκτυα LLN πρέπει να εξυπηρετούνται παράλληλα ένα πλήθος ανόμοιων εφαρμογών, οι οποίες μπορεί να έχουν διαφορετικές απαιτήσεις σχετικά με τους υπολογιστικούς και ενεργειακούς πόρους, με την αξιοπιστία της επικοινωνίας, το χρόνο διάδοσης (propagation delay) και με τον όγκο των διακινούμενων δεδομένων.
- **Ανομοιογένεια στις ανάγκες επικοινωνίας των κόμβων:** Κατά κανόνα οι κόμβοι του δικτύου επιτελούν διαφορετικές λειτουργίες και διαχειρίζονται διαφορετικής βαρύτητας δεδομένα. Ως αποτέλεσμα ο κάθε κόμβος είναι απαραίτητο να επικοινωνεί τα δεδομένα του με την κατάλληλη συχνότητα. Για παράδειγμα σε ένα δίκτυο IoHT, όταν υπάρχει η ανάγκη συνεχούς καταγραφής κάποιας βιολογικής λειτουργίας, όπως η καρδιακή λειτουργία του ασθενή, ο

αντίστοιχος κόμβος οφείλει να μεταδίδει πληροφορίες ανά τακτά χρονικά διαστήματα. Σε άλλες περιπτώσεις η μετάδοση δεδομένων πρέπει να λαμβάνει χώρα, μόνο αφότου παρατηρηθεί αξιόλογη μεταβολή στα καταγραφόμενα μεγέθη (π.χ. στην περίπτωση ενός έξυπνου θερμοστάτη). Τέλος, υφίσταται η δυνατότητα κοινοποίησης των πληροφοριών ενός κόμβου, μετά από σχετική απαίτηση ενός εξουσιοδοτημένου χρήστη του δικτύου.

- **Επεκτασιμότητα:** Ο αριθμός των πιθανών συνδέσεων μεταξύ των κόμβων ποικίλει στα διάφορα δίκτυα LLN. Ένα πρωτόκολλο δρομολόγησης είναι απαραίτητο να μπορεί να εφαρμοστεί αποτελεσματικά στο σύνολο των δικτύων αυτών, ανεξαρτήτως της πυκνότητας τους (Network Density).
- **Κινητικότητα:** Σε περιβάλλοντα IoHT γίνεται εκτεταμένη χρήση εμφυτεύσιμων και φορέσιμων συσκευών, συνεπώς ένα πρωτόκολλο δρομολόγησης για τα δίκτυα αυτά δεν μπορεί παρά να λαμβάνει υπόψη την κινητικότητα των έξυπνων συσκευών ως βασική παράμετρο λειτουργίας.

Η πιο χρησιμοποιούμενη λύση για τη δρομολόγηση σε δίκτυα LLN είναι το πρωτόκολλο RPL (Routing Protocol for Low-Power and Lossy Networks). Πρόκειται για ένα πρωτόκολλο δρομολόγησης βασισμένο στο IPv6, που έχει προτυποποιηθεί από τον οργανισμό IETF, η λειτουργία του οποίου βασίζεται στην προϋπόθεση ότι το δίκτυο εμπεριέχει έναν κεντρικό κόμβο (sink node) με υψηλότερες υπολογιστικές ικανότητες και ενεργειακούς πόρους, συγκριτικά με τους υπόλοιπους κόμβους του δικτύου [77].

Μολονότι το πρωτόκολλο RPL σε γενικές γραμμές ανταποκρίνεται επαρκώς στις απαιτήσεις των συγκεκριμένων δικτύων, δεν παύει να εμφανίζει αδυναμίες ασφάλειας. Ειδικότερα έχει αναδειχθεί η ευπάθεια του εναντίον διαφόρων επιθέσεων δρομολόγησης, όπως επιθέσεις καταβόθρα, επιθέσεις μαύρης τρύπας (Black Hole attacks), επιθέσεις Wormhole, επιθέσεις επιλεκτικής προώθησης (Selective Forwarding attacks) και επιθέσεις Hello Flooding.

Για την υπέρβαση αυτών των αδυναμιών έχει προταθεί η ενίσχυση του πρωτοκόλλου RPL από ένα πλήθος πρόσθετων μηχανισμών ασφαλείας. Μια βασική κατηγορία τέτοιων μηχανισμών αποτελείται από μηχανισμούς που αξιοποιούν εργαλεία κρυπτογράφησης στην προσπάθεια ανίχνευσης κόμβων που εμφανίζουν ύποπτη συμπεριφορά (π.χ. VeRA [78]). Παρότι τέτοιες προτάσεις μπορούν να συντελέσουν στην επίλυση των προβλημάτων του RPL, η υψηλή κατανάλωση ενεργειακών πόρων καθιστά τη δυνατότητα εφαρμογής τους περιορισμένη [79].

Μία ακόμη κατηγορία μηχανισμών, που θεωρούνται ευρέως ως ιδανικοί για τη διασφάλιση δικτύων LLN, αποτελείται από μηχανισμούς (π.χ. SecTrust-RPL [80]) οι οποίοι βασίζονται σε ένα σύστημα εμπιστοσύνης (trust-based solutions). Στα πλαίσια αυτού του συστήματος, σε κάθε κόμβο του δικτύου ανατίθεται μια μεταβλητή που δηλώνει το επίπεδο εμπιστοσύνης του. Μόνο κόμβοι των οποίων η μεταβλητή έχει τιμές πάνω από ένα καθορισμένο όριο μπορούν να συμπεριληφθούν στη διαδικασία

δρομολόγησης. Οι συγκεκριμένες προτάσεις, αν και πιο εφαρμόσιμες, φέρουν η κάθε μία τα δικά της μειονεκτήματα και τους δικούς της περιορισμούς [81].

Συμπερασματικά, η ανάπτυξη πρωτοκόλλων δρομολόγησης για τα δίκτυα WSN και κατά επέκταση για το IoHT, τα οποία θα συνδυάζουν υψηλό επίπεδο λειτουργικότητας και παρεχόμενης ασφάλειας, παραμένει ένα ανοικτό ζήτημα, η επίλυση του οποίου πρέπει να αποτελέσει προτεραιότητα.

4.3. Μη Τεχνικά Ζητήματα Ασφαλείας

4.3.1. Φυσική Ασφάλεια των συσκευών

Η συντριπτική πλειονότητα των προτάσεων για θέματα ασφαλείας του IoT περιορίζονται κυρίως σε λύσεις κυβερνοασφάλειας και λογισμικού. Παρόλα αυτά η φυσική ασφάλεια των συσκευών είναι εφάμιλλης αξίας και δεν πρέπει επ’ ουδενί να υποτιμάται, διότι κάθε συσκευή του δικτύου είναι εν δυνάμει ένα σημείο πρόσβασης σε ολόκληρο το σύστημα. Στα πλαίσια αυτής της εργασίας κρίνεται απαραίτητο να γίνει μια αναφορά, έστω και συνοπτική, στις πρακτικές και τα εργαλεία εκείνα που μπορούν να διασφαλίσουν τη φυσική υπόσταση των συσκευών ή να μετριάσουν τις επιπτώσεις της φυσικής προσβολής τους.

Στο επίπεδο κατασκευής μιας συσκευής, ένα μέτρο προστασίας θα μπορούσε να είναι η ενσωμάτωση των αγωγών που φέρουν κρίσιμα δεδομένα στα κατώτερα επίπεδα (υπόστρωμα) της ηλεκτρονικής πλακέτας (PCB). Το μέτρο αυτό μπορεί να συντελέσει στην αποτροπή επιθέσεων που περιλαμβάνουν σύνδεση συσκευής μέτρησης στο κύκλωμα (probing), επειδή κάτι τέτοιο θα οδηγούσε στην πλήρη καταστροφή της ηλεκτρονικής πλακέτας. Επίσης μπορεί να αποβεί χρήσιμη η εργαλειοποίηση μηχανισμών διαγραφής της μνήμης ή ολικής αχρήστευσης της συσκευής, όταν ανιχνεύεται προσπάθεια παραβίασης της (π.χ. tamper pins). Επιπροσθέτως για την αποτροπή σύνδεσης κάποιας κακόβουλης συσκευής είναι αναγκαίο το κλείδωμα θυρών (φυσικών ή οπτικών) που χρησιμοποιήθηκαν για την κατασκευή και τον ποιοτικό έλεγχο και δεν επιτελούν πλέον κάποια σημαντική λειτουργία. [82], [83]

Ένα σαφώς απλούστερο στην εφαρμογή του μέτρο, το οποίο παραδόξως δεν χρησιμοποιείται καθολικά, είναι η αποφυγή συμπερίληψης ευαίσθητων δεδομένων (αριθμός μοντέλου, προκαθορισμένος κωδικός πρόσβαση κλπ.) στην ετικέτα του προϊόντος ή τουλάχιστον η αποκόλληση της από τη συσκευή. Τέλος, όπως είναι αυτονόητο, ανάλογα με το οικονομικό κόστος πρέπει να εφαρμόζονται οι παρακάτω προδιαγραφές, όπου είναι εφικτό:

- Στιβαρές κατασκευές με μεγάλη μηχανική αντοχή
- Χρήση περιβλήματος ανθεκτικού στην παραβίαση

- Χρήση ειδικών βιδών (security screws)
- Χρήση ειδικών σφραγίδων (sealing labels) για τον εντοπισμό παραβιάσεων

Οι παραπάνω μηχανισμοί και προδιαγραφές δεν επαρκούν για να καταστήσουν τις συσκευές απρόσβλητες ενάντια σε φυσικές απειλές. Η φυσική ασφάλεια των συσκευών θα πρέπει επίσης να περιφρουρείται και στο περιβάλλον στο οποίο εγκαθίστανται, καθ' όλη τη διάρκεια του κύκλου ζωής τους. Οι συσκευές χρειάζεται να υπόκεινται τακτικά σε φυσικούς ελέγχους για τον εντοπισμό ενδείξεων παραβίασης, ενώ συσκευές που παρουσιάζουν τέτοιες ενδείξεις είναι αναγκαίο να αποσύρονται και να αντικαθίστανται τάχιστα. Επιπλέον, κρίνεται απαραίτητο, όπου αυτό είναι δυνατόν, οι συσκευές να είναι εγκατεστημένες ή να φυλάσσονται σε χώρους περιορισμένης πρόσβασης ή έστω να παρακολουθούνται από κάποιο κλειστό κύκλωμα τηλεόρασης (CCTV). [82]

4.3.2. Ενημέρωση και εκπαίδευση των ενδιαφερόμενων μερών

Ένας ακόμη νευραλγικός παράγοντας για την ασφάλεια συστημάτων IoHT, ο οποίος μέχρι τώρα δεν έχει λάβει τη δέουσα προσοχή, είναι η ενημέρωση, η τεχνική κατάρτιση και η εξοικείωση των ενδιαφερόμενων μερών αναφορικά με τη νέα τεχνολογία. Σε πρώτο στάδιο, είναι αναγκαία η ενημέρωση των παρόχων υγειονομικών υπηρεσιών σχετικά με τις αρχές που πρέπει να διέπουν τις πολιτικές ασφάλειας και ιδιωτικότητας στο IoHT. Προς την κατεύθυνση αυτή, κυβερνήσεις διαφόρων κρατών, όπως της Αυστραλίας [84] και του Καναδά [85], αλλά και οργανισμοί, όπως το FBI [86], έχουν εκδώσει κατευθυντήριες γραμμές και προτάσεις.

Οι πάροχοι με τη σειρά τους πρέπει να προνοήσουν για την ενημέρωση και τεχνική κατάρτιση των υπαλλήλων που απασχολούν, τόσο στο τμήμα πληροφορικής (IT department), όσο και του ιατρονοσηλευτικού προσωπικού. Στην περίπτωση των πρώτων, πρέπει να υπάρχει το απαραίτητο επίπεδο τεχνογνωσίας, ώστε να είναι σε θέση να αναγνωρίσουν ευπάθειες του συστήματος και απειλές, να λάβουν τα κατάλληλα μέτρα για την αντιμετώπιση επιθέσεων καθώς και να παρέχουν τεχνική υποστήριξη. Αναφορικά με τους εργαζόμενους στον κλάδο της υγείας, είναι απαραίτητη η ενημέρωση τους για τη σημασία της ασφάλειας και της ιδιωτικότητας των ιατρικών πληροφοριών και η εκπαίδευση τους σε ένα πιο πρακτικό επίπεδο, σχετικά με την ορθή χρήση της τεχνολογίας. Αυτό θα συμβάλλει αποφασιστικά στην αποφυγή λανθασμένων χειρισμών και ενδεχόμενης εξαπάτησης τους.

Τέλος, όσον αφορά τους ασθενείς, δηλαδή τους τελικούς αποδέκτες των υπηρεσιών υγειονομικής περίθαλψης, κρίνεται επίσης αναγκαία η ενημέρωση τους και η εξοικείωση τους με τη λειτουργία των έξυπνων ιατρικών συσκευών και του συστήματος γενικότερα. Όπως προαναφέρθηκε, αυτός ίσως είναι ένας από τους ελάχιστους τρόπους προστασίας έναντι επιθέσεων κοινωνικής μηχανικής.

Συμπεράσματα

Το Διαδίκτυο των Πραγμάτων αποτελεί μια πρόταση για ένα άλμα σε μια νέα τεχνολογική πραγματικότητα, μια πρόταση που αναπτύσσεται θεωρητικά για ένα διάστημα μεγαλύτερο από δύο δεκαετίες μέσα από αναρίθμητες προτάσεις, προβληματισμούς και αναθεωρήσεις. Η υιοθέτηση αυτής της τεχνολογίας στους διάφορους τομείς της ανθρώπινης δραστηριότητας υπόσχεται αυτοματοποιημένες λύσεις και οφέλη, που κάποια χρόνια πριν θα φάνταζαν αδιανόητα.

Μεταξύ τούτων των εφαρμογών ξεχωρίζει η εφαρμογή του (IoHT) σε μία από τις πιο κρίσιμες και θεμελιώδεις δομές της σύγχρονης κοινωνίας, το σύστημα της υγειονομικής περίθαλψης. Το IoHT περιλαμβάνει εξελιγμένες υπηρεσίες και εφαρμογές, οι οποίες συμβάλλουν στην αναβάθμιση όχι μόνο των σημερινών υπηρεσιών υγείας, αλλά και του βιοτικού επιπέδου γενικότερα. Εντούτοις, πληθώρα ζητημάτων και προκλήσεων που ανακύπτουν και παραμένουν αδιευθέτητα αποτελούν τροχοπέδη για την ανάπτυξη συστημάτων IoHT σε μεγάλη κλίμακα.

Η ασφάλεια στο IoHT ανάγεται σε κυρίαρχο ζήτημα, το οποίο απαιτεί την απαράμιλλη προσοχή της επιστημονικής κοινότητας, διότι απολύτως κανένας συμβιβασμός ή παράβλεψη δεν μπορεί να λάβει χώρα, όταν διακυβεύονται αγαθά ανεκτίμητης αξίας, όπως η ανθρώπινη ζωή και υγεία. Το πλήθος και η σοβαρότητα των απειλών και των επιθέσεων, που δυνητικά μπορούν να πλήξουν ανεπανόρθωτα τέτοιας σημασίας αγαθά, σκιαγραφούν ένα ζοφερό τοπίο. Παρόλα αυτά, η αναζήτηση καινοτόμων εφαρμόσιμων μηχανισμών και η προσπάθεια εκσυγχρονισμού και ενσωμάτωσης συμβατικών λύσεων για την περιφρούρηση και τη διαφύλαξη των αγαθών αυτών έχει να επιδείξει ενθαρρυντικά σημάδια, παρά τις όποιες αναπόφευκτες δυσκολίες στο σχεδιασμό και την προσαρμογή τους σε αυτό το νέο περιβάλλον.

Η ετοιμότητα και η αποτελεσματικότητα που θα επιδείξει η επιστημονική κοινότητα, όσον αφορά την αντιμετώπιση των απειλών και την αποσόβηση των σύμφυτων κινδύνων, θα κρίνουν εν πολλοίς εάν το IoHT θα αποτελέσει αυτήν την πολλά υποσχόμενη πραγματικότητα ή αν θα παραμείνει προς το παρόν μια ουτοπία εξαιτίας των σύνθετων αναγκών ασφαλείας του.

Προτάσεις μελλοντικής επέκτασης της εργασίας

Στα στάδια συγγραφής της παρούσας εργασίας διαπιστώθηκε ένας αριθμός ζητημάτων που χρήζουν ερευνητικής πραγμάτευσης μελλοντικά. Με σκοπό την εμβάθυνση σε θέματα ασφάλειας του IoT στον τομέα της υγείας είναι επιτακτικό σε πρώτη φάση να ερευνηθούν περαιτέρω οι τεχνολογίες που το συναποτελούν. Προς αυτήν την κατεύθυνση, διάφορες τεχνολογίες και πρωτόκολλα που προορίζονται για χρήση στο IoHT πρέπει να αποτελέσουν αντικείμενο συγκριτικών μελετών και προπάντων πειραματικών ερευνών σε συνθήκες που θα προσομοιάζουν σε πραγματικά

περιβάλλοντα IoHT. Κατά αυτόν τον τρόπο μπορεί αφενός να εξακριβωθεί η ορθότητα των ισχυρισμών των κατασκευαστών των τεχνολογιών αυτών αναφορικά με τις τεχνικές προδιαγραφές και σχετικά με το παρεχόμενο επίπεδο ασφάλειας αφετέρου δε να αναδειχθούν κενά ασφαλείας που ενδεχομένως δεν εντοπίστηκαν στα πλαίσια των θεωρητικών μελετών.

Αντικείμενο πειραματικής έρευνας πρέπει επίσης να αποτελέσουν οι προτεινόμενες λύσεις ασφαλείας, ώστε να εξεταστούν σε συνθήκες περιβάλλοντος IoHT η αξιοπιστία και η καταλληλότητα τους. Μέσω τέτοιων πειραματικών διαδικασιών δύναται να προκύψει μια ακριβής εικόνα των προβλημάτων και της βιωσιμότητας των υπαρχόντων λύσεων, ή οποία θα επιτρέψει την πιο εμπεριστατωμένη μελέτη των ζητημάτων ασφαλείας και την εξαγωγή ασφαλέστερων συμπερασμάτων.

Επιπροσθέτως, παρότι έγινε μια νύξη, στα πλαίσια της παρούσας εργασίας δεν επιχειρήθηκε η ιεράρχηση των κινδύνων που μπορεί να επιφέρει η κάθε απειλή, ωστόσο υπογραμμίστηκε η ανάγκη θέσπισης ενός ενιαίου πλαισίου για την εκτίμηση κινδύνων συγκεκριμένα για το IoHT και η πολύτιμη συνεισφορά του στην αντιμετώπιση αυτών των κινδύνων. Συνεπώς, θεωρείται σκόπιμο να ενθαρρυνθεί περαιτέρω έρευνα προς αυτή την κατεύθυνση.

Τέλος, όπως τεκμηριώθηκε στο τελευταίο κεφάλαιο, τα προτεινόμενα μέτρα ασφαλείας δεν επαρκούν για την πλήρη κάλυψη των σύνθετων αναγκών ασφαλείας του IoHT, η καταλληλότητα δε ορισμένων τίθεται συχνά υπό αμφισβήτηση ή έστω εγείρει σοβαρά ερωτήματα. Η ανάπτυξη λοιπόν αποτελεσματικών καινοτόμων λύσεων ασφαλείας και η πρόταση τροποποιήσεων που θα καταστήσουν συμβατικά μέτρα ασφαλείας συμβατά με τις ανάγκες του IoHT είναι μια ακόμα ερευνητική κατεύθυνση που παρουσιάζει ενδιαφέρουσες προοπτικές.

Βιβλιογραφία

[1] K. Ashton, "That 'Internet of Things' Thing," RFID Journal, 22 Jun 2009. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing. [Accessed 30 November 2021].

[2] C. Bormann, J. Vasseur and Z. Shelby, "The Internet of Things," IETF Journal, 1 October 2010. [Online]. Available: https://www.ietfjournal.org/the-internet-of-things/. [Accessed 30 November 2021].

[3] ITU Telecommunication Standardization Sector (ITU-T), "Y.4000/Y.2060: Overview of the Internet of things," ITU, Geneva, Switzerland, 15 June 2012.

[4] R. Minerva, A. Biru and D. Rotondi, "Define IoT: Towards a Definition of the Internet of Things (IoT)," 27 May 2015. [Online]. Available: https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf. [Accessed 30 November 2021].

[5] O. U. P. (OUP), "Definition of internet of things," 2021. [Online]. Available: https://www.lexico.com/definition/internet_of_things. [Accessed 30 November 2021].

[6] Gartner, "Definition of Internet Of Things (iot) - IT Glossary," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/internet-of-things. [Accessed 30 November 2021].

[7] M. Weiser, "The Computer for the 21 st Century," *Scientific American,* vol. 265, no. 3, September 1991.

[8] Postscapes, "Internet of Things (IoT) History," 11 December 2019. [Online]. Available: https://www.postscapes.com/iot-history/. [Accessed 30 November 2021].

[9] HQSoftware, "The History of IoT: a Comprehensive Timeline of Major Events, Infographic," 12 July 2018. [Online]. Available: https://hqsoftwarelab.com/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events-infographic/. [Accessed 30 November 2021].

[10] International Telecommunication Union (ITU), "ITU Internet Reports: The Internet of Things," ITU, Geneva, 2005.

[11] D. Evans, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," Cisco Internet Business Solutions Group (IBSG), 2011.

[12] V. Adat and B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems,* vol. 67, pp. 423-441, 2018.

[13] Leverege, "Introduction to IoT - How Does an IoT System Work," 2018. [Online]. Available: https://www.leverege.com/iot-ebook/how-iot-systems-work. [Accessed 30 November 2021].

[14] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE*

Transactions on Emerging Topics in Computing, vol. 5, no. 4, pp. 586-602, 1 Oct.-Dec 2017.

[15] N. S. Abouzakhar, A. Jones and O. Angelopoulou, "Internet of Things Security: A Review of Risks and Threats to Healthcare Sector," *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* pp. 373-378, 2017.

[16] F. Firouzi, B. Farahani, M. Ibrahim and K. Chakrabarty, "Keynote Paper: From EDA to IoT eHealth: Promises, Challenges, and Solutions," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 37, no. 12, pp. 2965-2978, December 2018.

[17] Z. Shelby, K. Hartke and C. Bormann, "The Constrained Application Protocol (CoAP)," June 2014. [Online]. Available: https://www.rfc-editor.org/info/rfc7252. [Accessed 30 November 2021].

[18] A. Banks and R. Gupta, "MQTT Version 3.1.1," OASIS Open, 10 December 2015. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html. [Accessed 30 November 2021].

[19] T. Salman and J. Raj, "A Survey of Protocols and Standards for Internet of Things," *Advanced Computing and Communications,* vol. 1, no. 1, March 2017.

[20] P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core," March 2011. [Online]. Available: https://www.rfc-editor.org/info/rfc6120. [Accessed 30 November 2021].

[21] M. K. Pratt, "Top 12 most commonly used IoT protocols and standards," 1 Apr 2021. [Online]. Available: https://internetofthingsagenda.techtarget.com/tip/Top-12-most-commonly-used-IoT-protocols-and-standards. [Accessed 30 November 2021].

[22] Leverege, "Breaking Down IoT Standards and Protocols," 10 March 2020. [Online]. Available: https://www.iotforall.com/glossary-iot-standards-and-protocols. [Accessed 30 November 2021].

[23] IoT Design Pro, "Different Types of Wireless Communication Protocols in IOT," 2 Sep 2019. [Online]. Available: https://iotdesignpro.com/articles/different-types-of-wireless-communication-protocols-for-iot. [Accessed 30 November 2021].

[24] Electronics Notes, "SigFox for M2M & IoT," [Online]. Available: https://www.electronics-notes.com/articles/connectivity/sigfox/what-is-sigfox-basics-m2m-iot.php. [Accessed 30 November 2021].

[25] K. K. Patel and S. M. Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture,Enabling Technologies, Application & Future Challenges," *International Journal of Engineering Science and Computing,* vol. 6, no. 5, May 2016.

[26] A. Onasanya and M. Elshakankiri, "Smart integrated IoT healthcare system for cancer care," *Wireless Networks,* vol. 27, p. 4297–4312, 2021.

[27] A. A. Mawgoud, A. I. Karadawy and B. S. Tawfik, "A Secure Authentication Technique in Internet of Medical Things through Machine Learning," 30 Nov 2020. [Online]. Available: https://arxiv.org/abs/1912.12143. [Accessed 30 November 2021].

[28] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering,* vol. 2017, p. 25, 2017.

[29] F. Alsubaei, A. Abuhussein and S. S. Shiva, "Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment," *2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops),* pp. 112-120, 2017.

[30] R. Khan, S. U. Khan, R. Zaheer and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," *2012 10th International Conference on Frontiers of Information Technology,* pp. 257-260, 2012.

[31] A. Alabdulatif, I. Khalil, X. Yi and M. Guizani, "Secure Edge of Things for Smart Healthcare Surveillance Framework," *IEEE Access,* vol. 7, pp. 31010-31021, 2019.

[32] S. M. R. ISLAM, D. KWAK, M. H. KABIR, M. HOSSAIN and K.-S. KWAK, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access,* vol. 3, pp. 678-708, 2015.

[33] A. J. Jara, M. A. Zamora and A. F. Skarmeta , "Drug identification and interaction checker based on IoT to minimize adverse drug reactions and improve drug compliance," *Personal and Ubiquitous Computing,* vol. 18, p. 5–17, 2014.

[34] A. A. Albesher, "IoT in Health-care: Recent Advances in the Development of Smart Cyber-Physical Ubiquitous Environments," *International Journal of Computer Science and Network Security,* vol. 19, no. 2, pp. 181-186, Feb 2019.

[35] M. N. Bhuiyan, M. M. Rahman, M. M. Billah and D. Saha, "Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities," *IEEE Internet of Things Journal,* vol. 8, no. 13, pp. 10474-10498, July 2021.

[36] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma and T. Soyata, "A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective," *IEEE INTERNET OF THINGS JOURNAL,* vol. 7, no. 1, pp. 53-71, Jan 2020.

[37] G. Saha, R. Singh and S. Saini, "A Survey Paper on the impact of "Internet of Things" in Healthcare," *2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA),* pp. 331-334, 2019.

[38] B. Stack, "Here's How Much Your Personal Information Is Selling for on the Dark Web," 6 Dec 2017. [Online]. Available: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. [Accessed 30 November 2021].

[39] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security," *IEEE Internet of Things Journal,* vol. 8, no. 11, pp. 8707-8718, June 2021.

[40] Γ. Πάγκαλος και Ι. Μαυρίδης, «Ενότητα 1: ΒΑΣΙΚΑ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ,» σε *ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΔΙΚΤΥΩΝ*, Θεσσαλονίκη, ΑΝΙΚΟΥΛΑ, 2002.

[41] B. Khamidov, S. Urmanov, E. Abdukhamidov and J. Bakhodirov, "Internet of Things: A security overview," March 2019. [Online]. Available: https://www.researchgate.net/publication/333619623_Internet_of_Things_A_security_overview. [Accessed 30 November 2021].

[42] I. Butun, P. Österberg and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials,* vol. 22, no. 1, pp. 616-644, Firstquarter 2020.

[43] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems,* vol. 73, p. 3–25, 2020.

[44] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray and Y. Jin, "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice," *Journal of Hardware and Systems Security,* vol. 2, pp. 97-110, 10 May 2018.

[45] S. Hamedheidari and R. Rafeh, "A novel agent-based approach to detect sinkhole attacks in wireless sensor networks," *Computers & Security,* vol. 37, pp. 1-14, Sep 2013.

[46] M. Jensen, J. Schwenk, N. Gruschka and L. L. Iacono, "On Technical Security Issues in Cloud Computing," *2009 IEEE International Conference on Cloud Computing,* pp. 109-116, 2009.

[47] M. R. Islam and K. M. Aktheruzzaman, "An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions," *Journal of Computer and Communications,* vol. 8, no. 4, pp. 11-25, 2 April 2020.

[48] A. Arampatzis, "What is Session Hijacking?," 12 April 2021. [Online]. Available: https://www.venafi.com/blog/what-session-hijacking. [Accessed 30 November 2021].

[49] B. Dickson, "The IoT ransomware threat is more serious than you think," [Online]. Available: https://www.iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/. [Accessed 30 November 2021].

[50] Cloudflare, "What is buffer overflow?," [Online]. Available: https://www.cloudflare.com/learning/security/threats/buffer-overflow/. [Accessed 30 November 2021].

[51] Cloudflare, "What is a brute force attack?," [Online]. Available: https://www.cloudflare.com/learning/bots/brute-force-attack/. [Accessed 30 November 2021].

[52] Cisco, "What Is Phishing?," [Online]. Available: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html. [Accessed 30 November 2021].

[53] National Institute of Standards and Technology (NIST), "Guide for Conducting Risk Assessments," Sep 2012. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final. [Accessed 30 November 2021].

[54] P. Radanlieva, D. C. De Rourea, C. Maple, J. R. Nurse , R. Nicolescud and U. Ani, "Cyber Risk in IoT Systems," 8 March 2019. [Online]. Available: https://www.researchgate.net/publication/331867864_Cyber_Risk_in_IoT_Systems. [Accessed 30 November 2021].

[55] J. R. Nurse, S. Creese and D. De Roure, "Security Risk Assessment in Internet of Things Systems," *IT Professional,* vol. 19, no. 5, pp. 20-26, 4 Oct 2017.

[56] P. Radanliev, D. C. De Roure, J. R. C. Nurse, R. M. Montalvo, S. Cannady, O. Santos, L. Maddox, P. Burnap and C. Maple, "Future developments in standardisation of cyber risk in the Internet of Things (IoT)," *SN Applied Sciences,* vol. 2, no. 169, p. 16, 8 Jan 2020.

[57] A. Guzman και A. Gupta, «Chapter 1: IoT Penetration Testing,» σε *IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices*, Packt, 2017, pp. 7-30.

[58] A. Skarmeta, D. G. Carrillo and A. Olivereau, "Chapter 3: End-Node Security," in *Internet of Things Security and Data Protection*, 1 ed., S. Ziegler, Ed., SPRINGER, 2019.

[59] Forcepoint, "What is an Intrusion Prevention System (IPS)?," [Online]. Available: https://www.forcepoint.com/cyber-edu/intrusion-prevention-system-ips. [Accessed 30 November 2021].

[60] IBM, "What is Security Information and Event Management (SIEM)," [Online]. Available: https://www.ibm.com/topics/siem. [Accessed 30 November 2021].

[61] P. Radoglou-Grammatikis, P. Sarigiannidis, E. Iturbe, E. Rios, M. Saturnino, A. Sarigiannidis, G. Eftathopoulos, Y. Spyridis, A. Sesis, N. Vakakis, D. Tzovaras, E. Kafetzakis, I. Giannoulakis, M. Tzifas, A. Giannakoulias, M. Angelopoulos and F. Ramos, "SPEAR SIEM: A Security Information and Event Management system for the Smart Grid," *Computer Networks,* vol. 193, 5 July 2021.

[62] D. D. López, M. B. Uribe, C. S. Cely, A. V. Torres, N. M. Guataquira, S. M. Castro, P. Nespoli and F. G. Mármol, "Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM," *Wireless Communications and Mobile Computing,* vol. 2018, p. 18, 25 Oct 2018.

[63] B. Al-Duwairi, W. Al-Kahla, M. A. AlRefai, Y. Abdelqader, A. Rawash and R. Fahmawi, "SIEM-based detection and mitigation of IoT-botnet DDoS attacks," *International Journal of Electrical and Computer Engineering,* vol. 10, no. 2, pp. 2182-2191, April 2020.

[64] A. Acien, A. Nieto, G. Fernandez and J. Lopez, "A comprehensive methodology for deploying IoT honeypots," *15th International Conference on Trust, Privacy and Security in Digital Business (TrustBus 2018),* vol. LNCS 11033, pp. 229-243, 2018.

[65] Cisco, "What Is a Firewall?," [Online]. Available:

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. [Accessed 30 November 2021].

[66] N. Maheshwari and H. Dagale, "Secure communication and firewall architecture for IoT applications," *2018 10th International Conference on Communication Systems & Networks (COMSNETS),* pp. 328-335, 2018.

[67] S. O'Brien, "Why Segmentation is More Effective Than Firewalls For Securing Industrial IoT," 10 July 2020. [Online]. Available: https://technative.io/why-segmentation-is-more-effective-than-firewalls-for-securing-industrial-iot/. [Accessed 30 November 2021].

[68] S. Zeadally, A. K. Das and N. Sklavos , "Cryptographic technologies and protocol standards for Internet of Things," *Internet of Things,* vol. 14, June 2021.

[69] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier and M. M. Mansour, "One Round Cipher Algorithm for Multimedia IoT Devices," *Multimedia Tools and Applications,* vol. 77, pp. 18383 - 18413, 2018.

[70] A. Shah and M. Engineer, "A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications," *Smart Innovations in Communication and Computational Sciences,* vol. AISC 851, pp. 283-293, 20 Nov 2018.

[71] Wikipedia, "Authentication," Wikimedia Foundation, 9 Sep 2021. [Online]. Available: https://en.wikipedia.org/wiki/Authentication. [Accessed 30 November 2021].

[72] Y. Sun, F. P.-W. Lo and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access,* vol. 7, pp. 183339-183355, 2019.

[73] A. Babaei and G. Schiele, "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges," *Sensors,* vol. 19, no. 14, 21 July 2019.

[74] B. Halak, M. Zwolinski και M. S. Mispan, «Overview of PUF-based hardware security solutions for the internet of things,» *2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS),* pp. 1-4, 2016.

[75] B. Ghaleb, A. Y. Al-Dubai, E. Ekonomou, A. Alsarhan, Y. Nasser, L. M. Mackenzie and A. Boukerche, "A Survey of Limitations and Enhancements of the IPv6 Routing Protocol for Low-Power and Lossy Networks: A Focus on Core Operations," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 2, pp. 1607-1635, Secondquarter 2019.

[76] A. Dhumane and D. R. Prasad, "Routing Challenges in Internet of Things," *CSI Communications,* pp. 19-20, Jan 2015.

[77] L. Steenbrink, *Routing in the Internet of Things,* Hamburg University of Applied Sciences, 2014.

[78] A. Dvir, T. Holczer and L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems,* pp. 709-714, 2011.

[79] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa and P. Lorenz, "Security Against Rank Attack in RPL Protocol," *IEEE Network,* vol. 34, no. 4, pp. 133-139, July - August 2020.

[80] D. Airehrour, J. A. Gutierrez and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet," *Future Generation Computer Systems,* vol. 93, p. 860–876, 2019.

[81] Y. Yu, K. Li, W. Zhou and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," *Journal of Network and Computer Applications,* vol. 35, p. 867–880, 2012.

[82] J. Borgini, "Don't forget IoT physical security when planning protection," 25 Sep 2020. [Online]. Available: https://internetofthingsagenda.techtarget.com/tip/Dont-forget-IoT-physical-security-when-planning-protection. [Accessed 30 November 2021].

[83] IoT Security Foundation, "Physical Security," [Online]. Available: https://www.iotsecurityfoundation.org/best-practice-guide-articles/physical-security/. [Accessed 30 November 2021].

[84] Commonwealth of Australia, "Code of Practice: Securing the Internet of Things for Consumers," 2020. [Online]. Available: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf. [Accessed 30 November 2021].

[85] Canadian Centre for Cyber Security (CCCS), "INTERNET OF THINGS SECURITY FOR SMALL AND MEDIUM ORGANIZATIONS," Oct 2019. [Online]. Available: https://cyber.gc.ca/sites/default/files/publications/ITSAP.00.012-en.pdf. [Accessed 30 November 2021].

[86] FEDERAL BUREAU OF INVESTIGATION (FBI), "Cyber Tip: Be Vigilant with Your Internet of Things (IoT) Devices," 13 Oct 2015. [Online]. Available: https://www.fbi.gov/news/stories/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices. [Accessed 30 November 2021].