ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Απειλές και προκλήσεις ασφάλειας των έξυπνων καταναλωτικών συσκευών του Διαδικτύου των πραγμάτων (IoT). Μελέτη περίπτωσης δοκιμών διείσδυσης σε έξυπνες συσκευές IoT

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΠΑΚΩΝΣΤΑΝΤΙΝΟΥ ΚΩΝΣΤΑΝΤΙΝΟΣ ΑΛΕΞΑΝΔΡΟΣ
(ΑΕΜ: 2571)

Επιβλέπων: Νικολάου Σπυρίδων
Λέκτορας

Καστοριά, Απρίλιος 2024

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Απειλές και προκλήσεις ασφάλειας των έξυπνων καταναλωτικών συσκευών του Διαδικτύου των πραγμάτων (IoT). Μελέτη περίπτωσης δοκιμών διείσδυσης σε έξυπνες συσκευές IoT

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΠΑΠΑΚΩΝΣΤΑΝΤΙΝΟΥ ΚΩΝΣΤΑΝΤΙΝΟΣ ΑΛΕΞΑΝΔΡΟΣ

(ΑΕΜ: 2571)

Επιβλέπων: Νικολάου Σπυρίδων

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Παρασκευή 12/04/2024

Νικολάου Σπυρίδων Λέκτορας	Βέργαδος Δημήτριος Λέκτορας	Βαρδάκας Ιωάννης Λέκτορας

Καστοριά, Απρίλιος 2024

Ευχαριστίες

Με το τέλος της πτυχιακής μου εργασίας νιώθω την ανάγκη αλλά και την υποχρέωση να ευχαριστήσω κάποιους ανθρώπους που συνέβαλαν σημαντικά στην πραγματοποίηση και ολοκλήρωσή της.

Πρώτο θα ήθελα να ευχαριστήσω τον καθηγητή που επέβλεψε την πτυχιακή μου εργασία, κύριο Σπυρίδων Νικολάου, για την άριστη συνεργασία μας και την συμβολή του στο ακαδημαϊκό κομμάτι αυτής.

Επιπλέον θα ήθελα να ευχαριστήσω την οικογένειά μου για την υποστήριξη τους και την πίστη τους στις δυνατότητές μου, όχι μόνο κατά την διάρκεια πραγματοποίησης της εργασίας μου, αλλά και καθ’ όλη την διάρκεια των σπουδών μου.

Περίληψη

Το Internet of Things (IoT) αποτελεί έναν τομέα της τεχνολογίας που αναπτύσσεται με ταχείς ρυθμούς, παρέχοντας πληθώρα ευκαιριών αλλά και αντιμετωπίζοντας προκλήσεις. Η αρχιτεκτονική του παρουσιάζει διάφορα μοντέλα και πρότυπα, με τα πιο δημοφιλή να είναι αυτά των τριών και πέντε επιπέδων. Το IoT επαναπροσδιορίζει τον τρόπο που αλληλεπιδρούμε με τις συσκευές και τα δίκτυα, δημιουργώντας νέες ευκαιρίες για εφαρμογές που βελτιώνουν την καθημερινή ζωή μας μέσω συνδεσιμότητας, αυτοματισμού και ευκολίας χρήσης.

Παρά τα επιτεύγματα, η ασφάλεια αποτελεί σημαντική πρόκληση για το IoT. Η χρήση μη ασφαλών πρωτοκόλλων επικοινωνίας και η έλλειψη αυθεντικοποίησης συσκευών μπορούν να αποτελέσουν πηγή ευπαθειών και απειλών για την ιδιωτικότητα και την ασφάλεια των δεδομένων. Για τον λόγο αυτό, είναι αναγκαίο να δημιουργηθούν κατευθυντήριες γραμμές και πρωτόκολλα ασφαλείας που θα ενισχύσουν την προστασία των συσκευών και των δεδομένων τους. Μελέτες περίπτωσης αποκαλύπτουν τις πιθανές απειλές και ευπάθειες του IoT, επισημαίνοντας παράλληλα στρατηγικές και προτάσεις για την αντιμετώπισή τους και την ενίσχυση της ασφάλειας στον τομέα αυτό. Ειδικότερα, οι μελέτες ευπάθειας εστιάζουν στις πιθανές αδυναμίες των συσκευών IoT, όπως η αδυναμία ενημέρωσης του λογισμικού και η ανεπαρκής προστασία των δεδομένων. Μέσω αυτών των αναλύσεων, αναδεικνύονται οι τομείς όπου απαιτείται η ενίσχυση της ασφάλειας, ώστε να αντιμετωπιστούν πιθανοί κίνδυνοι και απειλές για τους χρήστες και τα δίκτυα. Συνοψίζοντας, το Internet of Things αντιπροσωπεύει μια καινοτόμο και επαναστατική προσέγγιση στον τομέα της τεχνολογίας, προσφέροντας αμέτρητες ευκαιρίες για τη βελτίωση της ζωής μας. Παράλληλα, είναι αναγκαίο να διαχειριστούμε προσεκτικά τις πιθανές απειλές και ευπάθειες, ενισχύοντας τα μέτρα ασφαλείας και προστασίας των δεδομένων, προκειμένου να εξασφαλίσουμε ένα ασφαλές και αξιόπιστο περιβάλλον για την εφαρμογή και τη χρήση των συσκευών IoT.

Λέξεις Κλειδιά: *Διαδίκτυο των πραγμάτων, Έξυπνες καταναλωτικές συσκευές, Απειλές IoT, Προκλήσεις Ασφαλείας, Υποκλοπή επικοινωνίας μεταξύ συσκευών, Ανάλυση πακέτων Δικτύου, MITM επίθεση, Kali Linux, Wireshark, Nmap*

Abstract

The Internet of Things (IoT) is a rapidly growing area of technology, providing a wealth of opportunities and challenges. Its architecture presents various models and patterns, with the most popular being those of three and five layers. IoT is redefining the way we interact with devices and networks, creating new opportunities for applications that improve our daily lives through connectivity, automation and ease of use.

Despite the achievements, security is a major challenge for IoT. The use of insecure communication protocols and lack of device authentication can be a source of vulnerabilities and threats to data privacy and security. For this reason, it is necessary to create guidelines and security protocols that will enhance the protection of devices and their data. Case studies reveal the potential threats and vulnerabilities of IoT, while highlighting strategies and recommendations to address them and enhance security in this area. In particular, vulnerability studies focus on potential weaknesses of IoT devices, such as failure to update software and inadequate data protection. Through these analyses, areas where security enhancements are needed to address potential risks and threats to users and networks are highlighted. In summary, the Internet of Things represents an innovative and revolutionary approach to technology, offering countless opportunities to improve our lives. At the same time, it is necessary to carefully manage potential threats and vulnerabilities by strengthening security and data protection measures in order to ensure a secure and reliable environment for the implementation and use of IoT devices.

Key Words: *Internet of Thinks, Smart consumer devices, IoT threats, Security Challenges, Interception of communication between devices, Network packet analysis, MITM attack, Kali Linux, Wireshark, Nmap*

Πίνακας Περιεχομένων

Λίστα Εικόνων

Εισαγωγή

Οι στόχοι της πτυχιακής εργασίας είναι:

1. Η εξερεύνηση βιβλιογραφικών πηγών με περιπτώσεις-σενάρια ευπάθειας συσκευών του διαδικτύου των πραγμάτων (IoT)
2. Η ανάλυση των κινδύνων, των απειλών και των προκλήσεων που αφορούν το Διαδίκτυο των Πραγμάτων (IoT).
3. Η μελέτες περίπτωσης ευπάθειας επώνυμων εμπορικών προϊόντων έναντι στοχευμένων απειλών.

Στο πρώτο (1ο) κεφάλαιο παρουσιάζονται κάποιες εισαγωγικές έννοιες σχετικά με το Διαδίκτυο των πραγμάτων(IoT) και την αρχιτεκτονική, τα πρωτόκολλα, τα πλεονεκτήματα αλλά και κάποια από τα παραδείγματα των εφαρμογών IoT.

Στο δεύτερο (2ο) κεφάλαιο γίνεται μια αναφορά στις έξυπνες συσκευές , ποιες είναι οι λειτουργίες τους οι οποίες καθορίζουν την δυνατότητα ασταμάτητης συνδεσιμότητας και ανταλλαγής δεδομένων. Στη συνέχεια παρουσιάζονται μερικές από τις πιο δημοφιλείς έξυπνες συσκευές IoT.

Στο τρίτο (3ο) κεφάλαιο περιλαμβάνονται οι απειλές και προκλήσεις ασφαλείας στις IoT συσκευές μέσα από μια μελέτη περίπτωσης ενός συστήματος smart plug (έξυπνης πρίζας), γίνεται μια μελέτη τρωτότητας των έξυπνων οικιακών συσκευών με στατιστικά που αφορούν καταναλωτικές συσκευές ευρέως γνωστές.

Στο τρίτο (4ο) κεφάλαιο αναφέρονται τρείς διαφορετικές μελέτες περίπτωσης δοκιμών διείσδυσης σε έξυπνες καταναλωτικές συσκευές IoT. Τέλος, γίνεται αναφορά στα συμπεράσματα της πτυχιακής εργασίας.

1. Internet of Things

1.1 Τι είναι το Διαδίκτυο των Πραγμάτων

Το Internet of Things (IoT) είναι μια τεχνολογία που συνδέει αισθητήρες και διάφορες συσκευές, οτιδήποτε δηλαδή συνδέεται με το internet. Με αυτόν τον τρόπο επιτρέπει να ανταλλάσσουν δεδομένα και πληροφορίες μεταξύ τους. Δεν υπάρχει κάποιος συγκεκριμένος ορισμός για το διαδίκτυο των πραγμάτων διότι στην πραγματικότητα πολλές και διαφορετικές ομάδες έχουν θεσπίσει τον δικό τους ορισμό. Ο όρος Διαδίκτυο των πραγμάτων (IoT) έχει προσελκύσει την προσοχή προβάλλοντας το όραμα μιας παγκόσμιας υποδομής δικτυωμένων φυσικών αντικειμένων, επιτρέποντας την συνδεσιμότητα τους οποιαδήποτε στιγμή.

Τα τελευταία δέκα χρόνια το IoT είναι στο επίκεντρο της προσοχής μιας παγκόσμιας κοινότητας δικτυωμένων φυσικών αντικειμένων με σκοπό την εξ αποστάσεως διαχείριση τους. Επίσης το IoT μπορεί να θεωρηθεί ως ένα παγκόσμιο δίκτυο το οποίο επιτρέπει την επικοινωνία ανθρώπου με άνθρωπο, ανθρώπου με αντικείμενο αλλά και αντικείμενο με αντικείμενο παρέχοντας έτσι μια μοναδική ταυτότητα σε κάθε συσκευή IoT. Με λίγα λόγια λοιπόν, περιγράφει έναν κόσμο στον οποίο τα πάντα μπορούν να συνδεθούν μεταξύ τους ανά πάσα ώρα και στιγμή. Κατά συνέπεια κάθε συσκευή έχει την δική της IP και συνδέεται ασύρματα ή ενσύρματα στο δίκτυο. Τα δίκτυα στα οποία συνδέονται οι συσκευές παράγουν τεράστιους όγκους δεδομένων που ρέουν στους υπολογιστές για την ανάλυση τους έτσι ώστε να μπορούν να αντιληφθούν τις όποιες αλλαγές γίνονται στο περιβάλλον. Το συναρπαστικό με αυτή την τεχνολογία είναι ότι καθημερινά εξελίσσεται με αποτέλεσμα όλο και περισσότερες συσκευές να αυτοματοποιούνται και να γίνονται “έξυπνες” αυξάνοντας την ποικιλία τους.

Ιστορία του IoT

Η έννοια του Διαδικτύου των πραγμάτων (IoT) εμφανίστηκε τη δεκαετία του 1990, μια εποχή που το διαδίκτυο άρχιζε να απογειώνεται και ο κόσμος γνώριζε σημαντικές τεχνολογικές προόδους. Σημεία ορόσημα σημάδεψαν την πρώιμη εξέλιξη του IoT. Το 1990, ο John Romkey και ο Simon Hackett συνέδεσαν μια τοστιέρα στο διαδίκτυο χρησιμοποιώντας το Transmission Control Protocol / Internet Protocol (TCP/IP) με σκοπό να την χειρίζονται, καθιστώντας την πρώτη συσκευή IoT. Εννέα χρόνια αργότερα, ο Kevin Ashton, εκτελεστικός διευθυντής των εργαστηρίων Auto-ID Center στο Ινστιτούτο Τεχνολογίας της Μασαχουσέτης, επινόησε τον όρο «Internet of Things». Η ομάδα του Ashton εργαζόταν με σκοπό την αναγνώριση των ραδιοσυχνοτήτων (RFID) για τη διαχείριση της εφοδιαστικής αλυσίδας. Ο Ashton οραματίστηκε έναν κόσμο στον οποίο οι υπολογιστές θα κατέγραφαν και θα γνώριζαν τα πάντα για τα πράγματα που παρακολουθούν συλλέγοντας αυτόνομα δεδομένα.

Η νέα χιλιετία αποδείχθηκε μια κρίσιμη δεκαετία για την εξέλιξη του IoT. Το 2000, η “LG” (Life’s Good) παρουσίασε το πρώτο συνδεδεμένο στο διαδίκτυο ψυγείο, το “LG Internet Digital DIOS”, το οποίο παρείχε πολλές λειτουργίες πληροφόρησης και διαχείρισης, όπως την ένδειξη της θερμοκρασίας και την δυνατότητα παρακολούθηση τροφίμων στο εσωτερικό του. Ωστόσο, το προϊόν τελικά απέτυχε καθώς κρίθηκε αδικαιολόγητα ακριβό και οι πελάτες δεν είδαν την χρηστικότητα του. Στις αρχές της δεκαετίας του 2000, εμφανίστηκαν πολλές άλλες συσκευές οι οποίες μπορούσαν να συνδεθούν στο διαδίκτυο, όπως οι “έξυπνες” συσκευές φωτισμού το 2002 και το συνδεδεμένο στο διαδίκτυο μηχανικό κουνέλι “Nabaztag” από τη εταιρία “Violet” το 2005. Ο όρος "Internet of Things" ξεκίνησε επίσης να εμφανίζεται στα κύρια μέσα ενημέρωσης και τα συγγράμματα. Το 2005 σηματοδοτεί το επόμενο σημαντικό ορόσημο για το IoT όταν η ITU (Διεθνής Ένωση Τηλεπικοινωνιών) των Ηνωμένων Εθνών δημοσίευσε την πρώτη της αναφορά σχετικά με το αντικείμενο. Χάρη στην δημοτικότητα των έξυπνων συσκευών, συμπεριλαμβανομένων των smartphones, των υπολογιστών και των tablets, αυξήθηκε ο αριθμός των συνδεδεμένων στο διαδίκτυο συσκευών στο δεύτερο μισό της δεκαετίας του 2000.

Το πρώτο Ευρωπαϊκό Συνέδριο IoT πραγματοποιήθηκε το 2008 και το Εθνικό Συμβούλιο Πληροφοριών των ΗΠΑ αναγνώρισε το IoT ως μία από τις έξι τεχνολογίες που θα μπορούσαν να επηρεάσουν δυνητικά τις ΗΠΑ. Ο όμιλος διαδικτυακών επιχειρηματικών λύσεων της Cisco εκτίμησε πως μεταξύ των ετών 2008 και 2009, ο αριθμός των συνδεδεμένων συσκευών στο διαδίκτυο είχε ξεπεράσει τον ανθρώπινο πληθυσμό, γεγονός που αποτέλεσε σημείο ορόσημο για τη γέννηση του IoT. Σύμφωνα με την Cisco το 2010 οι συνδεδεμένες συσκευές στο διαδίκτυο προσέγγιζαν τα 12,5 δισεκατομμύρια αριθμός που τετραπλασιάστηκε το 2020.

Το 2010 ο τότε πρωθυπουργός της κινεζικής Λαϊκής Δημοκρατίας ανακήρυξε το IoT βασικό κλάδο της βιομηχανίας και ανακοίνωσε τα σχέδια τους για μεγάλες επενδύσεις, με στόχο να γίνουν οι πρωτοπόροι σ αυτόν τον τομέα. Την επόμενη χρονιά η εταιρεία ερευνών Gartner αναλύοντας την αγορά πρόσθεσε στον ετήσιο της κύκλο Hype Cycle το IoT. Οι έρευνές της επίσης έδειξαν την ραγδαία ανάπτυξη η οποία και διογκώθηκε την περίοδο 2014 - 2018.

Συμπερασματικά, η πρόοδος της τεχνολογίας έχει φέρει επανάσταση στον τρόπο που ζούμε, εργαζόμαστε και επικοινωνούμε. Ενώ η ψηφιακή εποχή έχει επιφέρει πολλά

Εικόνα 1. SEQ Εικόνα * ARABIC 1 - Η

οφέλη και ευκαιρίες, έχει επίσης θέσει σημαντικές προκλήσεις και κινδύνους. Είναι ζωτικής σημασίας για τα άτομα, τους οργανισμούς και τις κυβερνήσεις να παραμείνουν σε επαγρύπνηση και προορατικότητα για την αντιμετώπιση των απειλών στον κυβερνοχώρο και τη διασφάλιση ενός ασφαλούς περιβάλλοντος. Υιοθετώντας βέλτιστες πρακτικές και επενδύοντας σε μέτρα κυβερνοασφάλειας, μπορούμε να αξιοποιήσουμε τη δύναμη της τεχνολογίας και να ξεκλειδώσουμε πλήρως τις δυνατότητές της για ένα καλύτερο μέλλον. [1] [2] [3]

1.2 Ιστορική αναδρομή

Το Internet of Things (IoT) έχει φέρει μια επανάσταση στην επικοινωνία, καθιστώντας το ένα εργαλείο στην σύγχρονη εποχή. Τα τελευταία χρόνια έχει σημειωθεί σημαντική αύξηση στην εγκαθίδρυση προηγμένων τεχνολογιών επικοινωνίας. Υπολογίζεται ότι υπάρχουν περίπου 5 δισεκατομμύρια έξυπνες συσκευές ενεργές σε όλο τον πλανήτη και οι ειδικοί προβλέπουν ότι ο αριθμός των ενεργών συσκευών θα ξεπεράσει τα 25,4 δισεκατομμύρια το 2030. Έτσι λοιπόν παρουσιάζεται μια μεγάλη ευκαιρία για την ανάπτυξη νέων τεχνολογιών επικοινωνίας και την διερεύνηση τρόπων εκσυγχρονισμού των συσκευών μέσω του διαδικτύου. Ωστόσο είναι σημαντικό να κατανοήσουμε και τις εξελίξεις στο τομέα του IoT πριν αξιολογήσουμε τις δυνατότητες του. Στο Σχήμα 5 φαίνεται η εξέλιξη αλλά και τα επιτεύγματα του IoT τα τελευταία χρόνια.

Η γνώση του παρελθόντος μπορεί να μας βοηθήσει να προβλέψουμε το μέλλον και να αξιοποιήσουμε στο έπακρο οποιαδήποτε τεχνολογία. Υπάρχουν κάποιες στιγμές στην ιστορία του IoT που ξεχωρίζουν ως ορόσημα.

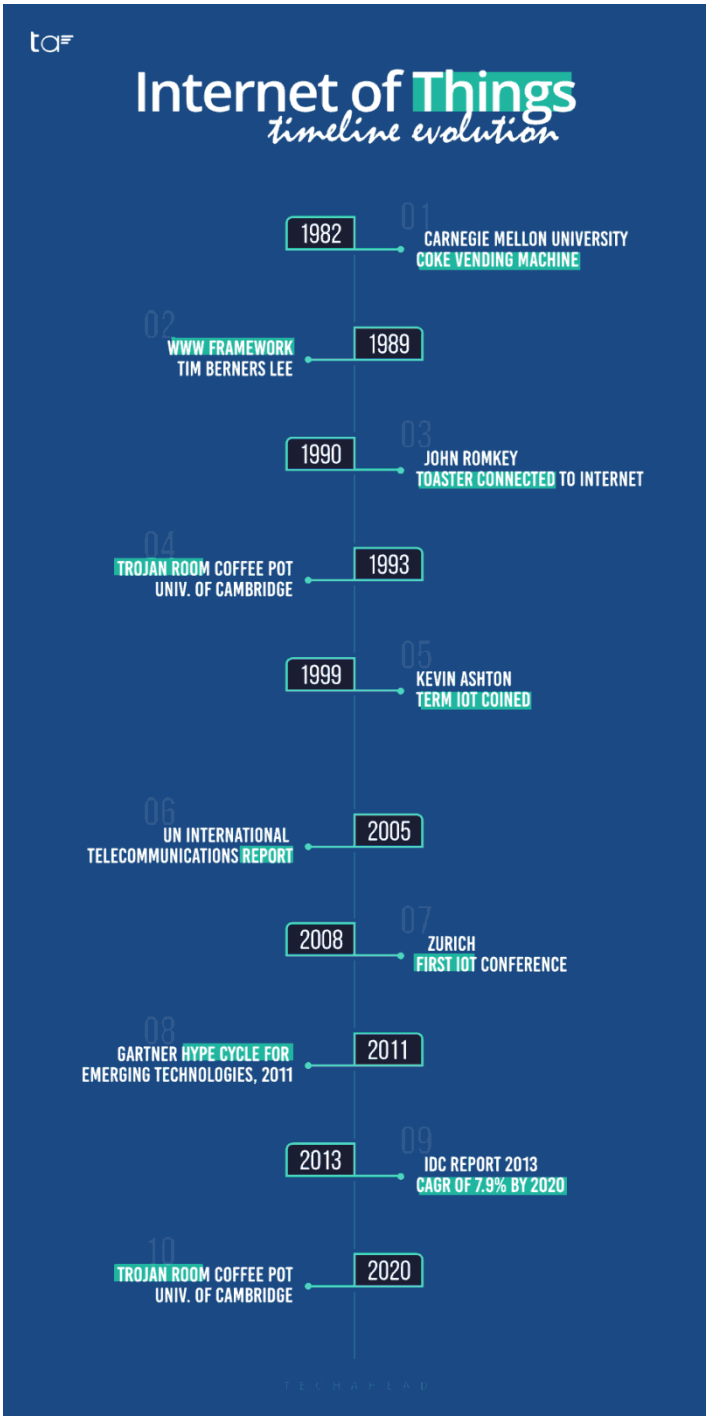
Η εξέλιξη του IoT ξεκινά με το ARPANET, το πρώτο συνδεδεμένο δίκτυο και τον προκάτοχο του Διαδικτύου όπως το γνωρίζουμε σήμερα.

- Το 1982, ένας μεταπτυχιακός φοιτητής στο Πανεπιστήμιο Carnegie Mellon των Η.Π.Α, ονόματι David Nichols, αναρωτήθηκε εάν ο αυτόματος πωλητής Coca-Cola

στο τμήμα επιστήμης των υπολογιστών περιείχε κουτάκια Coca-Cola ‘s. Ο ίδιος είχε βαρεθεί να πηγαίνει μέχρι το μηχάνημα αυτόματης πώλησης μόνο για να διαπιστώσει ότι δεν είχαν απομείνει μπουκάλια Coca-Cola ‘s. Ο Nichols συνεργάστηκε με δύο συμφοιτητές του, καθώς και με έναν ερευνητή μηχανικό για να αναπτύξει ένα πρόγραμμα που θα μπορούσε να παρακολουθεί την κατάσταση του αυτόματου πωλητή και να ενημερώνει τους μαθητές για το περιεχόμενο του αυτόματου πωλητή.

- Το 1989, ο Tim Berners-Lee πρότεινε το μοντέλο του World Wide Web, θέτοντας τα θεμέλια για το διαδίκτυο όπως το ξέρουμε σήμερα.
- Το 1990, ο John Romkey ανέπτυξε μια τοστιέρα που μπορούσε να ανοίξει και να κλείσει μέσω του Διαδικτύου, παρόλο που δεν υπήρχε Wi-Fi εκείνη την εποχή. Αυτή η τοστιέρα θεωρείται από πολλούς ως η πρώτη συσκευή IoT και σηματοδότησε την αρχή του Διαδικτύου των πραγμάτων.
- Το 1993, ερευνητές στο Πανεπιστήμιο του Cambridge ανέπτυξαν το “Trojan Room Coffee Pot”, το οποίο ουσιαστικά ήταν η πρώτη webcam εγκατεστημένη σε μια καφετιέρα στο εργαστήριο υπολογιστών του πανεπιστημίου. Η webcam κατέγραφε το εσωτερικό της καφετιέρας κάθε λίγα λεπτά και μπορούσε να μεταφέρει την εικόνα σε όλους τους υπολογιστές του πανεπιστημίου, έτσι οι χρήστες μπορούσαν να δουν το δοχείο του καφέ από απόσταση.
- Ο όρος Internet of Things επινοήθηκε από τον εκτελεστικό διευθυντή των εργαστηρίων της “Auto- ID Centre”, Kevin Ashton το 1999 στο πανεπιστήμιο της Μασαχουσέτης κατά την διάρκεια μιας παρουσίασης του στην “Procter & Gamble” σχετικά με τη σύνδεση της τεχνολογίας RFID στην εφοδιαστική αλυσίδα της P&G με το διαδίκτυο.
- Από το 2003 έως το 2004 ο όρος IoT άρχισε να εμφανίζεται σε κύριες εκδόσεις μεγάλων εφημερίδων όπως η “The Guardian” και η “Scientific American”. Την ίδια χρονιά αναπτύχθηκε και η τεχνολογία RFID από το Υπουργείο Άμυνας των ΗΠΑ με την βοήθεια της “Walmart” στα καταστήματά της.
- Το 2005, η Διεθνής Ένωση Τηλεπικοινωνιών των Ηνωμένων Εθνών αναγνώρισε το αντίκτυπο του IoT και προέβλεψε ότι θα δημιουργούσε ένα εντελώς νέο δυναμικό δίκτυο.
- Τον Μάρτιο του 2008 πραγματοποιείται το πρώτο συνέδριο IoT στη Ζυρίχη συγκεντρώνοντας ερευνητές και επαγγελματίες τόσο από τον ακαδημαϊκό χώρο όσο και από τη βιομηχανία του κλάδου, για να μοιραστούν γνώσεις και ιδέες. Την ίδια χρονιά, το Εθνικό Συμβούλιο Πληροφοριών των ΗΠΑ αναγνώρισε το Διαδίκτυο των πραγμάτων ως μία από τις έξι τεχνολογίες που προκάλεσαν επανάσταση.

- Το 2011 σύμφωνα με την Cisco Internet Business Solutions Group (CIBSG) το διαδίκτυο των πραγμάτων γεννήθηκε μεταξύ 2008 και 2009 όταν ο αριθμός ων συνδεδεμένων συσκευών ξεπέρασε τον αριθμό του ανθρώπινου πληθυσμού. Την ίδια χρονιά η Gartner συμπεριέλαβε το IoT στον κύκλο “hype” για τις αναδυόμενες τεχνολογίες.
- Η IDC το 2013 προέβλεψε σε μια έκθεση της ότι η αγορά του IoT θα αναπτυχθεί

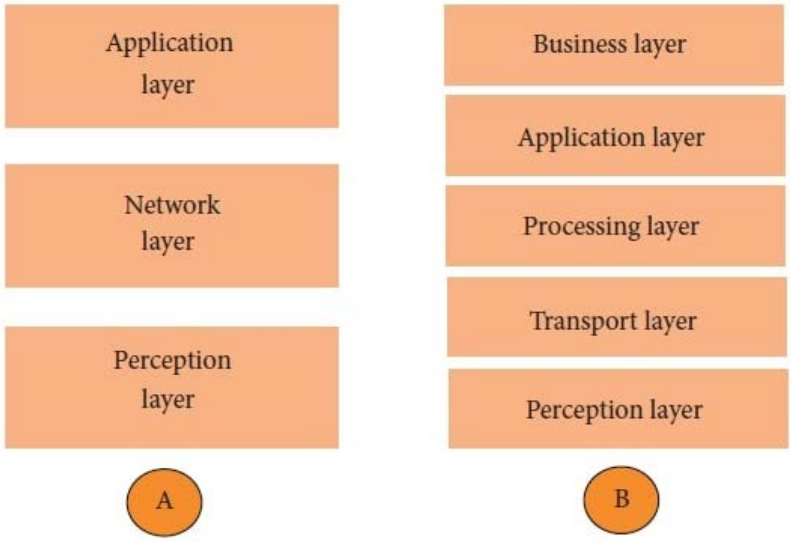


Εικόνα 2. Ορόσημα στην εξέλιξη του IoT

κατά 7,9% GAGR (Compound Annual Growth Rate) και θα φτάσει τα 8.9 δισεκατομμύρια δολάρια το 2020. [4] [5] [6]

1.3 Αρχιτεκτονική

Το πεδίο του Διαδικτύου των Πραγμάτων (IoT) είναι ευρύ και ποικίλο, με διάφορους ορισμούς και έννοιες. Δεν υπάρχει ένα ενιαίο κοινώς αποδεκτό αρχιτεκτονικό μοντέλο για το IoT αλλά διαφορετικοί φορείς και οργανισμοί έχουν προτείνει τα δικά τους συγκεκριμένα μοντέλα αντανακλώντας τις μεμονωμένες προοπτικές τους δίνοντας έμφαση σε διάφορες πτυχές του IoT. Τα πιο δημοφιλή αρχιτεκτονικά μοντέλα που επικρατούν είναι των τριών και πέντε επιπέδων. Στο μοντέλο των τριών επιπέδων βλέπουμε τα εξής :



Εικόνα 3. Αρχιτεκτονική του IoT

- **Επίπεδο αντίληψης (Perception layer)**: Είναι το χαμηλότερο επίπεδο και ίδιο σε όλα τα μοντέλα αρχιτεκτονικών, είναι μέρος του φυσικού επίπεδού που είναι συνδεδεμένο με τον πραγματικό κόσμο μέσω των αισθητήρων οι οποίοι συλλέγουν δεδομένα παρακολουθώντας τυχόν αλλαγές στο περιβάλλον. Τα δεδομένα που συλλέγονται μετατρέπονται σε ψηφιακή μορφή και αποστέλλονται στο αμέσως επόμενο επίπεδο.
- **Επίπεδο Δικτύου (Network layer)**: Το μεσαίο επίπεδο είναι το επίπεδο δικτύου, το οποίο είναι υπεύθυνο για την επεξεργασία τη μετάδοση δεδομένων αλλά και τη σύνδεση με άλλες έξυπνες συσκευές δικτύου και διακομιστές(servers). Ασχολείται με την μετάδοση δεδομένων τα οποία εισέρχονται σε ένα κεντρικό δρομολογητή(router). Κάποια από τα πρωτόκολλα που χρησιμοποιεί αυτό το επίπεδο είναι τα HTTP, MQTT και CoAp.

- **Επίπεδο εφαρμογής (Application layer)**: Το επίπεδο εφαρμογής δίνει το δικαίωμα στον τελικό χρήστη να χρησιμοποιεί τα δεδομένα που συλλέγονται μέσω των IoT συσκευών. Περιλαμβάνει εργαλεία ανάπτυξης και διαχείρισης των εφαρμογών μέσω των οποίων συνήθως παρέχονται υπηρεσίες IoT για τον τελικό χρήστη. Αντιπροσωπεύει το σημείο τομής του IoT και της βιομηχανικής τεχνολογίας, με στόχο την εκπλήρωση των ειδικών απαιτήσεων την βιομηχανία και την επίτευξη ενός έξυπνου βιομηχανικού οικοσυστήματος. [7] [8]

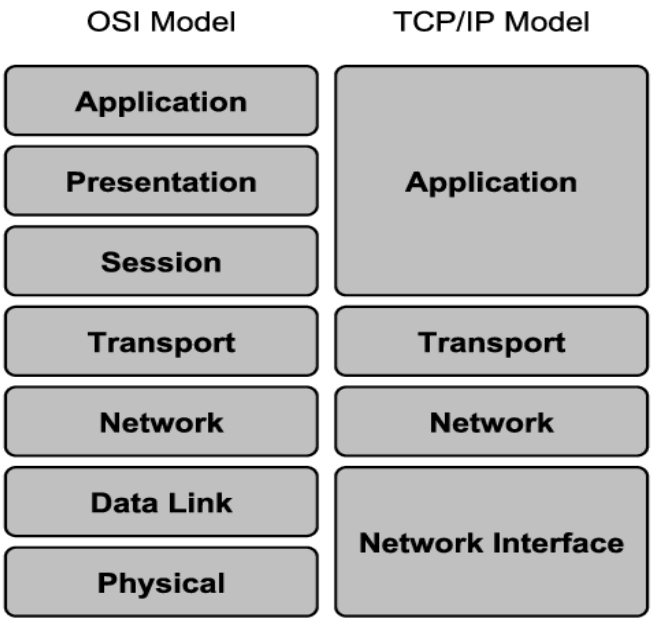
Αν και η αρχιτεκτονική τριών επιπέδων έχει χρησιμεύσει ως ένα πολύτιμο πλαίσιο κατανόησης των θεμελιωδών αρχών του IoT, δεν επαρκεί για την εξέταση της πολυπλοκότητας του IoT. Κατά συνέπεια σε κάποιες αναφορές έχουν προστεθεί τα επιπλέον επίπεδα:

- **Επίπεδο μεταφοράς (Transport layer)**: Το επίπεδο μεταφοράς είναι υπεύθυνο για την μετάδοση των δεδομένων του αισθητήρα προς το επίπεδο επεξεργασίας αλλά και αντίθετα, αυτή η μετάδοση πραγματοποιείται συνήθως ασύρματα μέσω των πρωτοκόλλων 3G, LAN, Bluetooth, RFID, και NFC.
- **Επίπεδο επεξεργασίας (Processing layer)**: Γνωστό ως το επίπεδο ενδιάμεσου λογισμικού, το επίπεδο επεξεργασίας έχει κρίσιμο ρόλο στην IoT αρχιτεκτονική καθώς αποθηκεύει, αναλύει και επεξεργάζεται μεγάλες ποσότητες δεδομένων από το επίπεδο μεταφοράς. Μπορεί επίσης να κάνει διαχείριση και να παρέχει μια ποικιλία από τεχνολογίες στα κατώτερα επίπεδα χρησιμοποιώντας βάσεις δεδομένων, υπολογιστικά νέφη αλλά και μονάδες επεξεργασίας δεδομένων.
- **Επιχειρηματικό επίπεδο (Business layer)**: Το επιχειρηματικό επίπεδο είναι το ανώτερο επίπεδο του πίνακα το οποίο διαχειρίζεται ολόκληρο το σύστημα IoT συμπεριλαμβανομένων των εφαρμογών, των επιχειρηματικών και κερδοσκοπικών μοντέλων αλλά και την ιδιωτικότητα των χρηστών.

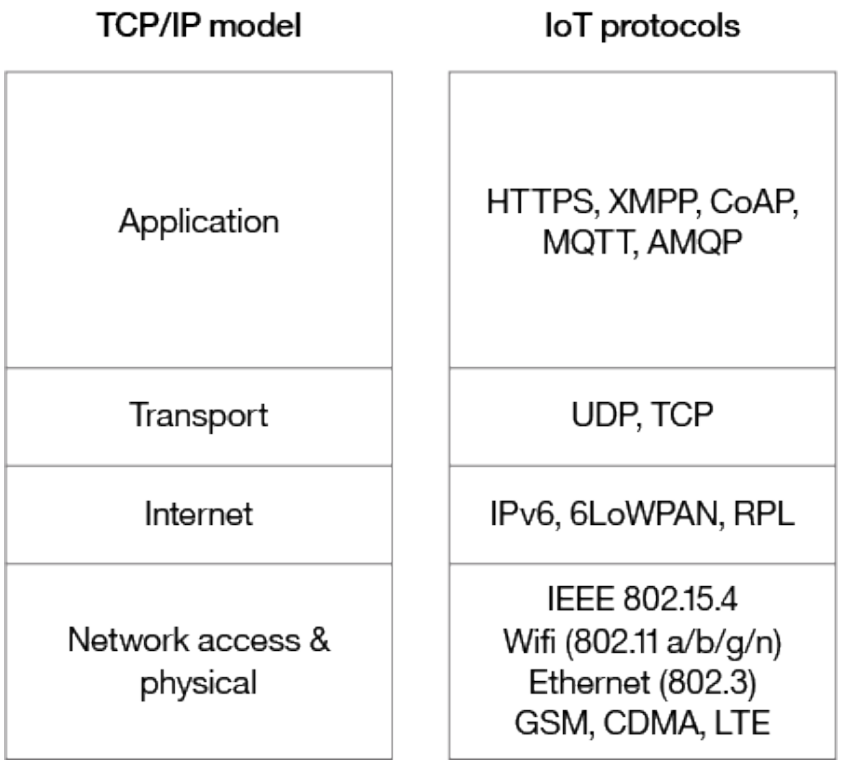
Ενώ η δομή τριών επιπέδων του Διαδικτύου των Πραγμάτων (IoT) ήταν χρήσιμη για την κατανόηση της τεχνικής της αρχιτεκτονικής κατά τα πρώτα στάδια της ανάπτυξής της, δεν μπορεί να εξηγηθεί πλήρως την πολυπλοκότητα της δομής και η έννοια του IoT. Ως αποτέλεσμα, να υπάρχει ποικιλία απόψεων μεταξύ των μελετητών όσον αφορά τον ορισμό και το πεδίο εφαρμογής του IoT. [7] [9]

1.4 Πρωτόκολλα

Στο διαδίκτυο των πραγμάτων (IoT) η σημασία των πρωτοκόλλων και των προτύπων συχνά παραβλέπεται, η επικοινωνία μεταξύ διαφόρων συσκευών, αισθητήρων IoT, πυλών, διακομιστών και εφαρμογών του χρήστη είναι ζωτικής σημασίας για το διαδίκτυο των πραγμάτων (IoT) και χωρίς τα κατάλληλα πρωτόκολλα η επικοινωνία θα αποτύγχανε. Τα πρωτόκολλα IoT είναι απαραίτητα για την ενεργοποίηση της επικοινωνίας, την ανταλλαγή δεδομένων αλλά και την αποστολή εντολών μεταξύ διαφόρων συσκευών και την διεξαγωγή κρίσιμων πληροφοριών προς τον τελικό χρήστη. Υπάρχουν διάφορα πρωτόκολλα και πρότυπα IoT ανάλογα με την περίπτωση χρήσης τα οποία κατηγοριοποιούνται σε διάφορα επίπεδα ανάλογα την περίπτωση χρήσης. Δημιουργήθηκε λοιπόν ένας τρόπος ταξινόμησης των στοιχείων της αρχιτεκτονικής IoT σε διάφορα επίπεδα. Το μοντέλο Open Systems Interconnection (OSI) το οποίο αποτελείται από επτά επίπεδα αρχιτεκτονικής με το φυσικό επίπεδο να ηγείται αυτών και να ακολουθούν το επίπεδο σύνδεσης δεδομένων, το επίπεδο δικτύου, το επίπεδο μεταφοράς, το επίπεδο συνεδρίας, το επίπεδο παρουσίασης και τελευταίο το επίπεδο εφαρμογής.



Εικόνα 4Μοντέλα OSI & TCP/IP



Εικόνα 5. Μοντέλο TCP/IP &Πρωτοκόλλα IoT

Ειδικοί αναφέρουν επίσης την αρχιτεκτονική του IoT σε μοντέλα τριών, τεσσάρων ή πέντε επιπέδων καθεμιά απ' αυτές μπορεί να υποδιαιρεθεί περαιτέρω σύμφωνα πάντα με την δομή ISO. Τα πρωτοκολλά του IoT κατατάσσονται σε δυο βασικές κατηγορίες, τα πρωτόκολλα δεδομένων (IoT data protocols) και τα πρωτόκολλα δικτύου (IoT network protocols).

1.4.1 Πρωτόκολλα IoT Επιπέδου Εφαρμογής

Πρωτόκολλα δεδομένων IoT (IoT data protocols)

- **XMPP (Extensible Messaging and Presence Protocol)**: Το XMPP βρίσκεται στο επίπεδο εφαρμογής είναι ελεύθερα διαθέσιμο ανοιχτού κώδικα πρωτόκολλο.
- **MQTT (Message Queuing Telemetry Transport)**: Το MQTT είναι ένα πρωτόκολλο επικοινωνίας για συσκευές σε δίκτυα machine-to-machine (M2M) μέσω ελαφρών μηνυμάτων.
- **CoAP (Constrained Application Protocol)**: Το CoAP είναι ένα πρωτόκολλο σχεδιασμένο για την επικοινωνία συστημάτων διαδικτύου με περιορισμένους υπολογιστικούς πόρους.

- **AMQP (Advanced Message Queuing Protocol)**: Το AMQP είναι σχεδιασμένο κυρίως για εφαρμογές επιχειρηματικής ανταλλαγής μηνυμάτων επιβάλλοντας τη συμπεριφορά του παρόχου μηνυμάτων και του πελάτη στο βαθμό που οι υλοποιήσεις από διαφορετικούς προμηθευτές είναι διαλειτουργικές
- **HTTP (HyperText Transfer Protocol)**: Το HTTP πρωτόκολλο επιπέδου εφαρμογής είναι υπεύθυνο για την παράδοση πολλαπλών πόρων υπερμέσων μέσω διαδικτύου, επιπλέον έχει σχεδιαστεί για την ταυτόχρονη επικοινωνία δύο συστημάτων.
- **DDS (Data Distribution Service)**: Το συγκεκριμένο πρωτόκολλο λειτουργεί ως ενδιάμεσο λογισμικό για την επικοινωνία από μηχανή σε μηχανή (M2M) και χρησιμοποιεί την ανταλλαγή δεδομένων μέσω της μεθόδου δημοσίευση εγγραφή.

1.4.2 Πρωτόκολλα IoT Επιπέδου Μεταφοράς

- **TCP (Transmission Control Protocol):** Το TCP είναι ένα αξιόπιστο πρωτόκολλο μετάδοσης δεδομένων που λειτουργεί στο επίπεδο μεταφοράς. Παρέχει αξιόπιστη παράδοση δεδομένων με μηχανισμό επανάληψης και επαλήθευσης. Ιδανικό για εφαρμογές που απαιτούν αξιόπιστη και σταθερή σύνδεση, όπως οι εφαρμογές βίντεο και φωνής στο IoT.
- **UDP (User Datagram Protocol):** Το UDP είναι ένα πιο ελαφρύ πρωτόκολλο μετάδοσης δεδομένων σε σχέση με το TCP. Δεν παρέχει μηχανισμούς επανάληψης ή επαλήθευσης, καθιστώντας το κατάλληλο για εφαρμογές που απαιτούν χαμηλή καθυστέρηση και δεν είναι τόσο ευαίσθητες στην απώλεια δεδομένων.

1.4.3 Πρωτόκολλα IoT Επιπέδου Δικτύου

Πρωτόκολλα δικτύου IoT (IoT Network Protocols)

- **IPv6 (Internet Protocol version 6):** Το IPv6 είναι η έκδοση του πρωτοκόλλου Διαδικτύου που αντικαθιστά το παλαιότερο IPv4. Προσφέρει ένα πολύ μεγαλύτερο χώρο διευθύνσεων IP, επιτρέποντας τη σύνδεση ένα πολύ μεγαλύτερου αριθμού συσκευών στο Διαδίκτυο. Το IPv6 είναι απαραίτητο για το μέλλον του IoT, καθώς η αύξηση του αριθμού των συνδεδεμένων συσκευών απαιτεί μεγαλύτερη διευθυνσιοδότηση.
- **LoRaWAN (Long Range Wan)**: Είναι ένα πρωτόκολλο ελέγχου πρόσβασης πολυμέσων και επιτρέπει στις συσκευές χαμηλής κατανάλωσης να επικοινωνούν απευθείας με τις εφαρμογές μέσω ασύρματης σύνδεσης μεγάλης εμβέλειας.
- **Bluetooth**: Το Bluetooth (IEEE 802.15) χρησιμοποιείται για την ad-hoc επικοινωνία, την μετάδοση δεδομένων και φωνής σε μικρές αποστάσεις.

- **ZigBee**: (IEEE 802.15.4) Ένα παρόμοιο πρωτόκολλο με το Bluetooth για την υποστήριξη των δικτύων ελέγχου και των δικτύων αισθητήρων και ιδανικό για μικρές συσκευές IoT που δεν διαθέτουν μεγάλη χωρητικότητα αποθήκευσης ισχύος.

1.4.4 Πρωτόκολλα IoT Επιπέδου Πρόσβασης στο Δίκτυο

- **Wi-Fi**: Wireless Fidelity (IEEE 802.11) σημαίνουν τα αρχικά αυτού του πρωτοκόλλου το οποίο χρησιμοποιείται για την ασύρματη επικοινωνία υψηλής ταχύτητας, επίσης είναι ευέλικτο και συμβατό με διάφορα δίκτυα πρωτοκόλλου Internet (IP)
- **Cellular networks (LTE,4G,5G)**: Τα περισσότερα συστήματα IoT βασίζονται πάνω στα δίκτυα κινητής τηλεφωνίας και μπορούν να υποστηρίξουν πολύ υψηλές ταχύτητες για την μεταφορά δεδομένων

- **CDMA (Code Division Multiple Access):** Το CDMA είναι ένα πρωτόκολλο κινητής τηλεφωνίας που χρησιμοποιείται κυρίως στη Βόρεια Αμερική και ορισμένες άλλες περιοχές. Χρησιμοποιεί την τεχνική της διαίρεσης με κωδικοποίηση για τη διαχείριση των κλήσεων και των δεδομένων σε ένα δίκτυο. Προσφέρει υψηλή ποιότητα και απόδοση, ενώ επίσης είναι αποτελεσματικό σε περιοχές με υψηλή πυκνότητα κλήσεων.

- **GSM (Global System for Mobile Communications):** Το GSM είναι ένα από τα παλαιότερα πρωτόκολλα κινητής τηλεφωνίας και εξακολουθεί να χρησιμοποιείται παγκοσμίως. Ξεκίνησε ως πρωτόκολλο ψηφιακής φωνητικής επικοινωνίας, αλλά αργότερα επεκτάθηκε για τη μετάδοση δεδομένων και το Internet. Παρέχει υπηρεσίες όπως φωνητική τηλεφωνία, SMS και GPRS (General Packet Radio Service) για τη μετάδοση δεδομένων. [10] [11] [12] [13] [14]

1.5 Πλεονεκτήματα

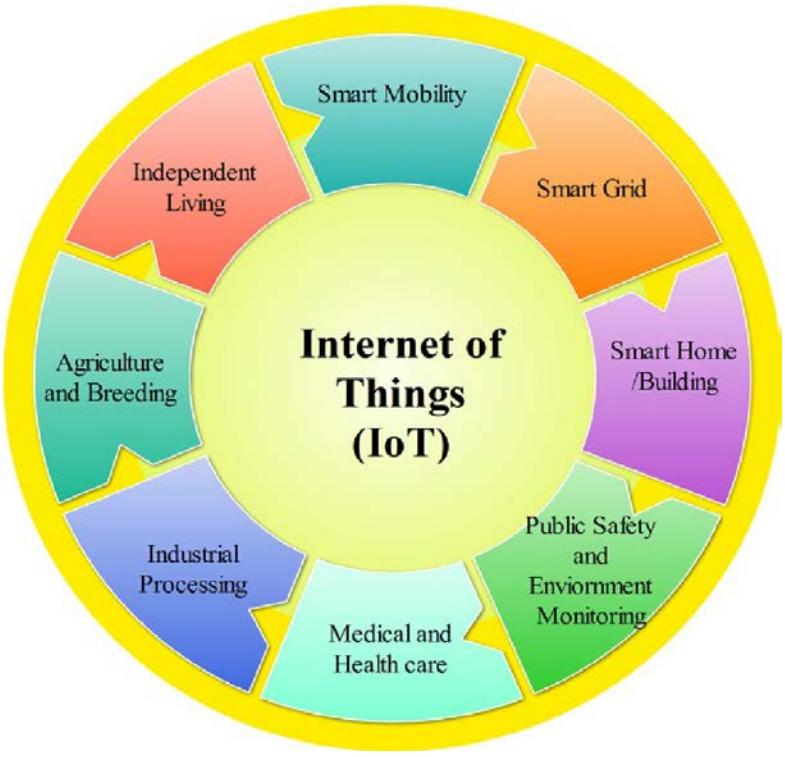
Οι IoT συσκευές παρέχουν μια σειρά πλεονεκτημάτων που ενισχύουν την παραγωγικότητα, βελτιστοποιούν την χρήση πόρων και βελτιώνουν την ασφάλεια και προστασία των συσκευών. Αναφορικά μερικά από τα πλεονεκτήματα των έξυπνων συσκευών.

- **Έλεγχος και αυτοματισμός (Control and Automation)**: Στις μέρες μας ένας έξυπνος λαμπτήρας ακούγεται κάτι απλό αλλά στην πραγματικότητα είναι από τις πιο δημοφιλείς IoT συσκευές σήμερα. Παρέχουν τον εξ αποστάσεως χειρισμό τους και δίνουν την δυνατότητα στον χρήστη να ρυθμίσει για παράδειγμα μια συγκεκριμένη ώρα της ημέρας, να σβήνουν αυτόματα τα φώτα στο σαλόνι. Ο έλεγχος και η αυτοματοποίηση είναι πλεονεκτήματα του IoT που ενσωματώνονται σε διάφορες συσκευές επιτρέποντας τις ακόμα και τον χειρισμό τους μέσω φωνητικών εντολών.

- **Πρόσβαση σε πληροφορίες πραγματικού χρόνου (Real-Time Access to Information)**: Βασικό χαρακτηριστικό των IoT συσκευών είναι η ταχύτητα με την οποία μπορούν να μοιράζονται τις πληροφορίες μεταξύ τους πράγμα που σημαίνει αδιάλειπτη ροή πληροφοριών που μπορούν να αποδειχτούν κρίσιμες.
- **Αναδυόμενες επιχειρήσεις (Emerging Business)**: Οι έξυπνες συσκευές έχουν κατακλίσει τον πλανήτη εδώ και δεκαετίες αυξάνοντας ραγδαία την παγκόσμια παραγωγή τους. Αρκετές επιχειρήσεις ειδικεύονται γύρω από αυτές τις συσκευές όπως την παραγωγή συσκευών για έξυπνα οχήματα ή την παραγωγή έξυπνων ρολογιών με λειτουργίες οι οποίες βοηθούν άτομα με τον έλεγχο της αρτηριακής πίεσης, του διαβήτη αλλά και του οξυγόνου στο αίμα.
- **Σύνθετη συλλογή δεδομένων (Advanced Data Collection)**: Η συγκεκριμένη λειτουργία μπορεί να παρέχει πληροφορίες για την λήψη λεπτομερών αποφάσεων και καταγραφή δεδομένων. Παράδειγμα αυτού θα μπορούσε να είναι μια επιχείρηση της οποίας τα δεδομένα από μια έξυπνη συσκευή σε πραγματικό χρόνο θα φανούν χρήσιμα σχετικά με τις αποφάσεις αγοράς, την βελτίωση στον έλεγχο των αποθεμάτων αλλά και την απαραίτητη πληροφόρηση σχετικά με την συμπεριφορά και τα αγοραστικά πρότυπα των καταναλωτών.
- **Βελτιωμένη αποδοτικότητα (Improved Efficiency)**: Το Διαδίκτυο των πραγμάτων λειτουργεί αυτονομία. Βασισμένο σε δεδομένα που συλλέγονται σε πραγματικό χρόνο καθιστώντας μη απαραίτητη τη συλλογή και επεξεργασία δεδομένων από τον άνθρωπο επιτρέποντάς του να επικεντρωθεί στην αξιοποίηση των συλλεγόμενων πληροφοριών και όχι στην ίδια τη συλλογή δεδομένων. Παράδειγμα αυτού είναι η πασίγνωστη εφαρμογή Google maps η οποία μέσω της συλλογής δεδομένων από τους χρήστες έχει ως αποτέλεσμα την παρακολούθηση της κίνησης και των χιλιομέτρων βελτιώνοντας την αποτελεσματικότητα χωρίς να βασίζεται στην ανθρώπινη αντίληψη.
- **Βελτιωμένη ποιότητα ζωής (Improved Quality of Life)**: Οι τρόποι με τους οποίους μπορεί να βελτιωθεί η ποιότητα ζωής είναι πολλοί, ένας από αυτούς είναι όλες οι έξυπνες συσκευές στον τομέα της ιατρικής όπου στην κυριολεξία θα μπορούσαν να σώσουν ζωές. Οι έξυπνες συσκευές και οι αισθητήρες στα φώτα κυκλοφορίας θα μπορούσαν να συλλέγουν δεδομένα διευκολύνοντας την κυκλοφοριακή συμφόρηση σε περιοχές με πολύ κόσμο.
- **Μείωση κόστους (Cost Reduction)**: Όσο οι IoT συσκευές αυξάνονται τόσο μειώνονται τα έξοδα παραγωγής και μεταφοράς των πρώτων υλών. Η μείωση του κόστους στις συσκευές τις κάνει όλο και πιο προσιτές αλλά ταυτόχρονα αποτελεί κίνητρο στους καταναλωτές για να επενδύσουν σε αυτές.

- **Υψηλότερη παραγωγικότητα (Higher Productivity)**: Με την συλλογή δεδομένων από τις συσκευές παρέχονται εξαιρετικά λεπτομερή δεδομένα που βελτιώνουν μερικές από τις διαδικασίες των καταναλωτών. Σαν παράδειγμα αναφορικά μια εταιρία ηλεκτρισμού θα μπορεί να εκτιμήσει τον λογαριασμό κοινής ωφέλειας ενός ακινήτου εξ αποστάσεως.
- **Μαζικά δεδομένα και ανάλυση πρόβλεψης (Big Data and Predictive Analysis)**: Μαζικά δεδομένα ή αλλιώς Big Data ονομάζεται η διαδικασία συλλογής και ανάλυσης μεγάλου όγκου πληροφοριών για διάφορους σκοπούς. Ένας από αυτούς θα μπορούσε να είναι σε μια εταιρία η παρακολούθηση των εργαζομένων της με σκοπό είτε την απογραφή είτε για την χρήση των οχημάτων τους με σκοπό την βελτίωση της αποτελεσματικότητας των διαδικασιών
- **Υγεία και ασφάλεια (Health and Safety)**: Η τεράστια εξέλιξη στον τομέα της υγείας θα μπορούσε να σώσει μια πληθώρα χρηστών οι οποίοι χρησιμοποιούν τις IoT συσκευές, καταγράφοντας τυχόν αλλαγές στην θερμοκρασία, τα επίπεδα οξυγόνου στο αίμα, την ινσουλίνη και στέλνοντας τα απευθείας σε κάποιον γιατρό ή μέλος της οικογένειας τους προλαμβάνουν από χρόνιες ασθένειες οι οποίες θέλουν παρακολούθηση συνεχώς. [15] [16] [17] [18] [19] [20]

1.6 Εφαρμογές IOT



Εικόνα 6. IoT εφαρμογές

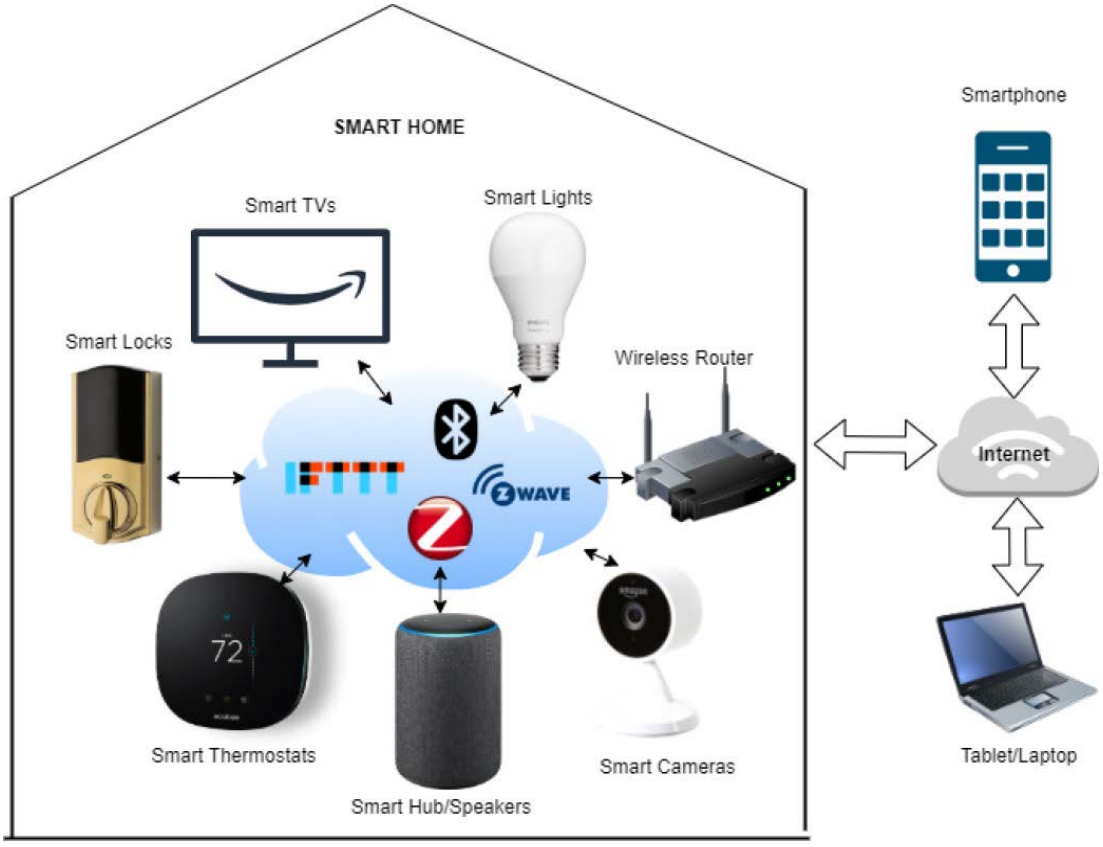
Το Διαδίκτυο των πραγμάτων (IoT) έχει αλλάξει τον τρόπο που αλληλοεπιδρούμε με τις συσκευές και τα δίκτυα διευκολύνοντας έτσι την ανάπτυξη όλο και περισσότερων εφαρμογών αναπτύσσοντας την βιομηχανία ραγδαία. Αυτές οι εφαρμογές επιτρέπουν την αλληλεπίδραση μεταξύ συσκευών και ανθρώπου διασφαλίζοντας έτσι ότι τα δεδομένα έχουν ληφθεί με ορθότητα και μέγιστη ταχύτητα. Ένα παράδειγμα είναι οι εφαρμογές μεταφορών και εφοδιαστικής αλυσίδας χρησιμοποιούν το IoT για την παρακολούθηση της κατάστασης των πραγμάτων που μεταφέρουν.

Πιο συγκεκριμένα η FedEx χρησιμοποιεί το SenseAware σύστημα παρακολούθησης για να ελέγχει τη θερμοκρασία, τη θέση και άλλες ζωτικές ενδείξεις ενός πακέτου της, συμπεριλαμβανομένου του πότε ανοίγει και αν έχει αλλοιωθεί κατά τη διαδρομή του. Οι IoT εφαρμογές μπορούν να επιλύσουν προβλήματα χωρίς την ανάγκη ανθρώπινης παρέμβασης.Το IoT έχει την δυνατότητα να επηρεάσει την κοινωνία, το περιβάλλον και την οικονομία, έννοιες όπως “έξυπνη κινητικότητα”(smart Mobility), “έξυπνο δίκτυο”(Smart Grid), “έξυπνα σπίτια/κτήρια”(Smart Homes/Buildings), δημόσια ασφάλεια και παρακολούθηση του περιβάλλοντος (Public Safety and Environment Monitoring), η ιατρική και η υγειονομική περίθαλψη(Medical and Healthcare), η βιομηχανική επεξεργασία(Industrial Processing), η γεωργία και η εκτροφή(Agriculture and Breeding) και η ανεξάρτητη διαβίωση (Independent Living) είναι μερικές από τις ιδέες που βασίζονται στο IoT. Η χρήση αυτών των εφαρμογών και τα πλεονεκτήματα τους έχουν παίξει σημαντικό ρόλο στην εξάρτηση του ανθρώπου από αυτές. Στο παραπάνω σχήμα απεικονίζονται διάφορες από τις εφαρμογές που αναφέρθηκαν τις οποίες θα δούμε πιο αναλυτικά παρακάτω :

- **Έξυπνα σπίτια/κτήρια “Smart Home/Building”**: Ονομάζονται όλα τα εξοπλισμένα σπίτια με ηλεκτρικές έξυπνες συσκευές (π.χ. θερμοστάτης, λάμπες, ψυγεία, καφετιέρες κ.α.) οι οποίες έχουν την δυνατότατα τον εξ αποστάσεως χειρισμό τους.
- **Έξυπνη διαχείρισης ενέργειας “Smart grid”**: Ένα προηγμένο δίκτυο παροχής ηλεκτρικής ενέργειας χρησιμοποιώντας την ψηφιακή τεχνολογία επικοινωνιών για την παρακολούθηση και ανταπόκριση σε αλλαγές χρήσης ενέργειας.
- **Έξυπνη υγειονομική περίθαλψη ”SmartHealthcare”**: Γνωστό και ως το διαδίκτυο των Ιατρικών Πραγμάτων (IoMT) ένας συστηματικός τρόπος εφαρμογής που συνδέει υπηρεσίες υγειονομικής περίθαλψης με τα συστήματα πληροφορικής μέσω διαφόρων δικτύων συνδεδεμένων υπολογιστών.

- **Έξυπνη κινητικότητα "Smart Mobility"**: Χρησιμεύει στο διαδίκτυο των οχημάτων (IoV) και προσφέρει λύσεις για την βελτίωση των τρόπων μεταφοράς αλλά και την ενίσχυση της ασφάλειας.
- **Δημόσια ασφάλεια και παρακολούθηση του περιβάλλοντος "Public Safety and Environment Monitoring"**: Περιλαμβάνουν την παρακολούθηση διαφόρων περιβαλλοντικών παραμέτρων όπως η ποιότητα νερού, καιρικές συνθήκες, σύστημα εντοπισμού διαρροής, προστασία απειλούμενων ειδών κ.α.
- **Βιομηχανική επεξεργασία "Industrial Processing"**: Το βιομηχανικό διαδίκτυο των πραγμάτων (IIoT) ονομάζεται η χρήση αισθητήρων για την βελτίωση των παραγωγικών και βιομηχανικών διαδικασιών. [21]
- **Έξυπνη Γεωργία και Έξυπνη Κτηνοτροφία "Agriculture and Breeding"**: Είναι μια προσέγγιση που έχει ως σκοπό την εξέλιξη της γεωργικής ανάπτυξης ενόψει της κλιματικής αλλαγής με την βοήθεια έξυπνων τεχνολογιών και συσκευών για την παρακολούθηση και τη βελτιστοποίηση των γεωργικών δραστηριοτήτων. [22] [23] [24] [25] [26] [27]

1.6.1 Έξυπνα σπίτια



Εικόνα 7. Παράδειγμα έξυπνου οικιακού περιβάλλοντος.

Το έξυπνο σπίτι ”smart home” μονοπωλεί στις IoT συσκευές, υπολογίζεται ότι παγκοσμίως υπάρχουν πάνω από 120 συνδεδεμένες συσκευές ανά δευτερόλεπτο. Έρευνα στις ΗΠΑ έδειξε ότι σε κάθε νοικοκυριό αντιστοιχεί κατά μέσο όρο οκτώ συνδεδεμένες συσκευές, νούμερο που υπολογίζεται να αυξηθεί έως και 14 συσκευές ανά άτομο τα επόμενα χρόνια. Οι IoT συσκευές περιλαμβάνουν ένα ευρύ φάσμα προϊόντων (κάμερες, φωνητικούς βοηθούς, θερμοστάτες κ.α.) και η σύνδεση αυτών δημιουργεί τα έξυπνα οικιακά περιβάλλοντα. Σαν παράδειγμα αυτού θα μπορούσαμε να φέρουμε μια οικογένεια όπου οι γονείς εργάζονται και δεν μπορούν να ‘’προσέξουν’’ τα παιδιά τους. Εκεί έρχεται η βοήθεια των IoT συσκευών. Μέσω της κάμερας, της έξυπνης κλειδαριάς, αλλά και της φωνητικής βοηθού τα παιδιά και οι γονείς αυτοματοποιούν κάποιες από τις ενέργειες του σπιτιού εξ αποστάσεως. [28]

1.6.2 Έξυπνη διαχείρισης ενέργειας

Εικόνα8. IOT - Έξυπνη διαχείριση ενέργειας

Με τον όρο έξυπνη διαχείριση ενέργειας αναφερόμαστε στην βελτιστοποίηση και την ενίσχυση της αποδοτικής χρήσης των ενεργειακών πόρων με την βοήθεια διάφορων συσκευών IoT οι οποίες ενσωματώνουν τεχνολογίες επιτρέποντάς τους να επικοινωνούν, να συλλέγουν και να αναλύουν δεδομένα σε πραγματικό χρόνο που σχετίζονται με την κατανάλωση, την παραγωγή και τη διανομή ενέργειας. Αυτές οι συσκευές επιτρέπουν στον χρήστη τον εξ αποστάσεως χειρισμό τους, την προσαρμογή των ρυθμίσεων ενός θερμοστάτη αλλά και την αυτόματη εκκίνηση λειτουργιών για εξοικονόμηση ενέργειας. Βασικό πλεονέκτημα τους βασισμένο σε δεδομένα και

προγνωστικά είναι η λήψη τεκμηριωμένης απόφασης σχετικά με την χρήση ενέργειας και η βελτιστοποίηση των περιόδων αιχμής της ζήτησης και ενσωμάτωσης ανανεώσιμων πηγών ενέργειας στο δίκτυο.

Πλεονεκτήματα των συσκευών έξυπνης διαχείρισης ενέργειας

- Εξοικονόμηση κόστους
- Μεγαλύτερη ενεργειακή απόδοση
- Απομακρυσμένη πρόσβαση
- Διορατικές αναφορές
- Μοτίβα κατανάλωσης
- Προσβασιμότητα

Παραδείγματα εφαρμογών

- **Έξυπνος φωτισμός, κλιματισμός και έλεγχος θερμοκρασίας**
  Τα συγκεκριμένα συστήματα τα οποία βασίζονται σε αισθητήρες μπορούν να εφαρμόσουν τις καλύτερες συνθήκες σε έναν χώρο προσαρμόζοντας συγκεκριμένα προφίλ κατανάλωσης ώστε να αποφεύγεται η σπατάλη ενέργειας.

- **Συστήματα διαχείρισης ενέργειας**
  Έξυπνοι μετρητές, αισθητήρες, εργαλεία ανάλυσης και εφαρμογές μερικά παραδείγματα συστημάτων διαχείρισης ενέργειας προς όφελος των τελικών χρηστών.

- **Πράσινη διαχείριση ενέργειας**
  Με την βοήθεια του IoT η πράσινη ενέργεια αναπτύσσεται όλο και περισσότερο με αποτέλεσμα οι ανεμογεννήτριες τα ηλιακά πάνελ κ.α. βοηθούν στην μείωση του μέσου λογαριασμού ενέργειας έως και 100%.

- **Αποθήκευση ενέργειας**
  Για την διαχείριση της πράσινης ενέργειας βοηθούν και τα συστήματα αποθήκευσης ενέργειας τα οποία αξιοποιούν τις ανανεώσιμες πηγές ενέργειας (αιολική, ηλιακή). Με την ενσωματωμένη τεχνολογία που διαθέτουν διαχειρίζοντας αποτελεσματικά την παραγόμενη ενέργεια επιτρέποντας στους χρήστες να γίνουν ενεργειακά ανθεκτικοί και ανεξάρτητοι κατά τη διάρκεια διακοπών ρεύματος και άλλων προβληματικών σεναρίων στη γραμμή

- **Συνδεδεμένοι σταθμοί ηλεκτροπαραγωγής**

Οι σταθμοί παραγωγής ηλεκτρικής ενέργειας με την χρήση αισθητήρων και συνεχή παρακολούθηση ελαχιστοποιούν τις δαπανηρές διακοπές λειτουργίας, τα ατυχήματα και τις διακοπές ρεύματος. Αρκετά από τα δίκτυα ανανεώσιμων πηγών ενέργειας δίνουν στον χρήστη μια διαφανή εικόνα για το από πού προέρχεται η ενέργεια αλλά και πληροφορίες αυτής. [29] [30] [31] [32] [33] [34] [35]

1.6.3 Έξυπνες μεταφορές

Μια τεχνολογία που ενσωματώνεται στα συστήματα μεταφορών για την βελτίωση της αποδοτικότητας, της ασφάλειας και της συνολικής κινητικότητας. Οι εκάστοτε συσκευές χρησιμοποιούν σύγχρονες τεχνολογίες όπως ασύρματη επικοινωνία, ανάλυση, επεξεργασία και αυτοματοποίηση δεδομένων σε πραγματικό χρόνο με στόχο την βελτιστοποίηση διαφόρων πτυχών των μεταφορών συμπεριλαμβανομένης της ροής της κυκλοφορίας, της διαχείρισης των οχημάτων, της πληροφόρησης των ταξιδιωτών και της συντήρησης των υποδομών. Οι συγκεκριμένες συσκευές συνήθως διαθέτουν αισθητήρες, κάμερες, συσκευές εντοπισμού GPS, μονάδες επικοινωνίας και ενεργοποιητές τα οποία τοποθετούνται στα οχήματα, σε οδούς, σε υποδομές για την συλλογή και ανταλλαγή δεδομένων σε πραγματικό χρόνο

Εικόνα 9. Έξυπνες μετακινήσεις

Πλεονεκτήματα των έξυπνων συσκευών μεταφοράς

- **Ασφάλεια**
  Τα αυτόνομα συστήματα μεταφορών στα οχήματα και στις υποδομές αποδεδειγμένα μειώνουν τον "ανθρώπινο παράγοντα" στα ατυχήματα καθώς δεν αποσπάται η προσοχή τους μειώνοντας τις πιθανότητες ενός ατυχήματος.

- **Διαχείριση**
  Σημαντική είναι και η διαχείριση των δεδομένων που συλλέγουν οι συσκευές επιτρέποντας στους διαχειριστές να παρακολουθούν καλύτερα τις λειτουργίες, να παρακολουθούν τις ανάγκες συντήρησης και να εντοπίζουν τις βασικές πηγές προβλημάτων που πρέπει να διορθωθούν.

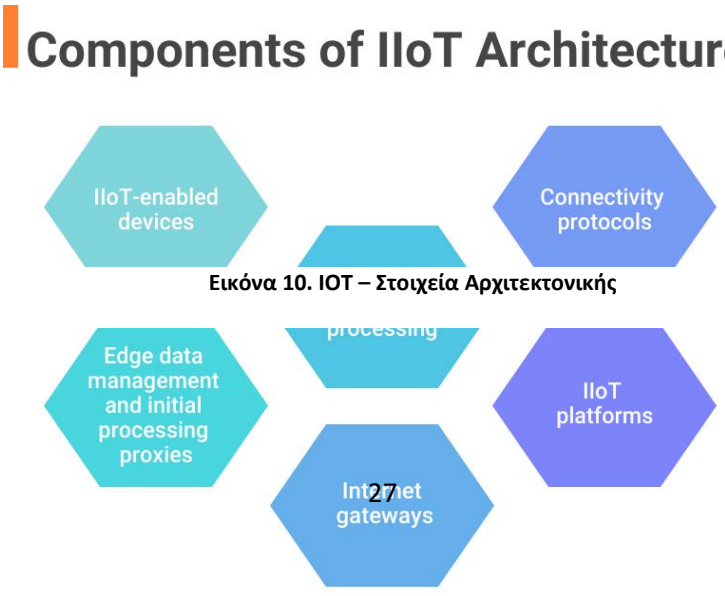
- **Αποτελεσματικότητα**
  Η καλύτερη διαχείριση βοηθάει στην αποδοτικότερη χρήση των μεταφορών εξασφαλίζοντας καλύτερα ποσοστά πληρότητας στα Μέσα Μαζικής Μεταφοράς άρα και καλύτερη εξυπηρέτηση των πολιτών.

- **Οικονομική απόδοση**
  Χάρις στους διαθέσιμους πόρους που χρησιμοποιούν οι έξυπνες μεταφορές μπορεί να μειωθεί το κόστος χάρη στην προληπτική συντήρηση, τη χαμηλότερη κατανάλωση ενέργειας και τους λιγότερους πόρους που χρησιμοποιούνται για ατυχήματα.

- **Ταχύτητα στατιστικών**
  Με τα σύγχρονα κέντρα διαχείρισης της κυκλοφορίας των πόλεων υπάρχει ταχύτητα στις ειδοποιήσεις για τα σημεία προβλημάτων ή τα ζητήματα σε ολόκληρη την πόλη που επηρεάζουν τη συμφόρηση στους δρόμους. [36] [37] [38] [39] [40]

1.6.4 Βιομηχανικό IoT

Με τον όρο Βιομηχανικό διαδίκτυο των πραγμάτων (IIoT) αναφερόμαστε στην χρήση έξυπνων αισθητήρων και μηχανισμών ενεργοποίησης με σκοπό την βελτίωση της παραγωγικότητας και αποδοτικότητας των βιομηχανικών διαδικασιών. Η λογική πίσω από την χρηστικότητας αυτής της λειτουργίας είναι ότι οι έξυπνες συσκευές μπορούν να συλλέγουν και να αναλύουν δεδομένα σε πραγματικό χρόνο πολύ καλύτερα από τον άνθρωπο αλλά τα χρησιμοποιούν για την πιο ακριβή λήψη επιχειρηματικών αποφάσεων. Χρησιμοποιείται κυρίως από εταιρίες αναφέροντας τον ως τον τρόπο που συνδέονται, παρακολουθούν, αναλύουν και ενεργούν με την χρήση των βιομηχανικών δεδομένων. Η General Electric είναι μεταξύ άλλων μία από τους ιδρυτές του



Εικόνα 10. IOT – Στοιχεία Αρχιτεκτονικής

βιομηχανικού διαδικτύου παράγοντας έξυπνες μηχανές για βιομηχανική χρήση παρέχοντας ταχύτερη σύλληψη ανάλυση δεδομένων λαμβάνοντας πιο ακριβής αποφάσεις.

Η αρχιτεκτονική του του βιομηχανικού διαδικτύου των πραγμάτων παρέχει συνδεσιμότητα δικτύου μεταξύ αισθητήρων, συσκευών IoT, συσκευών αποθήκευσης και διάφορων άλλων στρωμάτων. Μια τυπική αρχιτεκτονική περιέχει τα εξής :

- **Συσκευές IoT συνδεδεμένες στις άκρες ενός δικτύου**
  Αναφέρονται σε συσκευές δικτύου ενός οικοσυστήματος IoT. Βασιζόμενοι σε μια κεντρική μονάδα επεξεργασίας ή μια υπολογιστική συσκευή συλλογής δεδομένων όπως κάμερες, αισθητήρες και άλλου είδους οθόνες.

- **Διαχείριση δεδομένων Edge και αρχική επεξεργασία**
  Για την αξιοποίηση της τεχνητής νοημοσύνης είναι απαραίτητα τα δεδομένα υψηλής ποιότητας και όγκου ιδικά σε επίπεδο αισθητήρων για την επεξεργασία δεδομένων.

- **Cloud για προηγμένη επεξεργασία**
  Λόγο της περιορισμένης δυνατότητας των συσκευών IoT να επεξεργάζονται τα δεδομένα είναι σχεδόν βέβαιη η χρήση cloud (hub, Storage, Analytics, A user interface) για καλύτερη και πιο εμπεριστατωμένη επεξεργασία.

- **Internet Gateways**
  Συλλογή δεδομένων από τους αισθητήρες ενός δικτύου για την μετατροπή τους σε ψηφιακή κανάλια αποτελεί μέρος της διαδικασίας μιας πύλης διαδικτύου.

- **Πρωτόκολλα συνδεσιμότητας**
  Απαραίτητα για την μεταφορά δεδομένων είναι τα πρωτόκολλα και στην περίπτωση μιας βιομηχανίας προσαρμοσμένα ανάλογα τις προδιαγραφές που απαιτεί ένα κανάλι δεδομένων. Μερικά από αυτά τα πρωτόκολλα είναι τα εξής : AMQP, MQTT, CoAP

- **Πλατφόρμες IIoT (Βιομηχανικού IoT)**
  Οι πλατφόρμες του IoT είναι υπεύθυνες για την σύνδεση των συσκευών, των δεδομένων και του cloud ελέγχοντας τις διαδικασίες από άκρη σε άκρη σε ένα δίκτυο.

Πλεονεκτήματα του Βιομηχανικού IoT

- **Ενίσχυση αποδοτικότητας**

Η αυτοματοποίηση μιας διαδικασίας σε μια επιχείρηση είναι από τα μεγαλύτερα πλεονεκτήματα του βιομηχανικού IoT διότι μεγιστοποιεί την λειτουργική αποδοτικότητα.

- **Αύξηση παραγωγής**
  Με την αύξηση των συσκευών IoT και των συσκευών δικτύου ενδέχεται να προσφέρει μεγαλύτερη και συνεχή εικόνα αλλά και πληροφορίες σχετικά με την λειτουργία του εξοπλισμού.

- **Μείωση σφαλμάτων**
  Όπως αναφέραμε παραπάνω με την αύξηση των συσκευών μοιραία ωθεί τις εταιρίες σε λιγότερα σφάλματα και μικρότερη έξοδο ελλαττωματικών προϊόντων.

- **Πρόβλεψη των αναγκών συντήρησης**
  Με την ενσωμάτωση αισθητήρων και την καταγραφή δεδομένων από τον χώρο εργασίας (θερμοκρασία, υγρασία κ.α.) αποφεύγονται τα λάθη και αστοχίες προϊόντων, μειώνονται τα έξοδα και οι χρόνοι λειτουργίας των μηχανημάτων.

- **Διατήρηση ασφάλειας των εργαζομένων**
  Οι συσκευές IoT σε μια επιχείρηση βοηθούν στην διατήρηση μιας ομαλής κατάστασης στις γραμμές παραγωγής για ασφαλέστερο εργασιακό περιβάλλον.

- **Εξοικονόμηση κόστους ενέργειας**
  Πλέον οι περισσότερες συσκευές αυτοματοποιούνται με την χρήση αισθητήρων κάνοντας έτσι την παρακολούθηση τους πολύ ευκολότερη καταναλώνοντας λιγότερη ενέργεια και πόρους οπού σε διαφορετική περίπτωση θα ήταν επιζήμια για μια εταιρεία.

- **Βελτίωση των υπηρεσιών πεδίου και της εμπειρίας των πελατών**
  Ο χρόνος και η συμμετοχή του τεχνικού προσωπικού καθορίζει την εξυπηρέτηση και εμπειρία του πελάτη ενημερώνοντας τον για τυχόν κινδύνους και δυσκολίες με σκοπό την θετική εμπειρία. [41] [42] [43] [44]

1.6.5 Έξυπνη Γεωργία

Τα τελευταία χρόνια ο τομέας της γεωργίας έχει υποστεί μια αξιοσημείωτη τεχνολογική εξέλιξη, με την εμφάνιση έξυπνων γεωργικών συσκευών που αλλάζουν τις παραδοσιακές γεωργικές πρακτικές. Οι συσκευές αυτές που βασίζονται στις εξελίξεις του Διαδικτύου των πραγμάτων εγκαινιάζουν μια νέα εποχή αποδοτικών γεωργικών

συσκευών. Με αυτόν τον τρόπο ενσωματώνουν πληροφορίες και δεδομένα φέρνοντας την επανάσταση στον χώρο της γεωργίας από την αρχική φύτευση και την ακριβή άρδευση έως τη συνεχή παρακολούθηση. Με την χρήση αισθητήρων συνδεδεμένων σε ένα δίκτυο υπάρχει η δυνατότητα μέτρησης φυσικών ποσοτήτων (θερμοκρασίας, υγρασίας, φωτός, πίεσης, θορύβου, ταχύτητας, κατεύθυνσης, μεγέθους, βάρους κ.α.) από το περιβάλλον. Επιπλέον οι αισθητήρες αυτοί μετατρέπουν τις μετρήσεις σε σήμα και η ερμηνεία αυτών των σημάτων αποδίδεται μέσα από ένα όργανο. Μερικές από τις τεχνολογίες που χρησιμοποιεί η έξυπνη γεωργία είναι οι εξής :

- Αναλύσεις σε πραγματικό χρόνο
- Μηχανική μάθηση
- Αισθητήρες εμπορευμάτων
- Ενσωματωμένα συστήματα
- Ασύρματα δίκτυα αισθητήρων
- Συστήματα ελέγχου.
- Αυτοματισμοί

Οφέλη χρήσης του IoT στην γεωργία :

- **Κλιματικές συνθήκες**
  Με την κατάλληλη χρήση των αισθητήρων, οι οποίοι μπορούν να τοποθετηθούν σε μια γεωργική περιοχή συλλέγονται τα δεδομένα. Έπειτα από την συλλογή γίνεται η επιλογή των κατάλληλων καλλιεργειών που μπορούν να αναπτυχθούν και να διατηρηθούν στις συγκεκριμένες κλιματικές συνθήκες.

- **Γεωργία ακριβείας**
  Ο στόχος της ακρίβειας στην γεωργία είναι να βοηθά τους αγρότες να παράγουν δεδομένα με τη βοήθεια αισθητήρων και να αναλύουν αυτές τις πληροφορίες για να λαμβάνουν έξυπνες και γρήγορες αποφάσεις, με τεχνικές όπως η διαχείριση της άρδευσης, η διαχείριση του ζωικού κεφαλαίου, η παρακολούθηση των οχημάτων κ.α.

- **Έξυπνο θερμοκήπιο**
  Με την βοήθεια του IoT υπάρχει η δυνατότητα στους μετεωρολογικούς σταθμούς να ρυθμίζουν αυτόματα τις κλιματικές συνθήκες σύμφωνα με ένα συγκεκριμένο σύνολο οδηγιών με στόχο την οικονομική απόδοση και την αύξηση της ακρίβειας.

- **Ανάλυση δεδομένων**

Η αποθήκευση των δεδομένων σε μια διαδικτυακή βάση παίζει σημαντικό ρόλο στην ανάλυση τους. (π.χ. καιρικές συνθήκες, συνθήκες του ζωικού κεφαλαίου, συνθήκες των καλλιεργειών). Με την συγκεκριμένη ανάλυση ο εκάστοτε χρήστης αποκτά μια εικόνα για να μπορεί να λαμβάνει καλύτερες αποφάσεις σχετικά με τη καλλιέργεια του.

2 Έξυπνες συσκευές

2.1 Τι είναι οι έξυπνες συσκευές

Οι έξυπνες συσκευές έχουν αλλάξει τον τρόπο με τον οποίο αλληλεπιδρούμε με την τεχνολογία, προσφέροντας συνδεσιμότητα, αυτοματισμό και ευκολία. Μια έξυπνη συσκευή είναι μια συσκευή ηλεκτρονικά συνδεδεμένη στο διαδίκτυο η οποία μπορεί να χειρίζεται εξ αποστάσεως μέσω κινητού τηλεφώνου, υπολογιστή και άλλων ηλεκτρονικών συσκευών. Οι συσκευές αυτές αξιοποιούν αισθητήρες, επεξεργαστές και ασύρματη επικοινωνία για την συλλογή και ανάλυση δεδομένων με σκοπό την αυτοματοποίηση εργασιών και την αλληλεπίδραση με άλλες συσκευές. Μπορούμε να τις κατηγοριοποιήσουμε σε 3 μεγάλες κατηγορίες : Καταναλωτικές, Επιχειρηματικές, Βιομηχανικές

Παραδείγματα των κατηγοριών:

Wearable devices: Οι συσκευές αυτές συνήθως φοριούνται στον καρπό και περιλαμβάνουν έξυπνα ρολόγια, συσκευές παρακολούθησης φυσικής κατάστασης και υγείας. Τα δεδομένα που συλλέγουν και αναλύουν σχετίζονται με την υγεία και την φυσική κατάσταση.

Smart Entertainment Devices (Έξυπνες συσκευές ψυχαγωγίας): Αυτή η κατηγορία συσκευών περιλαμβάνει τηλεοράσεις, ηχεία, κονσόλες παιχνιδιών κ.α. Οι συγκεκριμένες συσκευές συνδέονται στο διαδίκτυο δίνοντας την δυνατότητα στον χρήστη να μεταδίδει περιεχόμενο πολυμέσων, να έχει πρόσβαση σε δικτυακές υπηρεσίες ελέγχοντας την ψυχαγωγία μέσω του κινητού τηλεφώνου.

Smart Home Appliances (Έξυπνες οικιακές συσκευές): Αφορά κυρίως τις έξυπνες οικιακές συσκευές όπως ψυγεία, πλυντήρια ρούχων, φούρνους, κλιματιστικά οι οποίες προσφέρουν τον εξ αποστάσεως χειρισμό τους αλλά και την παρακολούθηση τους απομακρυσμένα.

Connected Health Devices (Συνδεδεμένες συσκευές υγείας): Περιλαμβάνονται μια σειρά συσκευών στην υγειονομική περίθαλψη συμπεριλαμβανομένων συσκευών απομακρυσμένης παρακολούθησης ασθενών

Smart Lighting Systems (Έξυπνα συστήματα φωτισμού): Περιέχουν συσκευές όπως έξυπνους λαμπτήρες, φωτιστικά σώματα και κόμβους ελέγχου φωτισμού με την δυνατότητα διαχείρισης και αυτοματοποίησης του φωτός, συμπεριλαμβανομένης της φωτεινότητας, του χρώματος και του προγραμματισμού για λόγους ενεργειακής απόδοσης, ατμόσφαιρας και ασφάλειας.

Industrial IoT Devices (Βιομηχανικές συσκευές IoT): Στην συγκεκριμένη κατηγορία υπάγονται συσκευές βιομηχανικών εγκαταστάσεων όπως αισθητήρες, ενεργοποιητές, συστήματα παρακολούθησης και έξυπνα μηχανήματα. Με την βοήθεια αυτών των συσκευών γίνεται η πρόβλεψη λαθών, η προγνωστική συντήρηση, η βελτιστοποίηση διαδικασιών και αποδοτικότητας στις διαδικασίες παραγωγής.

Smart Transportation Devices (Έξυπνες συσκευές μεταφορών): Έξυπνο σύστημα διαχείρισης στόλου και κυκλοφορίας, συσκευή παρακολούθησης οχημάτων και συνδεδεμένα αυτοκίνητα είναι κάποιες από τις εφαρμογές που χρησιμοποιούνται στις μεταφορές προσφέροντας χαρακτηριστικά όπως πλοήγηση GPS, ενημερώσεις κυκλοφορίας σε πραγματικό χρόνο, απομακρυσμένη παρακολούθηση οχημάτων και δυνατότητες αυτόνομης οδήγησης.

Smart Energy Management Devices (Συσκευές έξυπνης διαχείρισης ενέργειας): Οι συγκεκριμένες συσκευές επικεντρώνονται στην παρακολούθηση, στην εξοικονόμηση και στην βελτιστοποίηση της ενέργειας. Η λίστα τους περιλαμβάνει έξυπνους μετρητές, συστήματα παρακολούθησης ενέργειας, έξυπνους θερμοστάτες και τεχνολογίες έξυπνου σπιτιού(smart home).

Smart Agriculture Devices (Έξυπνες γεωργικές συσκευές): Είναι η κατηγορία που περιλαμβάνει αισθητήρες, drones και συστήματα παρακολούθησης στην γεωργία για μεγαλύτερη ακρίβεια. Παρέχουν δεδομένα σε πραγματικό χρόνο σχετικά με τις συνθήκες του εδάφους, την πρόβλεψη του καιρού, την υγεία των καλλιεργειών και τις ανάγκες άρδευσης επιτρέποντας στους αγρότες να βελτιστοποιήσουν τη χρήση των πόρων και να αυξήσουν τις αποδόσεις των καλλιεργειών. [45] [46] [47] [48]

2.2 Ποιες είναι οι λειτουργίες τους

Οι IoT συσκευές έχουν ένα ευρύ φάσμα λειτουργιών που είναι απαραίτητες και καθοριστικές για την δυνατότητα ασταμάτητης συνδεσιμότητας και ανταλλαγής δεδομένων. Από την ανίχνευση και την παρακολούθηση περιβαλλοντικών παραμέτρων, όπως η θερμοκρασία, η υγρασία και η κίνηση ως την ασφαλή επικοινωνία δεδομένων μέσω διάφορων IoT πρωτοκόλλων (Wi-Fi, Bluetooth, Zigbee κ.α.), οι συσκευές IoT είναι κατάλληλα εξοπλισμένες για την μετάδοση σε πραγματικό χρόνο. Παρακάτω θα αναλύσουμε κάποιες από τις λειτουργίες των IoT συσκευών.

- **Ανίχνευση και παρακολούθηση (Detection and tracking)**
  Μια βασική λειτουργία που εκτελείται από τις IoT συσκευές είναι η ανίχνευση και η παρακολούθηση. Εξοπλισμένες με μια σειρά από αισθητήρες οι συσκευές IoT συλλέγουν δεδομένα από το περιβάλλον καταγράφοντας παραμέτρους όπως η θερμοκρασία, η υγρασία, η ένταση του φωτός, η κίνηση και η πίεση.

- **Επικοινωνία δεδομένων (Data Communication)**
  Οι συσκευές IoT βασίζονται σε μεγάλο βαθμό στην αποτελεσματική επικοινωνία δεδομένων για την ανταλλαγή πληροφοριών με άλλες συσκευές ή σε υπηρεσίες cloud. Όντας συνδεδεμένες είτε σε στο διαδίκτυο είτε σε τοπικά δίκτυα χρησιμοποιώντας πρωτόκολλα επικοινωνίας όπως Wi-Fi, Bluetooth, Zigbee, κυψελοειδή δίκτυα ή ethernet, οι συσκευές IoT εξασφαλίζουν ασφαλή και αξιόπιστη μετάδοση δεδομένων.

- **Επεξεργασία και ανάλυση δεδομένων (Data Processing and Analytics)**
  Παρά τους διάφορους υπολογιστικούς περιορισμούς οι συσκευές IoT έχουν την δυνατότητα εκτέλεσης βασικών εργασιών επεξεργασίας δεδομένων. Πριν από την εγκαθίδρυση των βασικών δεδομένων σε κεντρικό κόμβο (router) ή σε μια υπηρεσία cloud οι συσκευές ήταν υπεύθυνες για λειτουργίες όπως το φιλτράρισμα δεδομένων, τη συγκέντρωση δεδομένων αλλά και ανάλυση τους. Με την διεξαγωγή τοπικής επεξεργασίας δεδομένων, οι συσκευές IoT μειώνουν τη χρήση εύρους ζώνης δικτύου και ελαχιστοποιούν την καθυστέρηση, ενισχύοντας τη συνολική αποδοτικότητα του συστήματος.

- **Ενεργοποίηση και έλεγχος (Actuation and Control)**
  Βασική ικανότητα που χαρακτηρίζει τις IoT συσκευές είναι η αλληλεπίδραση τους με τον πραγματικό κόσμο μέσω μηχανισμών ενεργοποίησης και ελέγχου. Περιέχουν εκκινητές, διακόπτες, βαλβίδες, οθόνες και διάφορα άλλα τα οποία ανταποκρίνονται σε οδηγίες που λαμβάνουν με αποτέλεσμα την ανάλυση δεδομένων. Αυτή η ικανότητα επιτρέπει στις συσκευές IoT να ενεργοποιούν συγκεκριμένες ενέργειες ή να ρυθμίζουν την κατάσταση συνδεδεμένων συσκευών ή συστημάτων, προσφέροντας απτό αντίκτυπο σε διάφορες εφαρμογές.

- **Απομακρυσμένη διαχείριση (Remote Management)**
  Αρκετές IoT συσκευές διαθέτουν δυνατότητες απομακρυσμένης διαχείρισης δίνοντας την δυνατότητα στους χρήστες να διαμορφώνουν, να ενημερώνουν το λογισμικό και να αντιμετωπίζουν τα οποιαδήποτε προβλήματα απομακρυσμένα. Με την λειτουργία της απομακρυσμένης διαχείρισης οι συσκευές IoT εκσυγχρονίζουν τις λειτουργίες, ελαχιστοποιούν τον χρόνο διακοπής λειτουργίας και βελτιστοποιούν την απόδοση των συσκευών, και όλα αυτά χωρίς την ανάγκη φυσικής παρέμβασης.

- **Ασφάλεια και πιστοποίηση ταυτότητας (Security and Authentication)**

Υψίστης σημασίας η ασφάλεια των δεδομένων και η διατήρηση του απορρήτου για τις IoT συσκευές τις καθιστά να εφαρμόζουν τεχνικές κρυπτογράφησης με πρωτόκολλα ελέγχου ταυτότητας (PAP), διασφαλίζοντας την ασφαλή μετάδοση δεδομένων και αποτροπή μη εξουσιοδοτημένης πρόσβασης. Ισχυρά μέτρα ασφαλείας όπως η ασφαλής εκκίνηση, η πιστοποίηση ταυτότητας συσκευής και οι μηχανισμοί ελέγχου πρόσβασης διασφαλίζουν την ακεραιότητα των συστημάτων IoT.

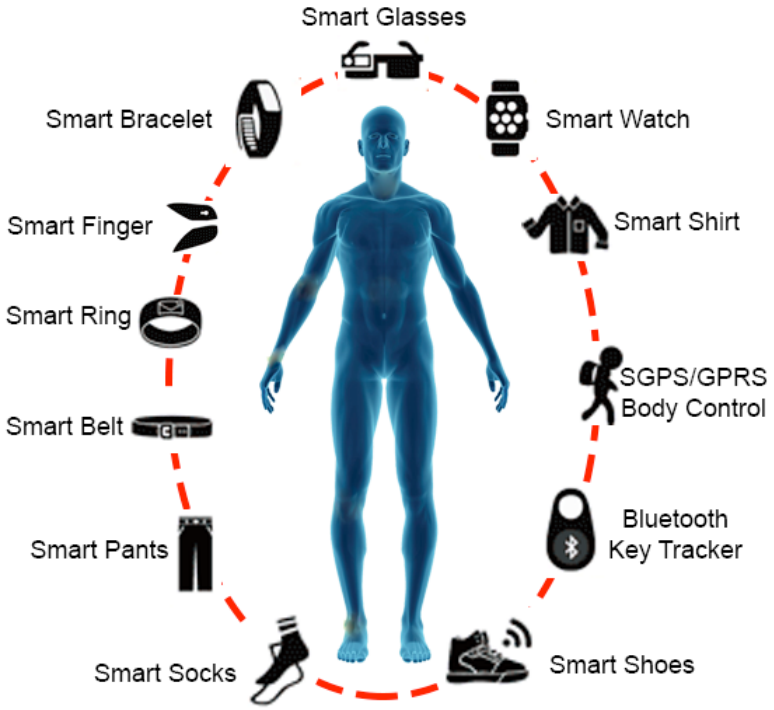
- **Διαχείριση ενέργειας (Energy Management)**
  Με δεδομένο ότι αρκετές συσκευές IoT λειτουργούν με περιορισμένες πηγές ενέργειας ή με κάποιου είδους μπαταρία η αποτελεσματική διαχείριση της ενέργειας είναι απαραίτητη. Οι IoT συσκευές χρησιμοποιούν διάφορες τεχνικές για τη βελτιστοποίηση της κατανάλωσης ενέργειας και την παράταση της διάρκειας ζωής της μπαταρίας, όπως στρατηγικές διαχείρισης ενέργειας, καταστάσεις αναστολής λειτουργίας και μέθοδοι συλλογής ενέργειας. Με την συγκεκριμένη προσέγγιση έχουν φτάσει στο σημείο οι συσκευές IoT να ελαχιστοποιούν την ανάγκη για συχνή επαναφόρτιση ή αντικατάσταση της μπαταρίας. [49] [50] [51] [52] [53] [54] [55] [56] [57] [58]

2.3 Κατηγορίες έξυπνων συσκευών

2.3.1 Φορετές συσκευές (Wearables)

Με τον όρο wearable devices εννοούμε την κάθε ηλεκτρονική συσκευή όπου είναι σχεδιασμένη για να φοριέται στο σώμα του εκάστοτε χρήστη. Μερικές κατηγορίες από αυτές όπως αξεσουάρ, ιατρικές συσκευές, ρούχα ή κάποια στοιχεία από ρούχα είναι παραδείγματα της φορητής τεχνολογίας με πρακτικές και διάφορες χρήσεις που τροφοδοτούνται από μικροεπεξεργαστές και την δυνατότητα επικοινωνίας με το διαδίκτυο.

Η φορητή τεχνολογία περιέχει ένα ευρύ φάσμα συσκευών όπως έξυπνα ρολόγια(smartwatches), γυαλιά εικονικής πραγματικότητας(VR glasses), ζώνες μέτρησης καρδιακών παλμών και διάφορες άλλες τεχνολογίες. Όλες αυτές οι συσκευές λειτουργούν ανάλογα με την κατηγορία στην οποία ανήκουν, συνήθως ενσωματώνοντας μικροεπεξεργαστές, μπαταρίες και συνδεσιμότητα με κάποιο smartphone ή το διαδίκτυο ώστε τα δεδομένα που συλλέγονται να καταγράφονται. Με ενσωματωμένους αισθητήρες που παρακολουθούν τις κινήσεις του σώματος βοηθούν στην παρακολούθηση τοποθεσίας, μέτρηση καρδιακών παλμών, οξυγόνο στο αίμα, επίπεδα γλυκόζης κ.α.



Εικόνα 11. Διαφορετικοί τύποι φορητών τεχνολογιών

Η ιστορία των φορητών συσκευών (wearable devices) ξεκινάει το 1961 με την δημιουργία ενός μικροτσίπ με σκοπό την πρόβλεψη το μέρος που θα προσγειωθεί η μπάλα στην ρουλέτα του καζίνο. Το 1980 η Sony κυκλοφόρησε την πρώτη συσκευή ακουστικών βαρηκοΐας και δέκα χρόνια μετά ο καναδός ερευνητής Steve Mann σχεδίασε την πρώτη ασύρματη web κάμερα. Η δεκαετία του 2000 η φορητή τεχνολογία σημειώνει αύξηση με την εισαγωγή των συσκευών Bluetooth. Από το 2010 και μετά αυτές οι συσκευές μπαίνουν ολοένα στην ζωή μας με πρωτοπόρο την Apple να κάνει ντεμπούτο στα smartwatch και την βιομηχανία των τυχερών παιγνίων να μας παρουσιάζει ακουστικά AR και VR.

Μερικά παραδείγματα wearable devices (φορητών συσκευών):

- **Αισθητήρες τοποθετημένοι στο σώμα (Body-mounted sensors)**
  Οι συγκεκριμένοι αισθητήρες έχουν ως στόχο την συλλογή, την παρακολούθηση και μετάδοση βιολογικών δεδομένων με σκοπό την υγειονομική περίθαλψη.
- **Έξυπνα ρούχα (Smart clothing)**
  Διάφορα έξυπνα ρούχα έχουν την δυνατότητα να μπορούν να εκτελούν διάφορες εργασίες ανάλογα με τα χαρακτηριστικά του υφάσματος που συλλέγουν από το περιβάλλον ή τον χρήστη. Χαρακτηριστικό παράδειγμα η

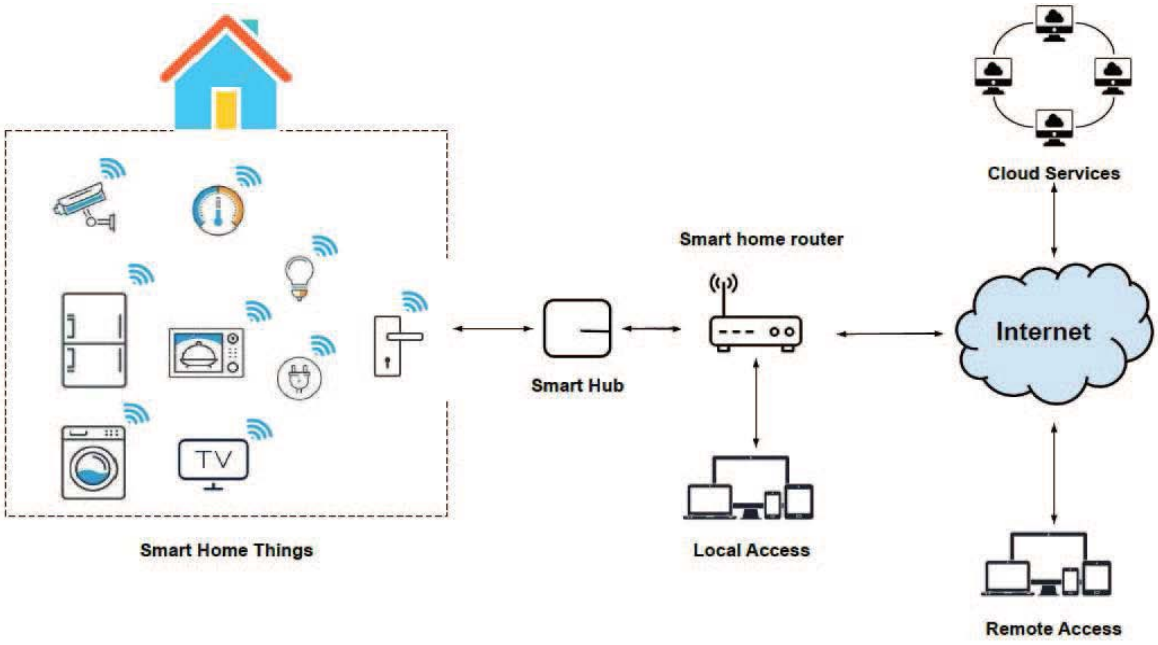
Εικόνα 12. Ένδυση με ηλιακές κυψέλες από την Tommy Hilfiger

γνωστή εταιρία Tommy Hilfiger κυκλοφόρησε ρούχα εξοπλισμένα με ηλιακές κυψέλες για την δυνατότητα φόρτισης συσκευών.

- **Fitness trackers**
  Τις συγκεκριμένες συσκευές τις συναντάμε σε μορφή περικάρπιων ιμάντων όπου παρακολουθούν ζωτικά σημεία σε τυχόν δραστηριότητα συνδεδεμένα με κάποια εφαρμογή για την αποθήκευση των δεδομένων. [59] [60] [61] [62] [63] [64] [65] [66] [67] [68]

2.3.2 Έξυπνες συσκευές ψυχαγωγίας

Στις μέρες μας μπορούμε να απολαμβάνουμε περιεχόμενο από την άνεση του σαλονιού μας με την βοήθεια της τεχνολογίας χάρη στις συσκευές οικιακής ψυχαγωγίας οι οποίες αναπτύσσονται ραγδαία. Ένα έξυπνο οικιακό σύστημα ψυχαγωγίας χρησιμοποιεί τεχνολογίες όπου παρέχουν στον χρήστη μια εμπειρία μοναδική. Συνήθως αποτελείται από την κεντρική μονάδα ελέγχου και όλες οι έξυπνες συσκευές συνδέονται σε αυτήν. Με λίγα λόγια η κεντρική μονάδα(smart hub) λειτουργεί σαν διακομιστής διαθέτοντας μνήμη αποθηκευτικό χώρο και διάφορες επιλογές συνδεσιμότητας.



Εικόνα13. Το μοντέλο EGRBAC για το Smart Home IoT

Υπάρχουν διαφορετικοί τύποι έξυπνων συσκευών ψυχαγωγίας, ακολουθούν με λίγα λόγια μερικοί από αυτοί.

- **Κέντρα πολυμέσων (Media centers)**
  Χρησιμοποιούνται για την αναπαραγωγή περιεχομένου σε κάποια τηλεόραση-οθόνη και επιτρέπουν την αποθήκευση όλων των ψηφιακών μέσων σε αυτά.

Συνήθως διαθέτουν σύνδεση wi-fiγια την αναπαραγωγή περιεχομένου από το διαδίκτυο.

- **Συστήματα οικιακού κινηματογράφου (Home theater system)**
  Τέτοια συστήματα δίνουν την δυνατότητα στον χρήστη να παρομοιάζει την εμπειρία του κινηματογράφου στο σαλόνι του σπιτιού του με τον surround ήχο που προσφέρουν κατάλληλο για κατανάλωση περιεχομένου. Περιλαμβάνουν ηχεία, δέκτη και ίσως κάποια συσκευή ροής ή blu-ray.

- **Ηχόμπαρες (Soundbars)**
  Μια τέτοια "μπάρα" βελτιώνει την ποιότητα του ήχου στην τηλεόραση με επιπλέον ηχεία τοποθετώντας την μπροστά σε αυτή.

- **Ασύρματα ηχεία (Wireless speakers)**
  Επιτρέπουν την χρήση σε οποιοδήποτε μέρος εξαιτίας της ασύρματης τεχνολογίας, μερικά από αυτά διαθέτουν φωνητικές εντολές και συνδεσιμότητα στο διαδίκτυο.
  Στην πραγματικότητα μπορούν να εισαχθούν στην κατηγορία των έξυπνων ηχείων διότι είναι ένας άλλος τύπος έξυπνων συστήματος ψυχαγωγίας με σκοπό την εύκολη μεταφορά του σε οποιοδήποτε μέρος. [69]

2.3.3 Έξυπνες οικιακές συσκευές

Η τεχνολογία εξελίσσεται καθημερινά και οι αυτοματισμοί γίνονται ολοένα πιο συνηθισμένοι, αυτό έχει δημιουργήσει την αύξηση των έξυπνων οικιακών συσκευών σε μεγάλο βαθμό. Η πρώτη ιδέα ξεκίνησε το 1975 με την τεχνολογία των ραδιοσυχνοτήτων για την αποστολή ψηφιακών πληροφοριών μέσω του υπάρχοντος καλωδιακού συστήματος του σπιτιού. Με την εισαγωγή του έξυπνου θερμοστάτη το 2010 πολλές εταιρίες πήραν έμπνευση να δημιουργήσουν έξυπνες συσκευές για την αυτοματοποίηση λειτουργιών ρουτίνας. Στις μέρες μας υπάρχει μια πληθώρα από έξυπνες αυτοματοποιημένες συσκευές έξυπνου σπιτιού όπως έξυπνοι λαμπτήρες, πρίζες, ψυγεία, θερμοστάτες, τηλεοράσεις και ηχεία, κουδούνια και πλήθος άλλων συσκευών.

Μερικά παραδείγματα Έξυπνων οικιακών συσκευών

- **Έξυπνες τηλεοράσεις(Smart Tv's)**
  Μπορούν να συνδεθούν στο διαδίκτυο και έχουν μια πληθώρα εφαρμογών και λειτουργιών όπως αναπαραγωγή βίντεο και μουσικής.

- **Έξυπνοι λαμπτήρες (Smart bulbs)**

Έχουν την δυνατότητα ρύθμισης της θερμότητας αλλά και της έντασης του φωτός απομακρυσμένα με την χρήση του κινητού μας τηλεφώνου.

- **Έξυπνοι θερμοστάτες (Smart thermostats)**
  Διαθέτοντας Wi-fiεπιτρέπουν στον χρήστη να παρακολουθεί και να ρυθμίζει την θερμοκρασία ακόμα και να προγραμματίζει τις ώρες που θα λειτουργεί ο έξυπνος θερμοστάτης, όλα αυτά εξ αποστάσεως παρέχοντας άνεση αλλά και την μέγιστη δυνατή αποδοτικότητα.

- **Έξυπνες κλειδαριές (Smart locks)**
  Προσφέρει πολλές έξυπνες λειτουργίες με την χρήση ενός smartphone

- **Έξυπνες κάμερες ασφαλείας (Smart security cameras)**
  Μειώνει τα θέματα ασφαλείας σε έναν χώρο παρέχοντας λειτουργίες παρακολούθησης και ανίχνευση κίνησης από τυχόν κακόβουλους ή μη εξουσιοδοτημένους χρήστες.

- **Έξυπνες συσκευές ταΐσματος (Smart feeder)**
  Κάνει πολύ πιο εύκολο το τάισμα ενός κατοικίδιου σε περίπτωση απουσίας του ιδιοκτήτη. [70] [71]

2.3.4 Έξυπνα συστήματα φωτισμού

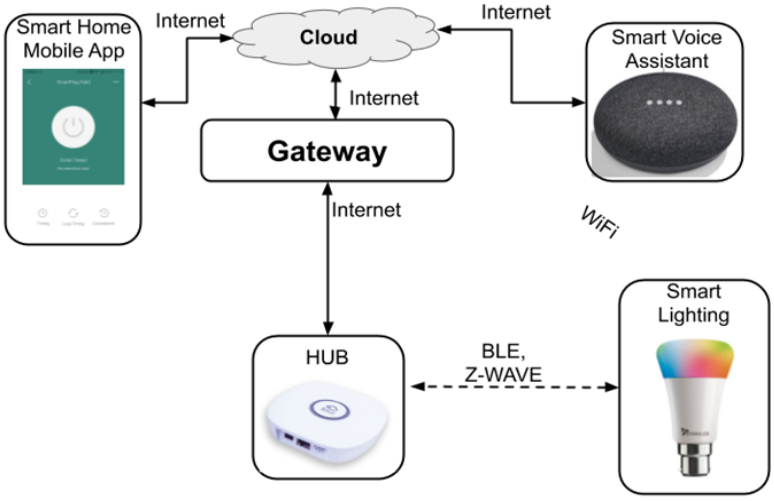
Τα έξυπνα συστήματα φωτισμού ή αλλιώς Smart Lighting Systems (SLSs) χαρακτηρίζονται ως “έξυπνα” προσδιορίζοντας έτσι τον αυτοματισμό και την αποδοτικότητα αυτών των συστημάτων ο οποίος επιτυγχάνεται μέσω της χρήσης τεχνολογίας IOT. Αυτά τα συστήματα αποτελούνται συνήθως από συνδεδεμένα φωτιστικά, αισθητήρες και συσκευές ελέγχου τα οποία οι χρήστες μπορούν να διαχειρίζονται εξ αποστάσεως μέσω smartphone, φωνητικών εντολών ή αυτοματοποιημένων χρονοδιαγραμμάτων. Σύμφωνα με τα χαρακτηριστικά τους χωρίζονται σε διάφορες κατηγορίες.

Η πρώτη κατηγορία αφορά τις “έξυπνες” λάμπες ή αλλιώς “Smart Light Bulbs”. Λάμπες με ασύρματη συνδεσιμότητα, όπως Wi-Fi, ZigBee ή Bluetooth, που επιτρέπουν στον χρήστη τον εξ αποστάσεως έλεγχο. Προσφέρουν επίσης πληθώρα δυνατοτήτων όπως την προσαρμογή της έντασης του φωτός, της χρωματικής απόχρωσης αλλά και την προσαρμογή διάφορων άλλων χαρακτηριστικών προσφέροντας έτσι στον χρήστη καλύτερο έλεγχο. Ο χρήστης έχει επίσης την δυνατότητα να συνδέσει παραπάνω από μια συσκευή στο smartphone του, έχοντας την δυνατότητα να χειρίζεται ταυτόχρονα

διάφορες συσκευές. Παράδειγμα τέτοιας συσκευής αποτελεί η “Mi LED Smart Bulb” της Xiaomi, η “Philips Hue E27” της Philips, και άλλες παρόμοιες συσκευές που χρησιμοποιούν την συγκεκριμένη τεχνολογία.

Μια δεύτερη κατηγορία αφορά τα συστήματα φωτός μέσω της ανίχνευσης κίνησης. Έχουν στόχο να παρακολουθούν και να ελέγχουν τον φωτισμό με διευθέτηση της χρονικής διάρκειας λειτουργίας της λάμπας. Ένα παράδειγμα τέτοιων συστημάτων φωτισμού είναι οι αισθητήρες κίνησης που χρησιμοποιούνται σε δημόσιους χώρους ανιχνεύοντας την ανθρώπινη κίνηση και ενεργοποιώντας με αυτόν τον τρόπο τον φωτισμό. Οι αισθητήρες επικοινωνούν με τους λαμπτήρες δημιουργώντας έτσι ένα αυτόνομο, αυτόματο και αποτελεσματικό σύστημα φωτισμού. Αυτά τα συστήματα όχι μόνο μειώνουν την κατανάλωση ενέργειας, αλλά καταφέρνουν και να περιορίσουν το κόστος συντήρησης καθώς οποιοδήποτε πρόβλημα είναι πιο εύκολο να εντοπιστεί και να διορθωθεί.

Η τρίτη κατηγορία αφορά τα “έξυπνα” φώτα συνδεδεμένα με διανομέα (smart lights connecting with hub). Τα έξυπνα οικιακά συστήματα ενισχύονται με την προσθήκη των έξυπνων φωτισμών τα οποία λειτουργούν με την ίδια τεχνολογία. Αυτές οι συσκευές λειτουργούν ως ενδιάμεσοι μεταξύ των έξυπνων λαμπτήρων και του smartphone ή άλλων συσκευών ελέγχου. Όπως παρουσιάζεται στην παρακάτω εικόνα, ο έξυπνος φωτισμός συνδέεται με το internet μέσω HUB. [72]



Εικόνα 14. Λειτουργία έξυπνου λαμπτήρα που συνδέεται με τον κόμβο

2.3.5 Συνδεδεμένες συσκευές έξυπνης περίθαλψης

Οι συσκευές οι οποίες παρακολουθούν την υγεία ενός ασθενή είναι σύνηθες φαινόμενο στις μέρες μας, μεταδίδοντας δεδομένα ζωτικής σημασίας στον εκάστοτε γιατρό επιτρέπει την παρακολούθηση της υγείας σε πραγματικό χρόνο. Λειτουργίες

όπως η καταγραφή καρδιακών παλμών, οξυγόνο στο αίμα, θερμοκρασία σώματος κ.α. έχουν προστεθεί στα περισσότερα έξυπνα ρολόγια πλέον καθώς όντως αποτελούν ένα στοιχείο μείωσης των ιατρικών δαπανών. Οι συγκεκριμένες συσκευές είναι ποικίλες από καθαρά ιατρική χρήση ως εμφύτευμα μέχρι συσκευές που απευθύνονται στον απλό καταναλωτή. Για την συλλογή των δεδομένων έχει ως βάση το cloud ή κάποια Διασύνδεση Προγραμματισμού Εφαρμογών (API).

- **Smart watches "έξυπνα ρολόγια''**
  Τα ''έξυπνα ρολόγια'' επιτρέπουν την μακροπρόθεσμη εξ αποστάσεως φροντίδα από τους γιατρούς απευθείας στο σπίτι του ασθενή απελευθερώνοντας χώρο για ασθενείς που χρειάζονται περισσότερη και πιο εντατική φροντίδα.
- **Φορητοί βιοαισθητήρες**
  Είναι ένα από τα κομμάτια της τεχνολογίας που θα χρησιμοποιούν τα εικονικά νοσοκομεία για την πρόληψη και ανίχνευση ασθενειών. Πρόκειται για φορητές συσκευές όπου εφαρμόζονται στο σώμα του ασθενή παρακολουθώντας την θερμοκρασία, τους καρδιακούς παλμούς, τους ρυθμούς αναπνοής, παρακολούθηση της αρτηριακής πίεσης κ.α.
- **Έξυπνα θερμόμετρα**
  Μία πρόσφατη τεχνολογία που εξελίχθηκε κατά την διάρκεια της πανδημίας covid-19 ώστε να συλλέγει πληροφορίες ακόμη και σε παγκόσμιο επίπεδο που λήφθηκαν προκειμένου να διαχωρίσει τις συνήθεις επιδημίες και του κοινού κρυολογήματος
- **Συνδεδεμένοι αναπνευστήρες**
  Βοηθούν στην αποφυγή των ασθενών από αναπνευστικές παθήσεις όπως το άσθμα εντοπίζοντας το και προσφέροντας ηχητικές και οπτικές ειδοποιήσεις στον ασθενή για την λήψη της δόσης.
- **Αυτόματο σύστημα χορήγησης ινσουλίνης**
  Απευθύνεται σε άτομα που πάσχουν από διαβήτη αυτοματοποιώντας την διαδικασία δειγματοληψίας αίματος από τον χρήστη αφήνοντας την έξυπνη συσκευή να κρίνει την κατάλληλη στιγμή χορήγησης της.
- **Άτομα της τρίτης ηλικίας**
  Δίνει περισσότερη ανεξαρτησία σε γηραιοτερα άτομα σε μια πιθανή κατάσταση έκτακτης ανάγκης όπως για παράδειγμα μιας πτώσης, μιας αύξησης της πίεσης και της θερμοκρασίας προειδοποιώντας για πιθανά τέτοια σενάρια. [73] [74] [75] [76] [77] [78] [79] [80]

3 Απειλές και προκλήσεις ασφαλείας στις IoT συσκευές

3.1 Τρωτά σημεία ασφάλειας του Διαδικτύου των Πραγμάτων: Μελέτη περίπτωσης του συστήματος Smart Plug.

3.1.1 Μη ασφαλή πρωτόκολλα επικοινωνίας

Καθώς τα πρωτόκολλα επικοινωνίας δεν υποστηρίζονται από τεχνικές κρυπτογράφησης, η ανεπιθύμητη εισβολή ενός κακόβουλου ατόμου θα του παρέχει τη δυνατότητα να αντιγράψει τη ροή δεδομένων του δικτύου και να στρέψει προς την αντίθετη πορεία τα πρωτόκολλα επικοινωνίας. Στην κατάσταση αυτή, το σύστημα υφίσταται ένα σύνολο ποικιλόμορφων εισβολών υποκλοπής.

3.1.2 Έλλειψη αυθεντικοποίησης συσκευής

Ο μακρινός διακομιστής που υποστηρίζεται από μια εφαρμογή που κάνει χρήση βυσμάτων ακροδεκτών κατά την επικοινωνία του, δεν πιστοποιεί τα βύσματα αυτά. Αυτό ισοδυναμεί ουσιαστικά με το άνοιγμα της πύλης για έναν κακόβουλο εισβολέα να πραγματοποιήσει τέσσερις διαφορετικές επιθέσεις.

1) Η κατασκευαστική πρόταση plug της Edimax κάνει χρήση της διεύθυνσης MAC ενός έξυπνου βύσματος ως εξακρίβωση του ακροδέκτη. Μπορούμε λοιπόν χρησιμοποιώντας μια διάταξη σάρωσης να προβούμε σε καταχρηστική επίθεση και να προσπελάσουμε τη βάση δεδομένων των διευθύνσεων MAC του θύματος, προκειμένου να εντοπίσουμε την ενεργή κατάσταση του συνόλου των έξυπνων ακροδεκτών που χρησιμοποιούνται από το ανυποψίαστο θύμα. Η κακόβουλη αυτή ενέργεια σάρωσης της συσκευής είναι σε θέση να φανερώσει, αν οι κάτοχοι κάνουν χρήση του αρχικού κωδικού πρόσβασης του κατασκευαστή ενός βύσματος, λαμβάνοντας υπόψη ότι ένα μεγάλο σύνολο χρηστών δεν προβαίνει σε αλλαγή αρχικού κωδικού πρόσβασης των έξυπνων συσκευών που διαθέτει [3] λόγω απουσίας ενδιαφέροντος σε πρακτικές ασφάλειας.

2) Στην περίπτωση που ο ακροδέκτης είναι σε σύνδεση με τη διάταξη του και δεν έχει πραγματοποιηθεί αλλαγή του κωδικού πρόσβασης, τότε μπορεί να εκτελεστεί απευθείας επίθεση στη συναρμολογημένη διάταξη προκειμένου να αποσπαστούν οι κωδικοί του. Στο σενάριο ενός συνήθη κωδικού πρόσβασης "1234", είναι εύλογο ότι

ένας κάτοχος έχει τη δυνατότητα να τον αλλάξει σε τετραψήφιο, αφού η εταιρεία κατασκευής δεν προβαίνει κατηγορηματικά την πολιτική της για τον κωδικό πρόσβασης στην τεκμηρίωσή του. Ο μακρινός διακομιστής δεν αφαιρεί το δικαίωμα για τις όποιες μεταβολές του κωδικού πρόσβασης κατά τη χρήση από μια εφαρμογή.

3) Στην περίπτωση των κατόχων που κάνουν χρήση κωδικών πρόσβασης με μεγάλο αριθμό ψηφίων, τότε μπορεί να εφαρμοστεί η επίθεση απομίμησης συσκευής, η οποία παραπλανά τους αυθεντικούς ακροδέκτες και προσομοιώνει ότι είναι νόμιμο, αναμένοντας την εφαρμογή από τον απομακρυσμένο διακομιστή να αποστείλει την άδεια ελέγχου αυθεντικότητας ενός κατόχου για τη συνδεσμολογία και τη χρήση του βύσματος. Σε αυτό το είδος της παραβίασης, οι κάτοχοι διαρρέουν τις άδειες ελέγχου αναγνώρισης μόλις ανοίξουν τις αντίστοιχες εφαρμογές του plug. Η επίθεση είναι μη αναγνωρίσιμη και αντιληπτή και οι κάτοχοι τους δύσκολα αντιλαμβάνονται ότι δέχονται κακόβουλη επιδρομή. Με αυτό τον τρόπο ο εισβολέας εργαλειοποιώντας τις παραπλανητικές άδειες εισόδου είναι σε θέση να ελέγξει καθολικά το εργοστασιακό βύσμα.

4) Στη συνέχεια, γίνεται μελέτη της μεθόδου επικαιροποίησης του υλικολογισμικού (firmware) και πραγματοποιείτε επίθεση στο υλικολογισμικό για να μεταφορτωθεί ένα κακόβουλο υλικολογισμικό στον ακροδέκτη. Με μία τέτοια καταχρηστική ενέργεια, ένας εισβολέας είναι σε θέση να προκαλέσει μια αντίστροφη & ύπουλη διαδρομή από τον ακροδέκτη στον επιθυμητό απομακρυσμένο διακομιστή και να αποκτήσει άδεια εισόδου root, στο plug σύστημα. Για μέτρα αντιμετώπισης σε τέτοιου είδους πιθανές παραβιάσεις που αξιοποιούν τις παραπάνω αδυναμίες, γίνεται παρουσίαση των παρακάτω κατευθυντήριων γραμμών για να την προφύλαξη των συστημάτων έξυπνων ακροδεκτών, περιέχοντας επιπλέον την εγγύηση της επικοινωνίας, πρωτόκολλα για την απομόνωση επιθέσεων παραβίασης, αμοιβαία εξακρίβωση ταυτότητας ανάμεσα της εφαρμογής ελέγχου και του σημείου τροφοδοσίας διαμέσου του απομακρυσμένου διακομιστή, σύστημα εξακρίβωσης επιδρομής για τη διερεύνηση μη φυσιολογικής συμπεριφοράς, διατάξεις κατά των bot και επιβεβαίωση της διατήρησης πληρότητας των δεδομένων.

3.2 Μελέτες ευπάθειας και στάσεις ασφάλειας των συσκευών IoT: Μια μελέτη περίπτωσης έξυπνου σπιτιού

3.2.1 Μελέτες τρωτότητας των έξυπνων οικιακών συσκευών

Α. Βιβλιογραφική ανασκόπηση

Στο πρόσφατο παρελθόν έχουν γίνει ενέργειες για την εξακρίβωση αδυναμιών σε συστήματα & διατάξεις IoT στο σύγχρονο χώρο του έξυπνου σπιτιού, όπου διερευνώνται τα κίνητρα ασφαλείας και οι κατηγοριοποιήσεις των κακόβουλων επιθέσεων. Η εργασία κατατάσσει τις καταχρηστικές ενέργειες σε τέσσερις διαφορετικές κατηγορίες: 1) φυσικές 2) δίκτυο, 3) λογισμικό και 4) κρυπτογράφηση. Η παραπάνω κατάταξη των κακόβουλων επιδρομών προσφέρει μια ευρύτερη δυνατότητα για τη διαδικασία παρατήρησης των αδυναμιών.

1) Φυσικές: Στην ομάδα των φυσικών επιθέσεων, το υλικολογισμικό μιας συσκευής - συστήματος IoT υφίσταται επίθεση. Ο εισβολέας οφείλει να κατέχει φυσική πρόσβαση στη συσκευή- σύστημα προκειμένου να εκτελέσει τέτοιου είδους επίθεση. Ορισμένες φυσικές επιθέσεις είναι οι εξής: προσβολή κόμβου(controller) διασύνδεσης του οικιακού router, ανεπιθύμητη διείσδυση ραδιοσυχνοτήτων (RF) σε πιστοποιητικά RF(RFID), κακόβουλες παρενοχλήσεις κόμβων σε ασύρματα δίκτυα αισθητήρων, διείσδυση κακόβουλων κόμβων, φυσική απώλεια, έγχυση κακόβουλου κώδικα.

Utility Categories	Popular Devices
Smart Security Cameras	Amazon Cloud Cam, NetGear Arlo Q, Nest Cam IQ, Wyze Cam Pan
Doorbell Cameras	Google Nest Hello, Ring Video Doorbell, Arlo Audio Doorbell
Smart Locks	Kwikset with Amazon Key, August Smart Lock Pro
Smart Speakers	Amazon Echo, Google Home Max, Apple's HomePod
Smart Hubs	Wink Hub 2, Samsung SmartThings Hub, Google Wifi
Smart Light Bulbs	Philips Hue, GE C-Life Smart Bulbs
Smart Thermostats	Nest Thermostat E, Ecobee4 SmartThermostat
Smart Switches	TP-Link HS200 Smart Wi-Fi Light Switch
Smart Security Systems	SimpleSafe, Ring
Smart Plugs	Belkin WeMo Insight Smart Plug, TP-Link Kasa Smart Wi-Fi Plug, Amazon Smart Plug
Smart Smoke Detectors	Google Nest Protect, Ring Alarm
Smart Appliances	LG Signature Series Refrigerator, Samsung Electric Cooktop, LG TurboSteam Washer and Dryer
Smart Vacuums	iRobot Roomba, Shark IQ Robot, ECOVACS DEEBOT

Εικόνα 15. Οικιακές Συσκευές Iot Ανά Κατηγορία Χρησιμότητας

2) Δίκτυο: Οι καταχρηστικές επιδρομές δικτύου ταξινομούνται με γνώμονα τις επιθέσεις που λαμβάνουν χώρα στο δίκτυο IoT. Σε αυτόν τον τύπο επίθεσης, δεν απαιτείται η φυσική παρουσία του εισβολέα σε απόσταση πλησίον του συστήματος IoT για την υλοποίηση της διείσδυσης. Οι επιθέσεις δικτύου όπως παρουσιάζονται στο [9] αφορούν την ανάλυση της κυκλοφορίας, η παραποίηση RFID, κλωνοποίηση, μη αδειοδοτημένη πρόσβαση, απόρριψη παροχής υπηρεσιών (DoS), πληροφορίες δρομολόγησης και sybil.

3) Λογισμικό: Οι επιθέσεις λογισμικού, που απαντώνται και ως firmware επιθέσεις, αξιοποιούν αδυναμίες που έχουν υπόσταση στο λογισμικό του IoT συστημάτων με τη μορφή κακόβουλου λογισμικού, όπως σκουλήκια, ιοί, κ.λπ. Κάποιες από τις επιθέσεις λογισμικού που έχουν παρουσιαστεί στο [9] είναι το phishing, τα κακόβουλα σενάρια, ο δούρειος ίππος, το spyware, το adware, και DoS που αξιοποιούν υπερχειλίσεις buffer, SQL injections και άλλους τύπους αδυναμιών. Αυτές οι αδυναμίες λογισμικού μπορεί η οντότητα τους να συναντιέται σε διαφορετικά επίπεδα μέσα στις τοπολογίες των

έξυπνων κατοικιών καθώς και στις υπηρεσίες cloud. Σε ένα επίπεδο συγκεκριμένης συσκευής, μια αδυναμία λογισμικού αφορά μια μεμονωμένη συσκευή. Σε ανώτερο επίπεδο όμως, όπως ελέγχου κόμβου, μια αστοχία λογισμικού επηρεάζει ολόκληρο τον κόμβο ελέγχου όπως για παράδειγμα το Smart Things της Samsung, το οποίο συντελεί πιθανότατα στον τρόπο λειτουργίας όλων των συσκευών που είναι συνδεδεμένες σε αυτόν τον κόμβο. Μια αδυναμία στο λογισμικό της υπηρεσίας cloud δεν επιδρά μόνο στις έξυπνες συσκευές που είναι σε σύνδεση στην υπηρεσία cloud, αλλά καθολικά σε όλα τα συστήματα και τις διατάξεις που δικτυώνονται σε αυτή την υπηρεσία νέφους.

4) Κρυπτογράφηση: Η τελευταία μορφή επιθέσεων αφορά αυτής της κρυπτογράφησης. Οι επιθέσεις κρυπτογράφησης συντελούνται όταν ένας εισβολέας καταστρατηγεί την τεχνική κρυπτογράφησης που κάνει χρήση ένα σύστημα IoT. Οι Costaetal μελέτησαν σε βάθος αδυναμίες κρυπτογράφησης σε συστήματα IoT. Λόγω του ότι συσκευές IoT έχουν μειωμένη υπολογιστική ισχύ για την υποστήριξη ισχυρών κρυπτογραφικών πρωτοκόλλων, είναι αθωράκιστες στο πλευρικό κανάλι, την κρυπτανάλυση και τις σε επιθέσεις man-in-the-middle [9].

Β. Επισκόπηση μελετών ευπάθειας

Στην εικόνα 16 εμφανίζεται η αξιολόγηση των μελετών έρευνας έχοντας υπόψη τις προαναφερθείσες τέσσερις κατηγορίες αδυναμίας στην ασφάλεια του IoT, δηλ. φυσική, δίκτυο, λογισμικό και κρυπτογράφηση.

Utility Categories	Physical	Network	Software	Encryption	Specific Devices	Study Source
Smart Security Cameras	No Studies Found	Man-in-the-Middle attacks	Cross-site request forgery Cross-site scripting Hard-coded credentials	Information disclosure Hard-coded credentials Man-in-the-Middle attacks Unprotected communication	TRENDnet IP-connected camera AvTech camera CCTV camera	[39-42, 61]
Smart Light Bulbs	No Studies Found	Man-in-the-Middle attacks	No required authentication	Unprotected communication No required authentication Man-in-the-Middle attacks	Philips Hue smart light bulbs JB Smart Bulb Hao Deng Smart Bulb TP-Link Smart LED Light Bulb	[36, 40, 43-48, 50]
Smart Thermostat	Exposed access Board level exploitation Chip level exploitation	Deduce Wi-Fi network passwords	Exposed cross device access Information disclosure USB booting capability	Deduce Wi-Fi network passwords USB booting capability	Google Nest Thermostat Nest Learning Thermostat - 2nd Generation (T200577) Honeywell 7 Day Programmable Wi-Fi Thermostat (RTH6580WF)	[40, 51-55]

Εικόνα 16. Αξιολόγηση Των Γνωστών Μελετών Ευπάθειας Των Έξυπνων Οικιακών Συσκευών

3.2.2 Αξιολόγηση των γνωστών μελετών ευπάθειας των έξυπνων οικιακών συσκευών

Η αξιολόγηση που έλαβε χώρα επάνω σε εργασίες αδυναμίας, στηρίχθηκε με την αναζήτηση βιβλιογραφίας που είχε ως θέμα ερευνητικές μελέτες με τρωτά σημεία ασφαλείας συστημάτων IoT. Οι λέξεις-κλειδιά που χρησιμοποιήθηκαν στις αναζητήσεις αφορούσαν κατηγορίες κοινής ωφέλειας, είδη στοχευμένων συσκευών έξυπνου σπιτιού, κατηγορίες ευπάθειας, κατασκευαστές IoT, είδη επιθέσεων. Τα εργαλεία αναζήτησης αφορούσαν πολλαπλές πηγές (π.χ. Google Scholar και IEEE) και κλάδους. Τα κριτήριά που τέθηκαν στις αναζητήσεις ήταν τα εξής:

1) Εντοπισμός τουλάχιστον πέντε δημοσιεύσεων σε κάθε κατηγορία χρήσης από την εικόνα 16.

2) Η πρώτη αναζήτηση αφορούσε στη βάση δεδομένων Google Scholar. Όταν δεν εντοπίστηκαν οι επιθυμητές δημοσιεύσεις ανά κατηγορία χρήσης στη Google Scholar, η αναζήτηση πραγματοποιήθηκε σε άλλες βάσεις δεδομένων. Αυτές που επιλέχθηκαν ήταν οι IEEE, ACM, Science Direct και Springer Link.

3) Επιλογή εργασιών μεταξύ 2010 και 2019.

4) Εντοπισμός λέξεων-κλειδιών υπηρετώντας συγκεκριμένα μοτίβα: κάθε χρησιμότητα κατηγορία + "αδυναμία" (π.χ. "έξυπνες κάμερες ασφαλείας vulnerability"), κάθε κατηγοριοποίηση αδυναμίας +"σε έξυπνα σπίτια" (π.χ. "ευπάθεια δικτύου σε έξυπνα σπίτια"), και μια συγκεκριμένη συσκευή + τρωτότητα ("Google Home Mini τρωτότητα ").Έγινε μελέτη κάθε άρθρου προκειμένου να εντοπιστούν τι είδους τρωτότητες βρέθηκαν σε μεμονωμένες συσκευές, όταν υπήρχαν. Το είδος των επιθέσεων τρωτότητας που εντοπίστηκαν σε κάθε κατηγορία χρήσης στις μελέτες που έγιναν προστέθηκαν στον εικόνα 16, και όταν δεν εντοπιζόταν ένα είδος επίθεσης, η ένδειξη "Δεν βρέθηκαν μελέτες" αναγραφόταν στον πίνακα για το συγκεκριμένο κριτήριο. Οι βιβλιογραφικές αναφορές κάθε μελέτης τρωτότητας τεκμηριωνόταν στην τελευταία στήλη. Έγινε επανάληψη κάθε βήματος για κάθε κατηγορία χρήσης. Η ανακεφαλαίωση των μελετών τρωτότητας των έξυπνων συσκευών που εμφανίζονται στην εικόνα 16, έδωσε μια ευρεία αξιολόγηση των πρόσφατων ερευνών στο πλαίσιο των τεσσάρων κατηγοριών ευπάθειας ασφαλείας του IoT. Διαπιστώνεται ένα κενό στην βιβλιογραφία σε ότι αφορά προγενέστερες μελέτες, καθώς δεν εμφανίζονται ολοκληρωμένες ώστε να αναπληρώνουν τους διάφορους τύπους συσκευών IoT και τους δημιουργούς που τις κατασκευάζουν.

1) Περιορισμοί της έρευνας: Η έρευνα αρκέστηκε σε ερευνητικές δημοσιεύσεις που εντοπίσαμε. Μία ομάδα ερευνητών στον τομέα της ασφάλειας δημοσίευσαν τις μελέτες τους για τις αδυναμίες μέσω ιστολογίου, φόρουμ, και άλλα είδη μέσων ενημέρωσης. Η βιβλιογραφία που εξετάσθηκε δεν συγκρίνει συγκεκριμένους γνωστούς κατασκευαστές έναντι λιγότερο γνωστών κατασκευαστών με κριτήριο τις διαπιστωθείσες τρωτότητες. Όμοια, η έρευνα δεν παρείχε πληροφορίες για τον χαρακτηρισμό αν οι στάσεις ασφαλείας διαφέρουν μεταξύ γνωστών και λιγότερο γνωστών συσκευών και κατασκευαστών. [28] [81]

4 Μελέτη περίπτωσης δοκιμών διείσδυσης σε έξυπνες καταναλωτικές συσκευές IoT

4.1 Μελέτη περίπτωσης ψηφιακών βοηθών

Είναι πλέον γεγονός πως από το 2018 και μετά, ολοένα και περισσότερες συσκευές οικιακών ψηφιακών φωνητικών βοηθών (HDVA) παίρνουν τη θέση τους στα σπίτια του αναπτυσσόμενου κόσμου. Σύμφωνα με προβλέψεις που έχουν δει το φως της δημοσιότητας, ο πληθυσμός τους προβλέπεται να αυξηθεί δεκατρείς φορές από το 2020 (1,1 εκατομμύρια) έως το 2025 (15,1 εκατομμύρια), με μια τάση ρυθμού ανάπτυξης ανά έτος 54.74%. Εξαιτίας των επίμονων προσπαθειών των μεγαλύτερων παραγωγών συσκευών HDVA (π.χ. Amazon και Google) και τους δημιουργούς λογισμικού φωνητικών υπηρεσιών για λογαριασμό τρίτων (όπως CapitalOne, Dominos, Honeywell) οι χρήστες διαθέτουν τη δυνατότητα να πραγματοποιούν έναν σημαντικό αριθμό υπηρεσιών κάνοντας χρήση φωνητικών εντολών.

Η παλέτα των υπηρεσιών αυτών περιλαμβάνει αναπαραγωγή μουσικής, παραγγελία έτοιμου φαγητού, αγορές & πωλήσεις μέσω διαδικτύου, επαναπρογραμματισμό εκδηλώσεων & ραντεβού, ενημέρωση μετεωρολογικών προβλέψεων, την πραγματοποίηση οικονομικών συναλλαγών, τον έλεγχο έξυπνων συσκευών (π.χ. γκαραζόπορτες, πρίζες, θερμοστάτες), ένα μικρό σύνολο από αυτές. Για την ευελιξία της χρήσης και το σύνολο των χρηστών, στην πλειονότητα των συσκευών HDVA (π.χ. Amazon Echo, Google Home) γίνεται υιοθέτηση ενός μηχανισμού συνεχόμενης ακρόασης ο οποίος είναι ο αποδέκτης φωνητικών εντολών σε διάρκεια.

Ειδικότερα, οι χρήστες δεν είναι απαραίτητο να έχουν πατημένο και κρατημένο ταυτόχρονα ένα μηχανικό κουμπί στις συσκευές τους πριν εκφέρουν τις εντολές. Το παραπάνω αποτελεί ειδοποιός διαφορά ανάμεσα των HDVA και των τηλεφωνικών βοηθών. Οι τηλεφωνικοί υποστηρικτές μετακινούνται μαζί με τους χρήστες και δέχονται αποκλειστικά φωνητικές εντολές αφού ξεκλειδώσουν τις τηλεφωνικές συσκευές. Τέτοιου είδους παροχές όμως μπορεί να είναι σε θέση να εκθέσουν τους χρήστες σε κινδύνους ασφαλείας λόγω της ελεύθερης φύσης των φωνητικών καναλιών.

Με αυτό τον τρόπο γίνεται αντιληπτό ότι το απαραβίαστο των HDVA οφείλει να ερευνηθεί ιδιαίτερα. Ένα ερώτημα που μπορεί να τοποθετηθεί στο σημείο αυτό είναι το εξής: Το σύνολο αυτών των εμπορικά διαθέσιμων συσκευών (COTS) HDVA κάνουν χρήση όλων των απαραίτητων δικλίδων ασφαλείας για την επαλήθευση ταυτότητας των χρηστών και την ασφάλεια τους από ακουστικές επιθέσεις; Όπως θα αναφερθεί στη συνέχεια της εργασίας σε ότι αφορά την Amazon Alexa και την Google Home η απάντηση είναι αρνητική. Σε τρεις παράγοντες ασφαλείας πραγματοποιείτε η ανεύρεση τρωτών σημείων από αυτούς και γίνεται η επινόηση δύο αποδεικτικών – υποτιθέμενων επιθέσεων. Μία συνήθης παραβίαση της ασφάλειας στο οικιακό περιβάλλον αποτελούν οι επιθέσε**ις** με ψεύτικες παραγγελίες.

Όλα τα εμπλεκόμενα μέρη, όπως οι πάροχοι HDVA υπηρεσιών (π.χ. Amazon), τα τεχνουργήματα HDVA και οι δημιουργοί φωνητικών υπηρεσιών, θα πρέπει να επιμεριστούν την ευθύνη. Οι κατασκευαστές και πάροχοι των Alexa και Google Home κάνουν χρήση ενός μοναδικού παράγοντα και μεθόδου επαλήθευσης ταυτότητας που έχει ως δεδομένο μια λεκτική αναφώνηση που προσομοιάζει με κωδικό πρόσβασης(π.χ. "Alexa", "Γεια σου, Google"). Για οποιοδήποτε άτομο ή μηχανή αναπαραγωγής που εκφέρει την επιλεγμένη λέξη επαλήθευσης ταυτότητας πριν από μια φωνητική εντολή, η λέξη επαλήθευσης ταυτότητας γίνεται αποδεκτή και εκτελέσιμη από τις συσκευές HDVA.

Οι ψηφιακοί φωνητικοί βοηθοί εκτελούν εντολές ήχου – φωνής δίχως να συνδέεται η λειτουργία τους από το αν οποιαδήποτε άτομο είναι στο πολύ κοντινό περιβάλλον. Ενεργοποιούνται για κάθε ήχο του οποίου το επίπεδο ακουστικής πίεσης (SPL) είναι υψηλότερο από τη στάθμη των 60dB. Επιπλέον, δεν πραγματοποιείτε έλεγχος εισόδου σε έξυπνες συσκευές Alexa, καθώς οι κατασκευάστριες εταιρίες θεωρούν ότι όλες οι φωνητικές εκχωρήσεις από την υπηρεσία Alexa είναι αβλαβείς. Κατά συνέπεια, είναι απροστάτευτες σε κινδύνους ασφαλείας από τη στιγμή που δύναται να λάβουν χώρα τεχνητά υποκατάστατα φωνητικών εντολών μέσω της υπηρεσίας Alexa.

Ως εκ τούτου, η λύση φαντάζει να είναι απλοϊκή. Οι ψηφιακοί φωνητικοί βοηθοί θα επιβεβαιώνουν τους κατόχους - χρήστες με τη βιομετρική σφραγίδα της φωνής τους

πρωτού δεχθούν φωνητικές εντολές. Εν τούτοις, σε επόμενη σκέψη, το παραπάνω μπορεί να μην είναι υλοποιήσιμη υπόθεση για τους εξής δύο λόγους. Πρώτον, η χροιά των φωνών των χρηστών μπορεί να ποικίλλει αντίστοιχα με την ηλικία, την κατάσταση υγείας ή την σωματική κατάσταση. Δεύτερον, η ανθρώπινη φωνή είναι ευπρόσβλητη σε εφορμήσεις επανάληψης. Ορισμένες προγενέστερες έρευνες έχουν προτείνει την χρήση κινητών συσκευών για την αυθεντικοποίηση των χρηστών. Για παράδειγμα, μια πρόταση παρουσιάζει μια ιδιωτική φορητή συσκευή η οποία παρακολουθεί & καταγράφει τις μικροδονήσεις του δέρματος των χρηστών.

Ακολούθως, οι μικροδονήσεις που παράγονται και καταγράφονται συνεχώς, αντιπαραβάλλονται με τα φωνητικά σήματα που λαμβάνονται από τους ψηφιακούς φωνητικούς βοηθούς. Στην παραπάνω τεχνική όμως ελλοχεύει ότι οι χρήστες μπορεί να εμφανίσουν απροθυμία να φορούν αυτό το μηχανισμό στο χώρο τους καθ όλη την παραμονή τους σε αυτόν. Μια προτεινόμενη λύση είναι οι χρήστες να πατήσουν ένα φυσικό κουμπί για τη άμεση εκκίνηση των συσκευών Alexa πριν την εκμετάλλευση υπηρεσίας τους. Κατά συνέπεια, το ουσιαστικό κίνητρο για τη διαχείριση των προηγουμένων, είναι το πώς να κατοχυρωθούν με τον κατάλληλο τρόπο οι ψηφιακοί φωνητικοί βοηθοί χωρίς να στοχοποιηθεί ο εκάστοτε χρήστης, ή να μειωθεί η ευκολία τους προσθέτοντας επιπλέον κόστος ανάπτυξης.

Μετά από ενδελεχή μελέτη της ευαισθησίας ασφάλειας που μελετήθηκε, έγινε αντιληπτό ότι οι επιθέσεις ακουστικού τρόπου, πραγματοποιούνται στην πλειοψηφία ενώ οι χρήστες απουσιάζουν από το σπίτι – ενώ στον αντίποδα, αυτές οι φωνητικές – ηχητικές επιθέσεις θα γίνονταν αισθητές από τα θύματα. Στην περίπτωση που οι ψηφιακοί φωνητικοί βοηθοί σταματούσαν να λάμβαναν φωνητικές εντολές όταν δεν υπάρχουν στον περιβάλλοντα χώρο άνθρωποι, οι κακόβουλες ακουστικές εντολές των δολιοφθορέων δεν θα γίνονταν αποδεκτές. Έτσι στο σκεπτικό αυτό, η προτεινόμενη πρόταση είναι η ανάπτυξη μιας εικονικής ασφάλειας Button (VSButton) στους ψηφιακούς φωνητικούς βοηθούς. Τα VSButton αναμορφώνουν την υποδομή COTS(**C**ommercial **O**ff-**T**he-**S**helf)WiFi που βρίσκει εφαρμογή στο νέο έξυπνο οικιακό περιβάλλον για την εξακρίβωση μικροσκοπικών ανθρώπινων κινήσεων στους εντός χώρους (π.χ. κινήσεις του χεριού).

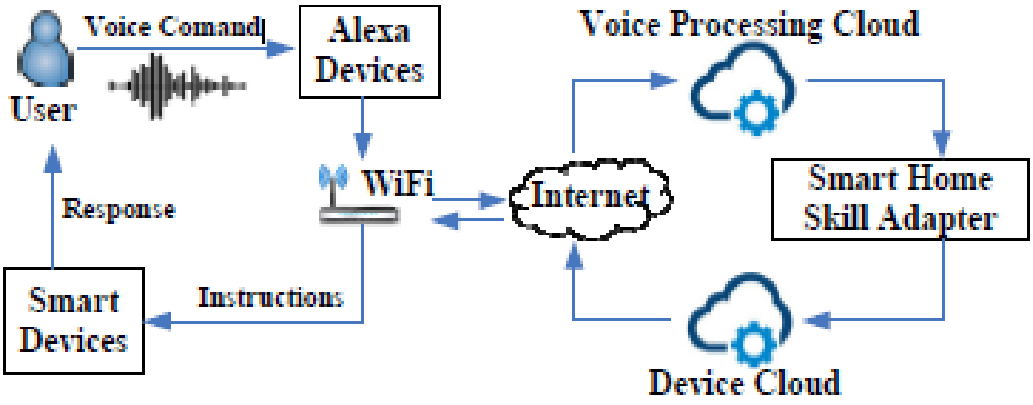
Μόλις γίνει εντοπισμός κινήσεων στο εσωτερικό περιβάλλοντα χώρο, το εικονικό κουμπί θα θέτει σε λειτουργία το μικρόφωνο των ψηφιακών φωνητικών βοηθών ώστε να δέχεται ακουστικές εντολές για ένα χρονικό διάστημα (π.χ.1λεπτό). Τα πειραματικά παραδοτέα καταδεικνύουν ότι το VSButton μπορεί να διακρίνει με μεγάλη συνέπεια τις κινήσεις στο εσωτερικό οικιακό περιβάλλον από τις περιπτώσεις απουσίας κινήσεων καθώς και εξωτερικών κινήσεων. Εξαιτίας της συγγένειας - ομοιότητας των δύο κύριων εκπροσώπων των ψηφιακών φωνητικών βοηθών, αυτών της Amazon Alexa και του Google Home,η παρουσίαση που θα ακολουθήσει αφορά της πρώτης, η οποία τυγχάνει μεγάλης εμπορικής αποδοχής. Όλα τα παραδοτέα όμως μπορούν να εφαρμοστούν και στις δύο διαθέσιμες προτάσεις, αφ εταίρου αν διευκρινίζεται επιμέρους.

Με λίγα λόγια, η συγκεκριμένη εργασία συμβάλει σε τρία σημεία ενδιαφέροντος:

1) Φανερώνονται τρία ευαίσθητα σημεία των ψηφιακών φωνητικών βοηθών έναντι φωνητικών επιθέσεων. Οι πάροχοι ακουστικών υπηρεσιών των ψηφιακών φωνητικών βοηθών κάνουν χρήση μονάχα ενός απλού & ασθενικού ελέγχου εξακρίβωσης ενός παράγοντα για τους χρήστες τους. Με αυτό τον τρόπο οι υπηρεσίες φωνής δεν διαθέτουν έλεγχο εισόδου με γνώμονα τη φυσική ύπαρξη. Απόρροια των παραπάνω γίνεται αντιληπτό πως οι προγραμματιστές παραγωγής φωνητικών υπηρεσιών HDVA δεν επιβάλλουν δικλείδες ασφαλείας στις διασυνδεδεμένες συσκευές τους. Έτσι γίνεται η επινόηση δύο προσβολών (όπως, παραβίαση σπιτιού και ψευδής παραγγελία) με βάση τις αδυναμίες που εντοπίστηκαν.

2) Γίνεται σχεδίαση και ανάπτυξη ενός προτεινόμενου μηχανισμού ασφαλείας (Virtual Security Button) ο οποίος θα αναβαθμίσει την ασφάλεια των φωνητικών υπηρεσιών HDVAδίχως να κάνει εκπτώσεις στην ευκολία του χρήστη. Από την αξιολόγηση των παραδοτέων φάνηκε πως οι ισχνές ανθρώπινες κινήσεις στο εσωτερικό οικιακό περιβάλλον (π.χ. κούνημα του χεριού) είναι ικανές να διεγείρουν τις HDVA συσκευές, σε αντιδιαστολή με τις μεγάλες κινήσεις σε εξωτερικούς χώρους (π.χ. άλμα) όπου δεν ενεργοποιούνται. Η προτεινόμενη λύση δύναται να λάβει χώρα ολιστικά σε όλους τους οικιακούς ψηφιακούς φωνητικούς βοηθούς με συγκεκριμένες κατά περίπτωση αναβαθμίσεις λογισμικού.

3) Συγκρινόμενη η πρόταση με προγενέστερες τεχνικές χειρονομιών και κινήσεων που υποστηρίζονται με WiFi αναγνώριση, το VSButton είναι σχεδιασμένο για να διαχωρίζει εσωτερικές και εξωτερικές κινήσεις, και να διαθέτει προσαρμοστικότητα σε μεταβολές του περιβάλλοντος. Πραγματοποιείται εισαγωγή δύο νέων διαδικασιών για την ολοκλήρωση τους. Πρώτον, πολλαπλασιάζει τους αντίκτυπους των κινήσεων στους εσωτερικούς χώρους, πραγματοποιώντας επιλεκτική δειγματοληψία στις κύριες συνιστώσες (βλ. ενότητα IV). Δεύτερον, πραγματοποιεί δυναμική προσαρμογή στις κύριες γραμμές CSI, οι οποίες υπάρχουν για να επισημαίνουν τις συνθήκες ανυπαρξίας κίνησης σε εσωτερικό οικιακό χώρο, σε διαφορετικά περιβάλλοντα κατά την εξέλιξη του χρόνου. Επομένως, δεν είναι αναγκαία οποιαδήποτε παραμετροποίηση από τη πλευρά του χρήστη για μεταβολές στο περιβάλλον, παρά μονάχα η αρχική ρύθμιση κατά την τοποθέτηση της συσκευής στο προβλεπόμενο χώρο. Και οι δύο προτεινόμενες τοπολογίες απουσιάζουν από τις προγενέστερες περιπτώσεις.



Εικόνα 17. Τρόπος λειτουργίας του ψηφιακού βοηθού Alexa.

Οι χρήστες των συσκευών Alexa, έχουν τη δυνατότητα ελέγχου έξυπνων συσκευών που διασυνδέονται με αυτές, προσφωνώντας φωνητικές εντολές άνοιξε πόρτα, λέγοντας και τα ονόματα τους(όπως π.χ. η πόρτα μου). Οι κατασκευαστές ψηφιακών φωνητικών βοηθών δίνουν τη δυνατότητα παραμετροποίησης των φωνητικών εντολών από τους χρήστες σύμφωνα με τις προσωπικές τους προτιμήσεις, κάτι όμως που δεν είναι υποχρεωτικό να συμβεί.

Εφόσον το πλήθος των ακουστικών που στέλνονται από τους ψηφιακούς φωνητικούς βοηθούς συγκεντρώνονται στο νέφος που είναι συνδεδεμένοι, οι όποιες κακόβουλες εντολές που προερχόμενες από αυτές, μοιραία διαμοιράζονται στο σύνολο τους αφού η διάδοση είναι αναπόφευκτη. Έτσι αυτή η αδυναμία ισχυρής ταυτοποίησης της πρόσβασης των χρηστών μεγεθύνει τη συνολική ευπάθεια των ψηφιακών βοηθών.

Επικύρωση

Για την επιβεβαίωση της προαναφερθείσας αδυναμίας, δοκιμάζουμε ένα σύνολο ευφυών συσκευών του εμπορίου που διαθέτουν τη δυνατότητα επικοινωνίας με την Alexa, για να εξετάσουμε εάν εκτελούν τις υπηρεσίες που επιθυμούμε σύμφωνα με το εργοστασιακό ρεπερτόριο εντολών. Έτσι κάποιες συσκευές που επιλέχθηκαν ήταν το γκαράζ, η έξυπνη πρίζα, ο έξυπνος διακόπτης.

Επιθέσεις

Στο σημείο αυτό σχεδιάστηκαν δύο παραβιάσεις που σχετίζονται με την ευπάθεια των εργοστασιακών εντολών της Alexa. Μια ψευδή παραγγελία και μια διάρρηξη σπιτιού. Πριν την έναρξη των επιθέσεων, θα πρέπει να γίνει διασπορά του κακοήθους μολυσμένου λογισμικού, προκειμένου να εντοπιστούν οι συσκευές «θύματα» Alexa που θα λειτουργήσουν με καταχρηστικό τρόπο σε βάρος των ιδιοκτητών τους, χωρίς τη φυσική παρουσία των χρηστών. Θα πρέπει να επισημανθεί πως δεν υπάρχει στοχευμένη επίθεση στο παραπάνω σενάριο, παρά μονάχα η ανίχνευση ευάλωτων συσκευών για την επικύρωση της αδυναμίας του ρεπερτορίου εντολών των εργοστασιακών ρυθμίσεων. Αν και το καταγεγραμμένο ποσοστό επιθέσεων σε συσκευές Alexa παραμένει παγκόσμια χαμηλό, αυτό όμως δε σημαίνει πως ο κίνδυνος πραγματοποίησης δόλιων ενεργειών με αχαρτογράφητες συνέπειες δεν είναι υπαρκτός.

Προτού γίνει η παρουσίαση των δύο εισβολών, θα επιχειρηθεί η απάντηση δύο ερωτημάτων που απορρέουν από το σενάριο.

1ο Ερώτημα: Με ποιόν μηχανισμό κάποιος μπορεί να καταχραστεί μια συσκευή Alexa δίχως να βρίσκεται πλησίον της;

2ο Ερώτημα: Πως είναι δυνατόν να ανιχνευθούν τα πιθανά θύματα που θα δεχθούν το μολυσμένο λογισμικό;

Ακολουθούν δύο περιπτώσεις που απαντούν στα δύο προαναφερθέντα ερωτήματα για να γίνει αντιληπτό πόσο πραγματοποιήσιμες είναι οι παραβιάσεις των συσκευών Alexa.

1η Περίπτωση: Ακουστική επίθεση στην συσκευή Alexa, δίχως αυτή να βρίσκεται πλησίον του δράστη.

Αυτό το σενάριο μπορεί να συμβεί όταν στο ίδιο χώρο συνυπάρχουν συσκευές αναπαραγωγής (π.χ. ραδιόφωνο ή μεγάφωνα κινδύνου στο εσωτερικό των κτηρίων). Η πιο δημοφιλή μέθοδος είναι με ένα ηχείο Bluetooth όπου ο δράστης με τη βοήθεια του έξυπνου κινητού του, συνδέεται σε αυτό και στη συνέχεια, πραγματοποιεί αναπαραγωγή φωνητικών εντολών προς το ψηφιακό βοηθό. Στο πείραμα επιβεβαίωσης ένα τηλέφωνο iphone και ένα ηχείο Bluetooth της Belkin. Το σύστημα της Alexa ανταποκρίθηκε στις εντολές που έλαβε από το ηχείο και έδωσε τις ανάλογες απαντήσεις. Επίσης μια έξυπνη τηλεόραση μπορεί να αναπαραγάγει ένα φωνητικό βίντεο και να ενεργοποιήσει την Alexa.Στην περίπτωση αυτή ο Θύτης με το έξυπνο κινητό του μέσω του λογισμικού παραβίασης μπορεί να υποκλέψει των κωδικό wifi της οικίας, δίχως να χρειάζεται άδεια root και να μεταδώσει στην έξυπνη τηλεόραση το πακέτο των φωνητικών εντολών.

2η Περίπτωση: Στο σημείο αυτό το τηλέφωνο ξενιστής πραγματοποιεί ανίχνευση σε οικιακό wifi προκειμένου να εντοπιστούν συσκευές Alexa και έξυπνες συσκευές που συνδεδεμένες μαζί της. Το malwave δίχως άδεια root διαμοιράζεται στο οικιακό wifi και γίνεται η αποστολή των εντολών.

4.1.1. Περιπτώσεις επιθέσεων συσκευών Alexa.

Παραβίαση σπιτιού: Μια γκαραζόπορτα Garageio διασυνδεμένη με μια συσκευή Alexa είναι εφικτό όταν δεχθεί την εντολή “Alexa θέλω το Garageio μου να ανοίξει την πόρτα μου”, να εκτελέσει την εντολή.

Πλασματική παραγγελία: Στη περίπτωση αυτή ο θύτης μέσω του κακόβουλου λογισμικού εκτελεί παραγγελία στο περιβάλλον του Amazon.com, προκαλώντας οικονομική ζημιά στο θύμα, καθώς το είδος και το ύψος της παραγγελίας μπορούν να περιλαμβάνουν αγαθά υψηλού κόστους. Είναι εξακριβωμένο ότι για αυτού του είδους ηλεκτρονικών αγορών, η Amazon παραδίδει τα δέματα στην είσοδο των κατοικιών δίχως να απαιτείται η υπογραφή του αγοραστή που έκανε την παραγγελία.

4.1.2 Εικονικό Κουμπί (Virtual Button)

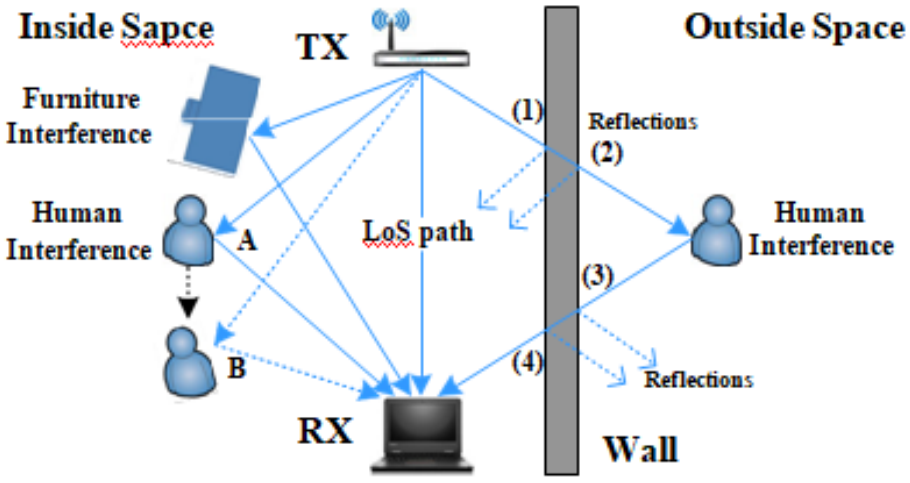
Στην ενότητα αυτή γίνεται η πρόταση ενός συστήματος εποπτείας της πρόσβασης μιας συσκευής Alexa αλλά και έξυπνων συσκευών καθώς θα γίνεται έλεγχος δύο παραγόντων πλέον, αυτός της φυσικής παρουσίας του ατόμου. Επιλέχθηκε το όνομα «εικονικό κουμπί» για τον χαρακτηρισμό του μηχανισμού, αφού η προσομοίωση της φυσικής παρουσίας ισοδυναμεί με τον χειρισμό ενός μηχανικού κουμπιού. Η απαίτηση μιας υπηρεσίας μέσω μιας έξυπνης συσκευής με το εικονικό κουμπί δεν εκτελείται αφού προϋποθέτει τη μηχανική διέγερσή του (απαίτηση φυσικής παρουσίας). Έτσι, με αυτήν την πρόταση, αποφεύγονται οι κακόβουλες φωνητικές επιθέσεις όταν δεν υπάρχουν άτομα στο χώρο πλησίον της. Το προτεινόμενο σύστημα διερευνά την ανθρώπινη ύπαρξη κάνοντας χρήση της υποδομής του υφιστάμενου Wi-Fikαι αυτό με ελάχιστη επιπρόσθετη χρήση του ασύρματου δικτύου όπως και της συσκευής Alexa, αφού σε ανεπαίσθητο βαθμό γίνεται παράμετρος ο τρόπος χρήσης του φωνητικού βοηθού. Η εξακρίβωση επιτυγχάνεται με την επιτήρηση του διαύλου θέσης κατάστασης (CSI), του φορέα που χρησιμοποιεί η υποδομή Wi-Fi του χώρου. Οι μεταβολές CSI σηματοδοτούν την ανθρώπινη ύπαρξη στο χώρο και το πως η Alexa βρίσκεται σε αναμονή φωνητικών εντολών. Η νέα παράμετρος που εισάγεται είναι αυτή της κίνησης του χεριού με τυχαίο τρόπο προκειμένου να έρθει η Alexaσε ετοιμότητα.

Ο μηχανισμός εξακρίβωσης ανθρώπινης παρουσίας στηριζόμενος στην τεχνολογία Wi-Fiπαρουσιάζει ευχρηστία και απουσία δαπανηρών οικονομικών απαιτήσεων, εξαιτίας

δύο λόγων: α) Η τεχνολογία Wi-Fi είναι μια ανερχόμενη τεχνολογία και έτσι δεν απαιτείται επιπλέον δαπάνη για τη δική μας περίπτωση και β) αρκεί μόνο μία αναβάθμιση λογισμικού από πλευράς της Alexa για να ξεπεραστούν τα όποια προβλήματα που προκύπτουν από τη χρήση τους. Προτού παρουσιαστεί ο σχεδιασμός του εικονικού κουμπιού θα προηγηθεί η παρουσίαση του CSI primer–αλφαβητάρι καθώς και του CSI based που αφορά την επαλήθευση φυσικής κίνησης βασιζόμενη στο φαινόμενο πολλαπλών διαδρομών που ακολουθούν οι πολλαπλές ανακλάσεις.

4.1.3 Αλφαβητάρι Primer

Η χρήση του έγκειται στον χαρακτηρισμό του καναλιού από πλευράς των ιδιοτήτων των σημάτων Wi-Fi. Το σημερινό χρησιμοποιούμενο Wi-Fi πρότυπο IEE χρησιμοποιεί την τεχνική διαίρεση συχνότητες με ορθογώνια πολυπλεξία (OFDM), διαιρώντας ένα κανάλι σε μία συστάδα υποφορέων χρησιμοποιώντας την τεχνολογία MIMO για αναβάθμιση



Εικόνα 18. Μια απεικόνιση εφέ πολλαπλών διαδρομών και πολλαπλών αντανακλάσεων

της ταχύτητας μετάδοσης των ροών.

Σε κάθε κανάλι εισόδου – εξόδου η τιμή CSI υποδηλώνει την ιδιοσυστασία ενός δευτερεύοντος φορέα ενός καναλιού.

Στη γλώσσα των μαθηματικών η τιμή των CSI primer ορίζεται με την εξίσωση yi = Hi* xi + ni, όπου xi είναι το εκπεμπόμενο – μεταδιδόμενο σήμα διαστάσεων Nτ, yi το NR

λαμβανόμενο σήμα από ένα δευτερεύοντα υποφορέα i που φέρει τις πληροφορίες CSI Hi. Το ni εκφράζει στο σχήμα μας και στην εξίσωση το διάνυσμα του θορύβου.

Οι συσκευές Wi-Fi του εμπορίου είναι ικανές να λαμβάνουν χιλιάδες τιμές σημάτων CSI το δευτερόλεπτο από πολλαπλούς δευτερεύοντες φορείς διαίρεσης συχνότητας ορθογώνιας πολυπλεξίας. Αυτό σημαίνει, πρακτικά, πως ανεπαίσθητες τροποποιήσεις CSI, προέρχονται από κινήσεις στο χώρο. Άρα, οι τιμές του CSI primer μας παραδίδουν ένα σύνολο περιγραφικών πληροφοριών.

4.1.4 Ανίχνευση ανθρώπινης κίνησης που βασίζεται σε CSI

Στην ενότητα αυτή θα επιχειρηθεί η περιγραφή της εργαλειοθήκης των φυσικών κινήσεων που συμβαίνουν σε έναν εσωτερικό χώρο με την εργαλειοποίηση των εφέ που παρέχει το CSI ως προς τις πολλαπλές διαδρομές που ακολουθούν οι πολλαπλές ανακλάσεις. Οι πολλαπλές διαδρομές εστιάζονται στον τρόπο μετάδοσης ενός σήματος που αυτό ακολουθεί και καταλήγει σε μια κεραία λήψης, ακολουθώντας διαφορετικά μονοπάτια. Στην εικόνα 18 απεικονίζεται :

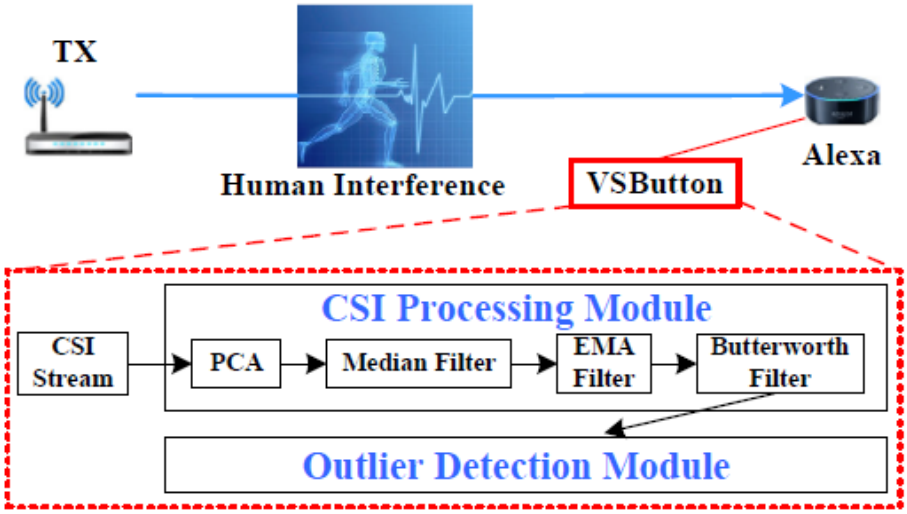
1. δέκτης Rx ο οποίος κάνει λήψη τις πολλαπλές ανακλάσεις του ίδιου αρχικού σήματος
2. το μονοπάτι της οπτικής επαφής (LoS)
3. μια αντανάκλαση από το άτομο που βρίσκεται στην θέση A και
4. μια αντανάκλαση από τα έπιπλα.

Οι διαφορετικές αποστάσεις που ακολουθούν τα διαδιδόμενα σήματα Wi-Fi, έχουν ως αποτέλεσμα την αλλαγή φάσης τους, που καταλήγει σε μια διαφοροποίηση τιμών του CSI. Με αυτόν τον τρόπο η ανθρώπινη παρουσία κινούμενη επιφέρει μεταβολή των σημάτων Wi-Fiστον χώρο και τροποποιεί τις τιμές του CSI. Έτσι τα εφέ πολλαπλής ανάκλασης σημάτων δηλώνουν την συστάδα των ανακλάσεων που λαμβάνονται από ένα δέκτη, τα οποία, διαδεδομένα στο χώρο, δημιουργούν πολλαπλά αντίγραφα του αρχικού φέροντος. Καθώς ένα άτομο κινείται μεταξύ εσωτερικού δύο εξωτερικών χώρων, ο βαθμός διακύμανσης CSI αυξομειώνεται εξαιτίας των διαφορετικών ανακλάσεων.

Αυτό αποτυπώνεται στο σχήμα 2 καθώς το σήμα υπόκεινται σε τέσσερις ανακλάσεις, εξασθενώντας καθώς περνάει από διαφορετικά μέσα (αέρας, τοίχος) με διαφορετικές κατευθύνσεις.

4.1.5 Σχεδιασμός εικονικού κουμπιού

Στην εικόνα 19 παρουσιάζεται μια προτεινόμενη σχεδίαση. Το εικονικό κουμπί είναι μαζί με την συσκευή HOVA και ανιχνεύει την ανθρώπινη δραστηριότητα διαμέσου των λαμβανόμενων μεταβλητών σημάτων CSI στο κανάλι επικοινωνίας ανάμεσα στην Alexa και του AP. Μ' αυτόν τον τρόπο το εικονικό κουμπί είναι σε θέση να εξακριβώσει την ανθρώπινη κίνηση μέσα στο χώρο που υπάρχει η συσκευή. Αξίζει να αναφερθεί πως υπάρχει η δυνατότητα η Alexa διαρκώς να δέχεται τιμές CSI καθώς περνάει ο χρόνος και στη συνέχεια να στέλνει πακέτα δεδομένων ICMP με σταθερή ροή στο AP και σε δεύτερο χρόνο να λαμβάνει τα απαντητικά πακέτα μηνυμάτων όπως παραπάνω.



Εικόνα 19. Σχεδιασμός εικονικού κουμπιού

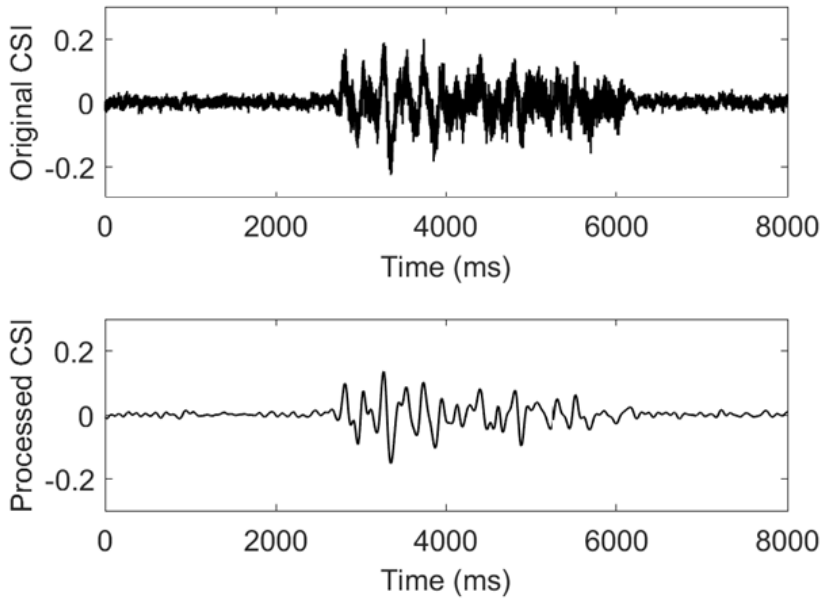
Ο εντοπισμός της ανθρώπινης δραστηριότητας με το εικονικό κουμπί ειδικεύεται σε δύο κυρίως στάδια, το στάδιο της κατεργασίας των σημάτων CSI και το στάδιο εντοπισμού οριακών τιμών. Έτσι κατά την αποδοχή των τιμών CSI, η αρχική λήψη απομακρύνει τον όποιο θόρυβο από αυτές, έτσι ώστε στη συνέχεια μα είναι εφικτή η

όποια μεγέθυνση των μοτίβων διακύμανσης CSI που δημιουργούνται από την ανθρώπινη δραστηριότητα.

Αφού ολοκληρωθεί η έξοδος των αποτελεσμάτων από τη λήψη του πρώτου σταδίου, κατά το δεύτερο στάδιο η επεξεργασία αφορά μια τεχνική εξακρίβωση οριακών τιμών σε πραγματικό χρόνο έτσι ώστε να γίνει ο καθορισμός των προτύπων CSI της ανθρώπινης παρουσίας μέσασε ένα δωμάτιο ή κλειστό χώρο. Ακολουθεί η αναλυτική παρουσίαση των δύο προαναφερόμενων σταδίων με παραδείγματα ταυτοποίησης ανθρώπινης σε κλειστούς χώρους.

ΣΤΑΔΙΟ ΕΠΕΞΕΡΓΑΣΙΑΣ CSI

Το στάδιο αυτό επιμερίζεται σε τρία μέρη: α) Ερμηνεία κεντρικών συνιστωσών (PCA), β) Διαχωρισμός διάμεσου και εκθετικού μεταβλητού μέσου όρου (EMA), γ) Φίλτρο διέλευσης χαμηλών συχνοτήτων Butterworth. Πρωταρχικά ενεργοποιείτε η βαθμίδα PCA, προκειμένου να μειωθούν οι μεγάλες αποκλίσεις των τιμών CSI, απομακρύνοντας εκείνο το κομμάτι που δεν αφορά τον εντοπισμό της ανθρώπινης δραστηριότητας. Τα δύο επόμενα μέρη αφορούν για το φιλτράρισμα και την αφαίρεση του θορύβου έκρηξης και των ακραίων στιγμιαίων μεταβολών υψηλής συχνοτικής τιμής στο σύνολο



των τιμών λήψης CSI.

Η εικόνα 20 αποδίδει συγκριτικά το αρχικό με το τελικό επεξεργασμένο σήμα CSI. Στην πράξη αποδεικνύεται πως το τελικό επεξεργασμένο σήμα δίνει στοχευμένες πληροφορίες για τον εντοπισμό κινήσεων σε ένα κλειστό χώρο.

ΜΟΝΑΔΑ PCA

Όπως

Εικόνα 20. Σύγκριση μεταξύ αρχικού/επεξεργασμένου CSI με την πάροδο του χρόνου.

προηγουμένως δηλώθηκε, η χρήση της βαθμίδας αυτής συνίσταται για την απομάκρυνση του θορύβου από το σήμα CSI, αποκαλύπτοντας τις υποφέρουσες πληροφορίες που αφορούν τις πραγματικές συσχετίσεις με την ανθρώπινη παρουσία. Έτσι ουσιαστικά έχουμε το κύριο δείγμα που αντιπροσωπεύει τις επιθυμητές συνιστώσες, στο σύνολο των χρονοσειρών CSI. Η PCA συντελεί στην αύξηση του ρυθμού επεξεργασίας καθότι το συλλεγμένο σήμα μπορεί να περιέχει αυξημένο όγκο πληροφορίας θορύβου. Στην πειραματική διαδικασία που ακολουθήθηκε, παρατηρήθηκε πως στα τέσσερα πρώτα αντιπροσωπευτικά δείγματα που λήφθηκαν, περιείχαν τις σπουδαιότερες μεταβολές, στη ρευστότητα CSI, όμως η πρώτη συνιστώσα είναι η πιο ευάλωτη στο θόρυβο από την όποια δραστηριότητα του χώρου. Έτσι πρακτικά χρησιμοποιούμε τις υπόλοιπες συνιστώσες για επεξεργασία & ανάλυση CSI.

ΦΙΛΤΡΑ MEDIAN & EMA.

Το επόμενο στάδιο επεξεργασίας αφορά τη χρήση δύο διαφορετικών φίλτρων. Ενός φίλτρου διάμεσου και ενός φίλτρου EMA, προκειμένου να απομακρύνουμε τις απότομες στιγμιαίες αυξήσεις του θορύβου και τις αιχμές του στη ρευστότητα των

τιμών CSI. Αυτό μπορεί να παρατηρηθεί καθώς οι εμπορικές βαθμίδες διασύνδεσης wifi, παρουσιάζουν κατασκευαστικά μια αστάθεια ισχύος στο εκπεμπόμενο σήμα που μεταδίδουν, καθώς επίσης και στις τοπικές συνθήκες που επικρατούν στο συγκεκριμένο χώρο και σχετίζονται με κλιματικές δυναμικές μεταβολές όπως η υγρασία του. Η βαθμίδα του φίλτρου Median μπορεί να εξορθολογήσει τις βραχυπρόθεσμες μεταβολές και να καταδείξει τις μακροπρόθεσμες συμπεριφορές. Πρέπει εδώ να αναφερθεί πως το παράθυρο moving που αφορά το σύνολο των κοντινών εγγραφών CSI που έχει ληφθεί, αποτελεί μια παράμετρο που μπορεί να τροποποιηθεί. Γίνεται χρήση ενός φίλτρου EMA για την ομαλοποίηση των τιμών CSI. Ενεργοποιεί δείκτες που σταθμίζουν τις τιμές καθώς μειώνονται με εκθετικό τρόπο σε σχέση με τις παλαιότερες τιμές CSI.

ΦΙΛΤΡΟ BUTTERWORTH.

Στο τελικό στάδιο γίνεται προσθήκη φίλτρου Butterworth διέλευσης χαμηλών συχνοτήτων για την αποκοπή των σημάτων υψηλής συχνότητας CSI, έχοντας γνώση πως οι κινήσεις του ανθρώπου δεν πραγματοποιούνται με υψηλό ρυθμό ταχύτητας. Πιο ειδικά, κατά την πειραματική διαδικασία μετρήθηκε μεταβολή του CSI λόγω της ανθρώπινης δραστηριότητας στο φάσμα των χαμηλών συχνοτήτων σε τιμές κοντά στα 100 Hz και με ένα φίλτρο αποκοπής στη συχνότητα αυτή, ο θόρυβος υψηλής τιμής, μπορεί να αποκοπεί.

ΦΑΣΗ ΑΝΙΧΝΕΥΣΗΣ ΑΚΡΑΙΩΝ ΤΙΜΩΝ.

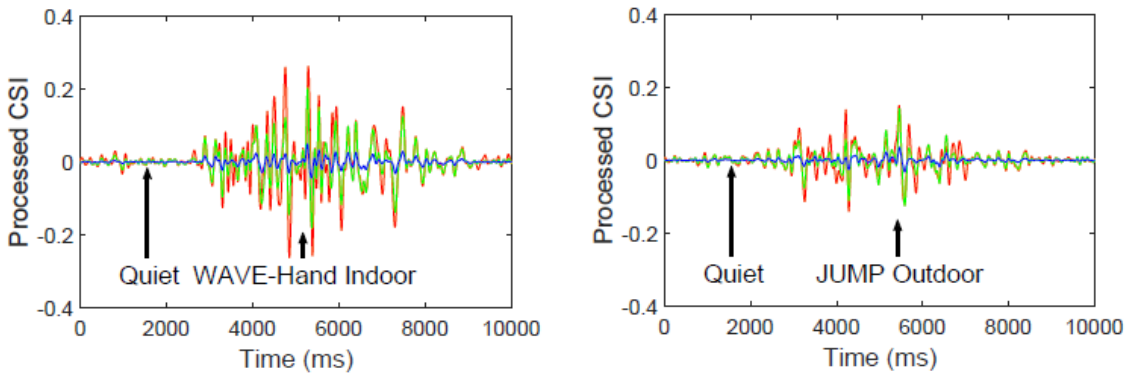
Στο στάδιο αυτό πραγματοποιείτε εντοπισμός της ανθρώπινης παρουσίας εφαρμόζοντας μια μεθοδολογία αναζήτησης οριακών τιμών σε ρεαλιστικό χρόνο, εργαλειοποιώντας υπερελλειψοειδής μεθόδους σε ροές δεδομένων που δεν εμφανίζουν σταθερότητα.

Η παραπάνω μέθοδος προσφέρει βελτιστοποίηση στην ακρίβεια των αποτελεσμάτων σε σύγκριση με τη συνήθη μέθοδο του μεταβλητού μέσου όρου, η οποία εντοπίζει μια δυσλειτουργία σε συνάρτηση με ένα όριο της απόστασης ανάμεσα στην παρούσα στιγμή και του μέσου όρου των προηγούμενων τιμών, μέσα από δύο θεωρήσεις. Αρχικά κάνει χρήση μιας νέας τεχνικής μέτρησης απόστασης της Mahalanobis που εμφανίζει

μεγαλύτερη ακρίβεια και δεύτερον αναμορφώνει τον εκθετικό μεταβλητό μέσο όρο(EMA) προκειμένου να επικαιροποιηθεί ο μέσος όρος της προηγούμενης ληφθείσας τιμής.

ΠΑΡΑΔΕΙΓΜΑ ΑΝΙΧΝΕΥΣΗΣ ΚΙΝΗΣΕΩΝ ΣΕ ΚΛΕΙΣΤΟΥΣ ΧΩΡΟΥΣ

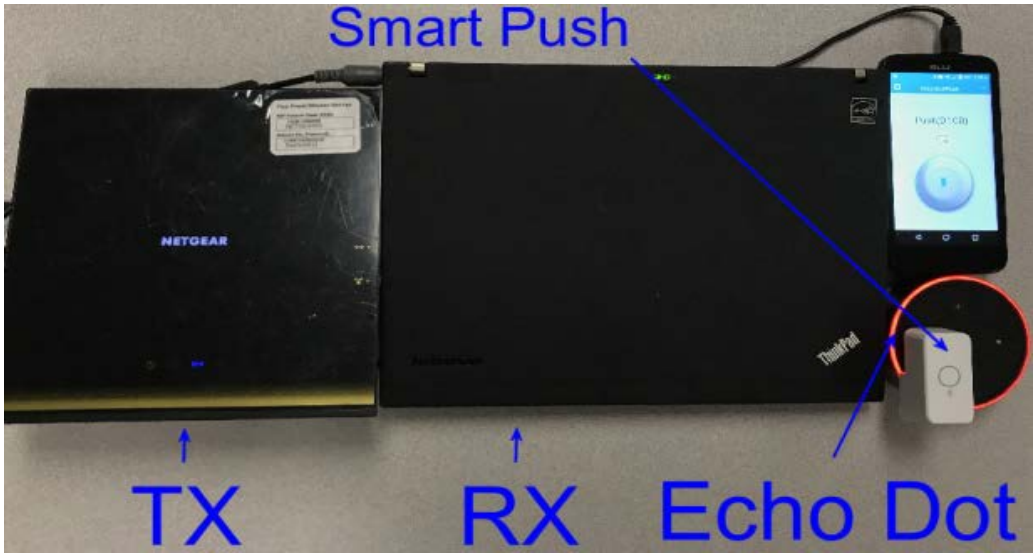
Στην ενότητα αυτή γίνεται η παρουσίαση της διαφοροποίησης που υφίστανται οι τιμές CSI από την κινητικότητα που υπάρχει σε εσωτερικούς και εξωτερικούς χώρους, ώστε να είναι αντιληπτό με μεγάλη ακρίβεια όταν η δραστηριότητα πραγματοποιείται σε εσωτερικό χώρο. Στα σχήματα που ακολουθούν εμφανίζονται οι τροποποιημένες τιμές για μια βραχεία κίνηση σε ένα δωμάτιο (όπως κούνημα χεριού), και μια άλλη πολύ μεγαλύτερη κίνηση σε εξωτερικό χώρο όπως ένα άλμα.



(α) Παραλλαγή CSI κίνησης εσωτερικού χώρου **(β) Παραλλαγή CSI κίνησης εξωτερικού χώρου**

Εικόνα 21. Σύγκριση παραλλαγών CSI εσωτερικού και εξωτερικού χώρου.

Αποκαλύπτεται πως έστω και μια ανεπαίσθητη κίνηση σε ένα δωμάτιο – εσωτερικό χώρο, είναι ικανή να επιφέρει μεγάλες μεταβολές τιμών CSI σε σχέση με μια ιδιαίτερα μεγάλη κίνηση που συμβαίνει σε εξωτερικό χώρο. Εν κατακλείδι, με την κατάλληλη



παραμετροποίηση, το εικονικό κουμπί καθίσταται ικανό να εντοπίζει με ακριβή τρόπο τις κινήσεις εσωτερικού χώρου και ακολούθως να θέτει σε λειτουργία την Alexa και να δέχεται με τη σειρά της ρεπερτόριο φωνητικών εντολών.

Εικόνα 22. Πρωτότυπο Εικονικό κουμπί.

ΕΦΑΡΜΟΓΗ & ΑΞΙΟΛΟΓΗΣΗ

Στο σημείο αυτό επιχειρείται η παρουσίαση της εφαρμογής του πρωτότυπου εικονικού κουμπιού καθώς και τα παραδοτέα από την αξιολόγηση του σε πραγματικές αλλά και σε εργαστηριακές συνθήκες.

Α. ΕΦΑΡΜΟΓΗ ΠΡΩΤΟΤΥΠΟΥ

Το καινοφανή εικονικό κουμπί στηρίχθηκε κατασκευαστικά σε εμπορικές συσκευές (COTS) όπως απεικονίζεται στην εικόνα 22. Ως διάταξη TX χρησιμοποιήθηκε ένας δρομολογητής wifi της Netgear R6300V2, που πήρε τη θέση του οικιακού wifi AP. Ο ρόλος του αφορά στην εκπομπή των πακέτων δεδομένων προς την συσκευή Alexa για τη λήψη των σημάτων CSI κατά την εξέλιξη του χρόνου. Στην εφαρμογή που προτείνετε γίνεται η χρήση της έκδοσης του πρωτοκόλλου 802.11n διότι οι συσκευές Alexa στο συγκεκριμένο χρόνο δεν υποστήριζαν την έκδοση 802.11 ac. Γνωρίζοντας πως οι διατάξεις Alexa δεν παρουσιάζουν ανοικτότητα για ανάπτυξη, η βαθμίδα ανίχνευσης κινήσεων, λαμβάνει χώρα σε έναν υπολογιστή, ο οποίος διαθέτει σήμανση RX. Οι HDVA

συσκευές μπορούν να δεχθούν τα εξαγόμενα του εντοπισμού κινήσεων από τον H/Y. Στην περίπτωση μας η μονάδα RX, αφορά έναν υπολογιστή Lenovo X200 εξοπλισμένο με κάρτα wifi της Intel (Link 5300), καθιστώντας τον λαμβάνει τις τιμές CSI από το αναπτυξιακό εργαλείο της εφαρμογής. Για την προσομοίωση ελέγχου κατά τη πρόσβαση στην συσκευή Alexa, η βαθμίδα ελέγχει το Microbot push για την ενεργοποίηση – φίμωση του ενσωματωμένου μικροφώνου της Alexa με τη βοήθεια ενός έξυπνου κινητού, μόλις εντοπιστεί από την πειραματική μονάδα μεταβολή στη θέση του ελέγχου πρόσβασης με κριτήριο τον εντοπισμό κινήσεων.

Συνοψίζοντας η κατασκευαστική πρόταση υλοποίησης του εικονικού κουμπιού περιλαμβάνει έναν ασύρματο δρομολογητή, έναν φορητό υπολογιστή, ένα έξυπνο κινητό και τέλος ένα Microbot, που αθροιστικά δίνουν ένα οικονομικό κόστος που δε χαρακτηρίζεται χαμηλό.

Β. ΑΞΙΟΛΟΓΗΣΗ

Στη συνέχεια παρουσιάζετε το σύνολο των πειραματικών ρυθμίσεων και γίνεται η αξιολόγηση των επιδόσεων του εικονικού κουμπιού σε τρία διαφορετικά εσωτερικά περιβάλλοντα : α) Σε τετράγωνο δωμάτιο, β) σε ορθογώνιο δωμάτιο, γ) σε δίχωρο διαμέρισμα. Η αξιολόγηση της απόδοσης γίνεται σε σχέση με τα τρία σενάρια κινήσεων που αφορούν την απουσία κίνησης, την κίνηση σε κλειστό χώρο και την κίνηση σε εξωτερικό καθώς και εάν αυτές οι διαφορετικές συνθήκες κίνησης στους χώρους γίνονται ορθά αναγνωρίσιμες. Επιστρατεύθηκαν έξι άτομα για τη συμμετοχή τους στην πειραματική διαδικασία. Τους προτρέψαμε να προβούν στην εκτέλεση συγκεκριμένων κινήσεων που αφορούσαν σε κινήσεις των χεριών, στο κάθισμα και στην ανασήκωση τους από μια καρέκλα και τέλος στην εκτέλεση άλματος τόσο στον εσωτερικό όσο και στον εξωτερικό χώρο ενός δωματίου. Οι κινήσεις αυτές αντιστοιχίζονται στους τρείς δείκτες της δραστηριότητας ενός ατόμου της ήπιας, της μεσαίας και της ισχυρής αντίστοιχα. Εδώ ο έλεγχος αφορά την μετρική απόσταση Mahalanobis για το σύνολο

των μετρήσεων και για τους τρεις τύπους κινήσεων, με την επισήμανση εάν οι κινήσεις που γίνονται σε κλειστούς χώρους, αναγνωρίζονται με ακρίβεια ή όχι.

ΠΕΙΡΑΜΑΤΙΚΕΣ ΜΕΤΡΗΣΕΙΣ

Σε όλα τα πειραματικά σενάρια η βαθμίδα RX του φορητού Η/Υ που διαθέτει Echo dot κάνει αποστολή διακοσίων μηνυμάτων κατηγορίας ICMP Echo Request το δευτερόλεπτο στον ασύρματο δρομολογητή wifi, προκειμένου να είναι σε θέση να κάνει λήψη CSI κατά την εξέλιξη του χρόνου. Μια αποστολή πακέτων CSI με συχνότητα δειγματοληψίας 200bps είναι αρκετή για να αποτελεί υλικό εξακρίβωσης κινήσεων. Η διάσταση ενός μηνύματος ICMP είναι μονάχα της τάξεως των 84 byte, καθιστώντας την ευρυζωνικότητα του δικτύου χαμηλή.

Οι τάξεις μεγέθους των παραθύρων των φίλτρων MEDIAN & EMA τοποθετούνται σε εννέα και δεκαπέντε αντίστοιχα. Από τα εξαγόμενα κατά την πειραματική διαδικασία, προκύπτει πως τα δύο παραπάνω μεγέθη των παραθύρων, είναι αρκετά ώστε η απόρριψη του θορύβου από τα δύο φίλτρα να γίνεται με μεγάλη ευκολία. Για το φίλτρο Butterworth η συχνότητα αποκοπής του ρυθμίστηκε στην τιμή $\omega_c = 2\pi * 100$ rad/s, καθώς όπως προαναφέρθηκε στην προηγούμενη ενότητα, ο ρυθμός μεταβολής των ανθρώπινων κινήσεων προκαλούν μεταβολές στις ροές CSI ασθενής συχνότητας που πρακτικά μετριούνται σε ένα πεδίο τιμών κοντά στα f = 100Hz.

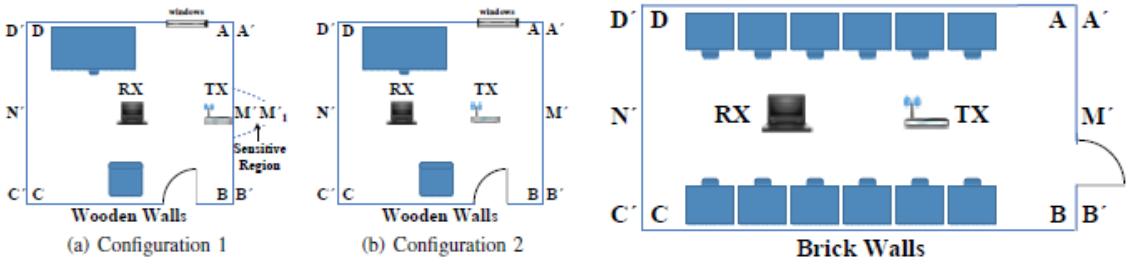
Τέλος αναφέρεται πως ο παράγοντας λήθης α, στο τμήμα που αφορά τον εντοπισμό οριακών – ακραίων τιμών, λαμβάνει την τιμή α = 0,98 που μεταφράζεται πως βαρύνουσα σημασία δίνεται στις τελευταίες λαμβανόμενες τιμές.

ΤΕΤΡΑΓΩΝΗ ΑΙΘΟΥΣΑ ΕΡΓΑΣΤΗΡΙΟΥ

Εδώ έγινε η ανάπτυξη του εικονικού κουμπιού μέσα σε ένα τετραγωνικής διάταξης ξύλινο δωμάτιο και στοιχειοθετήθηκε η αξιολόγηση της συμπεριφοράς του μέσα από δύο σενάρια εφαρμογής όπως γίνεται η απεικόνιση του στην εικόνα 23 Κατά το πρώτο πεδίο εφαρμογής, η μονάδα Η/Υ που διαθέτει RX βαθμίδα, επιλέχθηκε να τοποθετηθεί κεντροβαρικά στο χώρο, ενώ ο wifi δρομολογητής (TX) τοποθετήθηκε σε μια άκρη του

Εικόνα 23. Τετράγωνο δωμάτιο

δωματίου. Στο δεύτερο σενάριο εφαρμογής, ο Η/Υ και ο δρομολογητής τοποθετήθηκαν στα σημεία που απεικονίζονται στο σχήμα, προκειμένου η απόσταση του χώρου να τριχοτομηθεί σε ίσα διαστήματα. Κατά την πειραματική διαδικασία, τα έξι άτομα που συμμετείχαν, εκτέλεσαν όλο το ρεπερτόριο των κινήσεων που προαναφέρθηκε σε τέσσερις διακριτές θέσεις εντός του δωματίου καθώς και σε έξι θέσεις έξω από αυτό, όπως αποτυπώνεται στο σχήμα.



Εικόνα 24. Διαμόρφωση ορθογώνιου δωματίου

ΔΙΑΜΟΡΦΩΣΗ ΧΩΡΟΥ – ΠΕΔΙΟΥ ΕΦΑΡΜΟΓΗΣ

Το σύνολο των μετρήσεων των αποστάσεων Mahalanobis αποτυπώνεται στην εικόνα 25. Πρέπει να αναφερθεί πως κάθε τιμή του πίνακα είναι η ελάχιστη που μπορεί αυτή να λάβει στο σύνολο όλων των λαμβανομένων από τους συμμετέχοντες στο εσωτερικό του δωματίου, ενώ οι τιμές του εξωτερικού χώρου αφορούν τις μέγιστες τιμές.

Square Room	Indoor Locations				Outdoor Locations					
locations	A	B	C	D	A'	B'	C'	D'	M'	N'
WAVE-HAND	0.218	0.213	0.195	**0.191**	0.104	0.101	0.079	0.083	0.156	0.121
SIT-DOWN-STAND-UP	0.277	0.271	0.258	0.253	0.118	0.113	0.088	0.092	**0.238**	0.139
JUMP	0.392	0.391	0.371	0.366	0.132	0.128	0.099	0.103	**0.373**	0.165
DO NOTHING	0.026	0.021	0.027	0.024	0.023	0.027	0.028	0.023	0.020	0.023

Εικόνα 25. Απόσταση Mahalanobis Μετρημένη σε Τετράγωνο Δωμάτιο Με Διαμόρφωση 1

Με τη τεχνική αυτή είναι οφθαλμοφανές το γεγονός ότι το σύνολο των εσωτερικών κινήσεων δίνει διαφορετικό σετ μετρήσεων από αυτό των εξωτερικών σε σχέση με τη μεταβλητότητα των αποστάσεων Mahalanobis. Από την επεξεργασία των μετρήσεων που αφορά το είδος της κίνησης, όπως και που πραγματοποιείτε η κίνηση αυτή,

εξάγεται το αποτέλεσμα πως η τοποθέτηση του δρομολογητή δεν πρέπει να λαμβάνει χώρα σε τοίχο πλησίον υπαίθριου χώρου.

ΔΙΑΜΟΡΦΩΣΗ

Τα αποτελέσματα του πεδίου αυτού απεικονίζονται στον πίνακα 2.

Square Room	Indoor locations				Outdoor locations					
locations	A	B	C	D	A'	B'	C'	D'	M'	N'
WAVE-HAND	**0.312**	0.315	0.401	0.409	0.041	0.043	0.049	0.051	0.092	0.063
SIT-DOWN-STAND-UP	0.345	0.349	0.423	0.430	0.060	0.062	0.069	0.071	0.121	0.089
JUMP	0.401	0.407	0.451	0.459	0.069	0.071	0.084	0.086	**0.241**	0.099
DO NOTHING	0.025	0.021	0.022	0.024	0.028	0.026	0.021	0.022	0.023	0.025

Εικόνα 26. Απόσταση Mahalanobis Μετρημένη σε Τετράγωνο Δωμάτιο Με Διαμόρφωση 2

Διαπιστώνεται ότι η απόσταση Mahalanobis των εσωτερικών κινήσεων υπερβαίνει τη μέγιστη απόσταση από κάθε εξωτερική όπως αυτή καθορίστηκε στο σημείο Μ΄ του σχήματος. Εν κατακλείδι εδώ το εικονικό κουμπί είναι ικανό να θέσει σε λειτουργία την HDVA συσκευή μόνο με κινήσεις στο εσωτερικό του δωματίου.

ΟΡΘΟΓΩΝΙΟ ΔΩΜΑΤΙΟ

Η κατασκευή του δωματίου ήταν τοιχοποιία με τούβλα. Η διάταξη των βαθμίδων RX & TX έλαβαν θέσεις στα σημεία Ν΄& Μ΄ όπως απεικονίζονται στην εικόνα 24. Στην εικόνα 27 δίνονται τα αποτελέσματα . Το πρώτο συμπέρασμα που εξάγεται εδώ, ταυτίζεται με αυτό του ξύλινου δωματίου με τη δεύτερη διαμόρφωση και αποσαφηνίζεται ότι τα σήματα wifi απορροφούνται και εξασθενούν σημαντικά όταν διαπερνούν την τοιχοποιία από τούβλα σε σχέση με την ξύλινη.

Rectangle Room	Indoor locations				Outdoor locations					
locations	A	B	C	D	A'	B'	C'	D'	M'	N'
WAVE-HAND	**0.147**	0.150	0.180	0.183	0.020	0.022	0.025	0.027	0.035	0.030
SIT-DOWN-STAND-UP	0.181	0.184	0.216	0.217	0.024	0.026	0.028	0.029	0.039	0.033
JUMP	0.254	0.255	0.287	0.288	0.029	0.029	0.032	0.033	**0.042**	0.035
DO NOTHING	0.022	0.021	0.022	0.027	0.028	0.026	0.021	0.022	0.020	0.025

Εικόνα 27. Απόσταση Mahalanobis Μετρημένη σε Ορθογώνιο Δωμάτιο.

Από τα παραπάνω εξάγονται δύο διαπιστώσεις. Η πρώτη αφορά την υλική σύσταση του τοίχου που καθορίζει την αποδοτικότητα του εικονικού κουμπιού, καθώς όσο

μεγαλύτερη σκληρότητα και τραχύτητα παρουσιάζει ο τοίχος τόσο αυξάνεται η αποτελεσματικότητα του. Οι καλύτερες τιμές πάρθηκαν χρησιμοποιώντας τοιχοποιία από ξύλο και τούβλα.

Η δεύτερη διαπίστωση αφορά ότι θα πρέπει να αποφεύγεται η τοποθέτηση του εικονικού κουμπιού και του δρομολογητή πλησίον εξωτερικού χώρου. Έτσι κατά τις δοκιμές τοποθέτησης των δύο συσκευών, αποδείχτηκε πως το βέλτιστο σημείο ήταν αυτό στο κεντρικό σημείο του χώρου – δωματίου, καθώς και η κάλυψη του σήματος του wifi δρομολογητή εμφάνισε τις μεγαλύτερες τιμές στη θέση αυτή.

ΒΑΘΜΟΝΟΜΗΣΗ ΠΑΡΑΜΕΤΡΩΝ

Πριν από την έναρξη λειτουργίας του εικονικού κουμπιού, στην πράξη, είναι αναγκαίο να πραγματοποιείτε η βαθμονόμηση όλων των παραγόντων που καθορίζουν την απόδοση του, ορίζοντας το σημείο αναφοράς t, πάνω από την οποία θα εντοπίζονται οι κινήσεις ακραίων τιμών. Και αυτό καθώς το σημείο αναφοράς μπορεί να διαφοροποιηθεί αλλάζοντας το περιβάλλον ανάπτυξης. Η διεργασία της διαβάθμισης αναπτύσσεται σε δύο στάδια. Κατά το πρώτο, ο κάτοχος της HDVA συσκευής, αποφασίζει σε πιο σημείο του χώρου θα την τοποθετήσει και μετά οριοθετεί το χώρο μέσα στον οποίο θα ανιχνεύει την ανθρώπινη δραστηριότητα. Στη θέση αυτή του χώρου ο κάτοχος εκτελεί τη μικρότερη κίνηση του χεριού που μπορεί να σημειωθεί (όπως π.χ. κίνηση με 1rad/s) και καταγράφει την μικρότερη τιμή της απόστασης Mahalanobis.

Στο δεύτερο στάδιο ο κάτοχος εντοπίζει το σύνολο των εξωτερικών σημείων που δεν πρέπει να τοποθετηθεί η Alexa, πραγματοποιώντας σε εξωτερικό χώρο την πιο έντονη κίνηση (π.χ. άλμα) που μπορεί να γίνει και καταγράφει τη μέγιστη τιμή της αντίστοιχης απόστασης Mahalanobis. Το σημείο αναφοράς t προκύπτει από το μισό της διαφοράς των δύο αποστάσεων που μετρήθηκαν. Αξίζει εδώ να σημειωθεί πως η διεργασία της διαβάθμισης απαιτεί ελάχιστα λεπτά και μόνο μια φορά κατά την έναρξη της χρήσης της συσκευής δίχως την επανάληψη της διαδικασίας. Το παραπάνω είναι εφικτό καθώς το σύνολο των παραμέτρων είναι εξελιγμένο και εμφανίζει σταθερότητα κατά το

σχεδιασμό και αυτό που διαφοροποιείται είναι το σημείο αναφοράς t και οι κύριες γραμμές CSI που πρέπει να ακολουθούν τις μεταβολές του περιβάλλοντος ειδικότερα.

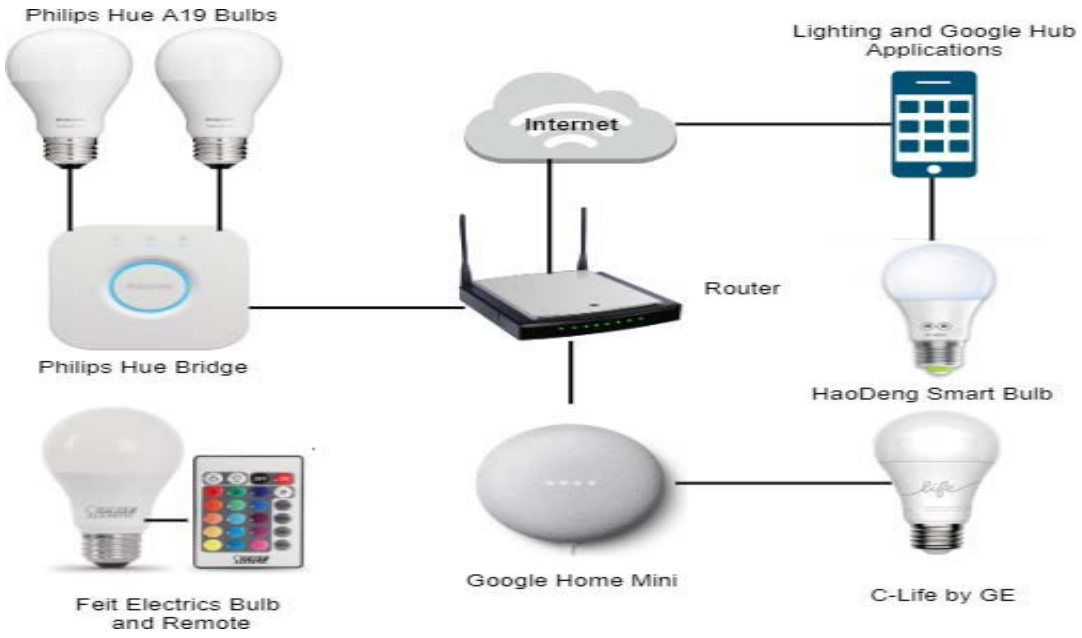
Το κατώφλι t είναι εξαρτώμενο από τα υλικά σύστασης των τοίχων, όπως και από την εσωτερική διαρρύθμιση και έτσι δεν απαιτείται διαρκής παραμετροποίηση παρά μονάχα στην αρχή. Οι γραμμές βάσης CSI που η χρήση τους συνίσταται για την εμφάνιση καταστάσεων δίχως την παρουσία κινήσεων σε εσωτερικούς χώρους, η προσαρμογή τους πετυχαίνεται αυτόματα σε περιβάλλοντα που παρουσιάζουν αλλαγές (όπως μετακινήσεις επίπλων σε μικρές αποστάσεις).

ΠΕΡΙΟΡΙΣΜΟΙ ΤΟΥ ΕΙΚΟΝΙΚΟΥ ΚΟΥΜΠΙΟΥ

- **Κινήσεις που δεν προκαλούνται από ανθρώπους.** Στην αρχέτυπη του έκδοση κατά τη σχεδίαση, αυτός ο παράγοντας δεν λήφθηκε υπόψη. Έτσι ένα κατοικίδιο ζώο πραγματοποιώντας ένα άλμα στο εσωτερικό του χώρου, είναι ικανό να ενεργοποιήσει τον HDVA.
- **Εξωτερική επίθεση στο οικιακό wifi.** Ένα σενάριο που όμως απαιτεί ιδιαίτερη πρακτικότητα, είναι αυτό της εξωτερικής παραβίασης από κακόβουλο άτομο προκαλώντας αυξομειώσεις της στάθμης του σήματος wifi του δρομολογητή, θέτοντας έμμεσα την ενεργοποίηση του εικονικού κουμπιού. Κάτι όμως που απαιτεί τους κωδικούς του χρήστη του δρομολογητή.
- **Επιμέρους συμβιβασμοί μεταξύ ευκολίας & ασφάλειας.** Προκειμένου να επιτευχθεί ο παραπάνω συμβιβασμός, μεγαλώνοντας το σημείο αναφοράς t, το εικονικό κουμπί αποκτά ισχυρή αναισθησία σε κινήσεις που γίνονται σε εξωτερικούς χώρους και αντίστοιχα οι χρήστες του HDVA διαθέτουν μικρότερο βελησνεκές αλληλεπίδρασης μαζί του.
- **Επίθεση με φυσική παρουσία.** Στο σχεδιασμό των επιθέσεων δεχθήκαμε πως τα κακόβουλα άτομα βρίσκονται έξω από τον εποπτευόμενο χώρο του σπιτιού και επιθυμούν να εισέλθουν. Στην περίπτωση που ένα άτομο καταφέρει να βρεθεί στον εσωτερικό χώρο, τότε θα είναι ικανό να πραγματοποιήσει πιο δόλιες πράξεις από το να προσβάλλει τη συσκευή HDVA. [82]

4.2 Μελέτη περίπτωσης έξυπνης λάμπας

Κατά τη διερεύνηση των τρωτών σημείων μεταξύ των συσκευών IoT, η αρχική μας μελέτη επικεντρώθηκε στην αλληλεπίδραση μεταξύ δύο διαφορετικών συσκευών, η οποία παρείχε κάποια εικόνα, αλλά δεν διέθετε επαρκή στοιχεία για να υποστηρίξουμε τους ισχυρισμούς μας με πειστικό τρόπο.



Εικόνα 28. Αρχιτεκτονική Έξυπνου Φωτισμού

Για να ενισχύσουμε τα συμπεράσματά μας, πραγματοποιήσαμε μια επακόλουθη αξιολόγηση τρωτότητας που αφορούσε τέσσερις συσκευές που ανήκαν στην ίδια κατηγορία: έξυπνος φωτισμός.

Οι συσκευές που εξετάσαμε προέρχονταν τόσο από γνωστές όσο και από λιγότερο γνωστές εταιρείες του κλάδου. Μεταξύ των διακεκριμένων κατασκευαστών ήταν η Philips Lighting (τώρα Signify) και η General Electric (GE), γνωστές για τα αντίστοιχα προϊόντα έξυπνου φωτισμού όπως το Philips Hue και οι έξυπνες λάμπες GE C-Life. Αυτές οι συσκευές προσφέρουν βασικές λειτουργίες όπως έλεγχο μέσω smartphone, φωνητικές εντολές και προγραμματισμό.

Εκτός από αυτούς τους μεγάλους κατασκευαστές, εξετάστηκαν προϊόντα έξυπνου φωτισμού από λιγότερο γνωστές εταιρείες όπως η Feit Electric Company, Inc. Που ασχολείται με την παραγωγή LED Party Bulbs και η HaoDeng, γνωστή για τον λαμπτήρα Bluetooth Mesh LED. Αυτά τα προϊόντα προσφέρουν χαρακτηριστικά όπως η

προσαρμογή του χρώματος και προηγμένες επιλογές ελέγχου μέσω ειδικών εφαρμογών.

Η μελέτη για τις ευπάθειες περιλάμβανε διάφορες πτυχές, συμπεριλαμβανομένων των φυσικών ευπαθειών, των ευπαθειών δικτύου, των ευπαθειών λογισμικού και των ευπαθειών κρυπτογράφησης. Τα αποτελέσματα αυτής της μελέτης παρουσιάζονται λεπτομερώς στην εικόνα 29, ενώ μια γραφική απεικόνιση της εγκατάστασης έξυπνου φωτισμού παρέχεται στην εικόνα 28.

Devices	Physical Vulnerability	Network Vulnerability	Software Vulnerability	Encryption Vulnerability
Philips Hue Smart Lighting	Motherboard Hack	Replay Attack DNSSEC DNS Spoofing Fake Server	"Keeps track of secret keys" Fake Server	Man-in-the-Middle attacks Unprotected communication (e.g., HTTP commands)
GE C-Life Smart Bulbs	Motherboard Hack	No Current Vulnerabilities Found	Unreliable Hub Linking	No Current Vulnerabilities Found
Feit Electric Party Bulbs	No Current Vulnerabilities Found	Not Applicable	Not Applicable	Not Applicable
HaoDeng Smart Bulbs	Motherboard Hack	Unencrypted communication	Buffer Overflow attack	Unprotected communication Information Disclosure

Εικόνα 29: Ευπάθειες Που Βρέθηκαν Στην Κατηγορία Έξυπνων Βοηθητικών Προγραμμάτων Φωτισμού

Κατά την ανάλυση, διαπιστώσαμε ότι οι γνωστοί πωλητές παρουσιάζουν συνήθως μια πιο προληπτική προσέγγιση όσον αφορά την αντιμετώπιση των ευπαθειών, κυκλοφορώντας συχνά σημειώσεις διορθώσεων και ενημερώσεις για την αντιμετώπιση ζητημάτων ασφαλείας. Για παράδειγμα, η Philips παρέχει λεπτομερείς σημειώσεις έκδοσης για το HueBridge V2, αντιμετωπίζοντας CVEs και NVDs.

Αντίθετα, οι λιγότερο γνωστοί προμηθευτές μπορεί να μην έχουν το ίδιο επίπεδο ελέγχου, αφήνοντας τις συσκευές τους δυνητικά πιο ευάλωτες. Για παράδειγμα, ενώ οι έξυπνοι λαμπτήρες της Feit Electric βρέθηκαν λιγότερο ευάλωτοι σε ορισμένες ευπάθειες λόγω των διαφορετικών μηχανισμών συνδεσιμότητάς τους, οι ευπάθειες σε συσκευές όπως η HaoDeng παραμένουν λιγότερο σαφείς λόγω της έλλειψης πληροφοριών σχετικά με την επιδιόρθωση.

Συμπερασματικά υπάρχει ανάγκη για πιο ολοκληρωμένες μελέτες ευπάθειας που να περιλαμβάνουν συσκευές από όλους τους προμηθευτές, ιδίως από λιγότερο γνωστούς κατασκευαστές. Συνιστάται επίσης η τυποποίηση των απαιτήσεων ασφαλείας σε όλες

τις συσκευές και τις κατηγορίες για τη βελτίωση της συνολικής στάσης ασφαλείας στο τοπίο του IoT. [28]

4.3 Μελέτη περίπτωσης έξυπνης Πρίζας. Τρωτά σημεία ασφαλείας του έξυπνου βύσματος(smart plug)

Στην ενότητα αυτή εξετάστηκαν τέσσερις τύποι επιθέσεων στον τομέα της κυβερνοασφάλειας. Αναλύθηκαν επίσης οι δυνητικές επιπτώσεις από την παραβίαση των βυσμάτων ασφαλείας χρησιμοποιώντας έξυπνα βύσματα για τη διερεύνηση των πιθανών ευπαθειών ασφαλείας.

4.3.1 Επίθεση Σάρωσης Συσκευής

Σε μια επίθεση σάρωσης συσκευής, ο επιτιθέμενος αναζητά όλα τα βύσματα που είναι συνδεδεμένα στο δίκτυο, προσδιορίζοντας τις διευθύνσεις MAC των smart plugs από συγκεκριμένο προμηθευτή. Σύμφωνα με έρευνα αρκετοί χρήστες δεν αλλάζουν τον προεπιλεγμένο κωδικό πρόσβασης μετά την εγκατάσταση μιας IoT συσκευής, βασίζοντας την ασφάλεια στον κατασκευαστή της εκάστοτε συσκευής. Κατά την φάση ελέγχου ταυτότητας μεταξύ των smart plugs και του ελεγκτή (controller), ο ελεγκτής λαμβάνει το 1070 πακέτο όταν το βύσμα είναι συνδεδεμένο αλλά και ο κωδικός σωστός. Κάποιος κακόβουλος θα θελήσει να δημιουργήσει ένα μήνυμα ελέγχου ταυτότητας που περιλαμβάνει την διεύθυνση MAC του βύσματος, το όνομα που επέλεξε ο χρήστης και τον κωδικό πρόσβασης, για να γίνει έλεγχος μεταξύ των θυμάτων εάν κάποιο χρησιμοποιεί ένα βύσμα με συγκεκριμένη MAC διεύθυνση και τον προεπιλεγμένο κωδικό πρόσβασης (π.χ. Admin: 1234). Το “Admin” είναι σκληρά κωδικοποιημένο και δεν λειτουργεί πραγματικά ως όνομα χρήστη, καθώς οι διευθύνσεις MAC των βυσμάτων λειτουργούν περισσότερο ως αναγνωριστικά χρηστών. Για μια επιτυχημένη επίθεση σάρωσης συσκευών το κλειδί είναι η γνώση των MAC διευθύνσεων της εκάστοτε IoT συσκευής. Δυστυχώς για τον επιτιθέμενο αυτές οι διευθύνσεις είναι γνωστές με μια απλή αναζήτηση του μοντέλου στο διαδίκτυο.

Το πρώτο μισό της διεύθυνσης MAC αναφέρεται στον κατασκευαστή ενώ το υπόλοιπο μισό στην εκάστοτε συσκευή. Συνήθως οι κατασκευαστές χρησιμοποιούν συγκεκριμένο

	Password Correct	Password Wrong
Plug Online	1070	no response
Plug Offline or N/A	5000	5000

εύρος διευθύνσεων για το κάθε μοντέλο, αυτό δίνει την δυνατότητα στον “κακόβουλο” να δοκιμάσει όλο τον χώρο διευθύνσεων MAC ενός κατασκευαστή σε μια επίθεση ωμής βίας.

Η εικόνα 30 παρουσιάζει τις πιθανές απαντήσεις σε ένα μήνυμα ελέγχου ταυτότητας που αποτελείται από έναν controller και ένα smart plug με συγκεκριμένη διεύθυνση MAC και κωδικό πρόσβασης. Εάν η συγκεκριμένη συσκευή είναι συνδεδεμένη και ο κωδικός πρόσβασης είναι σωστός, ο controller λαμβάνει το πακέτο 1070. Εάν ο κωδικός πρόσβασης είναι λανθασμένος, το smart plug απαντά με ένα πακέτο εντολής 1120, χωρίς να προωθήσει το μήνυμα στον controller. Για να αντιμετωπιστεί αυτό, ο επιτιθέμενος πρέπει να ορίσει ένα χρονοδιακόπτη και να προσπαθήσει περισσότερες φορές εάν δεν λάβει απάντηση. Εάν το smart plug είναι εκτός σύνδεσης ή δεν υπάρχει, ο διακομιστής απαντά με ένα πακέτο 5000 στον επιτιθέμενο. Αυτό κάνει δύσκολη την ανίχνευση αν το smart plug είναι εκτός σύνδεσης. Ωστόσο, αυτό δεν επηρεάζει την επίθεση σάρωσης συσκευών. Με βάση αυτές τις απαντήσεις, ο επιτιθέμενος μπορεί να εντοπίσει smart plug με προεπιλεγμένους κωδικούς πρόσβασης και βύσματα που δεν χρησιμοποιούν τον αλλαγμένο κωδικό.

4.3.2 Επίθεση Ωμής Βίας

Αφού πραγματοποιηθεί η επίθεση σάρωσης ο επιτιθέμενος μπορεί να εντοπίσει όλα τα smart plugs που δεν χρησιμοποιούν τους προεπιλεγμένους κωδικούς πρόσβασης. Στη συνέχεια, μπορεί επιλέγοντας τα να ξεκινήσει τη διαδικασία κατασκευής πακέτων (packet crafting) 1030, δοκιμάζοντας όλους τους πιθανούς κωδικούς πρόσβασης. Στην πραγματικότητα, ο επιτιθέμενος απλώς περιμένει μέχρι να λάβει τη σωστή απάντηση. Παρόλο που ο διακομιστής ελέγχου ταυτότητας δεν φαίνεται να αποκλείει αυτήν την επίθεση, αντιμετωπίζουμε μια περίπτωση όπου το smart plug της Edimax επιτρέπει στην πραγματικότητα κωδικούς πρόσβασης με έως και 20 χαρακτήρες, συμπεριλαμβανομένων αριθμών και κεφαλαίων / πεζών γραμμάτων, που δεν

αναφέρονται σε κανένα εγχειρίδιο ή διαδικτυακή πηγή. Αυτή η ενέργεια αποτρέπει με επιτυχία την επίθεση ωμής βίας εφόσον ο χρήστης επιλέξει έναν ασφαλή και πολύπλοκο κωδικό πρόσβασης. Ωστόσο, το σύστημα σύνδεσης εκτίθεται σε μια επίθεση παραποίησης συσκευής, η οποία μπορεί να διαρρεύσει οποιεσδήποτε διαπιστευτήρια του smart plug.

4.3.3 Επίθεση Απομίμησης Συσκευής

Η διαδικασία επίθεσης πλαστογράφησης συσκευής λειτουργεί με τη χρήση ενός λογισμικού bot που μιμείται ένα βύσμα και εκτελεί τον έλεγχο ταυτότητας με τον απομακρυσμένο ελεγκτή, προκειμένου να αποκτήσει απευθείας τα διαπιστευτήρια από τον ελεγκτή. Η διαδικασία αυτή συνίσταται σε τέσσερα βήματα:

1. Ο επιτιθέμενος επιλέγει ένα στόχο βύσμα με συγκεκριμένη διεύθυνση MAC και καταχωρίζει το πλαστογραφημένο βύσμα.

2. Το πλαστογραφημένο βύσμα επικοινωνεί με το σύστημα ελέγχου ταυτότητας, υποδιαστολή συμπεριφοράς ενός πραγματικού βύσματος και στέλνει ένα πακέτο εντολής 1010.
3. Όταν ένα θύμα ανοίγει την εφαρμογή στο smartphone, αυτή στέλνει αυτόματα το πακέτο 1030 στον ελεγκτή ελέγχου ταυτότητας.
4. Ο ελεγκτής προωθεί το μήνυμα στο πλαστογραφημένο βύσμα, το οποίο αποκτά τα διαπιστευτήρια.

Εάν ο επιτιθέμενος επιθυμεί να κρύψει την επίθεση spoofing από το θύμα, απαιτούνται πρόσθετα μέτρα σε σχέση με το spoofed plug. Υπάρχουν δύο σενάρια που πρέπει να ληφθούν υπόψη. Στην πρώτη περίπτωση, όπου το πραγματικό βύσμα και ο ελεγκτής βρίσκονται στο ίδιο WLAN, η παρουσία του spoofed plug δεν επηρεάζει καθόλου τη διαδικασία ελέγχου του πραγματικού βύσματος. Ο ελεγκτής εξακολουθεί να επικοινωνεί με το πραγματικό βύσμα στο WLAN, όπως αναλύεται στα βήματα 5β και 6β της ενότητας IV, και το plug ελέγχεται κανονικά με τα βήματα 7b και 8b. Επομένως, το θύμα δεν θα εντοπίσει καμία ανωμαλία στη διαδικασία.

Στη δεύτερη περίπτωση, όπου το βύσμα και ο ελεγκτής βρίσκονται σε διαφορετικά δίκτυα, η επίθεση spoofing δημιουργεί προκλήσεις. Ο ελεγκτής-θύμα επικοινωνεί με το πλαστογραφημένο βύσμα. Η πρόκληση είναι να μεταδοθούν από το παραποιημένο βύσμα οι εντολές του θύματος στο πραγματικό βύσμα, ώστε να μην διαφανεί η επίθεση στο θύμα. Για να το πετύχει αυτό, ο επιτιθέμενος πρέπει να διακόψει την αποστολή των πακέτων 1010 στον διακομιστή ελέγχου ταυτότητας. Αυτό έχει ως σκοπό την τερματισμό της επίθεσης spoofing και να επιτρέψει στο πραγματικό βύσμα να εγγραφεί στον διακομιστή ελέγχου ταυτότητας το συντομότερο δυνατό. Στη συνέχεια, ο επιτιθέμενος δημιουργεί μια σύνδεση TCP με τον υπολογιστή εντολών διακομιστή αναμετάδοσης και αποστέλλει τη διεύθυνση MAC του πραγματικού βύσματος-στόχου και το σωστό αναγνωριστικό αναμετάδοσης, σύμφωνα με το βήμα 9α της ενότητας IV. Έτσι, ο επιτιθέμενος καταφέρνει να λάβει τις εντολές του θύματος και να τις αναπαράγει στο πραγματικό βύσμα, χωρίς να ενημερωθεί το θύμα για την επίθεση.

4.3.4 Επίθεση Firmware

Ο επιτιθέμενος μπορεί να εγκαταστήσει κακόβουλο λογισμικό στο smartplug με σκοπό να το ελέγχει από απόσταση. Μόλις το κακόβουλο λογισμικό είναι ενεργοποιημένο στο smart plug, μπορεί να δημιουργήσει μια σύνδεση προς έναν απομακρυσμένο κακόβουλο διακομιστή, επιτρέποντάς του να αναλαμβάνει τον έλεγχο του βύσματος από απόσταση. Μέσω αυτής της ανάκρισης, ο επιτιθέμενος μπορεί να εκτελέσει περαιτέρω επιθέσεις, όπως την εγκατάσταση κακόβουλων προγραμμάτων στο smart plug.

Σε αυτήν την επίθεση, υποθέτουμε ότι ο επιτιθέμενος έχει πρόσβαση στο τοπικό δίκτυο του smart plug και μπορεί να παρακολουθήσει την κυκλοφορία μεταξύ του plug και του ελεγκτή. Έτσι, μπορεί να αντλήσει τον κωδικοποιημένο όνομα χρήστη και τον κωδικό πρόσβασης στην επικεφαλίδα HTTP. Έπειτα, ο επιτιθέμενος μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να αυθεντικοποιηθεί και να μεταφορτώσει κακόβουλο λογισμικό στον διακομιστή HTTP του βύσματος.

Ο επιτιθέμενος μπορεί να επεξεργαστεί το λογισμικό του βύσματος προσθέτοντας κακόβουλο κώδικα, καθώς ο κώδικας open course είναι προσβάσιμος από όλους. Αυτό

επιτρέπει στον επιτιθέμενο να εγκαταστήσει προσαρμοσμένο λογισμικό και να το μεταφορτώσει στον διακομιστή HTTP του smart plug. Το βύσμα αυτόματα θα εγκαταστήσει τον κακόβουλο κώδικα και θα επανεκκινήσει το σύστημα. Η υπηρεσία DHCP θα ξεκινήσει αυτόματα κατά την εκκίνηση και θα εκτελέσει τον κακόβουλο κώδικα. [81]

Συμπεράσματα & Μελλοντικές Επεκτάσεις

Στη συγκεκριμένη εργασία έγινε ανίχνευση μιας αδυναμίας ασφαλείας ενός HDVA και συγκεκριμένα της Alexa. Οι υπηρεσίες που προσφέρουν οι HDVA στηρίζονται μόνο σε έναν ασθενή έλεγχο πιστοποίησης ενός δείκτη, που όμως σχετικά εύκολα προσβάλλεται. Έτσι προτάθηκε ένας επιπλέον παράγοντας εξακρίβωσης ταυτότητας, αυτός της φυσικής παρουσίας. Έτσι ένας HDVA μπορεί να προσφέρει τις υπηρεσίες του μόνο όταν υπάρχει φυσική παρουσία ατόμου σε κοντινή μάλιστα απόσταση από αυτόν. Σχεδιάστηκε έτσι μια λύση που ονομάστηκε εικονικό κουμπί ασφαλείας ανιχνεύοντας την ανθρώπινη κίνηση. Η αξιολόγηση και η προτυποποίηση έγινε σε μία συσκευή Alexa. Στην πειραματική διαδικασία που ακολούθησε, διαπιστώθηκε ότι τόσο στο περιβάλλον του εργαστηρίου όσο και σε πραγματικό οι μετρήσεις που πάρθηκαν ήταν ακριβείς και αξιόπιστες.

Οι μελλοντικές εργασίες θα μπορούσαν να επικεντρωθούν στη διεξαγωγή πιο εκτεταμένων αξιολογήσεων ευπάθειας σε πλήρως εξοπλισμένα περιβάλλοντα έξυπνων σπιτιών, συμπεριλαμβανομένων συσκευών από λιγότερο γνωστούς κατασκευαστές.

Ελπίζουμε η προτεινόμενη πρόταση να γίνει το έναυσμα για περαιτέρω εξέλιξη στο χώρο της ασφάλειας των HDVA.

Βιβλιογραφία

A. G. Y. G. Mahesh Kavre, «IEEE Xplore,» 18 12 2019. [Ηλεκτρονικό]. Available:
1] https://ieeexplore.ieee.org/document/9105831.

J. V. D. V. P. R. H. A. P. Suresh, «IEEE Xplore,» 27 11 2014. [Ηλεκτρονικό]. Available:
2] https://ieeexplore.ieee.org/document/7043637/authors#authors.

A. Sunyaev, Internet Computing Principles of Distributed Systems and Emerging Internet-
3] Based Technologies, Springer Cham, 2020.

A. K. S. Khanna, «SpringerLink,» 28 5 2020. [Ηλεκτρονικό]. Available:
4] https://link.springer.com/article/10.1007/s11277-020-07446-4.

B. Jovanovic, «DataProt,» 6 2 2024. [Ηλεκτρονικό]. Available:
5] https://dataprot.net/statistics/iot-statistics/.

S. Aggarwal, «TechAhead,» 11 9 2020. [Ηλεκτρονικό]. Available:
6] https://www.techaheadcorp.com/knowledge-center/evolution-of-iot/.

T.-J. L. F.-Y. L. J. S. H.-Y. D. Miao Wu, «IEEE Xplore,» 20 8 2010. [Ηλεκτρονικό]. Available:
7] https://ieeexplore.ieee.org/document/5579493.

B. A. M. H. J. S. Ruth Ande, «ScienceDirect,» 9 2 2019. [Ηλεκτρονικό]. Available:
8] https://www.sciencedirect.com/science/article/abs/pii/S2210670719303725.

S. R. S. Pallavi Sethi, «Hindawi,» 18 1 2017. [Ηλεκτρονικό]. Available:
9] https://www.hindawi.com/journals/jece/2017/9324035/.

D. J. Debajit Datta, «ResearchGate,» 7 2020. [Ηλεκτρονικό]. Available:
1 https://www.researchgate.net/publication/344930533_Exploration_of_Various_Attacks_and
0] _Security_Measures_Related_to_the_Internet_of_Things.

«nabto,» [Ηλεκτρονικό]. Available: https://www.nabto.com/guide-iot-protocols-
1 standards/.
1]

«LoRa,» [Ηλεκτρονικό]. Available: https://lora-
1 developers.semtech.com/documentation/tech-papers-and-guides/lora-and-lorawan/.
2]

«RFWirelessWorld,» [Ηλεκτρονικό]. Available: https://www.rfwireless-
1

3] world.com/Terminology/DDS-protocol-architecture.html.

Y. C. T. Kunz, «IEEE Xplore,» 11 4 2016. [Ηλεκτρονικό]. Available:
1 https://ieeexplore.ieee.org/document/7496622.
4]

N. Zubovich, «SumatoSoft,» 31 3 2024. [Ηλεκτρονικό]. Available:
1 https://sumatosoft.com/blog/advantages-of-internet-of-things-10-benefits-you-should-
5] know.

D. Kovalenko, «LIGHT IT GLOBAL,» [Ηλεκτρονικό]. Available: https://light-it.net/blog/9-
1 prominent-benefits-of-iot-for-business/.
6]

«Javatpoint,» [Ηλεκτρονικό]. Available: https://www.javatpoint.com/iot-advantage-and-
1 disadvantage.
7]

«geeksforgeeks,» [Ηλεκτρονικό]. Available: https://www.geeksforgeeks.org/advantages-
1 and-disadvantages-of-iot/.
8]

«RS Online,» 3 2022. [Ηλεκτρονικό]. Available: https://uk.rs-
1 online.com/web/content/discovery/ideas-and-advice/iot-advantages.
9]

«tutorialandexample,» 11 12 2019. [Ηλεκτρονικό]. Available:
2 https://www.tutorialandexample.com/advantages-disadvantages-of-iot.
0]

B. P. L. R. Alexander S. Gillis, 8 2023. [Ηλεκτρονικό]. Available:
2 https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT.
1]

K. L. In Lee, «ScienceDirect,» 28 4 2015. [Ηλεκτρονικό]. Available:
2 https://www.sciencedirect.com/science/article/abs/pii/S0007681315000373.
2]

S. K. Abhishek Khanna, «ResearchGate,» 28 5 2020. [Ηλεκτρονικό]. Available:
2 https://www.researchgate.net/publication/341703088_Internet_of_Things_IoT_Applications
3] _and_Challenges_A_Comprehensive_Review.

A. D. R. M. P. Hamed Haddadpajouh, «Research Gate,» 13 11 2019. [Ηλεκτρονικό].
2 Available:

4] https://www.researchgate.net/publication/337260741_A_survey_on_internet_of_things_security_Requirements_challenges_and_solutions.

G. K. L. A. Chopra Kriti, «IEEE Xplore,» 14 2 2019. [Ηλεκτρονικό]. Available:
2 https://ieeexplore.ieee.org/document/8862269.
5]

S. V. S.R. Jino Ramson, «IEEE Xplore,» 5 3 2020. [Ηλεκτρονικό]. Available:
2 https://ieeexplore.ieee.org/abstract/document/9075807.
6]

A. H. Hussein, «Semantic Scholar,» 10 11 2019. [Ηλεκτρονικό]. Available:
2 https://www.semanticscholar.org/paper/Internet-of-Things-%28IOT%29%3A-Research-
7] Challenges-and-Hussein/ef32bce38bf492c2b8cf067eb14cb8693501d82d?p2df.

J. C. M. M. A. Brittany D. Davis, «IEEE Xplore,» 30 3 2020. [Ηλεκτρονικό]. Available:
2 https://ieeexplore.ieee.org/document/9050664.
8]

«Digiteum,» 9 2 2022. [Ηλεκτρονικό]. Available: https://www.digiteum.com/internet-of-
2 things-energy-management/.
9]

D. Prasad, «Help Wire,» 20 4 2023. [Ηλεκτρονικό]. Available:
3 https://www.helpwire.app/blog/iot-energy-management/.
0]

«igzy,» [Ηλεκτρονικό]. Available: https://igzy.com/iot-energy-management/.
3
1]

«Impacx,» [Ηλεκτρονικό]. Available: https://impacx.io/blog/smart-energy-management/.
3
2]

A. Hofer, «Softeq,» 26 11 2021. [Ηλεκτρονικό]. Available:
3 https://www.softeq.com/blog/smart-grid-solutions-9-examples-in-the-energy-grid-
3] management-market.

J. Sykes, «Solar Choice,» 4 11 2019. [Ηλεκτρονικό]. Available:
3 https://www.solarchoice.net.au/blog/home-energy-management-systems-a-smart-way-to-
4] save/.

N. Kadanvar, «Embedded Computing,» 24 6 2019. [Ηλεκτρονικό]. Available:

[35] https://embeddedcomputing.com/technology/iot/energy-management-the-internet-of-things-changes-everything.

[36] S. Mazur, «Digi,» 9 12 2020. [Ηλεκτρονικό]. Available: https://www.digi.com/blog/post/introduction-to-smart-transportation-benefits.

[37] «The Constructor,» [Ηλεκτρονικό]. Available: https://theconstructor.org/transportation/intelligent-transportation-system/1120/.

[38] K. O'Brien, «IBM,» 23 5 2023. [Ηλεκτρονικό]. Available: https://www.ibm.com/blog/smart-transportation/.

[39] «IOT for all,» 22 12 2020. [Ηλεκτρονικό]. Available: https://www.iotforall.com/what-makes-transportation-smart-defining-intelligent-transportation.

[40] «Celona,» [Ηλεκτρονικό]. Available: https://www.celona.io/private-mobile-network-blog.

[41] C. BasuMallick, «Spiceworks,» 2 3 2023. [Ηλεκτρονικό]. Available: https://www.spiceworks.com/tech/iot/articles/what-is-iiot/#lg=1&slide=0.

[42] A. S. Gillis, «Tech Target,» 8 2023. [Ηλεκτρονικό]. Available: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT.

[43] «Trend Micro,» [Ηλεκτρονικό]. Available: https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot.

[44] «Magellanx,» [Ηλεκτρονικό]. Available: https://magellanx.co/industrial-iot-solutions-examples/.

[45] S. R. S. S. Manuel Silverio-Fernández, «Viejournal Springer Open,» 9 5 2018. [Ηλεκτρονικό]. Available: https://viejournal.springeropen.com/articles/10.1186/s40327-018-0063-8.

T. J. T. D. H. N. Christian Koehler, «Research Gate,» 9 2015. [Ηλεκτρονικό]. Available:

4 https://dl.acm.org/doi/10.1145/2750858.2804288.
6]

H. H. G. C. F. N. C. Vijay Sivaraman, «Research Gate,» 6 2018. [Ηλεκτρονικό]. Available:
4 https://www.researchgate.net/publication/325562955_Smart_IoT_Devices_in_the_Home_S
7] ecurity_and_Privacy_Implications.

M. Lynch, «The Tech Edvocate,» 19 3 2023. [Ηλεκτρονικό]. Available:
4 https://www.thetechedvocate.org/what-is-a-smart-device/.
8]

A. I. G. M. Luigi Atzori, «Research Gate,» 5 10 2010. [Ηλεκτρονικό]. Available:
4 https://www.researchgate.net/publication/222571757_The_Internet_of_Things_A_Survey.
9]

M. G. M. M. M. A. M. A. Ala Al-Fuqaha, «IEEE Xplore,» 15 6 2015. [Ηλεκτρονικό].
5 Available: https://ieeexplore.ieee.org/document/7123563.
0]

R. B. S. M. M. P. Jayavardhana Gubbi, «Science Direct,» 9 2013. [Ηλεκτρονικό]. Available:
5 https://www.sciencedirect.com/science/article/abs/pii/S0167739X13000241.
1]

A. D. Rajkumar Buyya, «Research Gate,» 5 2016. [Ηλεκτρονικό]. Available:
5 https://www.researchgate.net/publication/309094566_Internet_of_Things_Principles_and_P
2] aradigms.

M. H. F. M. Dieter Uckelmann, «Spinger Link,» 2011. [Ηλεκτρονικό]. Available:
5 https://link.springer.com/book/10.1007/978-3-642-19157-2.
3]

M. Kranz, Building the Internet of Things.
5
4]

E. G. M. C. A. L. A. L. Claire Rowland, Designing Connected Products: UX for the Consumer
5 Internet of Things.
5]

M. Naser, «Vexxhost,» 26 2 2021. [Ηλεκτρονικό]. Available:
5 https://vexxhost.com/blog/internet-of-things-101/.
6]

«TechVidvan,» [Ηλεκτρονικό]. Available: https://techvidvan.com/tutorials/what-are-iot-

5 devices/.
7]

«ServiceNow,» [Ηλεκτρονικό]. Available: https://www.servicenow.com/products/field-
5 service-management/what-is-iot-device-management.html.
8]

D. B. D. R. S. H. A. J. M. H. S. R. M. P. J. A.-M. V. H. C. D. A. Joel J. P. C. Rodrigues, «IEEE
5 Xplore,» 4 1 2018. [Ηλεκτρονικό]. Available: https://ieeexplore.ieee.org/document/8246498.
9]

S. Siripathi, «Envatotuts,» 29 1 2018. [Ηλεκτρονικό]. Available:
6 https://code.tutsplus.com/wearable-development-platforms--cms-30213a.
0]

K. Yasar, «Tech Target,» 11 2023. [Ηλεκτρονικό]. Available:
6 https://www.techtarget.com/searchmobilecomputing/definition/wearable-technology.
1]

«Addevice,» 11 4 2024. [Ηλεκτρονικό]. Available:
6 https://www.addevice.io/blog/wearable-app-development.
2]

«Condeco,» 14 9 2018. [Ηλεκτρονικό]. Available:
6 https://www.condecosoftware.com/blog/the-history-of-wearable-technology/.
3]

J. D. L. E. D. Mary M Berglund, «Research Gate,» 9 2016. [Ηλεκτρονικό]. Available:
6 https://www.researchgate.net/publication/307910607_A_survey_of_the_historical_scope_a
4] nd_current_trends_of_wearable_technology_applications.

Y. H. T. N. G. L. Suranga Seneviratne, «Research Gate,» 7 2017. [Ηλεκτρονικό]. Available:
6 https://www.researchgate.net/publication/318717275_A_Survey_of_Wearable_Devices_and
5] _Challenges.

J. L. T. K. Kate Crawford, «Research Gate,» 8 2015. [Ηλεκτρονικό]. Available:
6 https://www.researchgate.net/publication/278682552_Our_metrics_ourselves_A_hundred_
6] years_of_self-tracking_from_the_weight_scale_to_the_wrist_wearable_device.

R. K. R. I. P. S. B. B. T. Poongodi, «SpringerLink,» 17 7 2019. [Ηλεκτρονικό]. Available:
6 https://link.springer.com/chapter/10.1007/978-3-030-23983-1_10.
7]

K. T. D. I. H. R. S. D. M. H. Mostafa Haghi, «National Library of Medicine,» 23 1 2017.

[Ηλεκτρονικό]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5334130/.

«Finite Solution,» 19 4 2021. [Ηλεκτρονικό]. Available: https://www.finitesolutions.co.uk/blog/smart-home-entertainment-systems/.

K. Yasar, «Tech Target,» 8 2023. [Ηλεκτρονικό]. Available: https://www.techtarget.com/iotagenda/definition/smart-home-or-building.

«Cleartax,» 16 8 2023. [Ηλεκτρονικό]. Available: https://cleartax.in/g/terms/smart-home.

«Smlease,» [Ηλεκτρονικό]. Available: https://www.smlease.com/entries/automation/what-is-smart-lighting-technology/.

N. Lars, «Wired,» [Ηλεκτρονικό]. Available: https://www.wired.com/insights/2014/06/connected-medical-devices-apps-leading-iot-revolution-vice-versa/.

R. Sentance, «Econsultancy,» 19 1 2021. [Ηλεκτρονικό]. Available: https://econsultancy.com/internet-of-things-healthcare/.

«Korewireless,» [Ηλεκτρονικό]. Available: https://www.korewireless.com/news/connected-health-what-it-is-and-how-it-works.

A. S. P. Constantinos S. Pattichis, «National Library of Medicine,» 16 10 2019. [Ηλεκτρονικό]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8519500/.

L. Catranis, «irdeto,» 22 6 2022. [Ηλεκτρονικό]. Available: https://blog.irdeto.com/healthcare/what-is-the-difference-between-connected-health-and-medtech/.

«Wipro,» [Ηλεκτρονικό]. Available: https://www.wipro.com/business-process/what-can-iot-do-for-healthcare-/.

R. V. Mike Thomas, «Builtin,» 31 5 2023. [Ηλεκτρονικό]. Available:

7 https://builtin.com/internet-things/iot-in-healthcare.
9]

A. Meola, «EMARKETER,» 12 1 2023. [Ηλεκτρονικό]. Available:
8 https://www.insiderintelligence.com/insights/iot-healthcare/.
0]

J. L. Y. X. C. G. K. W. X. F. Zhen Ling, «IEEE Xplore,» 23 5 2017. [Ηλεκτρονικό]. Available:
8 https://ieeexplore.ieee.org/document/7932855.
1]