ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Σχεδίαση και υλοποίηση έξυπνων κτιρίων με βάση IoT και επισκόπηση των απειλών και προκλήσεων για τις έξυπνες οικιακές συσκευές και εφαρμογές τους

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

των

ΚΙΑΚΟΣ ΣΤΥΛΙΑΝΟΣ ΑΕΜ: 2664

ΚΙΟΥΤΣΟΥΚΗΣ ΑΠΟΣΤΟΛΟΣ ΑΕΜ: 2694

Επιβλέπων : Σπυρίδων Νικολάου

Λέκτορας

Καστοριά - Σεπτέμβριος 2022

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Σχεδίαση και υλοποίηση έξυπνων κτιρίων με βάση IoT και επισκόπηση των απειλών και προκλήσεων για τις έξυπνες οικιακές συσκευές και εφαρμογές τους

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΚΙΑΚΟΣ ΣΤΥΛΙΑΝΟΣ ΑΕΜ: 2664

ΚΙΟΥΤΣΟΥΚΗΣ ΑΠΟΣΤΟΛΟΣ ΑΕΜ: 2694

Επιβλέπων : Σπυρίδων Νικολάου

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13/09/2022

.....	.....	.....
Σπυρίδων Νικολάου	Νίκος Δημόκας	Δημήτριος Ι. Βέργαδος
Λέκτορας	Επίκουρος Καθηγητής	Επίκουρος Καθηγητής

Καστοριά Σεπτέμβριος - 2022

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε θερμά τον καθηγητή μας κ. Σπυρίδων Νικολάου για την ανάθεση της παρούσας εργασίας, την καθοδήγηση και γενικά για την συνεχή βοήθεια που μας παρείχε καθ' όλη την διάρκεια εκπόνησής της. Επίσης, θα θέλαμε να ευχαριστήσουμε όλους τους καθηγητές και συμφοιτητές που συναντήσαμε σε αυτή η διαδρομή των σπουδών μας, καθώς όλοι συνετέλεσαν με τον δικό τους τρόπο για να φτάσουμε ως εδώ.

Και τέλος, θα θέλαμε να ευχαριστήσουμε ιδιαίτερα τις οικογένειές μας για την υποστήριξη και τη ενθάρρυνση που μας έδωσαν, τόσο κατά την σύνταξη της παρούσας εργασίας όσο και κατά την διάρκεια των σπουδών μας.

Περίληψη

Στην παρούσα εργασία με θέμα "Σχεδίαση και υλοποίηση έξυπνων κτιρίων με βάση IoT και επισκόπηση των απειλών και προκλήσεων για τις έξυπνες οικιακές συσκευές και εφαρμογές τους" παρουσιάζονται και αναλύονται διεξοδικά όλες εκείνες οι πληροφορίες που αφορούν στην τεχνολογία του Internet of Things και συγκεκριμένα στην εφαρμογή του στα έξυπνα κτίρια και ειδικότερα στις συνδεδεμένες έξυπνες οικιακές συσκευές.

Αρχικά παραθέτουμε τους απαραίτητους ορισμούς που απαιτούνται για την κατανόηση του θέματος της εργασίας από τον αναγνώστη. Οι ορισμοί είναι για το κομμάτι της τεχνολογίας που αφορά το IoT και το Cloud Computing που είναι το θεμέλιο πάνω στο οποίο βασίζεται η ανάπτυξη των έξυπνων κτιρίων. Στη συνέχεια αναφερόμαστε στην αρχιτεκτονική και την μοντελοποίηση του IoT με εξειδικευμένες πληροφορίες και τεχνικές λεπτομέρειες σχετικά με την πρακτική εφαρμογή και λειτουργία των συσκευών.

Έπειτα απαριθμούνται κάποιες από τις σημαντικότερες εφαρμογές του IoT στην καθημερινή ζωή, σε διάφορους επιχειρηματικούς και κοινωνικούς τομείς και αναλύεται τι είναι και σε ποια τεχνολογικά συστήματα βασίζεται η ανάπτυξή του. Στη συνέχεια παρουσιάζονται συγκεκριμένες εφαρμογές του IoT όπως είναι τα έξυπνα συστήματα θέρμανσης-ψύξης, ο έξυπνος φωτισμός και η πυρανίχνευση. Επιπρόσθετα, αναφέρουμε τα βασικά πλεονεκτήματα και μειονεκτήματα των έξυπνων κτιρίων και τις κατηγορίες στις οποίες διακρίνονται. Επιπλέον, αναφερόμαστε στα θέματα ασφαλείας και στις προκλήσεις που δημιουργούνται σχετικά με τα έξυπνα κτίρια, όπως είναι ζητήματα υγείας, κυβερνοεπιθέσεις, βλάβες και τεχνικά ζητήματα.

Τέλος, φτάνοντας στο τελευταίο κεφάλαιο της εργασίας επικεντρωνόμαστε σε κάποιες μελέτες περιπτώσεων αναφορικά με ζητήματα θεμάτων ασφαλείας των έξυπνων κτιρίων όπως για παράδειγμα είναι η μαζική επίθεση που έγινε το 2016 με την ονομασία Mirai Botnet. Συνεχίζοντας αναφέρουμε τις δύο έξυπνες οικιακές συσκευές με τις περισσότερες παραβιάσεις και τις διαδικασίες με τις οποίες προσβάλλονται.

Λέξεις Κλειδιά: *Διαδίκτυο των πραγμάτων, υπολογιστικό νέφος, έξυπνα κτήρια, συστήματα διαχείρισης BMS, πρότυπο κτιριακού ελέγχου KNX, διεθνές πρότυπο X10, τεχνολογία επικοινωνίας κοντινού πεδίου, Mirai Botnet, Bluetooth, BlueBorne*

Abstract

In this dissertation on "Design and implementation of smart buildings based on IoT and overview of the threats and challenges for smart home devices and their applications" all the information related to the Internet of Things technology and specifically its application on smart buildings and in particular connected smart home devices are presented and thoroughly analyzed.

First we mention the necessary definitions required for the reader's understanding of the topic of the paper. The definitions are for the IoT and Cloud Computing part of the technology that is the foundation on which the development of smart buildings is based. After that we address IoT architecture and modeling with specialized information and technical details about the practical implementation and operation of the devices.

Then some of the most important applications of IoT in everyday life, in various business and social sectors, are listed and we analyze what it is and on which technological systems its development is based. Next, specific IoT applications are presented, such as smart heating-cooling systems, smart lighting and fire detection.

In addition, we mention the main advantages and disadvantages of smart buildings and the categories in which they are distinguished. Furthermore, we address the security issues and the challenges that arise in relation to smart buildings, such as health issues, cyber-attacks, breakdowns and technical issues.

Finally, reaching the last chapter of the paper, we focus on some case studies regarding smart building security issues, such as the massive attack called the Mirai Botnet that took place in 2016. Continuing we mention the two smart home devices with the most breaches and the processes by which they are compromised.

Key Words: *Internet of Things, Cloud Computing, Smart Buildings, Building Management System BMS, Building control standard, International standard X10, Near Field Communication, Mirai Botnet, Bluetooth, BlueBorne*

Πίνακας Περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Εισαγωγή

Αρχικά θα θέλαμε να αναφέρουμε πως σε αυτή την εργασία αναφερόμαστε στα έξυπνα κτίρια τα οποία είναι σχεδιασμένα με τη τεχνολογία του διαδικτύου των πραγμάτων - IoT και αναλύουμε τις απειλές και τις προκλήσεις που προκύπτουν από τις εφαρμογές των επιμέρους έξυπνων συσκευών που χρησιμοποιούνται σε αυτά. Ξεκινώντας το πρώτο κεφάλαιο αναφέρουμε εισαγωγικές έννοιες και ορισμούς όπως το IoT, το Cloud Computing, την αρχιτεκτονική και τη μοντελοποίηση που είναι βασισμένη η τεχνολογία του IoT. Συνεχίζοντας σε πρακτική εφαρμογή βλέπουμε το μεγάλο φάσμα στο οποίο βρίσκει εφαρμογή όπως είναι η καθημερινή ζωή, η βιομηχανία και γενικότερα η οικονομία καθώς και εφαρμογές σε κοινωνικά θέματα και θέματα ασφαλείας.

Στο δεύτερο κεφάλαιο αναλύουμε τι είναι τα έξυπνα κτίρια και τις λειτουργίες και τεχνολογίες που χρησιμοποιούνται σε αυτά. Τέτοιες τεχνολογίες αποτελούν τα συστήματα διαχείρισης κτιρίων BMS και το πρότυπο κτιριακού ελέγχου KNX. Επίσης αναφέρουμε παραδείγματα τέτοιων έξυπνων εφαρμογών όπως είναι η έξυπνη θέρμανση-ψύξη κτιρίου, η λειτουργία έξυπνου φωτισμού και διάφορες άλλες εφαρμογές όπως η πυρανίχνευση κ.α. Κλείνοντας το δεύτερο κεφάλαιο παραθέτουμε τα βασικότερα πλεονεκτήματα και μειονεκτήματα των έξυπνων κτιρίων. Στο τρίτο κεφάλαιο αναφερόμαστε στα έξυπνα σπίτια και στις δομικές τεχνολογίες τους όπως είναι το πρότυπο X10, το Διεθνές πρότυπο KNX εφαρμογή στα έξυπνα σπίτια και στο σύστημα KNX / EIB – instabus. Ακόμη αναφερόμαστε στις κατηγορίες έξυπνων σπιτιών που είναι τα ελεγχόμενα, τα προγραμματιζόμενα και τα ευφυή σπίτια.

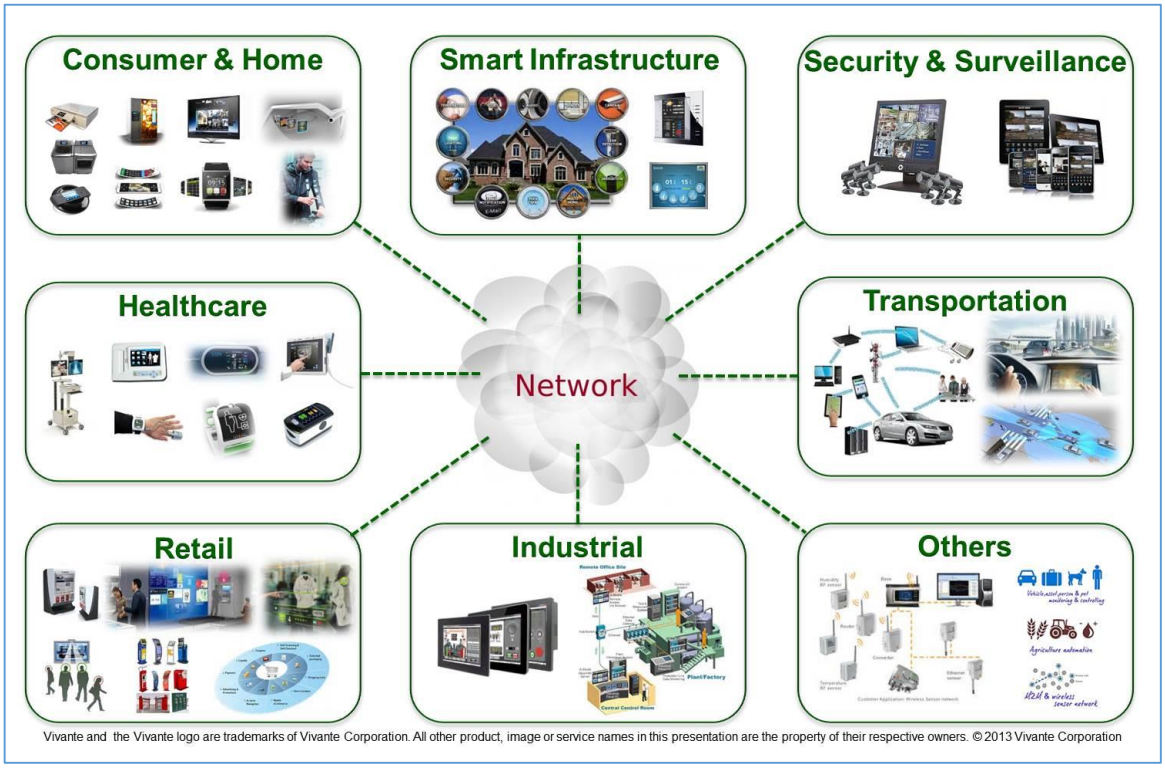
Στο τέταρτο κεφάλαιο εμβαθύνουμε σε θέματα ασφαλείας των έξυπνων κτιρίων όπως είναι η ακτινοβολία και οι επιπτώσεις που έχει στην υγεία. Επίσης, μελετούμε τις προκλήσεις που δημιουργούνται από τη ραγδαία εξέλιξη του IoT, όπως είναι οι επιθέσεις σε συστήματα RFID, οι απειλές και τα κενά ασφαλείας σε τεχνολογίες επικοινωνίας κοντινού πεδίου NFC, οι επιθέσεις σε δίκτυα αισθητήρων καθώς και οι βλάβες και τα τεχνικά ζητήματα που προκύπτουν στις έξυπνες συσκευές.

Στο τελευταίο κεφάλαιο μελετούμε περιπτώσεις θεμάτων ασφαλείας στα έξυπνα κτίρια/σπίτια. Αρχικά αναφερόμαστε στη περίπτωση επίθεσης με την ονομασία Mirai Botnet που έγινε το 2016 και αποτελεί μια από τις πιο σημαντικές και μαζικές επιθέσεις που έγιναν σε συσκευές IoT. Στη συνέχεια παραθέτουμε στοιχεία για τις δύο συσκευές IoT με τις περισσότερες παραβιάσεις στα έξυπνα σπίτια, αυτές οι συσκευές είναι οι έξυπνες τηλεοράσεις και τα έξυπνα οικιακά ηχεία καθώς και στη περίπτωση προσβολής των έξυπνων λαμπτήρων Hue της εταιρείας Philips.

1. Εισαγωγή στο IoT

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) [1] είναι ένα βασικό θέμα στον τομέα της τεχνολογίας, της μηχανικής και της πολιτικής και έχει γίνει έντονη αναφορά σε αυτήν τόσο σε επιστημονικά άρθρα όσο και στα μέσα μαζικής ενημέρωσης. Η τεχνολογία αυτή περιλαμβάνεται σε ένα ευρύ φάσμα δικτυωμένων προϊόντων, αισθητήρων και τεχνολογικών συστημάτων, τα οποία εκμεταλλεύονται τις προόδους στην υπολογιστική ισχύ, στην νανοτεχνολογία και τις διασυνδέσεις δικτύων, προσφέροντας νέες δυνατότητες άνευ προηγουμένου.

Επίσης, η τεχνολογία του IoT βρίσκει εφαρμογή με μεγάλη επιτυχία σε πολλούς τομείς όπως στον τομέα των έξυπνων υπηρεσιών υγειονομικής περίθαλψης με τις φορητές συσκευές (wearables), τις συσκευές παρακολούθησης της υγείας και τις δικτυακές ιατρικές συσκευές. Ακόμη μια εφαρμογή του IoT αφορά τις έξυπνες μεταφορές (smart transportation) με τα έξυπνα οχήματα (smart vehicles) και τα οχηματικά δίκτυα (VANETs), τα έξυπνα συστήματα ρύθμισης κυκλοφορίας με χρήση ενσωματωμένων αισθητήρων σε δρόμους και γέφυρες για τον έλεγχο της κυκλοφορίας που βάζουν τις βάσεις για τις “έξυπνες πόλεις” (smart cities). Επιπλέον, η τεχνολογία IoT έχει πολλές δυνατότητες εφαρμογής στον τομέα της γεωργίας και της κτηνοτροφίας (smart agriculture), της βιομηχανίας (smart industries), στον τομέα διανομής ηλεκτρικής ενέργειας (smart grids), κλπ.



Εικόνα 1. Τομείς που βρίσκει εφαρμογή το Διαδίκτυο των Πραγμάτων (Internet of Things)

Πηγή: https://bensontao.wordpress.com/2013/10/06/vivante-internet-of-things/

Η πρακτική εφαρμογή του IoT σε μια μεγάλη γκάμα προϊόντων και συσκευών, υπόσχεται να βελτιώσει πολλές πτυχές του σύγχρονου τρόπου ζωής. Τα προϊόντα που δημιουργούνται μέσω της νέας αυτής τεχνολογίας όπως οι Internet-enabled συσκευές, τα εξαρτήματα οικιακού αυτοματισμού και τα συστήματα ελέγχου ενέργειας οδηγούν τους καταναλωτές πιο κοντά στην ιδέα του “smart – home”, παρέχοντας με αυτόν τον τρόπο μεγαλύτερη αποτελεσματικότητα σε θέματα ασφάλειας και διαχείριση ενέργειας. Παρά όλα αυτά τα πλεονεκτήματα του IoT, δεν πρέπει να παραλείψουμε να αναφέρουμε ότι χρειάζεται ιδιαίτερη προσοχή και μελέτη σε όλες τις δυσκολίες που προκύπτουν στην πρακτική εφαρμογή όλων των παραπάνω. Τέλος οι ειδικοί προειδοποιούν ότι η τεχνολογία αυτή είναι ιδιαίτερα ευαίσθητη σε θέματα ασφάλειας και παραβίασης της ιδιωτικής ζωής.

1.1 Ορισμοί IoT- Internet of Things, Cloud Computing

Σε αυτή την ενότητα θα αναφέρουμε με λεπτομέρεια τι είναι το Διαδίκτυο των Πραγμάτων και τι είναι το Υπολογιστικό νέφος (Cloud computing), αυτές είναι κάποιες από τις πιο βασικές έννοιες που πρέπει να γνωρίζουμε για την κατανόηση της εργασίας.

1.1.1 Τι είναι το Διαδίκτυο των Πραγμάτων (Internet of Things)

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) [2] αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η διασύνδεση των έξυπνων ηλεκτρονικών συσκευών μεταξύ τους (είτε μέσω τοπικού δικτύου, είτε μέσω σύνδεσης στο διαδίκτυο).

Το IoT είναι μία από τις τρεις κορυφαίες τεχνολογικές εξελίξεις της επόμενης δεκαετίας (μαζί με το mobileInternet και την αυτοματοποίηση του knowledgework) και αποτελεί το επόμενο μεγάλο βήμα στον χώρο της τεχνολογίας.

Ο όρος Internet of Things επινοήθηκε στα τέλη της δεκαετίας του 1990 από τον επιχειρηματία Kevin Ashton [3]. Ο Ashton, ο οποίος είναι ένας από τους ιδρυτές του Auto-ID center στο MIT, ήταν μέρος μιας ομάδας που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το Διαδίκτυο μέσω μιας ετικέτας RFID.

Ο Ashton επινόησε τον όρο για να δώσει έμφαση στη δύναμη των συστημάτων ταυτοποίησης μέσω ραδιοσυχνοτήτων, γνωστά ως RFID (Radio Frequency Identification), που χρησιμοποιούνται από εταιρείες logistics με σκοπό να ελέγχουν και να παρακολουθούν τα προϊόντα χωρίς την παρουσία ανθρώπινου δυναμικού. Πλέον, το διαδίκτυο των πραγμάτων έχει γίνει ένας δημοφιλής όρος για την περιγραφή δυνατοτήτων στις οποίες η σύνδεση στο Internet και οι λειτουργίες των υπολογιστών επεκτείνονται σε μία ευρεία γκάμα από αντικείμενα, συσκευές, αισθητήρες και προϊόντα της καθημερινότητας.

Παρά το γεγονός πως ο όρος του IoT χρησιμοποιείται σε μεγάλη κλίμακα και σε παγκόσμιο επίπεδο, ακόμη δεν υπάρχει ένας διεθνώς αποδεκτός ορισμός. Οι διάφοροι ορισμοί που κυκλοφορούν στους επιστημονικούς κύκλους για να περιγράψουν και να αναφερθούν στο τι σημαίνει IoT και τα διακριτά χαρακτηριστικά του έχουν διαφορές και είναι προσεγγιστικοί. Μερικοί από τους πιο έγκυρους είναι οι παρακάτω:

- *“Ο όρος "Internet of Things" (IoT)* [4] *υποδηλώνει μια τάση όπου ένας μεγάλος αριθμός ενσωματωμένων συσκευών χρησιμοποιούν υπηρεσίες επικοινωνίας που προσφέρονται από Πρωτόκολλα του Διαδικτύου. Πολλές από αυτές τις συσκευές, που συχνά ονομάζονται «έξυπνα αντικείμενα», δεν λειτουργούν άμεσα από τον άνθρωπο αλλά υπάρχουν ως επιμέρους εξαρτήματα σε κτίρια ή οχήματα, ή υπάρχουν απλά στο περιβάλλον. Ακολουθώντας τη πρόταση «Ότι μπορεί να συνδεθεί θα είναι συνδεδεμένο», μηχανικοί και ερευνητές που σχεδιάζουν δίκτυα έξυπνων αντικειμένων πρέπει να εξασφαλίσουν πώς θα επιτευχθεί αυτό στην πράξη.”*
- *“Το Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων* [3] *(Internet of things) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό).”*
- *Πρακτικά κατά μια έννοια το Internet of Things* [5] *αφορά αντικείμενα της καθημερινότητάς μας. Τέτοια αντικείμενα είναι από αισθητήρες αυτόματης ρύθμισης θέρμανσης σε ένα σπίτι ή σε ένα κτίριο γενικότερα, μέχρι έναν εξοπλισμό ο οποίος στέλνει μέσω δικτύου ειδοποίηση στο προσωπικό*

συντήρησης για μια επικείμενη βλάβη. Ο στόχος-σκοπός με άλλα λόγια της καινοτομίας που έρχεται να φέρει το Internet of Things είναι ότι θα κάνει την ζωή μας πιο εύκολη.

- *Το Internet of things (IoT)* [6] *είναι μια παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που επιτρέπει προηγμένες υπηρεσίες μέσω της διασύνδεσης υλικών και άυλων πραγμάτων με βάση την παροντική και την υπό εξέλιξη διαλειτουργικότητα των τεχνολογιών της πληροφορίας και της επικοινωνίας.*

Οι παραπάνω ορισμοί αποδίδουν την έννοια του IoT σε συνάρτηση με το δίκτυο και την ικανότητα των υπολογιστών να εκτείνονται σε μια ομάδα αντικειμένων που δεν θεωρούνται ότι είναι υπολογιστές, επιτρέποντας στις συσκευές να παράγουν, να ανταλλάσσουν και να καταναλώνουν δεδομένα με περιορισμένη την ανθρώπινη συμμετοχή. Οι ορισμοί που αποδίδονται στο IoT δεν διαφωνούν αλλά τονίζουν διαφορετικές πτυχές του φαινομένου από διαφορετικές οπτικές γωνίες και πεδία εφαρμογής.

1.1.2 Τι είναι το Υπολογιστικό νέφος (Cloud computing)

Και στην περίπτωση του Cloud computing (υπολογιστικό νέφος) [7] υπάρχουν πολλοί διαφορετικοί ορισμοί για το τι εννοούμε με τον όρο αυτό. Το Cloud computing είναι η τεχνολογία αυτή που δίνει τη δυνατότητα στο χρήστη να κάνει χρήση λογισμικών, υπηρεσιών και δεδομένων, τα οποία δεν είναι αποθηκευμένα σε δικό του υπολογιστή αλλά τη δεδομένη στιγμή βρίσκεται σε κάποιον άλλο χώρο και ο εξοπλισμός που χρησιμοποιεί είναι διαφορετικός από αυτόν που υπάρχουν τα στοιχεία που κάνει χρήση. Βασικό στοιχείο της έννοιας του cloud computing είναι η σύνδεση στο ίντερνετ, μέσω του οποίου λειτουργεί. Η τεχνολογία αυτή δίνει τη δυνατότητα να διατίθενται προϊόντα λογισμικού με τη μορφή software as a service, δηλαδή λογισμικό που κάνουμε χρήση χωρίς να έχουμε αγοράσει αλλά πληρώνοντας ένα τίμημα, ή κάνοντας χρήση δωρεάν παρεχόμενου χώρου όπου υπάρχουν τέτοιου είδους υπηρεσίες.

Με απλά λόγια, το cloud computing είναι η παροχή υπηρεσιών υπολογιστών-διακομιστών, αποθηκευτικών χώρων, βάσεων δεδομένων, δικτύωσης, λογισμικού, αναλυτικών στοιχείων και πολλά άλλα μέσω του Διαδικτύου (cloud = σύννεφο). Οι εταιρείες που παρέχουν αυτές τις υπηρεσίες υπολογιστών ονομάζονται πάροχοι cloud και συνήθως χρεώνουν για υπηρεσίες cloud computing ανάλογα με τη χρήση, παρόμοια με τον τρόπο που χρεωνόμαστε για το νερό ή την ηλεκτρική ενέργεια στο σπίτι.

Εικόνα 2. Απεικόνιση Cloud Computing

Πηγή: https://timesofcloud.com/what-is-cloud-computing/

Οι Χρήσεις του cloud computing είναι πολλές και συχνά τις συναντάμε σε απλές λειτουργικότητες του internet, όταν χρησιμοποιούμε μια on line ηλεκτρονική υπηρεσία για την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, την επεξεργασία εγγράφων, την παρακολούθηση ταινιών, την ακρόαση μουσικής, την αναπαραγωγή παιχνιδιών ή την αποθήκευση εικόνων και άλλων αρχείων. Οι πρώτες υπηρεσίες cloud computing υπάρχουν μόλις μερικές δεκαετίες, αλλά ήδη αρκετοί οργανισμών από μικρές επιχειρήσεις έως πολυεθνικές εταιρείες, κρατικές υπηρεσίες έως μη κερδοσκοπικούς οργανισμούς χρησιμοποιούν αυτή την τεχνολογία για πολλούς λόγους.

Για παράδειγμα κάποια από τα πράγματα που μπορούμε να κάνουμε με το cloud computing είναι:

- Να δημιουργήσουμε νέες εφαρμογές και υπηρεσίες
- Να αποθηκεύσουμε, να δημιουργήσουμε αντίγραφα ασφαλείας και να ανακτήσουμε δεδομένα
- Να φιλοξενήσουμε ιστοσελίδες και ιστολόγια
- Να μεταδώσουμε ήχο και βίντεο
- Να παραδώσουμε λογισμικό κατόπιν παραγγελίας
- Να αναλύσουμε δεδομένα για μοτίβα και πραγματοποίηση προβλέψεων

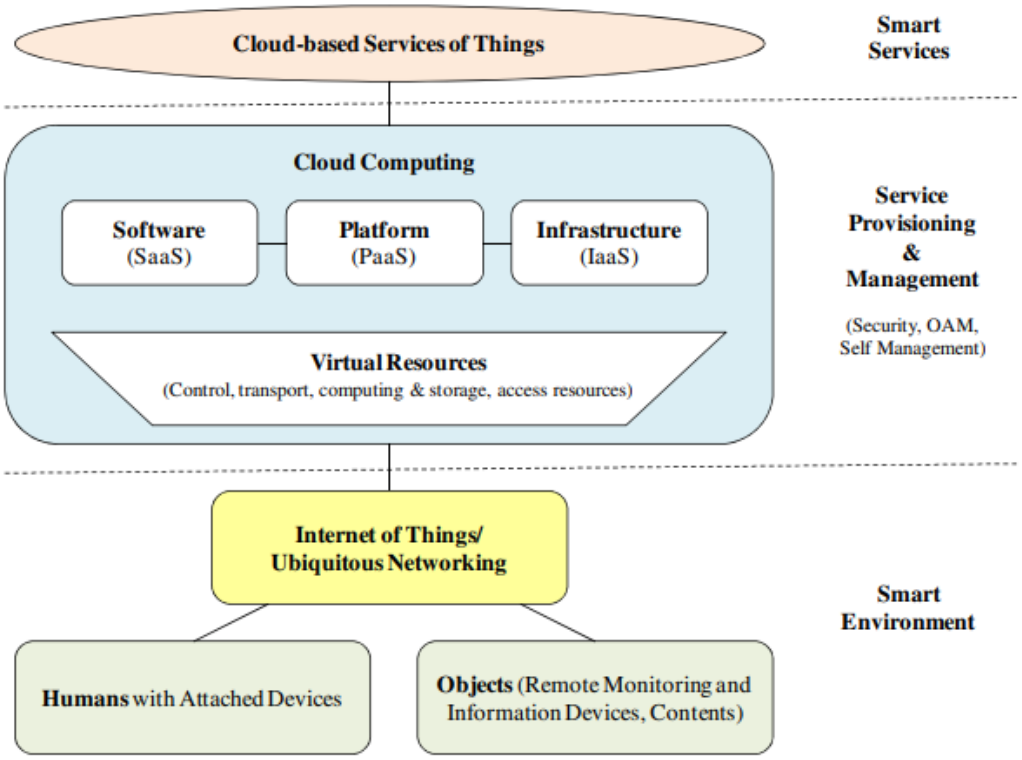
Η τεχνολογία του cloud computing επέφερε μεγάλη αλλαγή στους τρόπους με τους οποίους οι επιχειρήσεις διαχειρίζονται τα δεδομένα στην πληροφορική. Τα βασικότερα πλεονεκτήματα είναι πρώτον ότι μειώνει σημαντικά το κόστος για την αγορά υλικών και λογισμικών για τη δημιουργία και λειτουργία κέντρων δεδομένων, στη χρήση servers, της ενέργειας που χρειάζεται και των τεχνικών που απαιτούνται για την διαχείριση των

παραπάνω υποδομών. Δεύτερον η ταχύτητα που παρέχει μέσω της αυτοεξυπηρέτησης που δίνει μεγάλη ευελιξία χρησιμοποιώντας τη χωρητικότητα που επιθυμούν κάθε φορά. Τρίτον οι μεγαλύτερες υπηρεσίες cloud computing λειτουργούν σε ένα παγκόσμιο δίκτυο ασφαλών κέντρων δεδομένων, τα οποία αναβαθμίζονται τακτικά σύμφωνα με την τελευταία γενιά γρήγορου και αποδοτικού εξοπλισμού πληροφορικής. Αυτό προσφέρει πολλά πλεονεκτήματα σε ένα ενιαίο εταιρικό κέντρο δεδομένων, συμπεριλαμβανομένης της μειωμένης καθυστέρησης του δικτύου για τις εφαρμογές τους. Και τέταρτον το cloud computing καθιστά ευκολότερη και λιγότερο δαπανηρή την δημιουργία αντιγράφων ασφαλείας των δεδομένων, την αποκατάσταση καταστροφών και τη άμεση αποκατάσταση της λειτουργικότητας της επιχείρησης, επειδή τα δεδομένα μπορούν να αντικατοπτρίζονται σε πολλαπλές τοποθεσίες στο δίκτυο του παρόχου υπηρεσιών cloud.

Δεν είναι όλα τα ”σύννεφα” τα ίδια [8]. Υπάρχουν τρεις διαφορετικοί τρόποι για την ανάπτυξη πόρων cloud computing: δημόσιο cloud, ιδιωτικό cloud και υβριδικό cloud.

- **Public cloud (Δημόσιο σύννεφο):** Τα δημόσια σύννεφα ανήκουν και λειτουργούν από έναν πάροχο υπηρεσιών cloud, ο οποίος παρέχει τους υπολογιστικούς πόρους του, όπως διακομιστές και αποθήκευση μέσω του Διαδικτύου. Η Microsoft Azure είναι ένα παράδειγμα ενός δημόσιου σύννεφου. Με ένα δημόσιο σύννεφο, όλο το υλικό, το λογισμικό και άλλη υποστηρικτική υποδομή ανήκει και διαχειρίζεται ο πάροχος. Μπορείτε να αποκτήσετε πρόσβαση σε αυτές τις υπηρεσίες και να διαχειριστείτε το λογαριασμό σας χρησιμοποιώντας ένα πρόγραμμα περιήγησης ιστού.
- **Private cloud (Ιδιωτικό σύννεφο):** Ένα ιδιωτικό σύννεφο αναφέρεται σε πόρους υπολογιστικού νέφους, που χρησιμοποιούνται αποκλειστικά από μια επιχείρηση ή έναν οργανισμό. Ένα ιδιωτικό σύννεφο μπορεί να βρίσκεται φυσικά στο datacenter της επιχείρησης. Ορισμένες εταιρείες πληρώνουν επίσης τρίτους παρόχους υπηρεσιών για να φιλοξενήσουν το ιδιωτικό σύννεφο τους. Ένα ιδιωτικό σύννεφο είναι εκείνο στο οποίο οι υπηρεσίες και η υποδομή διατηρούνται σε ένα ιδιωτικό δίκτυο.
- **Hybrid cloud (Υβριδικό σύννεφο):** Τα υβριδικά σύννεφα συνδυάζουν δημόσια και ιδιωτικά σύννεφα, που συνδέονται μεταξύ τους με τεχνολογία που επιτρέπει την κοινή χρήση δεδομένων και εφαρμογών μεταξύ τους. Επιτρέποντας στα δεδομένα και τις εφαρμογές να μετακινούνται μεταξύ ιδιωτικών και δημόσιων σύννεφων, το υβριδικό σύννεφο παρέχει στις επιχειρήσεις μεγαλύτερη ευελιξία και περισσότερες επιλογές ανάπτυξης.

Οι έννοιες του υπολογιστικού νέφους και του διαδικτύου των πραγμάτων είναι στενά συνδεδεμένες καθώς η τεχνολογία του IoT είναι βασισμένη στην υπηρεσία του cloud computing για να λειτουργήσει σε πολλές εφαρμογές της. Στη συνέχεια θα δούμε ένα εννοιολογικό διάγραμμα που περιγράφει πως το IoT βασίζεται στην υπηρεσία cloud computing.



Εικόνα 3. Διαγραμματική απεικόνιση σχέσης μεταξύ Cloud Computing και IoT

Πηγή: https://www.researchgate.net/figure/A-conceptual-diagram-for-the-cloud-based-Internet-of-Things_fig2_221430997

1.2 Αρχιτεκτονική - Μοντελοποίηση IoT

Οι συσκευές του IoT από λειτουργικής πλευράς συνδέονται και επικοινωνούν μέσω τεχνικών μοντέλων επικοινωνίας. Τον Μάρτιο του 2015, το Συμβούλιο Αρχιτεκτονικής του Διαδικτύου (Internet Architecture Board, IAB) δημοσίευσε ένα πλαίσιο τεσσάρων μοντέλων επικοινωνίας που χρησιμοποιούνται για τη δικτύωση έξυπνων συσκευών. Στη συνέχεια αναφέρονται λεπτομερώς τα μοντέλα αυτά.

- **Μοντέλο Device to device:** Το μοντέλο επικοινωνίας αυτό αφορά δύο ή και περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους, χωρίς να μεσολαβεί ενδιάμεσος Server εφαρμογών. Οι συσκευές αυτές επικοινωνούν μέσω πολλών τύπων δικτύων, ανάμεσα τους είναι τα δίκτυα IP ή το Internet. Επίσης, συχνά αυτές οι συσκευές κάνουν χρήση πρωτοκόλλων όπως το Bluetooth, 40 Z-Wave, 41 ή ZigBee42 για την πρακτική εφαρμογή device to device επικοινωνίας.
- **Μοντέλο Device to Cloud:** Σε αυτό το μοντέλο επικοινωνίας η IoT συσκευή συνδέεται απευθείας σε μια διαδικτυακή υπηρεσία cloud όπως ένας πάροχος υπηρεσιών εφαρμογής, με σκοπό να ανταλλάσει δεδομένα και να διαχειρίζεται την κίνηση μηνυμάτων. Αυτός ο τρόπος επικοινωνίας συχνά χρησιμοποιεί

υπάρχοντες μηχανισμούς επικοινωνίας, όπως η κλασσικές Ethernet ή Wi-Fi συνδέσεις για να εγκαταστήσει μια σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο σε τελικό στάδιο συνδέεται με την υπηρεσία cloud.

- **Μοντέλο Device to Gateway:** Σε αυτό το επικοινωνιακό μοντέλο η συσκευή IoT συνδέεται μέσω μιας υπηρεσίας ALG (Application-Layer-Gateway) ως αγωγός για να επιτευχθεί μια σύνδεση με την υπηρεσία cloud. Με πιο απλά λόγια, αυτό σημαίνει ότι το μοντέλο Device to Gateway διαθέτει λογισμικό εφαρμογής το οποίο λειτουργεί ως διαμεσολαβητής μεταξύ της συσκευής και της υπηρεσίας cloud και παρέχει ασφάλεια και άλλες λειτουργίες όπως δεδομένα ή μετάφραση πρωτοκόλλων.
- **Μοντέλο Back End Data Sharing:** Τέλος [10], αυτό το μοντέλο χρησιμοποιεί μια αρχιτεκτονική επικοινωνίας η οποία επιτρέπει στους χρήστες της να εξάγουν και να αναλύουν τα δεδομένα του έξυπνου αντικειμένου από μια υπηρεσία cloud, σε συνδυασμό με δεδομένα άλλων πηγών. Αυτό το σύστημα επικοινωνίας είναι βασισμένο στο μοντέλο Device to Cloud, το οποίο επιτρέπει στις συσκευές IoT να ανεβάζουν τα δεδομένα μόνο για έναν πάροχο εφαρμογής. Αυτή η αρχιτεκτονική επικοινωνίας δίνει τη δυνατότητα τα δεδομένα που συλλέγονται από μια IoT συσκευή να συγκεντρώνονται και να αναλύονται.

1.2.1 Η αρχιτεκτονική του IoT και το μοντέλο ARM

Η αναγκαιότητα ύπαρξης μιας κοινής γλώσσας για τη λειτουργικότητα του IoT, είναι βασική προϋπόθεση για την άμεση ανάπτυξη καινοτόμων λύσεων που θα μπορούν να αξιοποιήσουν τις διαφορετικές τεχνολογίες που αναπτύχθηκαν για διαφορετικούς σκοπούς σε διαφορετικά πεδία εφαρμογής. Για πολλά χρόνια και έπειτα από αρκετή συζήτηση γύρω από τις βασικές έννοιες του IoT, το 2009 μία ομάδα ερευνητών από περισσότερες των 20 μεγάλων βιομηχανικών εταιρειών και ερευνητικών ιδρυμάτων, ένωσαν τις δυνάμεις τους για να τεθούν οι βάσεις για το τόσο σημαντικό κοινό έδαφος του Internet of Things, και έτσι δημιουργήθηκε το έργο IoT-Architecture (IoT-A).

Λαμβάνοντας υπόψη την τεχνική πλευρά, οι υπάρχουσες λύσεις δεν καλύπτουν τις απαιτήσεις της μελλοντικής εξέλιξης του IoT, τόσο από την άποψη της επικοινωνίας μεταξύ των έξυπνων συσκευών, όσο και από το συντονισμό και τη διαχείριση των πιο σύνθετων υπηρεσιών. Επίσης, το πεδίο εφαρμογής του IoT περιλαμβάνει πολλά διαφορετικά μοντέλα λειτουργίας τα οποία δεν είναι πάντοτε συμβατά. Η διαδικασία αυτή οδηγεί σε μία κατάσταση που η προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων εξετάζεται ανά περίπτωση και βάση της εκάστοτε νομοθεσίας, δημιουργώντας λύσεις στα παροντικά σχέδια, κάτι το οποίο δυσκολεύει τη δυνατότητα μεταφοράς, την διαλειτουργικότητα και την ανάπτυξη. Αδιαμφισβήτητα, η διάδοση του IoT είναι τόσο έντονη που είναι αδύνατον να δημιουργηθεί ένα πρωτόκολλο που θα

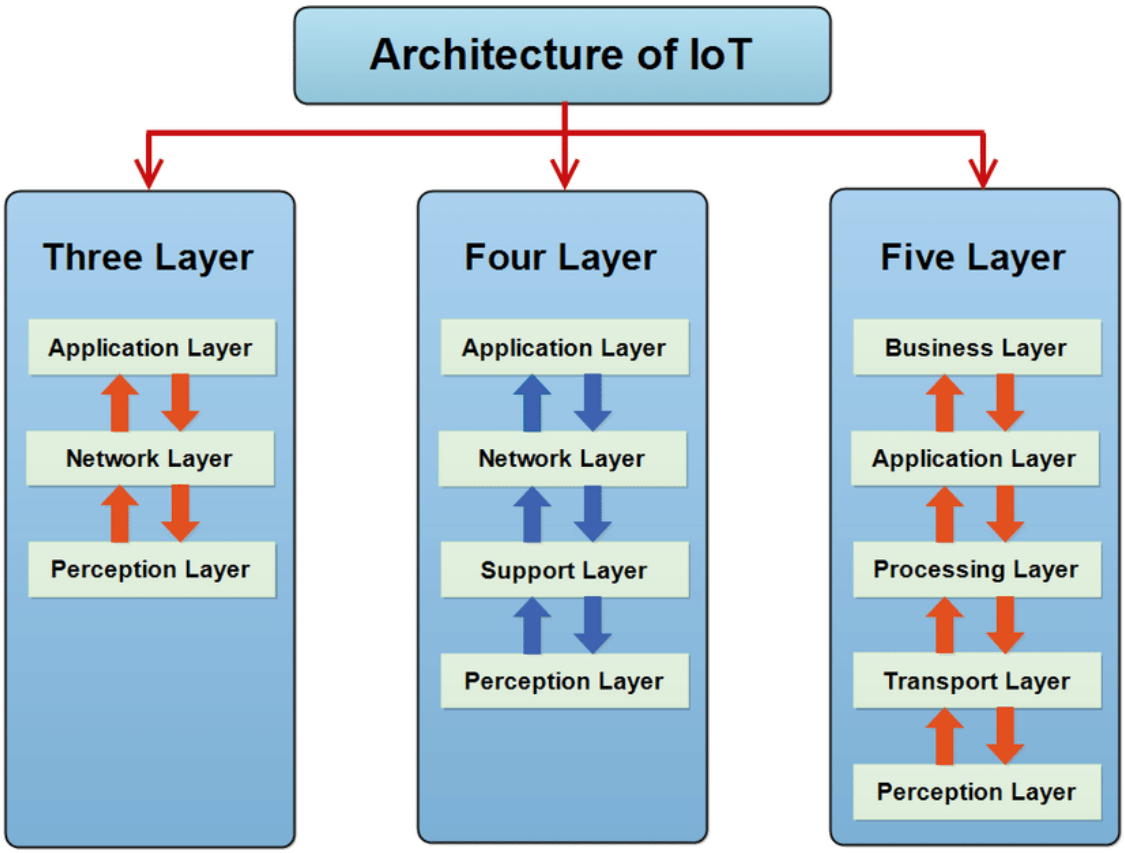
βρίσκει εφαρμογή σε όλους, όπως είναι το IP. Οι παραπάνω λόγοι οδηγούν σε ανάγκη για ένα σύστημα κοινής επικοινωνίας.

Ως αποτέλεσμα αυτής της ανάγκης [12] έχουν προκύψει κοινά χαρακτηριστικά για να σχηματιστεί η γραμμή βάσης του IoT Αρχιτεκτονικού Μοντέλου αναφοράς (ARM). Αρχικά είναι απαραίτητο πέρα από τα εργαστήρια χρειάζεται έρευνα και επαφή με τον πραγματικό κόσμο. Το IoT εντόπισε την νέα πραγματικότητα, όπου τα νέα δεδομένα μεταξύ έρευνας, ανάπτυξης, καινοτομίας και νέων τεχνολογιών είναι ακόμη ασαφή. Με την βοήθεια των τελικών χρηστών, οι οποίοι αποτέλεσαν μια ομάδα ενδιαφερομένων μερών για το IoT, νέες πληροφορίες και δεδομένα έχουν συλλεχθεί και χρησιμοποιηθεί στον σχεδιασμό του νέου μοντέλου αρχιτεκτονικής IoT. Η ομάδα αυτή αποτελεί τη σημαντικότερη πηγή για την απόκτηση πληροφοριών από εξωτερικές πηγές καθώς και για την πορεία της εφαρμογής του έργου. Επίσης, εργασίες και ερωτηματολόγια χρησιμοποιούνται για να ενισχύσουν την πρόοδο της ανάπτυξης του ARM και να ολοκληρώσουν τις έννοιες και τα μοντέλα.

Αυτή η πρακτική που συμπεριλαμβάνει την εμπλοκή των ενδιαφερόμενων μερών σε μεγάλο βαθμό χαρακτηρίζεται από περίπλοκα και δυναμικά περιβάλλοντα τα οποία καλύπτουν ένα ευρύ φάσμα ενδιαφερομένων. Αυτός θα μπορούσε να είναι και ένας πρακτικός ορισμός του IoT, πολύπλοκα και δυναμικά περιβάλλοντα που περιέχουν ένα ευρύ φάσμα ενδιαφερομένων. Διαπιστώθηκε ότι στα περισσότερα πεδία εφαρμογής όπως στην αυτοκινητοβιομηχανία, στην υγεία, στην εφοδιαστική και στις παραγωγικές διαδικασίες οι απαιτήσεις είχαν κοινά σημεία. Η βασική ανάγκη είναι να υπάρχει μια διαρκής παρακολούθηση σε πραγματικό χρόνο έτσι ώστε να μπορεί να υπάρξει διαλειτουργικότητα η οποία είναι ο βασικός στόχος αυτού του έργου.

1.2.2 Αρχιτεκτονική IoT τριών, τεσσάρων και πέντε επιπέδων

Δεν υπάρχει μία μοναδική και γενικευμένη περιγραφή σχετικά με την αρχιτεκτονική του IoT που να είναι αποδεκτή πλήρως σε παγκόσμιο επίπεδο και γενικότερα από τους ερευνητές[25]. Πολλές και διαφορετικές αρχιτεκτονικές έχουν προταθεί κατά καιρούς από τους ερευνητές, σύμφωνα με ορισμένους ειδικούς η αρχιτεκτονική του IoT αποτελείται από τρία επίπεδα ενώ κάποιοι άλλοι υποστηρίζουν τέσσερα επίπεδα ή ακόμη και πέντε. Πιστεύουν πως λόγω της ραγδαίας εξέλιξης του τομέα, η αρχιτεκτονική των τριών επιπέδων δεν πληροί της απαιτήσεις που προκύπτουν. Ακόμη, λόγω των προκλήσεων που δημιουργούνται σχετικά με την ασφάλεια και την ιδιωτικότητα προτάθηκε στη συνέχεια και το πέμπτο επίπεδο.



Εικόνα 4. Τα επίπεδα της αρχιτεκτονικής του IoT

Πηγή: https://www.researchgate.net/figure/The-layered-architectures-of-IoT-three-four-and-five-layers_fig6_327272757

1.2.2.1 Η αρχιτεκτονική των τριών επιπέδων

Η αρχιτεκτονική των τριών επιπέδων είναι η βασική αρχιτεκτονική και βασίζεται στην αρχική ιδέα του IoT. Προτάθηκε στα αρχικά στάδια ανάπτυξης του IoT και αποτελείται από τρία επίπεδα. Τα επίπεδα αυτά είναι το επίπεδο της αντίληψης, το επίπεδο του δικτύου και τέλος το επίπεδο της εφαρμογής.

Το πρώτο επίπεδο της αντίληψης είναι επίσης γνωστό και ως επίπεδο αισθητήρα, το οποίο θα μπορούσαμε να πούμε πως λειτουργεί όπως τα μάτια και τα αυτιά των ανθρώπων. Το έργο του είναι να αναγνωρίζει συγκεκριμένες συνθήκες και να συλλέγει πληροφορίες από αυτές. Υπάρχουν πολλοί τύποι αισθητήρων που συνδέονται με αντικείμενα με σκοπό τη συλλογή πληροφοριών, όπως οι RFID, 2-D barcode κ.α. Οι πληροφορίες που συλλέγονται από τους αισθητήρες μπορεί να αφορούν κάποια τοποθεσία, αλλαγές στον αέρα, το περιβάλλον, την κίνηση κτλ. Ωστόσο, αποτελούν τον κύριο στόχο κακόβουλων εισβολέων που επιθυμούν να υποκλέψουν πληροφορίες. Οι πιο κοινές απειλές σε αυτό το επίπεδο είναι η υποκλοπή στις επικοινωνίες όπου

προσπαθούν να κλέψουν πληροφορίες σε πραγματικό χρόνο οι οποίες μεταδίδονται μέσω διαδικτύου π.χ. κλήσεις, μηνύματα κειμένου, φαξ, βιντεοδιασκέψεις κ.α.

Το επίπεδο του δικτύου είναι επίσης γνωστό και ως επίπεδο μετάδοσης πληροφοριών. Λειτουργεί σαν γέφυρα μεταξύ του επιπέδου της αντίληψης και του επιπέδου της εφαρμογής. Μεταφέρει και μεταδίδει τις πληροφορίες που συλλέγονται από τα φυσικά αντικείμενα μέσω των αισθητήρων. Το μέσο για τη μετάδοση μπορεί να είναι είτε ασύρματο είτε ενσύρματο. Επίσης μέσω αυτού του επιπέδου διαχειριζόμαστε την σύνδεση των έξυπνων συσκευών και την επικοινωνία των δικτύων μεταξύ τους. Επομένως αποτελεί στόχο επιθέσεων και λόγω της χρήσης του δικτύου είναι αρκετά ευαίσθητο σε απειλές. Υπάρχει σημαντικό ζήτημα ασφάλειας σχετικά με τον έλεγχο ταυτότητας των πληροφοριών που διακινούνται στο δίκτυο.

Το επίπεδο της εφαρμογής ορίζει όλες τις εφαρμογές που χρησιμοποιούν την τεχνολογία IoT στις οποίες βασίζεται η λειτουργία του συστήματος. Οι εφαρμογές του IoT μπορεί να είναι τα έξυπνα σπίτια, οι έξυπνες πόλεις, η έξυπνη υγεία, η έξυπνη βιομηχανία κ.α. Αυτό το επίπεδο παρέχει τις υπηρεσίες που χρειάζεται η κάθε εφαρμογή ανάλογα με τους σκοπούς που εξυπηρετεί. Ένα από τα τρωτά σημεία αυτού του επιπέδου είναι το ζήτημα της ασφάλειας, για παράδειγμα για την εφαρμογή ισχυρής ασφάλειας σε ένα έξυπνο σπίτι είναι πολύ βασικό το ότι οι συσκευές που χρησιμοποιούνται έχουν ασθενή υπολογιστική ισχύ και μικρό αποθηκευτικό χώρο όπως το ZigBee.

1.2.2.2 Η αρχιτεκτονική των τεσσάρων επιπέδων

Όπως προαναφέραμε λόγω της εξέλιξης της τεχνολογίας του IoT οι ερευνητές πρότειναν ακόμη δύο επίπεδα. Το ένα από αυτά είναι το επίπεδο της υποστήριξης όπως ονομάστηκε, το οποίο χρησιμοποιείται για να κάνει όλο το σύστημα της αρχιτεκτονικής πιο ασφαλές από εισβολείς. Σε αυτό το μοντέλο με τα τέσσερα επίπεδα οι πληροφορίες δεν αποστέλλονται απευθείας στο επίπεδο δικτύου αλλά αποστέλλονται σε ένα υποστηρικτικό πρόσθετο επίπεδο. Το επίπεδο υποστήριξης έχει δύο αρμοδιότητες, πρώτα επιβεβαιώνει ότι οι πληροφορίες αποστέλλονται από τους αυθεντικούς χρήστες και στη συνέχεια προστατεύονται από απειλές. Υπάρχουν πολλοί τρόποι για να ταυτοποιήσουμε τους χρήστες και τις πληροφορίες.

Η πιο συχνά χρησιμοποιούμενη μέθοδος είναι ο έλεγχος ταυτότητας, όπου υλοποιείται με τη χρήση προ-κοινοποιημένων μυστικών κωδικών και κλειδιών πρόσβασης. Η δεύτερη αρμοδιότητα αυτού του επιπέδου είναι, η αποστολή των πληροφοριών στο επίπεδο δικτύου. Το μέσο για τη μετάδοση των πληροφοριών μπορεί να είναι ασύρματο ή ενσύρματο. Και σε αυτό το επίπεδο υπάρχουν διάφορες επιθέσεις που μπορούν να συμβούν, όπως επίθεση Dos, κακόβουλες ενέργειες, μη εξουσιοδοτημένη πρόσβαση κ.α.

1.2.2.3 Η αρχιτεκτονική των πέντε επιπέδων

Η αρχιτεκτονική των τεσσάρων επιπέδων έπαιξε σημαντικό ρόλο στην ανάπτυξη του IoT όμως υπήρξαν ορισμένα ζητήματα σχετικά με την ασφάλεια και την αποθήκευση των δεδομένων. Έτσι οι ερευνητές πρότειναν την αρχιτεκτονική των πέντε επιπέδων για να εξασφαλίσουν στο σύστημα περισσότερη ασφάλεια. Τα πρώτα τρία επίπεδα είναι όμοια με την αρχιτεκτονική των τριών και τεσσάρων επιπέδων, εδώ αλλάζει το τέταρτο επίπεδο και προστίθεται το πέμπτο. Το τέταρτο επίπεδο είναι το επίπεδο επεξεργασίας γνωστό και ως επίπεδο ενδιάμεσου λογισμικού, όπου συλλέγει τις πληροφορίες που του αποστέλλονται και τις επεξεργάζεται και εξαλείφει τις επιπλέον πληροφορίες που δεν έχουν νόημα και εξάγει τις χρήσιμες. Επίσης συμβάλλει και στη μείωση του μεγάλου όγκου δεδομένων που μπορεί να επηρεάσει αρνητικά την απόδοση του IoT. Ωστόσο υπάρχουν και πολλοί τύποι επιθέσεων οι οποίοι μπορούν να διαβάλλουν αυτό το επίπεδο και να προκαλέσουν ζημιές στο σύστημα.

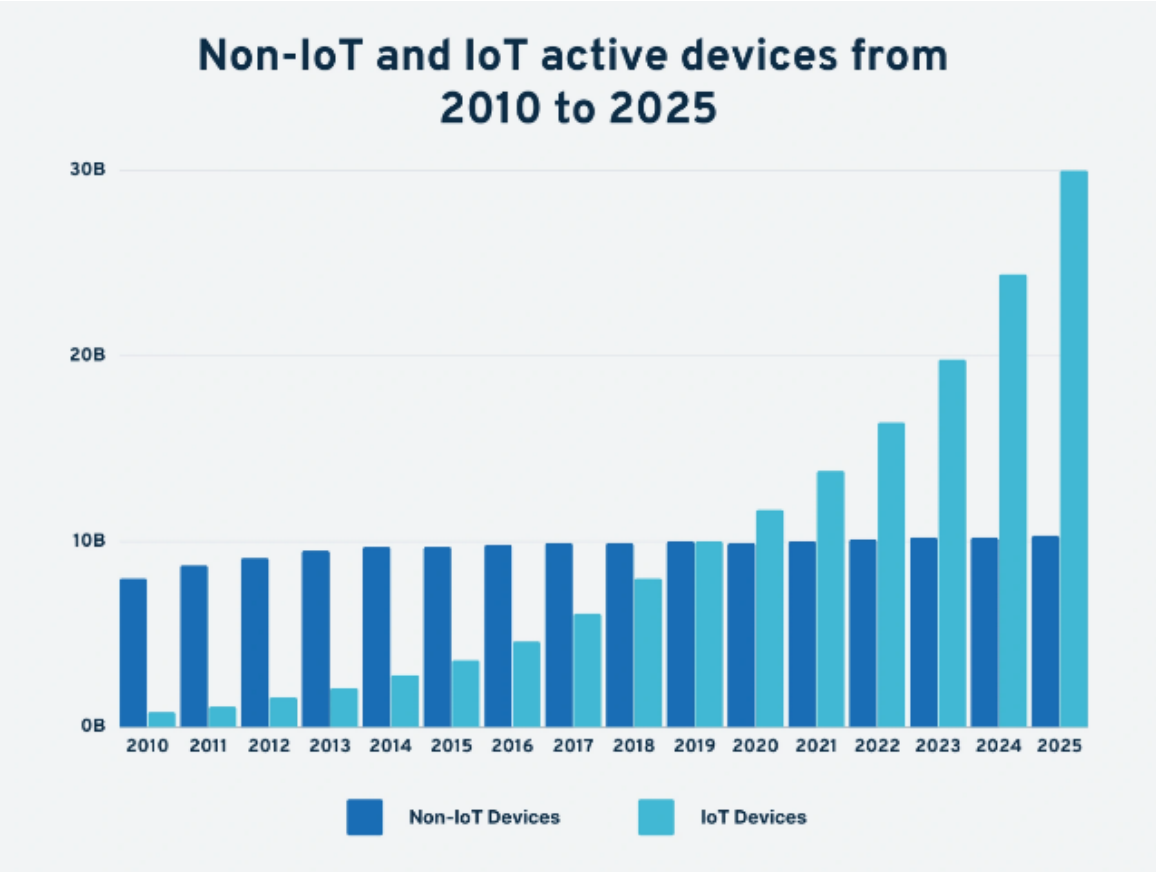
Το πέμπτο επίπεδο το οποίο ονομάζεται το επίπεδο της επιχείρησης αναφέρεται σε μια καλά σχεδιασμένη συμπεριφορά μιας εφαρμογής και λειτουργεί σαν διαχειριστής όλου του συστήματος. Έχει προδιαγραφές να διαχειρίζεται και να ελέγχει εφαρμογές, επιχειρηματικά μοντέλα και μοντέλα κερδών του IoT. Επίσης διαχειρίζεται το απόρρητο του χρήστη. Ακόμη σε αυτό το επίπεδο υπάρχει η δυνατότητα να καθορίζεται πως δημιουργούνται, αποθηκεύονται και αλλάζουν οι πληροφορίες. Ωστόσο, και σε αυτό το επίπεδο έχουν προκύψει ευαίσθητα σημεία όπου γίνονται κακόβουλες επιθέσεις οι οποίες δημιουργούν προβλήματα λόγω έλλειψης ελέγχου στον τομέα της ασφάλειας των δεδομένων.

1.3 Εφαρμογές IoT

Οι τομείς που βρίσκει εφαρμογή η τεχνολογία IoT είναι αμέτρητοι και συνεχώς αυξάνονται. Η ραγδαία εξέλιξη γενικότερα της τεχνολογίας δίνει συνεχώς έδαφος σε όλο και περισσότερες επιστήμες, κλάδους της οικονομίας όσο και κοινωνικούς φορείς να τη χρησιμοποιούν και να την εκμεταλλεύονται για να δώσουν λύσεις σε πρακτικά ζητήματα της καθημερινότητας αλλά και προς όφελος της εξέλιξης τους και του εκσυγχρονισμού τους. Οι εφαρμογές IoT δίνουν λύσεις στις ανάγκες σε ευρεία κλίμακα της τεχνολογίας, ειδικότερα στη νανοηλεκτρονική και στα cyber-physical systems (CPS). Σε κάθε περίπτωση η τεχνολογία αυτή θα μεταβάλλει τα δεδομένα και θα επιφέρει σημαντικές αλλαγές στην οικονομία κάθε χώρα καθώς επίσης θα επηρεάσει κάθε τομέα της καθημερινότητας. Στη συνέχεια της εργασίας θα αναφέρουμε κάποιους από τους βασικότερους τομείς που έκαναν άμεση εφαρμογή και θα παρουσιάσουμε πρακτικά παραδείγματα της εφαρμογής του IoT.

Στην παρακάτω εικόνα θα δούμε ότι το μέγεθος των συνδεδεμένων συσκευών ολοένα και περισσότερο αυξάνεται σε σχέση με τις μη συνδεδεμένες συσκευές. Σύμφωνα με τα τελευταία δεδομένα, υπάρχουν περίπου 7,74 δισεκατομμύρια συνδεδεμένες συσκευές IoT. Αυτός ο αριθμός μπορεί να φαίνεται τεράστιος ωστόσο, η τεχνολογία 5G

και άλλες παρόμοιες τεχνολογίες ο ρυθμός αυτός αναμένεται να αυξηθεί κατά πάνω από 3 φορές έως το 2030.



Εικόνα 5. Συνδεδεμένες και μη συνδεδεμένες συσκευές από το 2010 έως το 2025

Πηγή: https://explodingtopics.com/blog/iot-stats

1.3.1 Εφαρμογές του IoT στην καθημερινή ζωή

- **Έξυπνο αυτοκίνητο**

  Η επιστημονική φαντασία που συναντάμε σε ταινίες έχει αρχίσει να γίνεται πραγματικότητα χάρη στην δύναμη του IoT. Πλέον έχουν αρχίσει να κυκλοφορούν τα έξυπνα αυτοκίνητα τα οποία είναι αυτοκίνητα ή οποιαδήποτε άλλα οχήματα τα οποία μπορούν να ελέγχονται και να εκτελούν εντολές από ένα smartphone ή από οποιαδήποτε άλλη συσκευή. Για να μπορέσει να γίνει αυτό εφικτό θα πρέπει να χρησιμοποιηθούν πολλοί αισθητήρες για την επίτευξη τακτικής παρακολούθησης της τρέχουσας κατάστασης του αυτοκινήτου. Υπάρχει η δυνατότητα ελέγχου ύπαρξης εμποδίων στο μπροστινό μέρος του αυτοκινήτου έτσι ώστε να αποφεύγονται τυχόν ατυχήματα. Προβλέπει πιθανές βλάβες των εξαρτημάτων του αυτοκινήτου πριν συμβούν, γεγονός που το κάνει πιο ξεχωριστό από ένα κοινό αυτοκίνητο. Επίσης οι χρήστες μπορούν να θέσουν σε λειτουργία τον κινητήρα με φωνητική εντολή από ένα smartphone πριν οδηγήσουν.

- **Έξυπνο σπίτι**

  Με τον όρο έξυπνο σπίτι αναφερόμαστε σε ένα σύστημα όπου η κάθε συσκευή όπως το ψυγείο, ο θερμοστάτης, ο φούρνος μικροκυμάτων, το πλυντήριο ρούχων, ο φωτισμός, η πόρτα του σπιτιού, το σύστημα ασφαλείας κ.λπ. έχουν τη δυνατότητα να συνδέονται μέσω διαδικτύου και να ανταλλάσουν δεδομένα. Οι έξυπνες συσκευές μπορούν να ελέγχουν όλα τα παραπάνω από οποιοδήποτε μέρος του κόσμου. Η βασική διαφορά σε σύγκριση με ένα κοινό σπίτι είναι ότι η ποικιλία των αισθητήρων που υπάρχουν εξασφαλίζουν αποδοτικότερες λειτουργίες, ευελιξία στη χρήση και βελτιώνουν τα επίπεδα ασφάλειας. Επίσης ακόμη ένα πλεονέκτημα είναι η εξοικονόμηση ενέργειας στις οικιακές συσκευές, οι οποίες λαμβάνουν αποφάσεις με τη χρήση τεχνητής νοημοσύνης. Επιπλέον η τεχνολογία φωνητικών εντολών σε έξυπνες οικιακές συσκευές παρέχει σημαντική εξοικονόμηση χρόνου.

- **Έξυπνη πόλη**

  Η έξυπνη πόλη είναι ένα εξαιρετικά καινοτόμο παράδειγμα εφαρμογής του διαδικτύου των πραγμάτων. Αυτή η εφαρμογή αποτελείται από τόσες πολλές συνιστώσες χρήσης όπως τη διαχείριση της διανομής του νερού, τη ρύθμιση της κυκλοφορίας, τη διαχείριση της ηλεκτρικής ενέργειας, τη διαχείριση των απορριμμάτων κ.λπ. Η έξυπνη πόλη είναι από τις δημοφιλέστερες εφαρμογές του διαδικτύου των πραγμάτων, πολύ σύντομα οι επιδράσεις και οι αλλαγές που θα φέρει η εφαρμογή αυτή θα είναι ιδιαίτερα εμφανείς στη ζωή μας. Κάποια από τα σημαντικότερα οφέλη είναι η μείωση της ρύπανσης του αέρα και των υδάτων λόγω της τακτικής παρακολούθησης των ποσοστών τους που παρέχει τη δυνατότητα της έγκαιρης λήψης των κατάλληλων μέτρων. Μειώνει την κυκλοφοριακή συμφόρηση και τα ατυχήματα μέσω της χρήσης των έξυπνων αυτοκινήτων αλλά και αισθητήρων οι οποίοι ρυθμίζουν τους σηματοδότες. Οι κάτοικοι μπορούν να βασιστούν σε ασφαλή αυτοματοποιημένα συστήματα δημόσιων συγκοινωνιών. Κάποιοι αισθητήρες που συνδέονται με κτίρια μπορούν να ανιχνεύσουν σεισμικές δονήσεις και άλλα επικίνδυνα καιρικά φαινόμενα.

Εικόνα 6. Έξυπνη πόλη

Πηγή: https://www.dreamstime.com/stock-illustration-smart-city-concept-internet-things-different-icon-elements-modern-design-future-technology-living-image66876194

1.3.2 Εφαρμογές IoT στους τομείς της βιομηχανίας και της οικονομίας

- **Έξυπνη γεωργία**

  Η εφαρμογή του IoT στη γεωργία έχει δυνατότητες να κάνει τη γεωργική πρακτική πιο αποτελεσματική και ακριβή. Όσο περνάει ο καιρός οι εφαρμογές IoT βρίσκουν μεγάλη απήχηση στον τομέα της γεωργίας διότι έχουν θεαματικά αποτελέσματα στην παραγωγική διαδικασία. Οι αντίστοιχες εφαρμογές συλλέγοντας δεδομένα από ένα ορισμένο πεδίο, με τη παρακολούθηση μέσω οχημάτων και τις συνεχείς μετρήσεις της θερμοκρασίας και υγρασίας και πολλών άλλων απαραίτητων παραμέτρων, με την ανάλυση των οποίων συμβάλουν καθοριστικά και αποδοτικά στις λήψεις αποφάσεων. Κάποιες από τις πιο εξειδικευμένες λειτουργικότητες που παρέχονται είναι η ανάλυση των συνθηκών του εδάφους π.χ. του PH υποδεικνύοντας ποια είδη καλλιέργειας είναι κατάλληλα. Ακόμη ελέγχει την υγρασία του εδάφους και καθοδηγεί το συνδεδεμένο με τεχνολογία IoT σύστημα άρδευσης νερού.

  Η παρακολούθηση μιας τεράστιας σε έκταση καλλιέργειας είναι αρκετά δύσκολη διαδικασία. Μία καινοτόμα λύση έρχεται να δώσει το γεωργικό drone το οποίο είναι εναέριο όχημα που μπορεί με ευκολία να ερευνήσει το τεράστιο πεδίο της καλλιέργειας και να εντοπίσει διάφορα προβλήματα. Με αυτόν τον τρόπο βοηθά

άμεσα και καθοριστικά τις αγροτικές επιχειρήσεις να πάρουν ακριβείς αποφάσεις για τη διαχείριση της γης εξοικονομώντας παράλληλα πολύτιμο χρόνο. Ακριβέστερα αξιολογεί την υγεία των καλλιεργειών, την ανάπτυξή τους και με τους κατάλληλους αλγόριθμους επεξεργασίας εικόνας μπορεί να εντοπίσει τυχόν προσβολές από παράσιτα και ασθένειες. Επίσης έχει τη δυνατότητα να ψεκάζει λίπασμα και φυτοφάρμακα με τον πλέον πιο αποτελεσματικό τρόπο.

- **Συνδεδεμένα εργοστάσια**

  Οι εφαρμογές IoT αλλάζουν τον κόσμο μας, παρέχοντας έξυπνες λύσεις. Η ιδέα των συνδεδεμένων εργοστασίων περιλαμβάνει εργαλεία, μηχανήματα και αισθητήρες συνδεδεμένους στο διαδίκτυο. Είναι ένα συνδεδεμένο δίκτυο με διαφορετικές εργασίες όπως συντήρηση προγράμματος, αποστολή προϊόντων, έλεγχος ροής λειτουργίας και διακοπή ή παύση συγκεκριμένης διαδικασίας. Γενικά, ένας επόπτης παρακολουθεί ολόκληρο το έργο που πραγματοποιείται στο εργοστάσιο, αλλά η τεχνολογία IoT προτείνει απομακρυσμένη παρακολούθηση μέσω εφαρμογών επιτήρησης. Τα βασικότερα πλεονεκτήματα από αυτήν την εφαρμογή είναι ότι ο προγραμματισμός σε πραγματικό χρόνο μειώνει την επιπλέον κατανάλωση ενέργειας. Επίσης συχνά χρησιμοποιούνται έξυπνα οχήματα για τη μεταφορά και την αποθήκευση των προϊόντων κάτι το οποίο βοηθά στην εξοικονόμηση χρόνου και ενέργειας. Ακόμη η άμεση ανίχνευση βλαβών στο σύστημα διασφαλίζει την ποιότητα των προϊόντων. Τα έξυπνα εργοστάσια λειτουργούν όλο το εικοσιτετράωρο και μειώνουν το κόστος εργασίας.

Εικόνα 7. Έξυπνη βιομηχανία

Πηγή: https://bit.ly/2LkauGp

- **Διαχείριση εφοδιαστικής αλυσίδας από IoT**

  Η διαχείριση της εφοδιαστικής και των μεταφορών είναι από τους πρώτους τομείς που βρήκε εφαρμογή η τεχνολογία του IoT. Από την κατασκευή ενός προϊόντος έως την μεταφορά του στον τελικό καταναλωτή με τη σωστή και ασφαλή διατήρηση του αποθέματος αποτελεί μια σύνθετη και δύσκολη διαδικασία. Είναι πιθανό ότι ένα προϊόν μπορεί να χαθεί κατά τη μεταφορά του. Οι εφαρμογές IoT παρέχουν μια λύση μέσω παρακολούθησης GPS και ετικέτας RFID σε ένα προϊόν. Τα κυριότερα πλεονεκτήματα που προσφέρει είναι η ασφαλής και σίγουρη μεταφορά στο λιανοπωλητή, γεγονός που αυξάνει την αποδοτικότητα της αλυσίδας εφοδιασμού. Παρέχει ασφάλεια από κλοπές και διαφοροποιεί τα άρτια προϊόντα από τα κατεστραμμένα. Οι επόπτες λαμβάνουν άμεσα ειδοποιήσεις σε περίπτωση που συμβούν ζημιές και τεχνικές βλάβες. Αλλά το βασικότερο πλεονέκτημα είναι η παρακολούθηση των αποστολών ειδικά όταν γίνεται μεταξύ δύο χωρών, σε αυτές τις περιπτώσεις η χρήση της ειδικής ετικέτας στα προϊόντα παρέχει μεγάλη ασφάλεια.

- **IoT στη βιομηχανία συσκευασίας**

  Η βιομηχανία συσκευασίας επεκτείνεται συνεχώς καθώς αυξάνεται η ανησυχία των εταιρειών να παρέχουν ποιοτικά προϊόντα στα χέρια των πελατών τους. Οι εταιρείες χρησιμοποιούν εφαρμογές IoT στις συσκευασίες για δύο βασικούς σκοπούς. Ο πρώτος είναι για την προστασία του προϊόντος και ο δεύτερος αφορά ενσωματωμένες πληροφορίες για το προϊόν. Για παράδειγμα η διατήρηση ενός προϊόντος προϋποθέτει τη σωστή θερμοκρασία, έτσι υπάρχουν ενσωματωμένοι αισθητήρες IoT που μπορούν να αλλάξουν το χρώμα της συσκευασίας εάν η θερμοκρασία που έχει δεν είναι κατάλληλη. Όλες αυτές οι καινοτομίες που προσφέρει οδηγούν σε μία καλύτερη εμπειρία πελάτη.

1.3.3 Εφαρμογές IoT σε κοινωνικά θέματα και θέματα ασφάλειας

- **Συστήματα παρακολούθησης Κυκλοφορίας από το IoT**

  Το υπάρχον σύστημα παρακολούθησης της κυκλοφορίας όπου ένα φανάρι ελέγχει τη κίνηση και οι παραβάτες των κανόνων κυκλοφορίας παραμένουν μακριά από την κατάλληλη επιτήρηση είναι αρκετά ξεπερασμένα. Οι λύσεις που προσφέρουν οι εφαρμογές IoT σε αυτή την περίπτωση είναι πολύ αποτελεσματικές και βασίζονται στη χρήση της επεξεργασίας εικόνας. Επιπλέον, δυνατότητες που παρέχονται είναι η μέτρηση των οχημάτων σε κάθε πλευρά του δρόμου και μέσω της εφαρμογής του αλγόριθμου KNN υπολογίζεται ο χρόνος αναμονής κάθε πλευράς. Κάμερες παρακολούθησης μπορούν να εντοπίζουν και να καταγράφουν με χρήση εικόνας τους παραβάτες των κανόνων κυκλοφορίας και να λαμβάνονται αντίστοιχα τα κατάλληλα μέτρα και κυρώσεις από τους σχετικούς νόμους. Όλα αυτά έχουν ως αποτέλεσμα τη μείωση της ανθρώπινης

παρέμβασης για τη διαχείριση του συστήματος κυκλοφορίας. Η έρευνα συνεχίζεται και υπάρχουν στόχοι για λύσεις εντοπισμού κλεμμένων οχημάτων μέσω αντίστοιχων εφαρμογών.

- **Ανίχνευση δασικής πυρκαγιάς από το IoT**

  Οι δασικές πυρκαγιές είναι συχνό φαινόμενο σε πολλές χώρες με μεγάλες απώλειες τόσο σε ανθρώπινες ζωές όσο και σε φυσικούς πόρους. Συνήθως οι άνθρωποι παρατηρούν πυρκαγιές στα δάση όταν είναι πολύ αργά, όμως η πλατφόρμα εφαρμογών IoT μπορεί να προσφέρει αποτελεσματικές λύσεις με τη χρήση κατάλληλων ασύρματων αισθητήρων που μπορούν να ανιχνεύσουν τη δασική πυρκαγιά πριν εξαπλωθεί. Μια σειρά από αισθητήρες γύρω από το δάσος ανιχνεύουν την υγρασία από τον αέρα και στέλνουν ειδοποιήσεις ή αποθηκεύουν ανά τακτά χρονικά διαστήματα τις μετρήσεις στο cloud. Επίσης αισθητήρες όπως αισθητήρες θερμοκρασίας, αισθητήρες υγρασίας εδάφους, αισθητήρες υπερήχων, αισθητήρες επιταχυνσιόμετρου, στέλνουν αντίστοιχες αναφορές και ειδοποιήσεις. Η χρήση όσον αναφέρθηκαν μειώνουν σημαντικά τις καταστροφές των δασών σε περιπτώσεις πυρκαγιάς.

Εικόνα 8. Διαγραμματική απεικόνιση συστήματος πυρανίχνευσης IoT

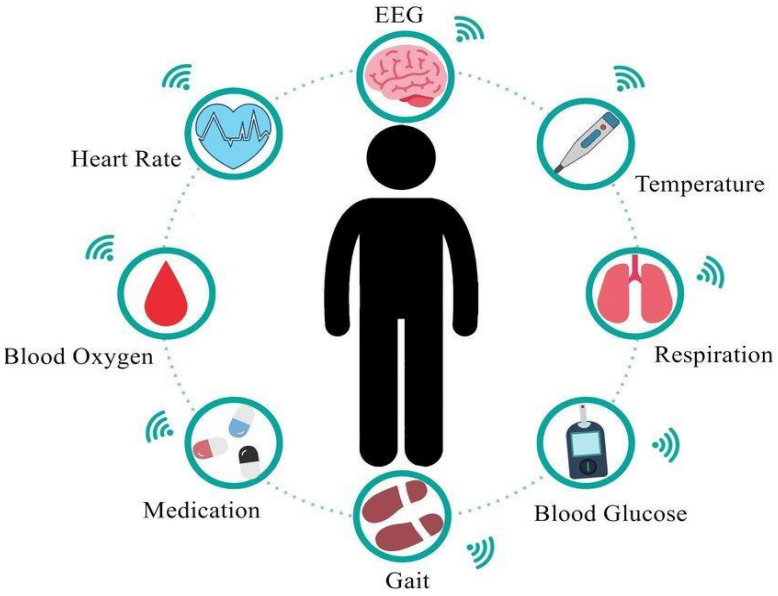
Πηγή: https://www.mokosmart.com/el/use-iot-fire-detector-sensor/

- **Δομική παρακολούθηση της υγείας**

  Η παρακολούθηση της υγείας σε τακτά χρονικά διαστήματα είναι απαραίτητη για την εξασφάλιση μεγαλύτερης διάρκειας ζωής. Οι εφαρμογές υγειονομικής περίθαλψης IoT αντιπροσωπεύουν έναν από τους ταχύτερα αναπτυσσόμενους τομείς της αγοράς IoT. Στην πραγματικότητα, η αξία αυτού του τομέα - που μερικές φορές ονομάζεται Internet of Medical Things (IoMT) - προβλέπεται να φτάσει τα 176 δισεκατομμύρια δολάρια μέχρι το 2026. Οι συσκευές IoT προσφέρουν μια σειρά από νέες ευκαιρίες στους επαγγελματίες υγείας να παρακολουθούν τους ασθενείς, καθώς και στους ασθενείς να παρακολουθούν τον εαυτό τους.

  Το πιο δημοφιλές παράδειγμα IoT στην υγειονομική περίθαλψη είναι η απομακρυσμένη παρακολούθηση ασθενών - που σημαίνει συσκευές IoT που

συλλέγουν δεδομένα ασθενών όπως καρδιακός ρυθμός, αρτηριακή πίεση και θερμοκρασία σώματος και πολλά άλλα από ασθενείς που δεν είναι φυσικά παρόντες σε μια μονάδα υγειονομικής περίθαλψης, εξαλείφοντας την ανάγκη των ασθενών να ταξιδέψουν στους παρόχους ή να τους συλλέξουν οι ίδιοι. Όταν μια συσκευή IoT συλλέγει δεδομένα ασθενών, τα προωθεί σε μια εφαρμογή όπου οι επαγγελματίες υγείας ή/και οι ασθενείς μπορούν να τα δουν. Μπορεί να χρησιμοποιηθούν αλγόριθμοι για την ανάλυση των δεδομένων προκειμένου να προταθούν θεραπείες ή να δημιουργηθούν ειδοποιήσεις. Άλλα παραδείγματα εφαρμογών IoT στην υγεία είναι η παρακολούθηση γλυκόζης, η παρακολούθηση υγιεινής χεριών, η παρακολούθηση της διάθεσης, η παρακολούθηση της νόσου του Πάρκινσον, έξυπνες συσκευές εισπνοής για το άσθμα, αισθητήρες κατάποσης, ρομποτική χειρουργική και άλλα.



Εικόνα 9. Το IoT στον τομέα της υγείας

Πηγή: https://www.researchgate.net/figure/A-medical-IoT-network-consists-of-devices-that-can-collect-analyze-and-act-on-patient_fig1_336602332

- **Έλεγχος αριθμού επισκεπτών με ανίχνευση smart Phone**

  Σε ένα γεγονός όπως μια δημόσια εκδήλωση σε μια πόλη υπάρχει ελεύθερη είσοδος για τους επισκέπτες. Η εφαρμογή του IoT σε τέτοιες περιπτώσεις παρέχει μια έξυπνη λύση για την καταμέτρηση των ατόμων αλλά και για την εξαγωγή χρήσιμων συμπερασμάτων ως προς τη συμπεριφορά τους. Με τη χρήση τριών αισθητήρων που βρίσκονται σε τρία σημεία του συμβάντος. Δύο βρίσκονται στην είσοδο και ένα άλλο είναι στον χώρο των δημόσιων συγκοινωνιών. Κάποιοι αισθητήρες σαρώνουν ολόκληρη τη περιοχή και ανιχνεύουν τον αριθμό των smartphone που υπάρχουν στην περιοχή, αποθηκεύοντας τα δεδομένα που συλλέγουν σε ένα cloud. Τα χρήσιμα συμπεράσματα που μπορούμε να λάβουμε

είναι η διάρκεια διαμονής των επισκεπτών, το σύνολο των επισκεπτών της εκδήλωσης και πολλά ακόμη δεδομένα. Αυτή η εφαρμογή θα μπορούσε να αποτελεί ένα χρήσιμο εργαλείο για τις υποδομές μια έξυπνης πόλης.

- **Εφαρμογή του IoT στη διαχείριση των αποβλήτων**

  Η διαχείριση των απορριμμάτων της πόλης είναι πάντα ένα δύσκολο πρόβλημα. Η εφαρμογή του δικτύου των πραγμάτων στη διαχείριση των απορριμμάτων καθιστά την όλη διαδικασία πιο έξυπνη και λειτουργική. Το σύστημα προτείνει ότι οι αισθητήρες θα συνδέονται με κάθε κάδο και εάν η ποσότητα των απορριμμάτων υπερβεί το όριο, κάθε κάδος θα στέλνει ειδοποιήσεις στο κεντρικό πρόγραμμα του cloud. Ο διαχειριστής της πόλης θα μπορεί να ελέγχει την τρέχουσα κατάσταση των απορριμμάτων κάθε τμήματος της πόλης. Επίσης θα μπορούσαν να χρησιμοποιηθούν αισθητήρες υπερήχων για την μέτρηση της πληρότητας στους κάδους. Μια πόλη θα ήταν πιο καθαρή και όμορφη με τη σωστή παρακολούθηση και χρήση των πόρων καθαριότητας.

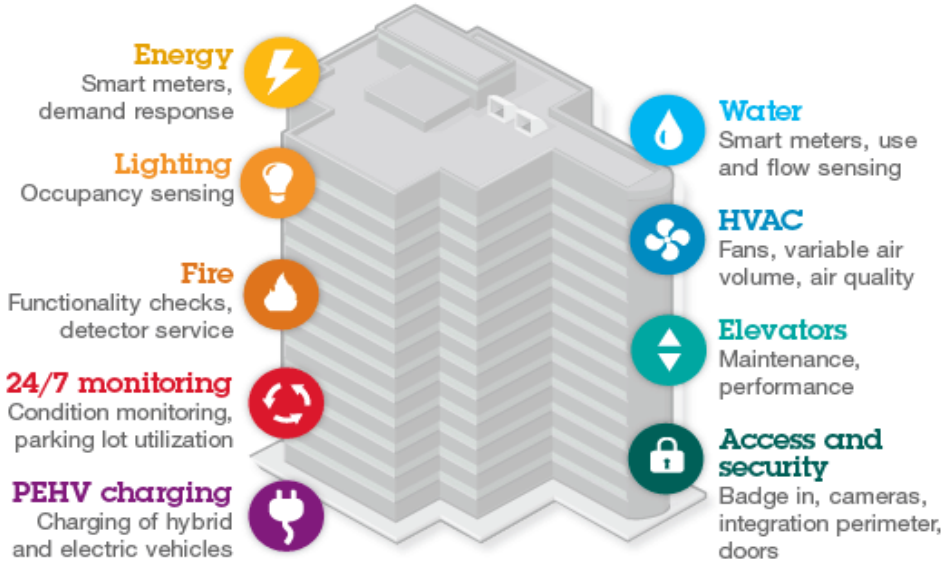
Τέλος [13] οι πρακτικές εφαρμογές της τεχνολογίας του IoT παρέχουν καθημερινά έξυπνες λύσεις σε αμέτρητους τομείς της καθημερινότητας του σημερινού κόσμου. Οι εφαρμογές του διαδικτύου των πραγμάτων θα διαμορφώσου τα δεδομένα του μέλλοντος σε μια διαφορετική βάση. Η έρευνες σε εφαρμογές IoT συνεχίζονται σε χιλιάδες διαφορετικές κατευθύνσεις και θεματικά πεδία, δεν υπάρχει αμφιβολία ότι πολύ σύντομα θα γίνει αναπόσπαστο μέρος της καθημερινότητας του σύγχρονου ανθρώπου. Ήδη οι μεγάλες εταιρείες επενδύουν πολλά χρήματα στον τομέα του IoT.

2. Έξυπνα κτίρια (Smart Buildings)

Ο τομέας των κτιρίων ευθύνεται για το 37%-41% περίπου της παγκόσμιας ετήσιας κατανάλωσης ενέργειας και έως και 30% για όλες τις παγκόσμιες εκπομπές αερίων θερμοκηπίου που σχετίζονται με την ενέργεια [14]. Προκειμένου να αντιμετωπιστεί το πρόβλημα της κλιματικής αλλαγής μέσω της μείωσης των εκπομπών αερίων του θερμοκηπίου, πρέπει να μειωθεί ο αντίκτυπος των κτιρίων. Άρα, είναι σημαντικό τα κτίρια να γίνονται όλο και πιο «έξυπνα» και βιώσιμα. Η έννοια των «έξυπνων» κτιρίων εμφανίστηκε αρκετά χρόνια πριν, αρχές της δεκαετίας του ογδόντα και με την πάροδο των χρόνων προτάθηκαν διάφοροι ορισμοί από διαφορετικές ομάδες χρηστών. Ένα έξυπνο κτίριο θα λέγαμε πως είναι η ενσωμάτωση των δομικών, τεχνολογικών και ενεργειακών συστημάτων.

2.1 Τί είναι τα έξυπνα κτήρια

Τα έξυπνα κτίρια χρησιμοποιούν συσκευές Internet of Things (IoT) για να παρακολουθούν διάφορα κτιριακά στοιχεία, να αναλύουν δεδομένα και να δημιουργούν πληροφορίες σχετικά με τα πρότυπα χρήσης που μπορούν να χρησιμοποιηθούν για τη βελτιστοποίηση των λειτουργιών του κτιρίου. Υπάρχει μια ποικιλία εξοπλισμού και λειτουργιών που μπορούν να τροφοδοτηθούν σε ένα έξυπνο κτίριο, το καθένα εξυπηρετώντας το δικό του μοναδικό σκοπό.



Εικόνα 10. Έξυπνα Κτίρια

Πηγή: https://www.mappedin.com/blog/use-cases/offices/your-guide-to-smart-buildings

Ένας έγκυρος ορισμός που έχει δοθεί για τα έξυπνα κτίρια [16], τα ορίζει ως οποιαδήποτε δομή που κάνει χρήση αυτοματοποιημένων διαδικασιών με σκοπό τον αυτόματο έλεγχο των λειτουργιών του κτιρίου, συμπεριλαμβανομένης της θέρμανσης, του εξαερισμού, του κλιματισμού, του φωτισμού, της ασφάλειας και άλλων συστημάτων. Το έξυπνο κτίριο χρησιμοποιεί αισθητήρες, ενεργοποιητές και μικροτσίπ, προκειμένου να συλλέγει δεδομένα και να τα αξιοποιεί ανάλογα με τις λειτουργίες και υπηρεσίες που πρέπει να εκτελούνται εντός αυτού. Όλες αυτές οι καινοτόμες λειτουργίες βοηθούν τους ιδιοκτήτες, τους φορείς εκμετάλλευσης και τους διαχειριστές εγκαταστάσεων να βελτιώσουν την αξιοπιστία και την απόδοση των εγκαταστάσεων, γεγονός που μειώνει τη χρήση ενέργειας, βελτιστοποιεί τον τρόπο χρήσης των δομών που υπάρχουν και ελαχιστοποιεί τις περιβαλλοντικές επιπτώσεις των κτιρίων.

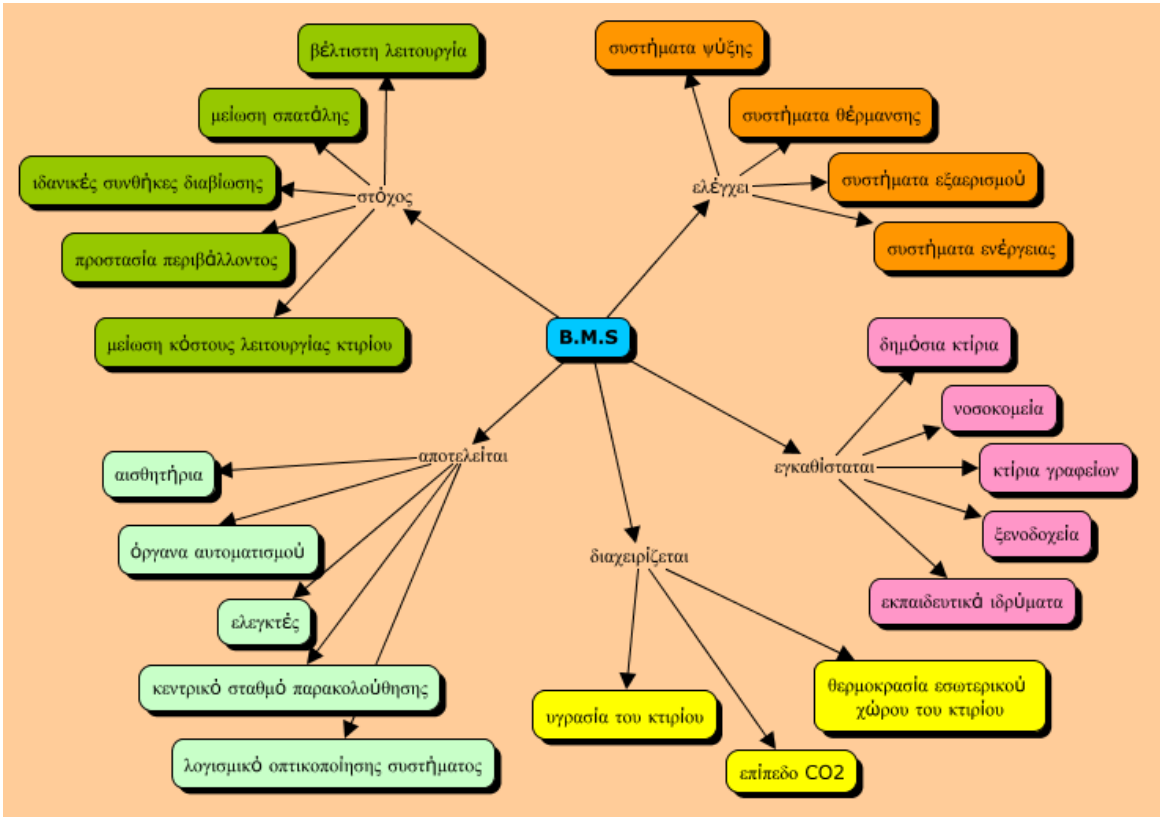
2.2 Λειτουργίες και Τεχνολογίες Έξυπνων Κτιρίων

2.2.1 Σύστημα Διαχείρισης Κτιρίου BMS (Building Management System)

Η έννοια “Σύστημα διαχείρισης κτιρίου” (BMS – Building Management System), επίσης αναφέρεται και ως σύστημα αυτοματισμού Κτιρίων (BAS – Building Automation System). Στην πράξη τα συστήματα BMS είναι υπολογιστικά συστήματα μέσω των οποίων ελέγχονται κάποιες ή οι περισσότερες διαδικασίες που καταναλώνουν ενέργεια σε ένα κτίριο. Αποτελεί δηλαδή, ένα δυναμικό ψηφιακό σύστημα ελέγχου που το εγκαθιστούμε στα διάφορα κτίρια με σκοπό να παρακολουθούμε και να ελέγχουμε τον ηλεκτρομηχανολογικό εξοπλισμό όπως το σύστημα του φωτισμού, τα συστήματα συναγερμού πυρκαγιάς , τα συστήματα HVAC (heating, ventilation, air conditioning), τους ανελκυστήρες, τον πίνακα ελέγχου, το σύστημα πρόσβασης και πολλά ακόμη συστήματα. Η εγκατάσταση ενός BMS συστήματος συνήθως συνδυάζεται και με άλλα συστήματα που βελτιώνουν την ενεργειακή απόδοση και τον αυτοματισμό των λειτουργιών ενός κτιρίου και σχεδόν ποτέ μεμονωμένα. Ένα σύστημα BMS συνήθως θα επιλεγεί για να εφαρμοστεί σε μεγάλα κτίρια όπως δημόσιες υπηρεσίες, πανεπιστήμια, κέντρα υγείας, εμπορικά κέντρα, δικαστικά μέγαρα, εγκαταστάσεις γραφείων διοίκησης μεγάλων εταιρειών και πολλά ακόμη παραδείγματα.

Επιπρόσθετα [16], σύμφωνα με τον ITU (International Telecommunication Union) το BMS μπορεί να θεωρηθεί ως ένα κεντρικό σύστημα ελέγχου το οποίο μπορεί συγκεντρωτικά να λαμβάνει αναφορές και να ελέγχει επιμέρους συστήματα αρκετά εξειδικευμένα όπως το σύστημα παρακολούθησης και ελέγχου ισχύος ενός κτιρίου, το σύστημα διαχείρισης των λυμάτων, το σύστημα συλλέκτη ηλιακής ενέργειας, συστήματα αυτόματου καθαρισμού σε διάφορους χώρους κ.α. Έτσι όλα αυτά τα συστήματα συνδέονται στο BMS και μας δίνεται η δυνατότητα μέσω αυτού να μπορούμε να τα επιβλέπουμε και να τα διαχειριζόμαστε από όποιο σημείο και να βρισκόμαστε.

Τα αποτελέσματα που θέλει να επιτύχει ένα σύστημα BMS είναι αρχικά όλες οι εγκαταστάσεις να λειτουργούν με τον καλύτερο δυνατό τρόπο[19], την φιλική χρήση των μηχανολογικών εξοπλισμών ως προς το περιβάλλον, την παροχή ανέσεων ως προς τις συνθήκες διαβίωσης, την εξοικονόμηση ενέργειας και κόστους. Επίσης, τα συστήματα BMS έχουν ως δυνατότητα να ρυθμίζουν τη θερμοκρασία, την υγρασία και τα επίπεδα διοξειδίου του άνθρακα εντός του κτιρίου, εδώ θα πρέπει να αναφέρουμε ότι όλα αυτά επιτυγχάνονται με την χρήση κατάλληλων αισθητήρων που είναι εγκατεστημένοι σε διάφορα μέρη του κτιρίου.



Εικόνα 11. Διαγραμματική απεικόνιση συστήματος BMS

Πηγή: http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/syst_elegxou_asfaleias_2018_final/____1.html

Το BMS σύστημα για να υπάρξει προϋποθέτει το συνδυασμό δύο πραγμάτων, πρώτον τη χρήση λογισμικού και δεύτερον τη σύνδεση του λογισμικού με τεχνικό υλικό. Τα προγράμματα λογισμικού που χρησιμοποιούνται συνήθως από ιδιώτες, είναι βασισμένα σε πρωτόκολλα επικοινωνίας όπως Profibus, BACnet, Instabus,Canbus κ.α. Το πρωτόκολλο επικοινωνίας ορίζεται ως η ψηφιακή γλώσσα η οποία επιτρέπει την επικοινωνία μεταξύ των συσκευών που συμμετέχουν στο BMS σύστημα. Οι εταιρείες που παράγουν BMS συστήματα χρησιμοποιούν πρωτόκολλα επικοινωνίας και ανοικτά πρότυπα όπως SOAP, XML, DeviceNet κ.α. Σχετικά με το τεχνικό υλικό του BMS περιλαμβάνει μία σειρά καλωδίων και εξαρτημάτων όπως είναι οι ψηφιακοί ελεγκτές που είναι οι κεντρικές μονάδες που εκτελούν εντολές λειτουργίας, τις εισόδους που είναι

οι μετρητές και οι αισθητήρες όπως για παράδειγμα θερμόμετρα, μετρητές κατανάλωσης ρεύματος κ.α., τις εξόδους όπως είναι τα ρελέ, βάνες κλπ και τέλος το ειδικό λογισμικό σε Η/Υ στο οποίο εκτελείται όλη η εποπτεία του συστήματος ελέγχοντας όλες τις επιμέρους παραμέτρους του συστήματος.

Ο κεντρικός σταθμός παρακολούθησης και ελέγχου είναι η κεφαλή σε ένα σύστημα BMS [19], σε αυτόν υπάρχουν το λογισμικό και όλα τα δεδομένα που αφορούν τις λειτουργίες της εγκατάστασης, και αποτελεί το κύριο μέσω επικοινωνίας του χειριστή με το σύστημα αυτοματισμού που επιτρέπει στον ελεγκτή να παίρνει αποφάσεις και να επαναπρογραμματίζει ανάλογα με τα δεδομένα που λαμβάνει. Οι κύριες δυνατότητες του κεντρικού σταθμού παρακολούθησης είναι:

- Γραφικές απεικονίσεις των συνθηκών των εγκαταστάσεων
- Γραφική αποτύπωση των παραμέτρων λειτουργίας
- Συλλογή και επεξεργασία σε συγκεκριμένα δεδομένα παραμέτρων
- Παραμετροποίηση σε επιλεγμένες ρυθμίσεις για τη δημιουργία σωστών συνθηκών
- Άμεση ενημέρωση για τις τιμές μετρήσεων που είναι εκτός εγκεκριμένων ορίων
- Διαχείριση έναρξης και λήξης λειτουργίας σε μηχανήματα με συγκεκριμένα ωράρια
- Έλεγχος απομακρυσμένα μέσω συστημάτων παρακολούθησης (ακόμη και με δυνατότητα οπτικοποίησης) με χρήση διαδικτυακών συνδέσεων

Οι αισθητήρες και τα όργανα αυτοματισμού, αποτελούν τα μάτια και τα αυτιά του συστήματος BMS. Είναι τοποθετημένα σε κατάλληλα σημεία του κτιρίου έπειτα από μελέτη, ώστε να μας δίνουν τις καλύτερες δυνατές πληροφορίες για να επιτευχθεί ο έλεγχος με ασφάλεια και εγκυρότητα. Σε αυτούς συμπεριλαμβάνονται οι παντός είδους θερμοστάτες, οι μετρητές υγρασίας, οι μετρητές διοξειδίου του άνθρακα (CO2), οι μετρητές φωτεινότητας και γενικά όλα αυτά τα εξαρτήματα που μας δίνουν μια πλήρη εικόνα για την ενεργειακή κατάσταση του κτιρίου. Είναι δεδομένο ότι οι αισθητήρες αυτοί, ελέγχουν την κατάσταση των συνθηκών που επικρατούν στο κτίριο και δίνουν την απαραίτητη ενημέρωση στον χρήστη του συστήματος να προβεί στις αντίστοιχες ενέργειες ρύθμισης των συνθηκών.

Όσο απαραίτητοι είναι οι αισθητήρες σε ένα σύστημα BMS [19], άλλο τόσο είναι τα όργανα και οι συσκευές αυτοματισμού. Στην πράξη, οι αισθητήρες παρακολουθούν τις συνθήκες που επικρατούν σε ένα κτίριο, ο χρήστης τις αξιολογεί και τα όργανα αυτοματισμού εκτελούν την εντολή που δίνεται ώστε να επιτευχθούν οι καλύτερες δυνατές συνθήκες. Ουσιαστικά, αποτελούν εκτελεστικά όργανα. Οι αντλίες υδάτων, τα ηλεκτρικά ρελέ, τα PLC, οι αντλίες καυσίμων, οι ηλεκτροκινητήρες, οι καυστήρες κ.α., συμπεριλαμβάνονται στον όρο που αναφέρουμε ως “όργανα αυτοματισμού”.

Παρακάτω θα δούμε έναν πίνακα στον οποίο αποτυπώνεται αναλυτική λίστα των σημείων ελέγχου του συστήματος (BMS) από το απομακρυσμένο σημείο κέντρου ελέγχου ΙΟΡ 1. Τα δεδομένα αφορούν την εταιρεία ΔΕΔΔΗΕ Α.Ε. (ΝΕΟ ΜΗΧΑΝΟΓΡΑΦΙΚΟ ΚΕΝΤΡΟ ΣΕ ΚΤΙΡΙΟ) επί της οδού Αυτοκρ. Νικολάου 2 στην Αθήνα. Στον Πίνακα καταγράφονται παρατηρήσεις όπως θερμοκρασίες, τιμές υγρασίας μέσω αισθητήρων, ηλεκτρικών πινάκων, επαγωγικών διακοπτών, αυτόνομου ανιχνευτή καπνού, και σε τερματική επαφή κινητήρα βαλβίδας τριών θέσεων που αφορούν εγκαταστάσεις σε χώρους όπου λειτουργούν μηχανές, σε τερματικές κλιματιστικές μονάδες, σε χώρο ηλεκτρονικών πινάκων του ισογείου, στον εναλλάκτη ανάκτησης θερμότητας αέρα και τέλος στο ψύκτη νερού.

Πίνακας 1. Αναλυτική λίστα σημείων ελέγχου συστήματος (BMS) από απομακρυσμένο σημείο κέντρου ελέγχου

ΑΠΟΜΑΚΡΥΣΜΕΝΟ ΚΕΝΤΡΟ ΕΛΕΓΧΟΥ ΙΟΡ 1								
α/α	ΕΓΚΑΤΑΣΤΑΣΗ/ΕΞΟΠΛΙΣΜΟΣ/ΕΞΑΡΤΗΜΑ	ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ					ΟΡΓΑΝΟ/ ΣΥΣΚΕΥΗ ΕΛΕΓΧΟΥ	ΠΑΡΑΤΗΡΗΣΕΙΣ
		DI	DO	AI	AO	ΠΕΡΙΓΡΑΦΗ		
1.	ΧΩΡΟΣ ΜΗΧΑΝΩΝ							
1.1	Μέτρηση θερμοκρασίας χώρου			6		Αντίσταση	Αισθητήριο θερμοκρασίας χώρου	0…+50ο C
1.2	Μέτρηση σχετικής υγρασίας χώρου			3		0V…10VDC	Αισθητήριο υγρασίας χώρου	0…100% rh
2.	ΧΩΡΟΣ ΜΗΧΑΝΩΝ - ΤΕΡΜΑΤΙΚΕΣ ΚΛΙΜΑΤΙΣΤΙΚΕΣ ΜΟΝΑΔΕΣ (INROW) CCU-01…CCU-06							6 συσκευές
2.1	Ένδειξη γενικής βλάβης τοπικής κλιματιστικής συσκευής	6				NC επαφή	Ηλεκτρικός πίνακας κλιματιστικής συσκευής	
2.2	Παράμετροι λειτουργίας τοπικής κλιματιστικής συσκευής	ΜΕΣΩ ΛΟΓΙΣΜΙΚΟ				Διασύνδεση	Ηλεκτρικός πίνακας κλιματιστικής συσκευής	Modbus RTU, 270 regist ***
3.	ΧΩΡΟΣ ΗΛΕΚΤΡΙΚΩΝ ΠΙΝΑΚΩΝ ΙΣΟΓΕΙΟΥ							
3.1	Μέτρηση θερμοκρασίας χώρου			1		Αντίσταση	Αισθητήριο θερμοκρασίας χώρου	0…+50ο C
3.2	Μέτρηση σχετικής υγρασίας χώρου			1		0V…10VDC	Αισθητήριο υγρασίας χώρου	0…100% rh
4.	ΕΝΑΛΛΑΚΤΗΣ ΑΝΑΚΤΗΣΗΣ ΘΕΡΜΟΤΗΤΑΣ ΑΕΡΑ - ΑΕΡΑ							
4.1	Εκκίνηση ανεμιστήρων εναλλάκτη		2			NO επαφή	Ηλεκτρικός πίνακας κίνησης	
4.2	Επιβεβαίωση ροής αέρα ανεμιστήρων εναλλάκτη	2				NO επαφή	Επαγωγικός διακόπτης με ρυθμιζόμενο S.P.	
4.3	Ένδειξη θέσης διακοπή Η-0-Α ανεμιστήρων εναλλάκτη	2				NO επαφή	Ηλεκτρικός πίνακας κίνησης	Θέση "αυτόματο"
4.4	Ένδειξη κατάστασης ρελέ ισχύος ανεμιστήρων εναλλάκτη	2				NO επαφή	Ηλεκτρικός πίνακας κίνησης	
4.5	Μέτρηση θερμοκρασίας αέρα προσαγωγής			1		Αντίσταση	Αισθητήριο θερμοκρασίας αεραγωγού	-30…+80oC
4.6	Μέτρηση θερμοκρασίας αέρα απόρριψης			1		Αντίσταση	Αισθητήριο θερμοκρασίας αεραγωγού	-30…+80oC
4.7	Μέτρηση θερμοκρασίας νωπού αέρα			1		Αντίσταση	Αισθητήριο θερμοκρασίας αεραγωγού	-30…+80oC
4.8	Μέτρηση σχετικής υγρασίας νωπού αέρα			1		0…10VDC	Αισθητήριο σχετικής υγρασίας αεραγωγού	0…100%r.h.
4.9	Μέτρηση ρυπαρότητας των φίλτρων αέρα			1		0…10VDC	Αισθητήριο διαφορικής πίεσης αέρα	0…500Pa
4.10	Ένδειξη ανίχνευσης καπνού στον αεραγωγό νωπού αέρα	1				NC επαφή	Αυτόνομος ανιχνευτής καπνού αεραγωγού	Φωτοηλεκτρονικός, IP54
5.	ΨΥΚΤΗΣ ΝΕΡΟΥ CHILLER 1							
5.1	Ενεργοποίηση λειτουργίας		1			NO επαφή	Ηλεκτρικός πίνακας αυτομαισμού ψύκτη	
5.2	Επιβεβαίωση λειτουργίας	1				NO επαφή	Ηλεκτρικός πίνακας αυτομαισμού ψύκτη	
5.3	Ένδειξη γενικής βλάβης	1				NC επαφή	Ηλεκτρικός πίνακας αυτομαισμού ψύκτη	
5.4	Μέτρηση θερμοκρασίας νερού εισόδου			1		Αντίσταση	Ηλεκτρικός πίνακας αυτομαισμού αντλ.θερμ.	-30…+80oC, 100mm
5.5	Μέτρηση θερμοκρασίας νερού εξόδου			1		Αντίσταση	Ηλεκτρικός πίνακας αυτομαισμού αντλ.θερμ.	-30…+80oC, 100mm
5.6	Έλεγχος δίοδος βαλβίδας νερού τύπου πεταλούδας		1			NO επαφή	Κινητήρας βαλβίδας τριών θέσεων	positioning time<6sec
5.7	Ένδειξη κλειστής θέσης δίοδου βαλβίδας νερού	1				NO επαφή	Τερμ. Επαφή κινητήρα βαλβίδας τριών θέσεων	
5.8	Ένδειξη ανοικτής θέσης δίοδου βαλβίδας νερού	1				NO επαφή	Τερμ. Επαφή κινητήρα βαλβίδας τριών θέσεων	
5.9	Ένδειξη και έλεγχος παραμέτρων λειτουργείας αντλ. Θερμ.	ΜΕΣΩ ΛΟΓΙΣΜΙΚΟ				Διασύνδεση	Ηλεκτρικός πίνακας αυτομαισμού αντλ.θερμ.	BACNet,(45d.p./ψύκτη)

Πηγή: https://docplayer.gr/16187203-Parartima-a-analytiki-lista-simeion-eleghoy-systimatos-apomakrysmenoy-eleghoy-bms.html

2.2.2 Πρότυπο Κτιριακού Ελέγχου KNX

Όλο και περισσότερο αυξάνεται η ανάγκη για εύκολη και πιο άμεση διαχείριση σε πολλούς τομείς που αφορούν τη ομαλή λειτουργία ενός κτιρίου όπως είναι το σύστημα του φωτισμού, της ασφάλειας του κλιματισμού κ.α. Παράλληλα αυξάνεται και η ανάγκη για εξοικονόμηση της ενέργειας έτσι ώστε η λειτουργία των κτιρίων να είναι πιο αποδοτική και φιλική προς το περιβάλλον. Συνεπώς απαιτείται ένα έξυπνο σύστημα διαχείρισης ελέγχου και παρακολούθησης των αντίστοιχων λειτουργιών σε ένα κτήριο.

Ένα τέτοιο σύστημα συνήθως προϋποθέτει περισσότερη καλωδίωση εντός και εκτός του κτηρίου, για να επιτευχθεί η σύνδεση μεταξύ αισθητήρων, ενεργοποιητών και του κέντρου ελέγχου. Η εγκατάσταση μεγάλης καλωδίωσης απαιτεί μεγάλο κόστος, είναι χρονοβόρα λόγω της μελέτης και του σχεδιασμού που προϋποθέτει και ενέχει σημαντικούς κινδύνους δυσλειτουργιών, βλαβών και ατυχημάτων. Το παγκόσμιο πρότυπο κτιριακού ελέγχου KNX, μπορεί να ξεπεράσει την διαδικασία των καλωδιώσεων. Μέσω του προτύπου KNX μεταφέρονται δεδομένα μεταξύ των εξαρτημάτων διαχείρισης του κτιρίου με τη χρήση μιας κοινής γλώσσας. Όλες οι συσκευές bus συνδέονται είτε με καλώδιο συνεστραμμένων αγωγών, είτε με ραδιοσυχνότητες, ή με γραμμές ισχύος ή με IP/Ethernet και ανταλλάσουν δεδομένα μέσω του KNX με το οποίο είναι συνδεδεμένες.

Οι συσκευές bus [18] μπορεί να είναι διάφοροι τύποι αισθητήρων ή να είναι ενεργοποιητές που χρειάζονται για να επιτευχθεί ο έλεγχος των διάφορων εφαρμογών λειτουργίας του κτηρίου, για παράδειγμα ο προγραμματισμός και η αυτοματοποίηση στη λειτουργία του φωτισμού, σε τυχόν ηλεκτρικά ρολά που χρησιμοποιούνται, σε συστήματα συναγερμού, σε συστήματα ελέγχου πρόσβασης, στη διαχείριση της θερμοκρασίας κ.α.

2.3 Εφαρμογές Έξυπνων Κτιρίων

Οι κτιριακοί αυτοματισμοί είναι η δυναμική διείσδυση των ηλεκτρονικών συσκευών και εφαρμογών στο χώρο των οικοδομικών κατασκευών. Ο όρος «building automation» ή «smart buildings» χρησιμοποιούνται για να χαρακτηρίσουν ένα σύγχρονο κτίριο στο οποίο εφαρμόζονται συνδυαστικά οι νέες τεχνολογίες των αυτοματισμών, ασφαλείας, οπτικοακουστικών μέσων, πληροφορικής και τηλεπικοινωνιών και το διαφοροποιούν από τις συμβατικές κατασκευές. Δεν υπάρχουν περιορισμοί στις εφαρμογές που μπορεί να περιλαμβάνει ένα «έξυπνο κτίριο». Στα επόμενα υποκεφάλαια θα αναφερθούμε σε κάποιες από αυτές τις εφαρμογές.

2.3.1 Εφαρμογή ως προς την θέρμανση / ψύξη του κτιρίου

Μία από τις πιο βασικές εφαρμογές των έξυπνων κτιρίων είναι η δυνατότητα επιλογής και ρύθμισης της θερμοκρασίας των κτιρίων, μέσω της ρυθμιστικής λειτουργίας χειμερινής περιόδου και θερινής περιόδου με σκοπό τη διαμόρφωση του κυκλώματος διανομής μέσω των αντλιών θερμότητας και της κεντρικής κλιματιστικής μονάδας (ΚΚΜ)

του συστήματος ανάλογα με την αντίστοιχη περίοδο. Οι δυνατότητες που παρέχει το αντίστοιχο σύστημα BMS είναι:

- Ρύθμιση λειτουργίας σε Χειμερινή/Θερινή περίοδο
- Προκαθορισμένο πρόγραμμα λειτουργίας ανάλογα με τις ημέρες και ώρες λειτουργίας του κτιρίου
- Μέτρηση και καταγραφή της τρέχουσας θερμοκρασίας του κτιρίου ανά τακτά χρονικά διαστήματα
- Εντοπισμός και αποστολή ενημέρωσης σε περίπτωση βλάβης του συστήματος
- Απομακρυσμένη ενεργοποίηση των λειτουργιών ON, OFF, Auto της ΚΚΜ
- Καθορισμός επιλεγμένου εύρους τιμών (min-max) θερμοκρασίας αέρα για ψύξη & θέρμανση.
- Ενεργοποίηση βαλβίδας ύγρανσης
- Λειτουργία ενεργοποίησης προστασία σε περίπτωση παγετού μέσω ενημέρωσης του συστήματος της θερμοκρασίας και της υγρασίας εκτός του κτιρίου

2.3.2 Εφαρμογή ως προς την λειτουργία φωτισμού του κτιρίου

Ένα οργανωμένο σύστημα ελέγχου φωτισμού ενός κτηρίου μέσω δεδομένων που λαμβάνει από αισθητήρες που υπάρχουν σε διάφορα μέρη του κτιρίου, μπορεί να υπολογίζει την εξωτερική φωτεινότητα και ανάλογα να ρυθμίζει τον εσωτερικό φωτισμό με την κατάλληλη ένταση κάνοντας παράλληλα οικονομική χρήση της ενέργειας. Ακόμη υπάρχουν ανιχνευτές κινήσεων και παρουσίας ατόμων στο χώρο όπου ενεργοποιούν ή απενεργοποιούν αντίστοιχα τον φωτισμό αυτοματοποιημένα χωρίς να χρειάζεται ανθρώπινη παρέμβαση. Επίσης υπάρχει και η λειτουργία αυτόματης σκίασης κατά την οποία ρυθμίζονται αυτόματα τα rollers των παραθύρων δημιουργώντας την κατάλληλη σκίαση όταν αυτό απαιτείται κυρίως τους καλοκαιρινούς μήνες όπου υπάρχει έντονη ηλιακή ακτινοβολία.

2.3.3 Εφαρμογή ως προς την πυρανίχνευση και τον εντοπισμό ύπαρξης πλημμύρας στο κτίριο και την γενικότερη ασφάλεια

Όσον αφορά τα θέματα ασφάλειας στα κτίρια [20], υπάρχει η δυνατότητα εγκατάστασης συστήματος με αισθητήρες μέτρησης καπνού και μονοξειδίου του άνθρακα εντός των κτιριακών εγκαταστάσεων. Σε περίπτωση που οι αισθητήρες εντοπίσουν τιμές ανώτερες των αποδεκτών μεταδίδουν άμεσα ειδοποιήσεις έκτακτης ανάγκης λόγω πυρκαγιάς και ταυτόχρονα ενεργοποιείται αυτόματα συναγερμός με τη δυνατότητα μετάδοσης ηχογραφημένου μηνύματος που ενημερώνει σε ποιο σημείο εντοπίζεται ο καπνός και την καλύτερη δυνατή επιλογή εξόδου από το κτίριο. Επίσης

αντίστοιχα υπάρχει η δυνατότητα εντοπισμού ύπαρξης πλημμύρας μέσω αισθητήρων που ανιχνεύουν υγρό σε διάφορους χώρους που δεν θα έπρεπε να υπάρχει όπως για παράδειγμα σε γραφεία, αποθήκες, διαδρόμους του κτιρίου κ.α. με σκοπό την προστασία των χώρων την αποφυγή βλαβών και την καταστροφή εξοπλισμών.

Ακόμη είναι τοποθετημένοι σε πολλά σημεία του κτηρίου αισθητήρες κίνησης οι οποίοι ανιχνεύουν την κίνηση και σε συνδυασμό με συστήματα συναγερμών μπορούν να ελέγχουν την ασφάλεια του κτιρίου σε ημέρες και ώρες που δεν λειτουργεί με σκοπό την προστασία και την αποτροπή διαρρήξεων και παραβιάσεων.

2.4 Πλεονεκτήματα και Μειονεκτήματα Έξυπνων Κτιρίων

Τα έξυπνα κτίρια όπως έχουμε ήδη αναφέρει έχουν πολλές λειτουργικότητες [22], είναι ιδιαίτερα καινοτόμα και προσφέρουν μια μεγάλη σειρά από λύσεις σε διάφορα θέματα. Ωστόσο παρά τα πολλά τους πλεονεκτήματα, προκύπτουν και κάποια ζητήματα ως προς την πρακτική εφαρμογή τους που θα τα μελετήσουμε στη συνέχεια.

2.4.1 Τα βασικά Πλεονεκτήματα των Έξυπνων Κτιρίων

Ασφάλεια

Ένα από τα πιο σημαντικά πλεονεκτήματα που πρέπει να αναφέρουμε είναι η ασφάλεια εντός του κτιρίου και η σωστή λειτουργία των ηλεκτρονικών συσκευών που παρέχονται στα έξυπνα κτίρια, μέσω του ελέγχου της αυξομείωσης της τάσης του ρεύματος και της άμεσης ειδοποίησης σε περίπτωση δυσλειτουργίας ή βλάβης. Επίσης υπάρχει η αυτόματη λειτουργία παροχής ρεύματος μόνο στις μπρίζες στις οποίες έχουν κάποια συσκευή συνδεδεμένη. Επιπλέον μέσω αισθητήρων υπάρχει η δυνατότητα ανίχνευσης διαρροών σε νερό και φυσικό αέριο και άμεσης ενημέρωσης μέσω ειδοποιήσεων στις αρμόδιες υπηρεσίες και στον ιδιοκτήτη. Σχετικά με την ασφάλεια του κτιρίου σε περίπτωση διάρρηξης, υπάρχει το κλειστό κύκλωμα παρακολούθησης όπου έχει εγκατεστημένους αισθητήρες και κάμερες, που μπορούν να ελέγχουν τα άτομα τα οποία βρίσκονται στο χώρο αν έχουν πρόσβαση σε αυτό και κάποια από τα στοιχεία της ταυτότητας τους. Επιπρόσθετα, οι κεντρικές είσοδοι του κτηρίου μπορούν να διαθέτουν συστήματα που ειδοποιούν σε περίπτωση παραβίασης του χώρου ή να ρυθμίζονται να κλείνουν αυτόματα μετά από προκαθορισμένο χρονικό διάστημα και παράλληλα να στέλνουν ειδοποίηση. Ακόμη σε τυχόν παραβίαση του κτιρίου ηχεί ο συναγερμός και παράλληλα μέσω δικτύου τηλεφωνίας ειδοποιείται ο ιδιοκτήτης του κτηρίου ή οι αρμόδιοι διαχειριστές και η αστυνομία. Τέλος σε περίπτωση ανίχνευσης κινήσεων και θορύβων κατά την διάρκεια της νύχτας υπάρχει διακόπτης ο οποίος ενεργοποιεί φωταψία σε ολόκληρο το κτίριο.

Μείωση λειτουργικού κόστους

Ένα ακόμη πολύ σημαντικό όφελος των έξυπνων κτιρίων είναι η αποδοτικότητά του η οποία εξασφαλίζεται μέσω της μείωσης του λειτουργικού κόστους του. Ειδικότερα υπάρχουν έρευνες οι οποίες αποδεικνύουν ότι η χρήση της τεχνολογίας αυξάνει σημαντικά την ενεργειακή αποδοτικότητα των κτιρίων. Αν για παράδειγμα υπολογίσουμε τα κέρδη που προκύπτουν από αυτή την εξοικονόμηση ενέργειας σε μεγάλες πολυεθνικές εταιρείες που έχουν στο ενεργητικό τους τεράστια κτίρια και σε πολλές περιπτώσεις εκμισθώνουν ολόκληρα οικοδομικά τετράγωνα, τα οφέλη είναι τεράστια. Υπάρχει αντίστοιχη έρευνα που αναφέρει ότι το 40% της ενέργειας που καταναλώνεται στις περισσότερες χώρες αφορά την λειτουργία των κτιρίων.

Φιλική προσέγγιση προς το περιβάλλον

Σε συνέχεια όλων των παραπάνω που αναφέρθηκαν τα έξυπνα κτίρια παράλληλα είναι και αρκετά φιλικά προς το περιβάλλον. Αρχικά, η εξοικονόμηση της ενέργειας που επιτυγχάνεται προστατεύει τους φυσικούς πόρους αλλά και τους πόρους των ορυκτών καυσίμων. Επίσης καινοτομίες όπως η τοποθέτηση των ηλιακών πάνελ μειώνουν ακόμη περισσότερο την ανάγκη χρήσης των καυσίμων. Για παράδειγμα ένα «οικολογικά έξυπνο κτίριο» είναι το Edge, ένα κτίριο γραφείων που βρίσκεται στο Άμστερνταμ, αποτελεί την έδρα της εταιρείας Deloitte και οι περισσότεροι από 28.000 αισθητήρες σε οίκημα 40.000 τετραγωνικών μέτρων δίνουν ενημέρωση από την ενέργεια που δαπανάται έως την υγρασία και το επίπεδο φωτισμού. Οι εργαζόμενοι έχουν τη δυνατότητα να συνδέονται με το κτίριο μέσω μιας εφαρμογής που διευκολύνει την καθημερινή εργασία στο γραφείο. Το κτίριο αποτελείται από 15 ορόφους και είναι εφοδιασμένο με ηλιακή ενέργεια που παράγεται χάρη στα πάνελ που έχει σε έναν από τους τοίχους και στη στέγη. Το νερό που χρησιμοποιείται για θέρμανση και κλιματισμό συλλέγεται χάρη σε έναν υδροφόρο ορίζοντα που βρίσκεται κάτω από το κτίριο. Αυτά είναι μερικά από τα χαρακτηριστικά που οδήγησαν το κτίριο The Edge να επιτύχει το υψηλότερο αποτέλεσμα στην ιστορία της βιωσιμότητας (98,36%), σύμφωνα με την περιβαλλοντική υπηρεσία αξιολόγησης BREEAM.

Εικόνα 12. Το πιο βιώσιμο κτίριο στον κόσμο, The Edge, Άμστερνταμ

Πηγή: https://ecolution.co.za/2017/09/28/5-of-the-worlds-greenest-buildings/

2.4.2 Τα βασικά Μειονεκτήματα των Έξυπνων Κτιρίων

Στη συνέχεια θα πρέπει να αναφερθούμε και στα μειονεκτήματα των έξυπνων κτιρίων που μπορεί να είναι μικρής σημαντικότητας σε σύγκριση με επαναστατικά καινοτόμα πλεονεκτήματά τους, ωστόσο είναι υπαρκτά και δεν πρέπει να τα υποτιμούμε [23].

Κόστος: Είναι εύλογο το γεγονός πως κάποια από τα συστήματα αυτοματισμών και ελέγχων που διαθέτουν τα έξυπνα κτίριο, λόγω της εξειδίκευσης που έχουν μπορεί να είναι αρκετά ακριβά. Και αν σκεφτούμε πρακτικά ένα μεγάλο κτιριακό συγκρότημα, μεγάλες εργοστασιακές εγκαταστάσεις, σε τέτοιες περιπτώσεις τα κόστη που απαιτούνται για την εγκατάσταση και την συντήρηση τέτοιων συστημάτων ενδεχομένως να είναι υπέρογκα.

Ικανότητες και γνώσεις χειρισμού του συστήματος: Είναι προφανές πως για να λειτουργήσουν όλα τα συστήματα που έχουμε αναφέρει στα προηγούμενα κεφάλαια, απαιτούνται άνθρωποι με εξειδικευμένες γνώσεις ως προς το χειρισμό τους και τον τρόπο λειτουργίας τους. Θα μπορούσαμε να πούμε πως «τα έξυπνα κτίρια χρειάζονται και έξυπνους χειριστές», αυτό ταυτόχρονα σημαίνει πως δεν μπορούν όλοι να ανταπεξέλθουν στο χειρισμό τους και χρειάζεται να καταρτιστούν κατάλληλα γενικότερα γύρω από την τεχνολογία αλλά και εξειδικευμένα στα επιλεγμένα συστήματα. Αυτό πρακτικά μεταφράζεται σε χρόνο και χρήμα.

Υποδομές και εξοπλισμός: Ακόμη ένα μειονέκτημα είναι η έλλειψη ή η μειωμένη ύπαρξη υποδομών και αντίστοιχων εφαρμογών που συναντάμε σε πολλές χώρες. Αυτό συμβαίνει διότι οι λειτουργικότητες των έξυπνων κτιρίων απαιτούν υψηλή ισχύ επεξεργασίας και μεγάλο αποθηκευτικό χώρο για επεξεργασία και αποθήκευση των δεδομένων. Επίσης οι προγραμματιστικοί αλγόριθμοι που απαιτούνται για την λειτουργία των συστημάτων συνήθως δημιουργείται εξατομικευμένα διότι ακόμη δεν υπάρχουν έτοιμα set up σε ευρεία κυκλοφορία. Επιπρόσθετα, η κατασκευή των έξυπνων κτιρίων θα πρέπει να έχει συμβατή συνδεσιμότητα με τα ηλεκτρικά οχήματα ώστε να υπάρχουν υποδομές για την φόρτισή τους, κάτι το οποίο θα αυξάνει το λειτουργικό κόστος τους.

GDPR: Με βάση την ιδιαίτερη σημασία που δίνεται τα τελευταία χρόνια γύρω από τα δικαιώματα των ανθρώπων ως προς την ασφάλεια των προσωπικών τους δεδομένων και στοιχείων και σύμφωνα με τους αυστηρούς νόμους που έχουν θεσπιστεί σχετικά με αυτό το ζήτημα. Τα συστήματα ελέγχου των έξυπνων κτιρίων με την αποθήκευση και επεξεργασία τέτοιων δεδομένων έρχονται σε αντίθεση με τους αντίστοιχους νόμους. Με αποτέλεσμα να πρέπει να ενεργοποιηθούν νομικά τμήματα από την πλευρά των κτιρίων για να μπορέσουν να διαχειριστούν και να δώσουν λύσεις σε τέτοιου είδους νομικά ζητήματα.

3. Έξυπνα Σπίτια (Smart Homes)

3.1 Τι είναι τα έξυπνα σπίτια

Σε αυτό το κεφάλαιο θα δούμε την εφαρμογή του IoT σε ιδιωτικό επίπεδο και από τα έξυπνα κτήρια θα αναφερθούμε στα έξυπνα σπίτια. Οι έντονοι ρυθμοί του σύγχρονου τρόπου ζωής δημιουργούν διαρκώς νέες ανάγκες, οι οποίες απαιτούν την διαχείριση τους από ένα σύστημα αυτοματισμών και ελέγχου. Η φράση "έξυπνο σπίτι" χρησιμοποιείται για οποιαδήποτε οικία, ενσωματώνει σε μικρότερο ή μεγαλύτερο βαθμό τη δυνατότητα ρύθμισης και ελέγχου ορισμένων ηλεκτρομηχανολογικών εγκαταστάσεων.

Το σπίτι με νοημοσύνη σκέπτεται και ενεργεί βάση των καθημερινών αναγκών και συνηθειών, δίνοντας στον χρήστη τον απόλυτο έλεγχο σε συστήματα ασφάλειας, θέρμανσης, φωτισμού, ηλεκτρικών συσκευών, περιεχομένων multimedia κ.α. Οι λειτουργίες αυτές ελέγχονται με το πάτημα ενός κουμπιού, είτε ο ιδιοκτήτης βρίσκεται εντός του κτιρίου είτε βρίσκεται σε κάποια απομακρυσμένη περιοχή.

Το έξυπνο σπίτι προσφέρει πλήθος δυνατοτήτων οι οποίες εξασφαλίζουν μεγαλύτερη ασφάλεια και προστασία της ιδιοκτησίας των κατόχων, με σύγχρονους τρόπους που προηγουμένως δεν υπήρχαν. Για παράδειγμα με τα συστήματα ασφαλείας οι κάτοικοι ενός σπιτιού μπορούν:

- Να ειδοποιηθούν ότι επιχειρείται διάρρηξη και παράλληλα να προκληθεί πανικός στους επίδοξους διαρρήκτες ενεργοποιώντας την σειρήνα και τον φωτισμό σε ολόκληρο το σπίτι. Το σύστημα μπορεί να ειδοποιήσει τον ιδιοκτήτη στο κινητό του τηλέφωνο, το Κέντρο Λήψεων Σημάτων και εφόσον έχει γίνει η σχετική ρύθμιση ειδοποιείται αυτόματα και η αστυνομία.
- Αν αντιληφθούν ύποπτες κινήσεις και θορύβους κατά την διάρκεια της νύχτας, να πραγματοποιήσουν φωταψία σε ολόκληρη την οικία με το πάτημα ενός διακόπτη.
- Να ειδοποιηθούν από το σύστημα για πλημμύρα, πυρκαγιά, ακραία καιρικά φαινόμενα, βλάβες του ηλεκτρομηχανολογικού εξοπλισμού κ.α.
- Να έχουν οπτική αναπαράσταση της οικίας τους μέσω εγκατάστασης μίας ή περισσότερων καμερών οι οποίες θα μεταφέρουν την εικόνα του σπιτιού στον υπολογιστή ή στο κινητό του ιδιοκτήτη.

Όπως γίνεται αντιληπτό ένα έξυπνο σπίτι έχει ανεξάντλητες δυνατότητες σε θέματα ασφαλείας οι οποίες προσαρμόζονται στις εκάστοτε ανάγκες των ανθρώπων.

Ένα έξυπνο σπίτι προσφέρει εξατομικευμένες συνθήκες άνεσης με το πλήθος λειτουργιών που διαθέτει. Μέσα από το σύστημα εγκατάστασης δίνεται η δυνατότητα να ενεργοποιηθούν ή να απενεργοποιηθούν πολλές λειτουργίες της οικίας με την χρήση ενός smartphone όπως να τίθεται σε λειτουργία ο θερμοσίφωνας πριν φτάσει κάποιος στο σπίτι, να ανάβουν τα εξωτερικά φώτα του σπιτιού όταν βρίσκεται κοντά, να ρυθμίζει την θέρμανση, να κλείνει την παροχή ρεύματος σε κάποια συσκευή που έμεινε ανοιχτή κ.α. Με αυτόν τον τρόπο αποκτάται ο απόλυτος έλεγχος της οικίας ρυθμίζοντας πολλές από τις λειτουργίες του σπιτιού με τη χρήση ενός σύγχρονου κινητού τηλεφώνου.

Επιπρόσθετα [15], για μεγαλύτερη άνεση και ευκολία μπορούν να προγραμματιστούν πιθανά σενάρια τα οποία εφαρμόζονται με το πάτημα ενός πλήκτρου στο κινητό ή με την λειτουργία έναν διακόπτη. Ενδεικτικά κάποια από τα σενάρια μπορεί να είναι:

- **Λειτουργία Φεύγω:** Όταν φεύγουν οι κάτοικοι από το σπίτι να απενεργοποιούνται οι ηλεκτρολογικές συσκευές, η θέρμανση, η ύδρευση, το φυσικό αέριο , να υπάρχει ενημέρωση αν όλες οι πόρτες και τα παράθυρα είναι κλειδωμένα, να ενεργοποιείται ο συναγερμός κ.α.
- **Λειτουργία Διακοπές:** Όταν απουσιάζουν οι ιδιοκτήτες για διακοπές να ενεργοποιούνται ή να απενεργοποιούνται σε τυχαίες και λογικές ώρες ηλεκτρικές συσκευές και φώτα προκαλώντας την αίσθηση σε πιθανούς διαρρήκτες ότι το σπίτι κατοικείται, να ενημερώνεται ο ιδιοκτήτης για πιθανούς κίνδυνους και καταστροφές εποπτεύοντας με κάμερες τον εσωτερικό χώρο.
- **Λειτουργία Έρχομαι:** Η επιστροφή στο σπίτι να συνεπάγεται κατόπιν επιθυμίας του χρήστη την ενεργοποίηση ηλεκτρικών συσκευών όπως θέρμανσης, κλιματιστικού, θερμοσίφωνα κ.α. Συνεπώς ο κατάλληλος προγραμματισμός του συστήματος με βάση τις καθημερινές ανάγκες βελτιστοποιεί την ποιότητα της ζωής των κατοίκων.

Εικόνα 13. Υπόδειγμα έξυπνου σπιτιού

Πηγή: http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/syst_elegxou_asfaleias_2018_final/__8.html

Στα έξυπνα σπίτια μέσω της ορθολογικής χρήσης των ηλεκτρομηχανολογικών εγκαταστάσεων επιτυγχάνεται μεγάλο όφελος ως προς την εξοικονόμηση ενέργειας και της γενικότερης οικονομικής χρήσης. Πιο ειδικά:

- Η κατάλληλη χρήση των διαθέσιμων αυτοματισμών για την θέρμανση μπορεί να εξασφαλίσει σημαντική μείωση στην κατανάλωση ενέργειας. Με αυτόν τον τρόπο η άσκοπη σπατάλη ενέργειας, όταν ο κάτοικος για παράδειγμα απουσιάζει από την οικία του ή τα παράθυρα είναι ανοιχτά, μειώνεται σταδιακά.
- Ελαχιστοποιείται το κόστος λειτουργίας της ηλεκτρομηχανολογικής εγκατάστασης απενεργοποιώντας ηλεκτρικές συσκευές και φωτά που δεν χρησιμοποιούνται από τους κατοίκους.
- Αυξάνεται ο χρόνος ζωής των μηχανημάτων και ταυτόχρονα μειώνονται τα έξοδα συντήρησης τους. Η συνολική εξοικονόμηση ενέργειας για τους ιδιοκτήτες των έξυπνων σπιτιών εκτιμάται ότι ανέρχεται στο 35% κατά μέσο όρο. Επίσης, ένα ενσωματωμένο σύστημα αυτοματισμού αυξάνει την αξία ενοικίασης και πώλησης της οικίας προσφέροντας άνετη διαβίωση και μεγαλύτερη εξοικονόμηση ενέργειας και εσόδων από ένα συμβατικό σπίτι.

Τέλος, το κόστος κατασκευής ενός έξυπνου σπιτιού διαφέρει από κατοικία σε κατοικία και εξαρτάται από πολλούς παράγοντες όπως αν είναι προϋπάρχον το οίκημα ή υπό κατασκευή, πόσες λειτουργίες και ποιες θέλουμε να διαχειριστούμε έξυπνα, ποιες είναι οι παρούσες και μελλοντικές απαιτήσεις του κτιρίου κ.α. Αν η κατοικία βρίσκεται στο στάδιο της μελέτης των ηλεκτρομηχανολογικών εγκαταστάσεων, τότε προτείνεται να υπάρξει μια ενημέρωση από τον υπεύθυνο μηχανικό για τα συστήματα του Έξυπνου Σπιτιού (Smart Home) και πως θα μπορούσαν να ενσωματωθούν ανάλογα στην μελέτη. Όσον αφορά τις υφιστάμενες κατοικίες, η ορθή λύση προκύπτει κατόπιν σοβαρής μελέτης, η οποία θα τεκμηριώνει τις προτεινόμενες αλλαγές σε καλωδίωση και εγκαταστάσεις. Η σωστή αξιολόγηση των οφελών και του χρόνου απόσβεσης του έργου αποτελούν κομβικό σημείο για την τελική απόφαση.

3.2 Δομικές Τεχνολογίες έξυπνων σπιτιών

Παρακάτω θα αναφερθούμε σε κάποιες από τις πιο βασικές και διαδεδομένες δομικές τεχνολογίες που βασίζονται οι λειτουργίες των έξυπνων σπιτιών. Οι τεχνολογίες αυτές είναι εντελώς απαραίτητες για την εφαρμογή όλων των συστημάτων IoT διότι μέσω αυτών εξασφαλίζεται η επικοινωνία και η διασυνδεσιμότητα μεταξύ των συσκευών οικιακής χρήσης και των συστημάτων διαχείρισης και ελέγχου.

3.2.1 Διεθνές πρότυπο X10

Το διεθνές πρότυπο X10 είναι ένα βιομηχανικό και ανοικτό πρότυπο για την ανταλλαγή δεδομένων κυρίως μεταξύ ηλεκτρονικών οικιακών συσκευών, είναι διαδεδομένο και ως domotics. Χρησιμοποιεί κατά βάση το δίκτυο ρεύματος 220V ως δίκτυο σηματοδότησης και ελέγχου. Κάθε bit σήματος X10 είναι μια ριπή (burst) συχνότητας 120KHz και διάρκειας 1ms και μεταδίδεται όταν η ημιτονοειδής τάση 220V περνάει από τη στάθμη των 0V (zero-crossing).

Αυτό το πρότυπο επικοινωνίας δημιουργήθηκε το 1975 από την Pico Electronics στη Σκωτία με σκοπό να επιτευχθεί ο χειρισμός από απόσταση των τοπικών συσκευών και του ηλεκτρονικού και ηλεκτρολογικού εξοπλισμού. Ήταν το πρώτο τεχνολογικό δίκτυο γενικού σκοπού και παραμένει το περισσότερο διαδεδομένο. Αν και υπάρχουν πολλές σύγχρονες εναλλακτικές λύσεις, συμπεριλαμβανομένου των KNX, INSTEON, BACnet και LonWorks, το X10 παραμένει το πιο δημοφιλές στα οικιακά συστήματα αντίστοιχων εφαρμογών, με αρκετά μεγάλη προτίμηση από τους ενδιαφερόμενους σε παγκόσμια κλίμακα.

3.2.2 Διεθνές πρότυπο KNX (εφαρμογή Έξυπνο Σπίτι)

Το επίσης διεθνές πρότυπο KNX είναι μία καινοτόμα τεχνολογία αμφίδρομης επικοινωνίας και διαχείρισης λειτουργιών στις οικιακές συσκευές. Μια ενιαία σύνδεση ανάμεσα σε όλες τις συσκευές μιας οικιακής εγκατάστασης επιτρέπει την επεξεργασία και ανταλλαγή δεδομένων. Η πρακτική εφαρμογή αυτού του συστήματος ελέγχου και επικοινωνίας, για να εξυπηρετήσει τις ανάγκες των ανθρώπων που το επέλεξαν απαιτεί την χρήση ηλεκτρονικού υπολογιστή και αντίστοιχου λογισμικού τα οποία προσαρμόζονται ανάλογα με την περίπτωση.

Εικόνα 14. Τα επιμέρους συστήματα του προτύπου KNX

Πηγή: http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/syst_elegxou_asfaleias_2018_final/__8.html

Οι αντίστοιχες συσκευές αυτού του συστήματος, αντικαθιστούν τις συμβατικές συσκευές διαχείρισης της ηλεκτρολογικής εγκατάστασης, για παράδειγμα τους διακόπτες ή τα ρελέ και δημιουργούν νέες δυνατότητες και λειτουργίες ως προς την χρήση του χώρου και των εγκαταστάσεων. Το πρότυπο KNX ουσιαστικά είναι ένα δίκτυο απομακρυσμένου ελέγχου ανοιχτής αρχιτεκτονικής με πολλά οφέλη, τα σημαντικότερα αυτών είναι:

- ότι είναι σύμφωνο με τον Ευρωπαϊκό κανονισμό EN50090
- ότι χρησιμοποιεί τον καλύτερο τεχνικό εξοπλισμό από τις πιο επιτυχημένες εταιρείες
- παρέχει μεγάλο εύρος επιλογών στις συσκευές ελέγχου με μεγάλες προοπτικές εξέλιξης για το μέλλον
- ότι παρέχει τη δυνατότητα αντικατάστασης μιας συσκευής η οποία έχει ξεπεραστεί με μια αντίστοιχα αναβαθμισμένη
- ότι μπορούν να διαχειριστούν το σύστημα πολλοί χρήστες λόγω του ότι υπάρχει δυνατότητα εκπαίδευσης από την EIBA
- και τελευταίο και ιδιαίτερα σημαντικό ότι η τεχνική αυτού του προτύπου λειτουργεί και εξελίσσεται για περισσότερα από δέκα χρόνια και αποτελεί μια ασφαλή και δοκιμασμένη επιλογή.

3.2.3 Σύστημα KNX / EIB – instabus

Κάνοντας μια σύντομη ιστορική αναδρομή [19], η δημιουργία του EIB instabus έγινε στα τέλη της δεκαετίας του ’80, τότε κάποιες από τις πιο πετυχημένες εταιρείες στον τομέα της εφαρμοσμένης ηλεκτρικής τεχνικής δημιούργησαν μια ομάδα που ανέπτυξε το instabus. Η ιδέα ήταν απλή και είχε ως σκοπό ένα εύκολα διαχειρίσιμο ηλεκτρικό σύστημα ελέγχου οικιακών εφαρμογών σε ένα κτίριο από διάφορες απομακρυσμένες θέσεις. Μέσα από όλη αυτή τη προσπάθεια προέκυψε η δημιουργία της EIBA (European Installation Bus Association). Έπειτα από τη δημιουργία της EIBA όλα τα προϊόντα που παράγονταν βασισμένα πάνω στην τεχνική EIB θα έπρεπε να πληρούν κάποια πρότυπα και προϋποθέσεις, ώστε έπειτα από τη διενέργεια ελέγχου να αποδίδεται στο κάθε προϊόν αντίστοιχη πιστοποίηση από την EIBA.

Τα οφέλη που προκύπτουν από τη δημιουργία του συστήματος EIB - instabus τόσο ως προς την πρακτική εφαρμογή του, όσο και κατά τη σύγκρισή του με τα αντίστοιχα συμβατικά συστήματα διαχείρισης ηλεκτρικής ενέργειας είναι:

- Η προσαρμοστικότητά του με σχετικά χαμηλού κόστους εφαρμογές σε ηλεκτρικές εγκαταστάσεις κτιρίων διάφορων μεγεθών αλλά καλύπτοντας παράλληλα μεγάλες απαιτήσεις
- Η οικονομική διαχείριση της ενέργειας
- Η χρονικά σύντομη και εύκολη ηλεκτρολογική εγκατάστασή του
- Η μείωση της πιθανότητας να γίνει κάποιο βραχυκύκλωμα στο σύστημα, λόγω της μείωσης του πλήθους των καλωδίων που χρειάζονται για την εφαρμογή του
- Η δυνατότητα εύκολης επέκτασης της εφαρμογής του, και η σχετικά οικονομική αναβάθμιση και συντήρησή του

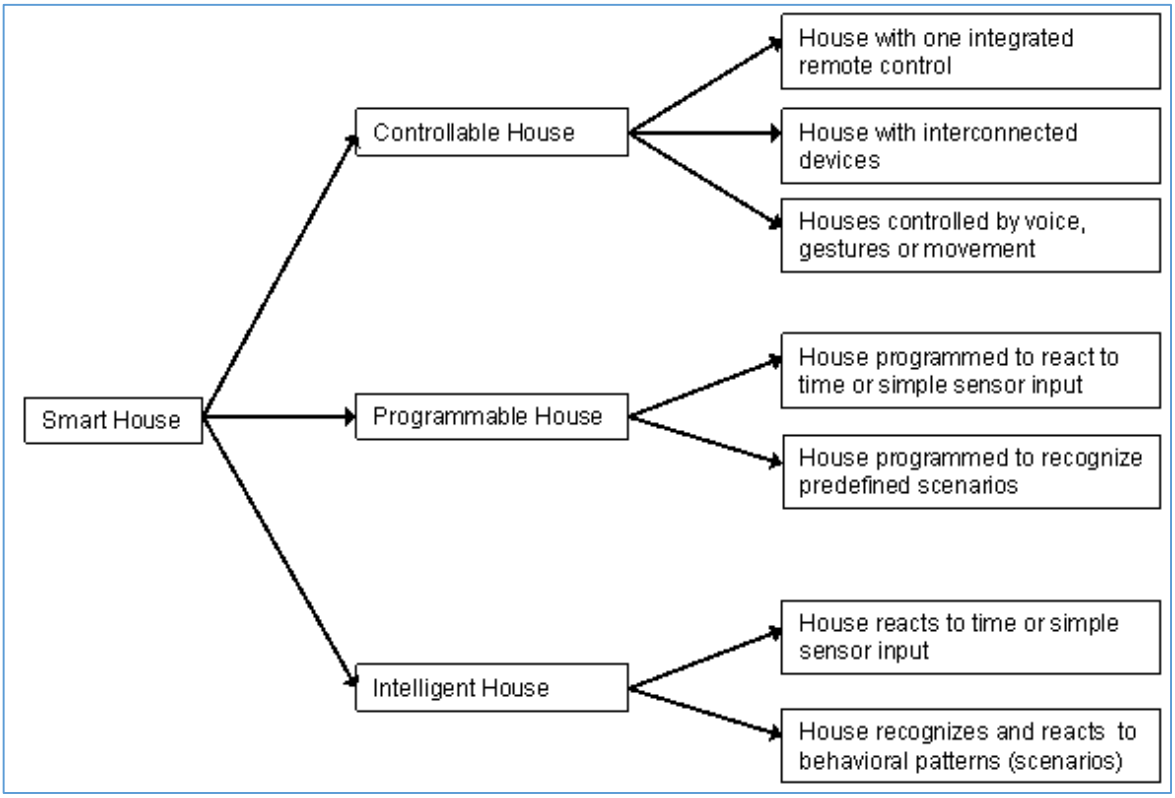
- Η εύκολη χρήση του ενιαίου Software που διαθέτει
- Η δυνατότητα που έχει να επικοινωνεί με άλλα ηλεκτρικά συστήματα ακόμη και παλαιότερης τεχνολογίας
- Η δυνατότητα ελέγχου του συστήματος μέσω τηλεφωνικού δικτύου
- Η συνεχής τεχνική υποστήριξη που παρέχεται

Όσον αφορά τον τρόπο λειτουργίας του EIB-instabus, οι συσκευές χειρισμού ή αισθητήρες (sensors) στέλνουν εντολές στη μονάδα BCU (Bus Coupling Unit) μέσω 10 τυποποιημένων υποδοχών για την αμφίδρομη μετάδοση σημάτων μεταξύ των δύο αυτών μερών και την ταυτόχρονη ηλεκτροδότηση της συσκευής χειρισμού. Οι μονάδες BCU συμμετέχουν στην αποστολή και στη λήψη δεδομένων έτσι ώστε να διασφαλίζουν τη σωστή τροφοδοσία των ηλεκτρονικών τμημάτων του συστήματος, να αποθηκεύουν στη μνήμη τους σημαντικές πληροφορίες και να συνδέονται μεταξύ τους με το καλώδιο επικοινωνίας. Παραδείγματα τέτοιων συστημάτων είναι οι θερμοστάτες, οι ανιχνευτές κίνησης, οι χρονοδιακόπτες κ.α.Τα βασικά δομικά στοιχεία του συστήματος είναι εξαρτήματα του EIB instabus μέσω των οποίων εξασφαλίζεται η απαραίτητη τιμή τάσης, η μεταφορά των δεδομένων, η σωστή και άμεση επικοινωνία μεταξύ των διαφόρων συσκευών στη γραμμή bus και γενικά η σωστή και ασφαλή λειτουργία του συστήματος.

Καταλήγοντας έπειτα από την περιγραφή των παραπάνω δομικών συστημάτων τεχνολογίας για την πρακτική εφαρμογή ενός έξυπνου σπιτιού, θα πρέπει να τονίσουμε ότι στην αγορά προσφέρονται πολλές ολοκληρωμένες εφαρμογές αυτού του είδους. Εναπόκειται στην επιλογή του πελάτη ανάλογα με τις ανάγκες που θέλει να καλύψει και την οικονομική δυνατότητα που έχει για το τι θα επιλέξει τελικά για την αυτοματοποίηση του σπιτιού του. Από την άλλη πλευρά ένα σύγχρονο σπίτι πρωτίστως για λόγους ασφάλειας θα πρέπει να διαθέτει συστήματα όπως για παράδειγμα πυρασφάλειας, συναγερμού κ.α. Οπότε είναι εξ αρχής περισσότερο συμφέρουσα η επιλογή εγκατάστασης ενός ολοκληρωμένου δικτύου, παρά τμηματικά να προσθέτουμε επιμέρους συστήματα κατά το πέρασμα του χρόνου.

3.3 Κατηγορίες Έξυπνων σπιτιών

Στη συνέχεια θα δούμε και θα αναλύσουμε την κατηγοριοποίηση των έξυπνων σπιτιών σε τρείς βασικές κατηγορίες σύμφωνα με το τεχνικό πανεπιστήμιο της Δανίας [23] οι κατηγορίες αυτές είναι τα ελεγχόμενα σπίτια (controllable house), τα προγραμματιζόμενα σπίτια (programmable house) και τα ευφυή σπίτια (intelligent house) όπως αποτυπώνονται στο παρακάτω διάγραμμα.



Εικόνα 15. Διαγραμματική απεικόνιση των κατηγοριών του Έξυπνου Σπιτιού

Πηγή: http://www.imm.dtu.dk/~cdje/SmartHouseWebSite/taxonomy.html#taxonomy

3.3.1 Τα Ελεγχόμενα Σπίτια (Controllable House)

Τα ελεγχόμενα σπίτια είναι η πρώτη κατηγορία, σε αυτήν την κατηγορία ο τύπος του έξυπνου σπιτιού ασχολείται με τη βελτίωση του τρόπου με τον οποίο ελέγχεται ο ποικίλος οικιακός εξοπλισμός του σπιτιού. Ειδικότερα είναι ένα σπίτι στο οποίο οι κάτοικοι μπορούν να ελέγχουν αρκετές συσκευές με προηγμένους και ιδιαίτερα αποτελεσματικούς τρόπους σε σύγκριση με τα συμβατικά σύγχρονα σπίτια. Παρακάτω θα δούμε τρείς τέτοιος τύπους σπιτιών.

- **Σπίτι με ενσωματωμένο τηλεχειριστήριο.** Σε αυτήν την περίπτωση σπιτιού ένα πλήθος υποσυστημάτων και συσκευών μπορεί να ελεγχθεί από ένα τηλεχειριστήριο ή έναν πίνακα ελέγχου. Δεν υπάρχουν ιδιαίτερες τεχνικές δυσκολίες στην πρακτική εφαρμογή αυτού του συστήματος. Το βασικό που πρέπει να υπάρχει είναι η ασύρματη ή ενσύρματη επικοινωνία μεταξύ των συσκευών και της μονάδας ελέγχου. Ένα παράδειγμα αυτής της τεχνολογίας είναι ένα ενσωματωμένο τηλεχειριστήριο για το βίντεο και την τηλεόραση ή ένα κύριο χειριστήριο Bang & Olufsen.
- **Σπίτι με διασυνδεδεμένες συσκευές.** Εδώ οι συσκευές συνδέονται μεταξύ τους, τέτοιες συσκευές είναι οι τηλεοράσεις, VCR, ραδιόφωνα, υπολογιστές

και πρόσθετα ηχεία, οθόνες, μικρόφωνα ή κάμερες κ.α. Αυτός ο τύπος συστήματος επιτρέπει την ανταλλαγή δεδομένων μεταξύ των συσκευών και κάνει πιο προσιτή την ψυχαγωγία και διευκολύνει την επικοινωνία μεταξύ ατόμων σε διαφορετικά δωμάτια του σπιτιού.

- **Σπίτι που ελέγχεται με κίνηση, φωνή ή χειρονομία.** Το σπίτι αυτό ουσιαστικά είναι παρόμοιο με το σπίτι της πρώτης περίπτωσης, η μόνη διαφορά είναι ότι εδώ μία ορατή μονάδα ελέγχου αντικαθίσταται με μία αόρατη που ελέγχεται με τη φωνή, τις χειρονομίες ή τις κινήσεις. Ο εξοπλισμός που απαιτείται είναι το εύκολο κομμάτι αυτής της περίπτωσης, το λογισμικό όμως είναι μια δύσκολη υπόθεση διότι οι δυνατότητες αναγνώρισης φωνής οι χειρονομιών πρέπει να είναι αξιόπιστες. Οι τεχνολογίες που χρησιμοποιούνται σε αυτήν την περίπτωση είναι παρόμοιες με αυτές της λειτουργίας της φωνητικής κλήσης των σύγχρονων τηλεφώνων.

3.3.2 Τα Προγραμματιζόμενα Σπίτια (Programmable House)

Τα προγραμματιζόμενα σπίτια, είναι η δεύτερη ευρύτερη κατηγορία των έξυπνων σπιτιών. Εδώ η υποδομή μας επιτρέπει να προγραμματίζουμε το σπίτι έτσι ώστε να ενεργοποιεί , να διακόπτει ή να προσαρμόζει ορισμένες συσκευές σε συγκεκριμένες συνθήκες. Σε αυτή την περίπτωση έχουμε δύο υποκατηγορίες:

- Η πρώτη υποκατηγορία είναι προγραμματιζόμενα σπίτια που αντιδρούν στο χρόνο με την απλή εγκατάσταση αισθητήρα. Έτσι ο χρόνος επιτρέπει σε κάποιες συσκευές να ενεργοποιούνται ή να απενεργοποιούνται σε μία συγκεκριμένη στιγμή, επίσης ακόμη ένα απλό παράδειγμα χρήσης αισθητήρα είναι ένας θερμοστάτης όπου ενεργοποιείται ή απενεργοποιείται όταν η θερμοκρασία στο σπίτι φτάσει σε ένα συγκεκριμένο επίπεδο. Ή ένας αισθητήρας που ανάβει τα φώτα αυτόματα όταν νυχτώσει και χαμηλώσει το φώς.
- Η δεύτερη υποκατηγορία είναι τα προγραμματιζόμενα σπίτια που αξιολογούν και αναγνωρίζουν καταστάσεις. Αυτά τα σπίτια έχουν τη δυνατότητα να διαχειρίζονται δεδομένα και πληροφορίες συνολικά και ταυτόχρονα από πολλούς και διαφορετικούς αισθητήρες. Αυτό επιτυγχάνεται με τη χρήση αξιόπιστου λογισμικού το οποίο έχει προγραμματιστεί με βάση κάποια σενάρια τα οποία αποθηκεύονται στη μονάδα επεξεργασίας και είναι παρόμοια με τα πραγματικά γεγονότα που συμβαίνουν εντός του σπιτιού. Σε αυτήν τη περίπτωση υπάρχει ανάγκη για συνεχή ενημέρωση και προσαρμογή του λογισμικού ανάλογα με τις αλλαγές που συμβαίνουν κατά τις μεταβολές του περιβάλλοντος. Παράδειγμα ενός τέτοιου σεναρίου είναι κατά την επιστροφή του κατοίκου στο σπίτι, όταν αυτός ξαπλώνει στον καναπέ κατά τις

νυχτερινές ώρες, αν παραμείνει ακίνητος για προκαθορισμένο χρονικό διάστημα να χαμηλώνει ο φωτισμός και να παίζει για λίγο χρονικό διάστημα χαλαρωτική μουσική.

3.3.3 Τα Ευφυή Σπίτια (Intelligent House)

Τα ευφυή σπίτια, είναι η τελευταία κατηγορία των Έξυπνων Σπιτιών. Αυτή η κατηγορία σπιτιών είναι αρκετά όμοια με την προηγούμενη, ωστόσο η βασική της διαφορά είναι ότι δεν χρειάζεται να προγραμματίζονται οι λειτουργίες και τα σενάρια που αναφέραμε προηγουμένως, διότι το σπίτι έχει τη δυνατότητα να το κάνει μόνο του. Η "νοημοσύνη του σπιτιού" παρατηρεί το περιβάλλον και τους κατοίκους του στην καθημερινότητα τους και αντιλαμβάνεται τις επαναλαμβανόμενες κινήσεις και ενέργειές τους. Όταν εντοπιστούν επαναλαμβανόμενες κινήσεις το σπίτι θα προγραμματιστεί αυτόματα έτσι ώστε την επόμενη φορά που θα εντοπιστεί το ίδιο σενάριο το σπίτι θα ενεργοποιεί και θα απενεργοποιεί ανάλογα τις συγκεκριμένες συσκευές που θα χρειάζονται.

Υπάρχουν πολλά Έξυπνα Σπίτια που σχεδιάζονται από ερευνητικές ομάδες σε Πανεπιστήμια και βιομηχανίες. Τα έργα αυτά επικεντρώνονται σε διάφορα στοιχεία, όπως τις κατευθυντήριες γραμμές και τις απαιτήσεις σχεδιασμού έως τις πραγματικές υλοποιήσεις ενός ευφυούς σπιτιού. Οι έρευνες εξετάζουν τεχνολογικά προβλήματα υλικών και θέματα ασφάλειας, ιδιωτικότητας ή κοινωνικά που σχετίζονται με τα Έξυπνα Σπίτια. Στη συνέχεια υπάρχει μια λίστα με τα πιο ενδιαφέροντα και σημαντικά έργα μαζί με σύντομη περιγραφή τους.

- Η Phillips πραγματοποιεί μια σειρά από έρευνες στις τεχνολογίες του σπιτιού (Όλα τα έργα είναι διαθέσιμα στον ιστότοπο έρευνας ευφυΐας περιβάλλοντος Phillips). Ένα από τα έργα που πραγματοποίησε ονομάζεται **World Wide Information, Communication and Entertainment (WWICE)**. Το έργο εστιάζει στην επικοινωνία μέσα στο σπίτι. Το βασικό στοιχείο είναι μια φορητή οθόνη που μπορεί εύκολα να συνδεθεί με όλες τις συσκευές που υπάρχουν και χρησιμεύει τόσο για σκοπούς ελέγχου όσο και για ανταλλαγή πολυμέσων. Οποιοδήποτε μέσο εμφανίζεται ή αναπαράγεται σε οποιαδήποτε οθόνη ή ηχείο ενός δωματίου μπορεί να μεταφερθεί στη φορητή οθόνη και αντίστροφα. Επίσης, ορισμένες συσκευές μέσα στο σπίτι συνδέονται μεταξύ τους, γεγονός που επιτρέπει στους κατοίκους να χρησιμοποιούν τους πόρους που παρέχονται από οποιοδήποτε εξοπλισμό σε οποιοδήποτε δωμάτιο ενός σπιτιού. Πρόσθετη λειτουργικότητα είναι η έννοια της σύνδεσης μεταξύ διαφορετικών σπιτιών. Έτσι, οι φίλοι μπορούν να παρακολουθήσουν την ίδια ταινία ή να ακούσουν την ίδια μουσική ενώ κάνουν συνομιλία μέσω βίντεο. Όλες οι ενέργειες ελέγχονται από τον χρήστη, μέσω της φορητής οθόνης.

- Ένα άλλο έργο που πραγματοποιήθηκε από την Phillips ονομάζεται **PHENOM**. Η υποδομή του βασίζεται στη σύνδεση μεταξύ διαφορετικών συσκευών σε ένα σπίτι. Για παράδειγμα, ένα άλμπουμ φωτογραφιών θα μπορούσε να εμφανίζεται σε οποιοδήποτε μέρος του σπιτιού. Επίσης, υπάρχει μια φορητή συσκευή οθόνης αφής που μπορεί να χρησιμοποιηθεί για τη διαχείριση της εμφάνισης διαφορετικών πόρων. Και τα δύο έργα που αναφέρονται παραπάνω δοκιμάζονται σε ένα μέρος που ονομάζεται HomeLab. Είναι ένα εργαστήριο, όπου η Phillips δοκιμάζει τα έργα της. Υπάρχουν μερικοί εθελοντές που ζουν σε ένα σπίτι για μια δεδομένη περίοδο και οι ερευνητές μπορούν να παρατηρήσουν τις αλληλεπιδράσεις τους με το σύστημα. Αυτό καθιστά τα έργα ανθρωποκεντρικά και επιτρέπει την απάντηση στο πιο σημαντικό ερώτημα των αυτοματοποιημένων σπιτιών (θα επωφεληθούν πραγματικά οι άνθρωποι από την τεχνολογία και ποια θα ήταν η επίδραση του αυτοματισμού σπιτιού στους ανθρώπους). Αν και το πρωτότυπο PHENOM φαίνεται να περιορίζεται στην εμφάνιση φωτογραφιών, η υποκείμενη υποδομή έχει σχεδιαστεί για να μαθαίνει αυτόματα τις προτιμήσεις των χρηστών, επομένως αυτό είναι ένα παράδειγμα ενός έξυπνου έργου.
- Το **Προσαρμοστικό Σπίτι**, σχετίζεται γενικά με την τεχνολογία ευφυούς σπιτιού. Το έργο πραγματοποιείται από τον Michael C. Mozer στο Πανεπιστήμιο του Κολοράντο στο Boulder. Στο όραμα που ορίζεται από το έργο τονίζεται ότι το σπίτι είναι έξυπνο και ότι έχει πολλά πλεονεκτήματα σε σχέση με ένα προγραμματιζόμενο σπίτι. Οι λειτουργίες του έργου εστιάζονται στην πιο βασική και κερδοφόρα ανάγκη για ευφυή μέσα στα σπίτια, που είναι η εξοικονόμηση ενέργειας. Το υλοποιημένο σπίτι ελέγχει πλήρως τη θέρμανση, τον εξαερισμό, τον κλιματισμό, το ζεστό νερό και τα εσωτερικά φώτα. Ο στόχος του σπιτιού είναι να μειώσει τη χρήση όλων αυτών των πόρων, αλλά ταυτόχρονα να εξασφαλίσει την άνεση των κατοίκων. Όλες οι αποφάσεις λαμβάνονται από το σύστημα ελέγχου του σπιτιού, το οποίο υλοποιείται με τη χρήση νευρωνικών δικτύων. Οι αποφάσεις λαμβάνονται φυσικά με τον σωστό τρόπο. Έτσι οι κινήσεις των κατοίκων του σπιτιού παρατηρούνται και εντοπίζονται διαφορετικά σενάρια. Η αναγνώριση αυτών των σεναρίων επιτρέπει στο σπίτι να ελέγχει τη θέρμανση ή τον αερισμό. Ως αποτέλεσμα, το σπίτι αρχίζει να ελέγχει τις παραμέτρους του σπιτιού σύμφωνα με τις προτιμήσεις των κατοίκων. Επί του παρόντος, το έργο διερευνά πιθανές επεκτάσεις των δυνατοτήτων του σπιτιού. Ένα από αυτά είναι η πρόβλεψη για το πότε θα επιστρέψουν οι κάτοικοι στα σπίτια τους για να ενεργοποιήσουν τη θέρμανση την κατάλληλη στιγμή. Και τέλος τα φώτα στο σπίτι προορίζονται να ελέγχονται με τέτοιο τρόπο, ώστε να ρυθμίζονται τα σωστά μοτίβα φωτός και τα φώτα να μπορούν να ανάβουν και να σβήνουν αυτόματα, όταν ένας κάτοικος πηγαίνει από το ένα δωμάτιο στο άλλο.

- **Microsoft House**. Το σπίτι του μέλλοντος κατασκευασμένο από τη Microsoft είναι ένα διαμέρισμα με επιφάνεια περίπου 750 τετραγωνικά μέτρα, το οποίο έχει δημιουργηθεί σε ένα από τα κτίρια στην πανεπιστημιούπολη της Microsoft στην Ουάσιγκτον. Είναι ένα μέρος γεμάτο ηλεκτρονικά συστήματα που οραματίζεται το πώς θα μπορούσαν να μοιάζουν οι χώροι διαβίωσης στο μέλλον. Το σπίτι παρουσιάζει πολλές προηγμένες τεχνολογικές λύσεις. Οι ηλεκτρονικές συσκευές είναι διασυνδεδεμένες μεταξύ τους. Το σπίτι δίνει τη δυνατότητα ελέγχου email στην οθόνη της τηλεόρασης. Ένας προβολέας στην κουζίνα επιτρέπει την εμφάνιση διαφορετικών μέσων στον τοίχο και υπάρχει ένα μέρος με τεράστια οθόνη που αποτελεί κέντρο για την οικιακή ψυχαγωγία - μουσική, ταινίες ή βίντεο. Επίσης η οθόνη αφής έξω από την κύρια είσοδο του σπιτιού μπορεί να καταγράψει ένα μήνυμα που αργότερα θα μπορούσε να εμφανιστεί σε διάφορα σημεία μέσα στο σπίτι. Για λόγους ελέγχου υπάρχουν υπολογιστές τσέπης που είναι ενσωματωμένοι στους τοίχους σε διάφορα σημεία του σπιτιού. Είναι δυνατός ο έλεγχος των συσκευών πολυμέσων στο σπίτι και επιπλέον άλλου εξοπλισμού, όπως όλα τα φώτα. Το έργο επικεντρώνεται στην ενοποίηση των μέσων ενημέρωσης και ελέγχου, όπου ο κάτοικος είναι ο άμεσος ελεγκτής.

4. Θέματα Ασφαλείας Έξυπνων Κτιρίων/Σπιτιών

Τα έξυπνα κτίρια [24] παρέχουν βελτιωμένη ενεργειακή απόδοση και δημιουργούν ένα άνετο και ευέλικτο περιβάλλον μέσω της αυτοματοποίησης των συσκευών. Από την άλλη πλευρά όμως, είναι ιδιαίτερα ευάλωτα σε κακόβουλες επιθέσεις και στην παραβίαση των προσωπικών δεδομένων. Επιπρόσθετα, ένα μεγάλο ζήτημα είναι ότι το έξυπνο σπίτι βασίζεται στην ασύρματη επικοινωνία συσκευών, και αυξάνει σημαντικά την έκθεση των κατοίκων του αλλά και γενικά των γειτόνων τους σε ηλεκτρομαγνητικά πεδία υψηλών συχνοτήτων, τα οποία έχουν ενταχθεί στα πιθανά καρκινογόνα και συνδέονται με ένα πλήθος προβλημάτων υγείας.

Σε αυτό το κεφάλαιο θα αναλύσουμε θέματα ασφαλείας γύρω από την «έξυπνη τεχνολογία» γενικότερα και θα μελετήσουμε το πως επηρεάζει άμεσα τον άνθρωπο μέσω τις εκπομπής ακτινοβολίας, σε θέματα υγείας, σχετικά με το ιδιωτικό απόρρητο και τις διάφορες συνέπειες σε περιπτώσεις βλαβών. Επίσης θα αναφερθούμε σε περιπτώσεις επιθέσεων ευρείας κλίμακας και κακόβουλων λογισμικών.

4.1 Αρνητικές επιπτώσεις των έξυπνων κτιρίων

4.1.1 Τι είναι η ακτινοβολία

Οι ηλεκτρομαγνητικές ακτινοβολίες είναι ενεργειακά πεδία που δημιουργούνται από ηλεκτρικά φορτισμένα σωματίδια, υπάρχουν φυσικές ακτινοβολίες όπως η ηλιακή ακτινοβολία, το μαγνητικό πεδίο της γης κ.α. Υπάρχουν και τεχνικές ακτινοβολίες οι οποίες προέρχονται από τα καλώδια της ΔΕΗ, τις κεραίες, τα κινητά τηλέφωνα, τα ραντάρ και γενικότερα από πολλές ηλεκτρικές συσκευές. Οι ακτινοβολίες χωρίζονται στις δύο παρακάτω κατηγορίες ανάλογα με την συχνότητα μετάδοσης τους [29]:

- Τις μη ιοντίζουσες ακτινοβολίες χαμηλών και υψηλών συχνοτήτων τις οποίες συναντούμε σε συστήματα που εκπέμπονται σε συχνότητες που μεταφέρουν σχετικά μικρή ενέργεια, ανίκανη κατά την αλληλεπίδραση να προκαλέσει ιοντισμό των ατόμων, δηλαδή διάσπαση των χημικών δεσμών στα μόρια των κυττάρων και προκαλεί μόνο θερμικές επιδράσεις στους ιστούς και στα κύτταρα. Οι βλάβες στον οργανισμό προξενούνται από τη θέρμανση των ακτινοβολούμενων ιστών. Επιδράσεις χαμηλού επιπέδου (μη θερμικές), προκαλούνται από μικρές πυκνότητες ισχύος (της τάξης των λίγων μW/cm²), ώστε να μην παρατηρείται αύξηση της θερμοκρασίας των ιστών. Παραδείγματα πηγών τέτοιων συχνοτήτων είναι οι ηλεκτρικές-ηλεκτρονικές συσκευές, τα καλώδια του δικτύου της ΔΕΗ, τα κινητά τηλέφωνα και τις κεραίες κινητής τηλεφωνίας, το ασύρματο ίντερνετ (WI-FI), τα φορητά τηλέφωνα και τις βάσεις τους (DECT), τις συσκευές Bluetooth, τα διάφορα ραντάρ κ.α.

- Τις ιοντίζουσες ακτινοβολίες που μεταφέρουν ενέργεια ικανή να εισχωρήσει στην ύλη και να προκαλέσει ιοντισμό των ατόμων, να διασπάσει βίαια χημικούς δεσμούς και να προκαλέσει βιολογικές βλάβες στον ανθρώπινο οργανισμό. οι οποίες έχουν συχνότητα μεγαλύτερη από το ορατό φως. Οι πιο γνωστές ιοντίζουσες ακτινοβολίες είναι οι ακτίνες Χ που χρησιμοποιούνται ευρέως στην ιατρική επιστήμη, η υπεριώδη ακτινοβολία, το αέριο ραδόνιο, το ουράνιο, διάφορα ραδιενεργά υλικά που βρίσκονται σε πετρώματα κ.α.

Εικόνα 16. Ηλεκτρομαγνητικό Φάσμα

Πηγή: https://pedion24.gr/electromagnetic-radiation/

Πολλές από τις έξυπνες συσκευές εκπέμπουν ηλεκτρομαγνητικά πεδία υψηλών συχνοτήτων συνήθως στην συχνότητα των 2,4 GHz, τέτοιες συσκευές είναι οι συσκευές που συνδέονται και εκπέμπουν σήμα wifi (modem ή router) καθώς επίσης και συσκευές που λειτουργούν μέσω Bluetooth. Όλες αυτές οι συσκευές εκπέμπουν ακτινοβολία ακόμη και όταν είναι σε κατάσταση αναμονής, αυτό συμβαίνει για να μην χάσουν την σύνδεση με την κεντρική μονάδα. Έχει παρατηρηθεί ότι στα έξυπνα κτίρια υπάρχει αρκετά αυξημένη ακτινοβολία, αυτό συμβαίνει διότι οι έξυπνες συσκευές πρακτικά λειτουργούν ως κεραίες που λειτουργούν όλο το εικοσιτετράωρο.

4.1.2 Εκπομπή ακτινοβολίας και επιπτώσεις στην υγεία

Σχετικά με το ζήτημα της ακτινοβολίας και τις επιπτώσεις στην υγεία του ανθρώπου[26], έχει ανακοινωθεί επίσημα από το 2011 ότι οι ασύρματη ακτινοβολία έχει συμπεριληφθεί από τον Παγκόσμιο Οργανισμό Υγείας στις πιθανές αιτίες πρόκλησης του καρκίνου. Στη συνέχεια [27] το 2017 ο τότε σύμβουλος του ΠΟΥ Δρ. Miller, εξειδικευμένος μελετητής στην επιδημιολογία του καρκίνου πρότεινε να ενταχθεί η

ασύρματη ακτινοβολία ανεξάρτητα από την πηγή που προέρχεται είτε είναι από τις συσκευές κινητής τηλεφωνίας, είτε είναι από τα router, είτε είναι ακόμη και από τις κεραίες κινητής τηλεφωνίας στις αποδεδειγμένες αιτίες που συμβάλλουν στην εμφάνιση του καρκίνου. Ωστόσο, παρά το γεγονός ότι έχουν γίνει έντονες συστάσεις γύρο από αυτό το θέμα, δύσκολα θα ενταχθεί η ασύρματη ακτινοβολία στα αποδεδειγμένα καρκινογόνα. Ίσως γιατί στην εποχή μας, η παγκόσμια οικονομία βασίζεται σε μεγάλο βαθμό στην χρήση της κινητής τηλεφωνίας και των ασύρματων δικτύων.

Επιπλέον, το Ευρωπαϊκό Κοινοβούλιο [28] ασχολήθηκε σχετικά με αυτό το ζήτημα και πρότεινε η Ευρωπαϊκή Ένωση να συμπεριλάβει στην πολιτική της για την ποιότητα του αέρα στο εσωτερικό των κτιρίων τη μελέτη σε ασύρματες οικιακές συσκευές όπως τα δίκτυα wifi και τις ασύρματες τηλεφωνικές συσκευές τύπου DECT, των οποίων η χρήση έχει αυξηθεί σημαντικά το τελευταίο διάστημα τόσο σε δημόσιους χώρους, όσο και σε ιδιωτική χρήση. Ψήφισμα Ευρωπαϊκού Κοινοβουλίου σχετικά με τα προβλήματα υγείας που σχετίζονται με τα ηλεκτρομαγνητικά πεδία (2008/2211).

Ωστόσο, [30] υπάρχει διαφωνία μεταξύ των επιστημόνων σχετικά με τα επίπεδα μη ιοντίζουσων ακτινοβολιών που έχουν επιπτώσεις στην υγεία του ανθρώπου. Τα έως σήμερα όρια ασφαλείας που έχουν θεσπιστεί, λαμβάνουν υπόψη μόνο τις θερμικές επιδράσεις από υψηλής έντασης ακτινοβολίες. Συνήθως, η έκθεση των ανθρώπων δεν είναι πολύ συχνή σε τέτοιες ακτινοβολίες οι οποίες πηγάζουν από ισχυρές πηγές ακτινοβολίας και προϋποθέτουν την κοντινή απόσταση για να προκαλέσουν σοβαρές βλάβες στην υγεία, όπως για παράδειγμα είναι οι ραδιοτηλεοπτικές κεραίες. Από την άλλη πλευρά, όλο και περισσότεροι επιστήμονες υποστηρίζουν ότι σύμφωνα με τα νεότερα δεδομένα εντοπίζονται βλάβες στην υγεία και από χαμηλότερες πηγές ακτινοβολίας με μη θερμικά επίπεδα έκθεσης.

4.2 Προκλήσεις που δημιουργούνται από την ραγδαία εξέλιξη του IoT

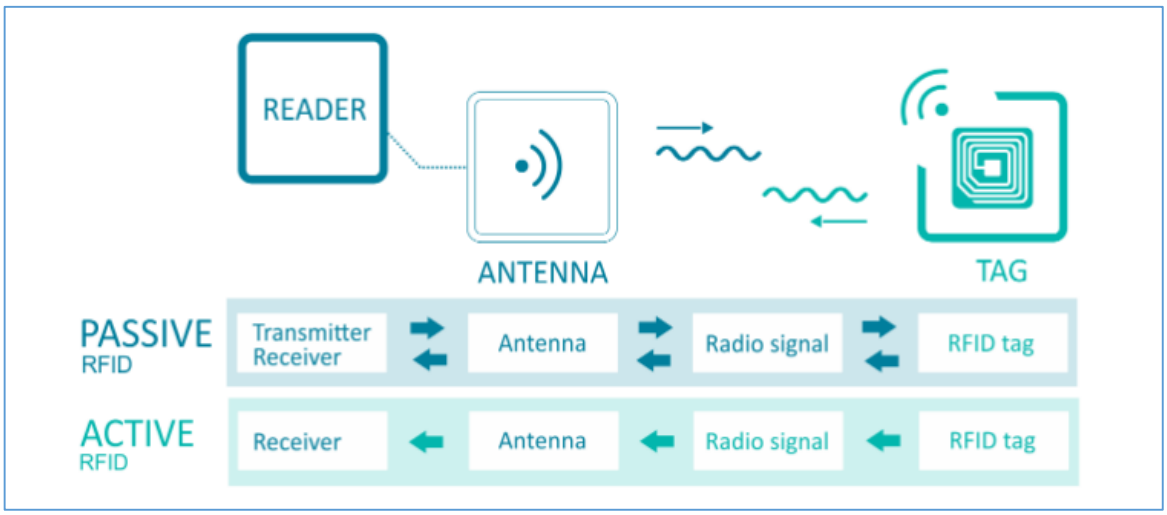
Είναι γεγονός πως ο αριθμός των συσκευών IoT που χρησιμοποιούνται καθημερινά αυξάνεται ραγδαία σε πολύ σύντομο χρονικό διάστημα και αυτό από την άλλη πλευρά το κάνει πολύ ευάλωτο σε επιθέσεις και υποκλοπές προσωπικών δεδομένων, διότι δεν είναι δυνατόν να αναπτυχθούν σε τόσο σύντομο χρονικό διάστημα τα αντίστοιχα μέτρα ασφάλειας και προφύλαξης που απαιτούνται από την αρχή της χρήσης του. Οι καταναλωτές και ο κόσμος των επιχειρήσεων ανησυχεί όλο και περισσότερο για τα θέματα ασφάλειας στο χώρο του διαδικτύου των πραγμάτων. Ωστόσο, οι προσπάθειες που καταβάλλονται στο να αποτρέπονται κάθε είδους απειλές από τους διάφορους επιτηδείους του διαδικτύου είναι σε πολύ καλό επίπεδο και τα μέτρα που λαμβάνονται στις περισσότερες περιπτώσεις είναι αρκετά ικανοποιητικά ώστε να μην δημιουργούνται προβλήματα στη χρήση των συνδεδεμένων συσκευών.

Μια από τις βασικότερες προκλήσεις που δημιουργείται από τη χρήση του IoT και υπάρχει άμεση ανάγκη εύρεσης λύσης, είναι το θέμα της ασφάλειας. Εξαιτίας της

συνεχής και πολλαπλής συνδεσιμότητας μεταξύ των έξυπνων συσκευών που συνδέονται είτε μεταξύ τους είτε και με διάφορα άλλα συστήματα ελέγχου και διαχείρισης, υπάρχει μεγάλη επικινδυνότητα να συμβούν φαινόμενα παραβίασης και υποκλοπής των δεδομένων που μεταφέρονται.

4.2.1 Επιθέσεις σε συστήματα RFID

Τα συστήματα RFID [31] χρησιμοποιούνται ευρέως τις τελευταίες δεκαετίες σε πληθώρα συσκευών μεταφέροντας πληροφορίες μεταξύ μιας ετικέτας και μιας συσκευής ανάγνωσης. Ωστόσο, όπως και σε άλλες τεχνολογίες έτσι και εδώ οι hackers έχουν εκμεταλλευθεί κενά ασφαλείας. Οι βασικοί τύποι ετικετών RFID συνήθως δεν διαθέτουν κρυπτογράφηση ή ταυτοποίηση η οποία προστατεύει σε μεγάλο βαθμό από κακόβουλες επιθέσεις. Αυτό έχει σαν αποτέλεσμα να υπάρχει μεγάλος κίνδυνος να υποκλαπούν τα δεδομένα αν κάποια συσκευή τρίτου παρεμβληθεί μεταξύ της κάρτας RFID και της αντίστοιχης συσκευής ανάγνωσης. Οι συνηθέστερες επιθέσεις σε αυτά τα συστήματα είναι ο μη εντοπισμός (untraceability), ο αποσυγχρονισμός (de-synchronisation), η διαρροή πληροφοριών (information leakage) και οι επιθέσεις επανάληψης (replay attacks).



Εικόνα 17. Απεικόνιση συστήματος RFID

Πηγή: https://www.aucxis.com/en/rfid/rfid-technology

Στις επιθέσεις αποσυγχρονισμού οι ‘’εχθροί’’ εντοπίζουν τις ετικέτες και αποκαλύπτουν την τοποθεσία τους δημιουργώντας δυσλειτουργίες στη μετάδοση πληροφοριών του συστήματος. Στις επιθέσεις επανάληψης οι ‘’εχθροί’’ κάνουν κατάχρηση των πληροφοριών που έχουν διαρρεύσει προκαλώντας σημαντικά προβλήματα στον χρήστη ο οποίος δεν έχει άμεσα ενημέρωση και γνώση αυτής της κακόβουλης χρήσης.

Ακόμη μια πολύ επικίνδυνη επίθεση στις ετικέτες συμμετρικού κλειδιού, είναι η επίθεση του ενδιάμεσου (Man in the Middle) κατά την οποία ο επιτιθέμενος με κρυφή

δράση επεμβαίνει στο σύστημα ελέγχοντας όλη την μετάδοση των πληροφοριών. Αυτού του είδους οι επιθέσεις ακόμη δεν μπορούν να αντιμετωπιστούν διότι παρακάμπτουν κάθε είδους κρυπτογραφία.

Παράλληλα με την ανάπτυξη των κακόβουλων δράσεων διενεργούνται μεγάλες προσπάθειες δημιουργίας μέτρων προστασίας και αντιμετώπισής τους. Στις βασικές ετικέτες RFID το μεγαλύτερο πρόβλημα ασφάλειας είναι η ταυτοποίηση του χρήστη. Για την ανίχνευση των κλώνων που δημιουργούνται για την επίθεση, έχει δημιουργηθεί το ονομαζόμενο βασικό πρωτόκολλο επαλήθευσης ταυτότητας το οποίο περιλαμβάνει το χαρακτηριστικό της δοκιμής μιας ετικέτας που στέλνει ένα σύνολο τυχαίων κωδικών PIN σε μία τυχαία θέση. Εάν η απόκριση της ετικέτας είναι έγκυρη, η ετικέτα μπορεί να θεωρηθεί κλώνος. Το πρωτόκολλο ταυτοποίησης, το οποίο παρέχει μεγάλο ποσοστό προστασίας από τέτοιου είδους επιθέσεις, προϋποθέτει την χρήση μιας συσκευής ανάγνωσης ετικετών και είναι κατάλληλη για τις περισσότερες βασικές ετικέτες RFID.

Ακόμη ένα μέτρο για την αντιμετώπιση υποκλοπής δεδομένων σχετικά με τον φορέα μιας ετικέτας είναι ο τερματισμός της ετικέτας. Αυτό το αποτέλεσμα μπορεί να επιτευχθεί με δύο τρόπους, ο ένας τρόπος που χρησιμοποιείται κυρίως στον τομέα του λιανικού εμπορίου είναι η τοποθέτηση αφαιρούμενων ετικετών που χρησιμοποιούνται για την μετάδοση πληροφοριών σχετικά με τις τιμές των προϊόντων. Αυτές οι ετικέτες απλά αφαιρούνται από το προϊόν μόλις αυτό αγοραστεί από τον καταναλωτή. Ο δεύτερος τρόπος ο οποίος θεωρείται πολύ πιο δραστικός είναι ο τερματισμός τις ετικέτας αμέσως μετά την πληρωμή του προϊόντος.

4.2.2 Τεχνολογία επικοινωνίας κοντινού πεδίου (NFC) και απειλές

Η τεχνολογία επικοινωνίας κοντινού πεδίου (NFC – Near Field Communication) είναι ένα σύνολο πρωτοκόλλων επικοινωνίας που επιτρέπει την επικοινωνία μεταξύ δύο ηλεκτρονικών συσκευών σε συγκεκριμένη απόσταση μέσω ασύρματης σύνδεσης. Εφαρμογές αυτής της τεχνολογίες συναντάμε στις ανέπαφες συναλλαγές και γενικά σε συσκευές όπως smartphone και tablet. Η επικοινωνία κοντινού πεδίου βασίζεται στην αναγνώριση ραδιοσυχνοτήτων (RFID) που αναφερθήκαμε προηγουμένως.

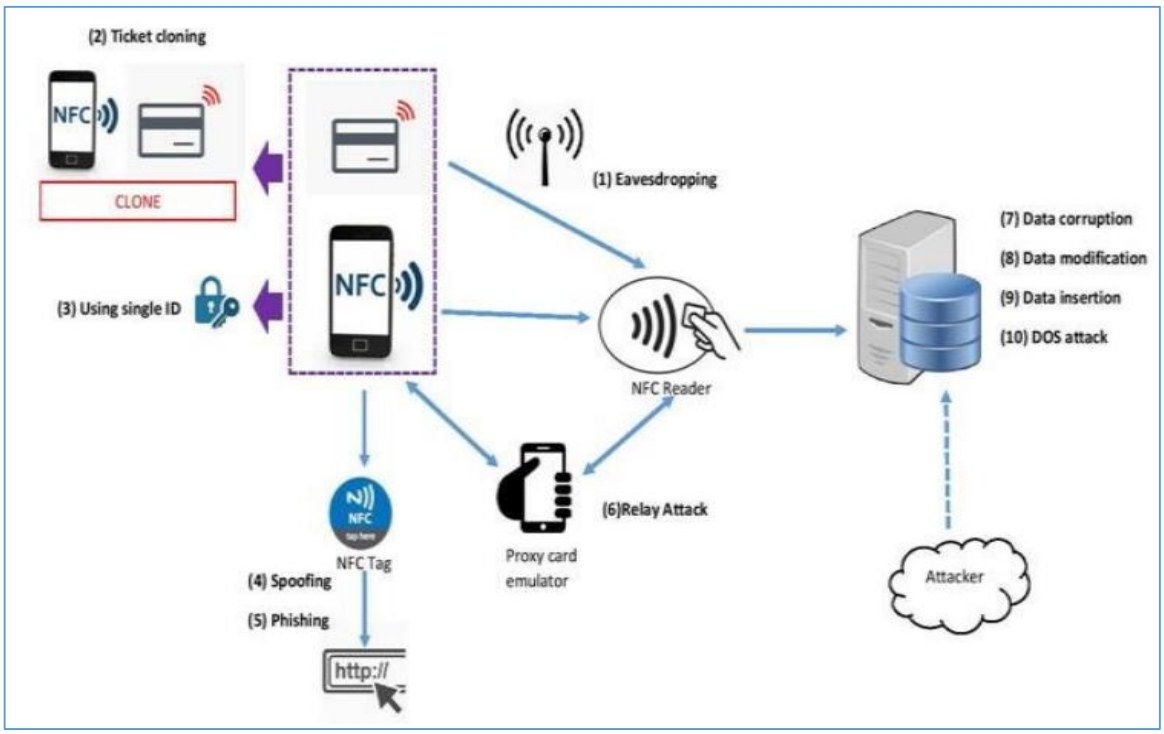
Παρά την μεγάλη χρησιμότητα αυτής της τεχνολογίας και της ευρείας χρήσης της σε διάφορους τομείς είναι αρκετά ευαίσθητη σε πολλούς τύπους επιθέσεων με αποτέλεσμα να δημιουργούνται σοβαρά προβλήματα στους χρήστες. Η πιο συχνή επίθεση είναι η υποκλοπή (eavesdropping), η υποκλοπή ουσιαστικά είναι ένα πρόβλημα το οποίο προσβάλει την ασφάλεια των δεδομένων και επηρεάζει όλες τις ασύρματες τεχνολογίες. Στην πράξη η υποκλοπή διενεργείται καθώς η επικοινωνία μέσω κυμάτων ραδιοσυχνοτήτων εκτελείτε μεταξύ δύο συσκευών παρά το γεγονός πως η απόσταση μεταξύ τους είναι αρκετά μικρή, ένας τρίτος μπορεί να εισβάλει να λάβει και να αποκωδικοποιήσει το σήμα παρακολουθώντας την επικοινωνία.

Μια άλλη μορφή επίθεσης είναι η εισαγωγή δεδομένων (data insertion), σε αυτήν την περίπτωση η συσκευή του εισβολέα είναι πιο γρήγορη από τη δεύτερη συσκευή που απαντά στο σύστημα μας. Έτσι ο εισβολέας στέλνει ψευδή και πλαστά δεδομένα πριν προλάβουν να αποσταλούν τα πραγματικά δεδομένα της συναλλαγής. Σε περίπτωση που η αποστολή των ψευδών και αληθινών δεδομένων γίνει ταυτόχρονα τότε δημιουργείται σφάλμα στα δεδομένα.

Επίσης, μια ακόμη μορφή επίθεσης είναι η άρνηση εξυπηρέτησης DoS (Denial of Service) η οποία συμβαίνει προκαλώντας προβλήματα στην ανταλλαγή πληροφοριών του συστήματος με αποτέλεσμα οι πληροφορίες που αποστέλλονται από τη μία συσκευή να μην είναι δυνατόν να αποκωδικοποιηθούν από τη δεύτερη η οποία τα λαμβάνει αφού έχουν προσβληθεί και παραποιηθεί.

Τέλος, μια αρκετά επικίνδυνη κακόβουλη επίθεση που έχουμε ήδη αναφερθεί και στην προηγούμενη υποενότητα, είναι η επίθεση του ενδιάμεσου MitM (Man in the Middle) [32] είναι μια από τις πιο δημοφιλής τακτικές που χρησιμοποιούνται για την υποκλοπή και παραποίηση πληροφοριών. Όπως είναι και διακριτό από την ονομασία του, ο εισβολέας παρεμβαίνει ανάμεσα στα δύο μέρη που έχουν σύνδεση ιδιωτικής συνομιλίας μεταξύ τους και ελέγχει όλη την συνομιλία χωρίς να γίνεται αντιληπτός από τους χρήστες. Τέτοιου είδους επιθέσεις είναι επιτυχής μόνο όταν ο εισβολέας καταφέρνει τον ταυτόχρονο έλεγχο ταυτότητας και των δύο μερών του συστήματος. Τα περισσότερα κρυπτογραφικά πρωτόκολλα που έχουν δημιουργηθεί για προστασία παρέχουν πάντα κάποια μορφή ελέγχου ταυτότητας τελικού σημείου ειδικά για τον αποκλεισμό τέτοιων επιθέσεων.

Στις περισσότερες επιθέσεις του ενδιάμεσου ο εισβολέας χρησιμοποιεί ως επί το πλείστον ένα δρομολογητή WiFi για να υποκλέψει τα δεδομένα της επικοινωνίας. Αυτή η τεχνική μπορεί να εφαρμοστεί με την εκμετάλλευση ενός δρομολογητή με ορισμένα κακόβουλα προγράμματα για την παρεμπόδιση της ορθής σύνδεσης του χρήστη στο δρομολογητή. Έτσι, ο εισβολέας διαμορφώνει πρώτα τον φορητό υπολογιστή του ως σημείο πρόσβασης WiFi, επιλέγοντας ένα όνομα που χρησιμοποιείται συνήθως σε έναν δημόσιο χώρο, όπως ένα αεροδρόμιο ή ένα καφενείο. Μόλις ο χρήστης συνδεθεί σε αυτόν τον κακόβουλο δρομολογητή για να φτάσει σε ιστότοπους, όπως ιστότοπους τραπεζικών συναλλαγών στο διαδίκτυο ή ιστότοπους εμπορίου, ο εισβολέας καταγράφει στη συνέχεια τα διαπιστευτήρια του χρήστη για μελλοντική χρήση.



Εικόνα 18. Τύποι επιθέσεων σε σύστημα NFC

Πηγή: https://www.researchgate.net/figure/Types-of-NFC-Security-Attacks_fig2_329642316

Οι περισσότερες από τις αποτελεσματικές άμυνες ενάντια σε τέτοιου είδους επιθέσεις δρουν μόνο στο δρομολογητή ή στον διακομιστή. Χρησιμοποιώντας μια ισχυρή κρυπτογράφηση μεταξύ του χρήστη και του διακομιστή ο διακομιστής επαληθεύσει το αίτημα μέσω ενός ψηφιακού πιστοποιητικού το οποίο επιτρέπει τη δημιουργία της σύνδεσης με ασφάλεια. Μια άλλη μέθοδος πρόληψης τέτοιων επιθέσεων είναι να μην γίνεται σύνδεση σε ανοιχτούς δρομολογητές WiFi για να περιοριστούν σημαντικά οι κακόβουλοι ενδιάμεσοι.

4.2.3 Επιθέσεις στα δίκτυα των αισθητήρων

Τα ασύρματα δίκτυα αισθητήρων [35] είναι αρκετά ευαίσθητα σε επιθέσεις διαφορετικών τύπων που διενεργούνται σε διαφορετικά επίπεδα του πρωτοκόλλου στρωμάτων. Το φυσικό στρώμα αφορά τη ροή μετάδοσης των πληροφοριών, την ανίχνευση σημάτων και την κρυπτογράφηση των πληροφοριών. Βάλλεται από επιθέσεις τύπου παρεμβολής και αλλοίωσης. Το στρώμα ζεύξης δεδομένων είναι υπεύθυνο για την πολυπλεξία των ροών δεδομένων, για την ανίχνευση πακέτων δεδομένων και για τη διασφάλιση συνδέσεων τύπου σημείου σε σημείο ή σημείου σε πολλαπλά σημεία. Οι συνηθέστεροι τύποι επιθέσεων εδώ είναι η εξάντληση πόρων και η μεροληψία. Το επίπεδο δικτύου διασφαλίζει την προώθηση των πακέτων και την αντιστοίχηση των διευθύνσεων, οι επιθέσεις που απευθύνονται σε επίπεδο δικτύου αποτυπώνονται στον παρακάτω πίνακα.

Πίνακας 2. Κατηγορίες επιθέσεων στα δίκτυα των αισθητήρων

Ονομασία Επίθεσης	Περιγραφή τρόπου επίθεσης
Επίθεση Sybil (Sybil attack)	Γίνεται με τη διαρροή πολλαπλών ταυτοτήτων στο δίκτυο επηρεάζοντας τη διατήρηση της τοπολογίας και τα σχήματα ανοχής σε σφάλματα.
Επίθεση σκουληκότρυπας (Wormhole attack)	Σε αυτήν την περίπτωση ένας αριθμός κακόβουλων κόμβων προσποιούνται ότι συνδέουν δύο απομακρυσμένα σημεία του δικτύου, προκαλώντας επιπλοκές στην ροή της κίνησης των δεδομένων.
Επίθεση πλημμύρας Hello (Flood attack)	Μέσω των πακέτων HELLO που χρησιμοποιούνται από τους χρήστες, οι εισβολείς δημιουργούν δυσλειτουργία στο σύστημα με αποτέλεσμα το πακέτο να μην φτάνει στον τελικό προορισμό του.
Επίθεση Παρεμβολής (Jamming)	Είναι μια επίθεση σε ασύρματα δίκτυα παρεμβάλλοντας στις ραδιοσυχνότητες του δικτύου.
Επίθεση Αλλοίωσης (Tampering)	Λόγω του χαμηλού κόστους των κόμβων αισθητήρων οι επιθέσεις αλλοίωσης αποκτούν φυσική πρόσβαση στον κόμβο και εξάγουν τα δεδομένα του κόμβου.
Επιθέσεις μεροληψίας	Γίνονται στο στρώμα σύνδεσης ς (Link Layer) και μπορεί να θεωρηθεί ως μια ήπια επίθεση DoS (Άρνηση Υπηρεσίας). Έτσι, ο επιτιθέμενος προσπαθεί να προκαλέσει την λήξη του χρονικού ορίου αποστολής δεδομένων των κόμβων το οποίο μπορεί να αποδυναμώσει σοβαρά ένα ολόκληρο δίκτυο.
Παραποίηση και επαναποστολή	Στόχος της παραποίησης και επαναποστολής δεδομένων διαδρομής είναι η παρεμβολή στην κίνηση ενός δικτύου. Οι επιθέσεις αυτές μπορεί να περιλαμβάνουν τα ακόλουθα: • δημιουργία κυκλικών διάδρομων • επιμήκυνση η κόντεμα διαδρομών και • επιτομή δικτύων και η δημιουργία ψευδών μηνυμάτων λάθους
Επιθέσεις βύθισης (Sinkhole)	Στην περίπτωση αυτή ο στόχος είναι να εξασφαλιστεί ότι όλη η κίνηση μιας συγκεκριμένης περιοχής του δικτύου ρέει μέσα από έναν παραβιασμένο κόμβο στον οποίο ο επιτιθέμενος έχει τον πλήρη έλεγχο. Έτσι οι εχθροί μπορούν να καταστείλουν ή να τροποποιήσουν τα πακέτα δεδομένων.

Πηγή:https://hellanicus.lib.aegean.gr/bitstream/handle/11610/18539/IoT%20Security%20Thesis.pdf?sequence=1

Αναφορικά με τις επιθέσεις [35] που αναφέρονται στον παραπάνω πίνακα τα αντίμετρα τα οποία χρησιμοποιούνται για την προστασία των δικτύων είναι η κρυπτογράφηση στο στρώμα σύνδεσης (link layer), η επαλήθευση ταυτότητας και ο έλεγχος ταυτότητας είναι τα αποτελεσματικότερα μέτρα προστασίας κατά των εξωτερικών επιθέσεων από κακόβουλες ενέργειες. Εάν εφαρμοστούν σωστά τα μέτρα προστασίας, τα συστήματα μπορούν να προστατευτούν από τις επιθέσεις Sybil, τις πλημμύρες HELLO, την πλαστογράφηση και τον αποσυγχρονισμό. Από την άλλη πλευρά οι επιθέσεις που εκτελούνται από ισχυρούς επιτιθέμενους αποτελούν σοβαρή απειλή για το δίκτυο διότι δεν υπάρχει κανένα πλήρως αποτελεσματικό μέτρο προστασίας. Οι πιο επικίνδυνες απειλές προέρχονται από το εσωτερικό του δικτύου και είναι οι επιθέσεις βύθισης και σκουληκότρυπας. Το πιο γνωστό αντίμετρο σε τέτοιες περιπτώσεις είναι το πρωτόκολλο γεωγραφικής δρομολόγησης που μπορεί να προστατεύσει το δίκτυο αισθητήρων από εσωτερικές κακόβουλες επιθέσεις.

4.2.4 Βλάβες και τεχνικά ζητήματα στις συσκευές IoT

Όπως έχουμε αναφέρει ήδη σε προηγούμενα κεφάλαια τα έξυπνα συστήματα IoT τις περισσότερες φορές ελέγχονται από εφαρμογές που είναι προγραμματισμένες για να παρέχουν πολλές και διαφορετικές μορφές αυτοματισμένων ενεργειών. Διάφοροι τύποι αισθητήρων, ανιχνευτών έξυπνοι φωτισμοί, έξυπνα συστήματα ψύξης, θέρμανσης, συναγερμών κ.α. ελέγχονται από τις εφαρμογές και πολλές φορές απομακρυσμένα. Δυστυχώς έχουν υπάρξει πολλά περιστατικά όπου συνέβησαν δυσλειτουργίες και τεχνικά ζητήματα τα οποία επέφεραν ανυπολόγιστες συνέπειες. Σε περιπτώσεις σφαλμάτων (bugs) των συσκευών ή των ενεργειών προγραμματισμού από τους χρήστες δίνονται λανθασμένες εντολές που προκαλούν επικίνδυνες καταστάσεις που ενίοτε έχουν καταστροφικές συνέπειες. Τέτοια παραδείγματα είναι να μην λειτουργεί το σύστημα συναγερμού, να μην κλειδώνουν οι πόρτες, την απενεργοποίηση της θέρμανσης όταν αυτή απαιτείται κ.α. Στη συνέχεια θα αναφερθούμε σε μια έρευνα [36] όπου αναλύονται και παρουσιάζονται οι βασικές κατηγορίες σφαλμάτων (bugs) στα συστήματα IoT και οι βασικές αιτίες που τα προκαλούν βασισμένη σε ποσοτικές και ποιοτικές αναλύσεις σφαλμάτων με τη βοήθεια προγραμματιστών εξειδικευμένων στην τεχνολογία του IoT. Τα σφάλματα του IoT είναι μια σχετικά νέα έννοια, είναι πολυδιάστατα και μπορεί να εκδηλωθούν σε διαφορετικά επίπεδα χρήσης.

4.2.5 Κατηγοριοποίηση σφαλμάτων IoT

A. **Υλικό συσκευής:** Τα σφάλματα σε αυτήν την υποκατηγορία σχετίζονται με τις φυσικές πτυχές των συσκευών IoT. Στα παραδείγματα περιλαμβάνονται σφάλματα που σχετίζονται με ζητήματα καλωδίωσης , προβλήματα με φυσικούς αισθητήρες και ενεργοποιητές των συσκευών. Άλλα κοινά σφάλματα σε αυτήν την κατηγορία είναι αυτά που συνδέονται με περιορισμό στη μνήμη των συσκευών, στην

κατανάλωση ενέργειας ή στην ικανότητα επεξεργασίας. Ένα τέτοιο παράδειγμα αποτελεί μια συσκευή με χαμηλή μπαταρία η οποία δημιουργεί λανθασμένα δεδομένα στο cloud. Παρόμοια περίπτωση αναφορών σφαλμάτων που έχουν συλλεχθεί στην έρευνα είναι βλάβες που έχουν προκληθεί από χαμηλή μπαταρία ή διακοπή του ρεύματος. Ακόμη σε μερικές περιπτώσεις η λειτουργία εξοικονόμησης ενέργειας έχει προκαλέσει απροσδόκητα αποτελέσματα όπως σημαντικές καθυστερήσεις στις λειτουργίες του συστήματος. Μια άλλη ομάδα προβλημάτων υλικού των συσκευών είναι τα προβλήματα σχετικά με την εκκίνηση ή επανεκκίνηση της συσκευής.

Β. Λογισμικό συσκευής: Τα σφάλματα λογισμικού διακρίνονται σε τρείς υποκατηγορίες.

- Η πρώτη αφορά απροσδόκητη εξαίρεση του λογισμικού της συσκευής και δημιουργεί προβλήματα κολλήματος.
- Η δεύτερη υποκατηγορία περιλαμβάνει θέματα που σχετίζονται με τη διαμόρφωση της συσκευής, η οποία μπορεί να ορίζεται ως εξωτερική οδηγία που αποστέλλεται στη συσκευή για συγκεκριμένο σκοπό. Αυτό συμβαίνει κυρίως στα πρώτα στάδια εισαγωγής μιας συσκευής στην τεχνολογία του IoT. Απαιτείτε κάθε συσκευή να έχει ρυθμιστεί σωστά με τέτοιο τρόπο ώστε να είναι συμβατή με τα υπόλοιπα στοιχεία του υλικού και του λογισμικού και επίσης να μπορεί να επικοινωνεί με τα άλλα μέρη του δικτύου. Ζητήματα που σχετίζονται με τη διαμόρφωση της συσκευής με διαπιστευτήρια Wi-Fi ή με τη προσαρμογή της συσκευής στη σωστή έκδοση του λογισμικού αποτελούν κοινά παραδείγματα.
- Τρίτη και πιο κοινή υποκατηγορία είναι προβλήματα που προκύπτουν από την αναβάθμιση του λογισμικού. Υπάρχουν πολλές περιπτώσεις όπου το λογισμικό της συσκευής έχει ενημερωθεί με παλαιότερη έκδοση και έχει προκαλέσει βλάβες στο σύστημα IoT.

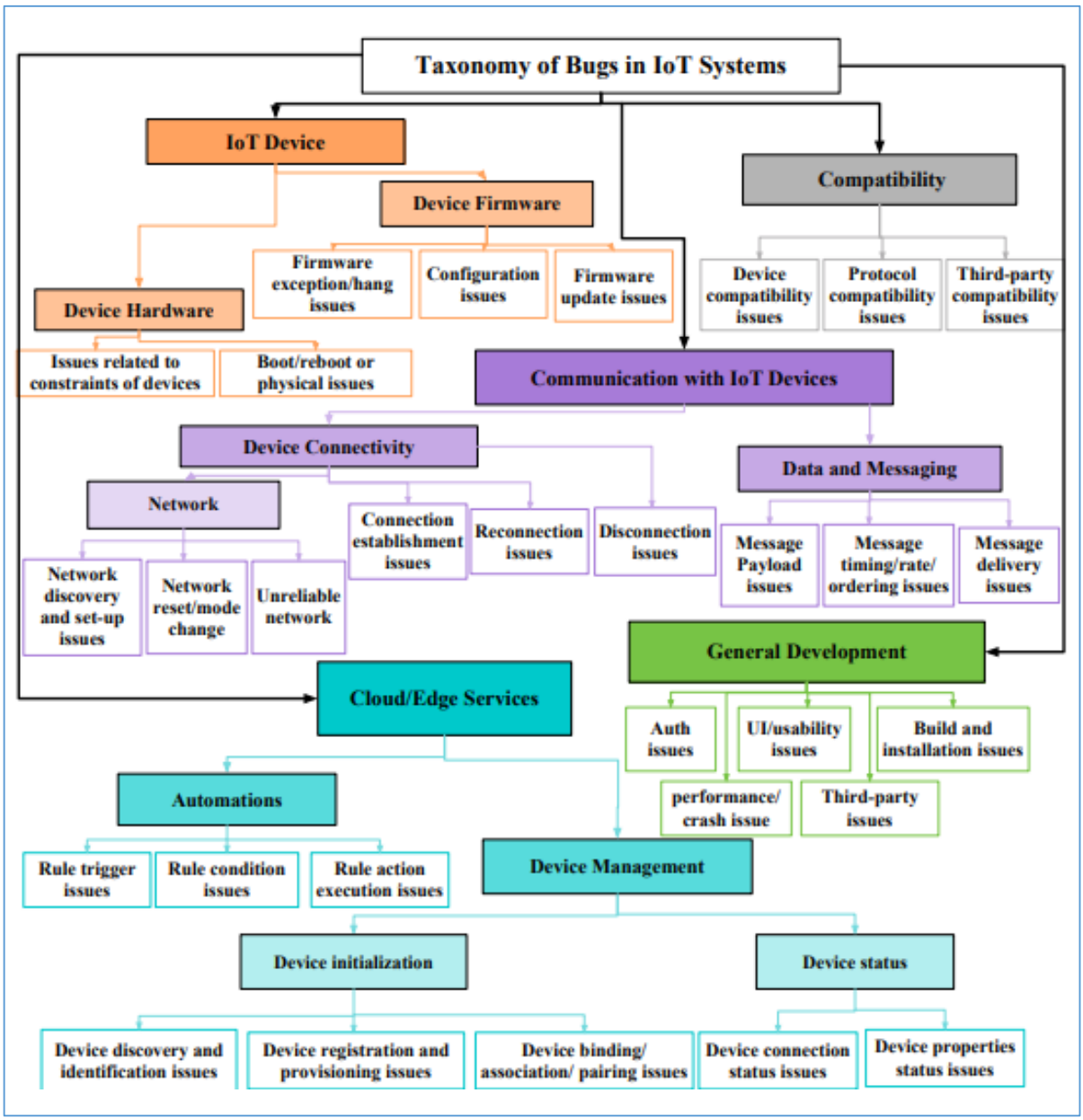
Γ. Συμβατότητα: Όταν ένα σφάλμα εμφανίζεται μόνο σε έναν συγκεκριμένο τύπο συσκευής, πρωτόκολλο επικοινωνίας ή στοιχείο τρίτου μέρους, εμπίπτει στην κατηγορία συμβατότητας. Για παράδειγμα, ένα κοινό πρόβλημα ασυμβατότητας συσκευής προκύπτει όταν ορισμένες συσκευές αναφέρουν τα δεδομένα που τις χαρακτηρίζουν σε διαφορετικές μορφές, με αποτέλεσμα τα άλλα μέρη του συστήματος να μην μπορούν να επεξεργαστούν τα δεδομένα τους. Άλλα καινά σφάλματα συνδέονται με ζητήματα συμβατότητας ορισμένων συνδυασμών αισθητήρων και ελεγκτών. Για παράδειγμα ασυμβατότητα του αισθητήρα θερμοκρασίας με τον αντίστοιχο μικροελεγκτή του συστήματος. Ακόμη μια περίπτωση είναι τα προβλήματα διαλειτουργικότητας διαφορετικών πρωτοκόλλων. Μια κοινή κακή πρακτική που συναντάμε είναι όταν αναπτύσσεται κώδικας για συγκεκριμένο πρωτόκολλο ή για συγκεκριμένη συσκευή. Ωστόσο, κάποιες φορές οι

προγραμματιστές δεν έχουν άλλη επιλογή από το να ακολουθήσουν αυτήν την επιρρεπή σε σφάλματα τακτική για να παρακάμψουν τους περιορισμούς τρίτων κατασκευαστών.

Δ. **Σφάλματα επικοινωνίας μεταξύ συσκευών IoT:** Τα σφάλματα που σχετίζονται με την επικοινωνία συσκευών IoT είτε μεταξύ τους είτε με άλλα μέρη του συστήματος, εμπίπτουν σε αυτή την κατηγορία. Γενικά υπάρχουν δύο τύποι σφαλμάτων σε αυτήν την κατηγορία:
   - Η συνδεσιμότητα συσκευής, η οποία σχετίζεται με το δίκτυο στο οποίο βασίζεται η συσκευή για την πρόσβασή της στο διαδίκτυο. Ένα τέτοιο παράδειγμα είναι όταν η συσκευή δεν μπορεί να ανακαλύψει ένα έγκυρο και διαθέσιμο δίκτυο, όπως ένα τοπικό σημείο πρόσβασης και έτσι χάνει την πρόσβασή της στο διαδίκτυο. Τις περισσότερες φορές όταν η θέση της συσκευής αλλάζει από ένα δωμάτιο σε ένα άλλο ή σε ένα άλλο κτίριο θα πρέπει να επαναδιαμορφωθεί στο νέο σημείο πρόσβασης.
   - Δεδομένα και μηνύματα, εδώ περιλαμβάνονται σφάλματα που σχετίζονται με τα δεδομένα και την αποστολή μηνυμάτων εντός του συστήματος IoT. Συνήθως, τα μηνύματα είναι είτε εντολές που αποστέλλονται σε συσκευές μέσω του cloud είτε είναι δεδομένα περιγραφικών πληροφοριών που λαμβάνονται από άλλα μέρη του συστήματος. Ορισμένα σφάλματα προκαλούν αστοχίες στην παράδοση αυτών των μηνυμάτων από τον αποστολέα στον παραλήπτη.

Ε. **Σφάλματα στις υπηρεσίες cloud:** Σε αυτή τη κατηγορία περιλαμβάνονται σφάλματα που σχετίζονται με τις υπηρεσίες που παρέχονται από τους απομακρυσμένους διακομιστές cloud. Για παράδειγμα όταν διαχειριζόμαστε μια συσκευή από απόσταση τότε θα πρέπει η συσκευή να είναι συνδεδεμένη σε έναν διακομιστή cloud και να αναφέρει την κατάστασή της όταν αυτό ζητηθεί. Τα προβλήματα διαχείρισης συσκευών περιλαμβάνουν προβλήματα που προκαλούν αποτυχίες στην παραπάνω διαδικασία επικοινωνίας.

Συμπερασματικά, λαμβάνοντας υπόψη όλους τους παραπάνω τύπους σφαλμάτων που περιγράφονται σε αυτό το υποκεφάλαιο διαπιστώνουμε ότι το πολλά υποσχόμενο διαδίκτυο των πραγμάτων έχει αρκετά τρωτά σημεία που δεν μπορούν να παραβλεφθούν από όποιον επιθυμεί να επενδύσει σε τέτοια τεχνολογικά συστήματα και να βασιστεί σε αυτά. Αλλά πρέπει να μελετήσει διεξοδικά τις λύσεις που υπάρχουν στην κάθε περίπτωση που τον ενδιαφέρει. Ωστόσο το Διαδίκτυο των πραγμάτων παρά τα προβλήματα που έχει παραμένει μια από τις μεγαλύτερες τεχνολογικές καινοτομίες τις εποχής μας.



Εικόνα 19. Διαγραμματική απεικόνιση των σφαλμάτων του συστήματος IoT

Πηγή: https://open.library.ubc.ca/soa/cIRcle/collections/ubctheses/24/items/1.0401501

5. Μελέτες Περίπτωσης (Case Studies) Θεμάτων Ασφαλείας Έξυπνων Κτηρίων/Σπιτιών

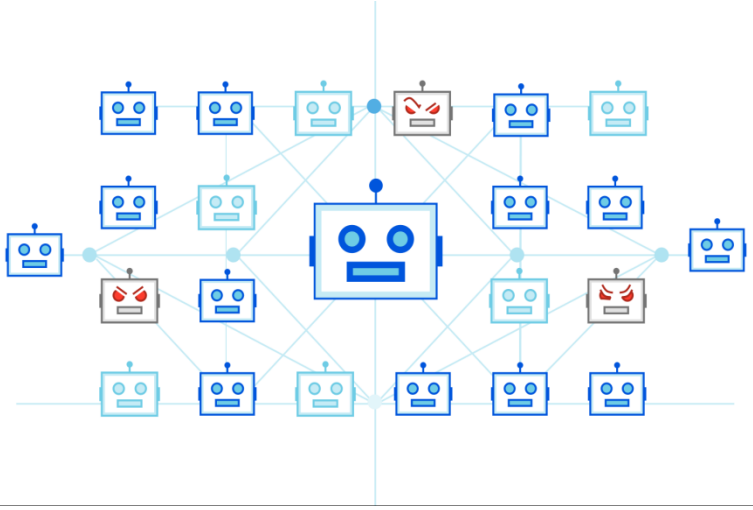
Σε αυτό το κεφάλαιο όπου είναι και το τελευταίο της παρούσας εργασίας, θα αναφερθούμε σε περιπτώσεις κακόβουλων επιθέσεων και θα παρουσιάσουμε την ροή ενεργειών που ακολουθήθηκε για να γίνουν οι επιθέσεις μέσω του δικτύου ενάντια σε έξυπνες συσκευές IoT. Συγκεκριμένα θα αναφερθούμε αρχικά στο κακόβουλο λογισμικό Mirai Botnet που πρωτοεμφανίστηκε το 2016 και στη συνέχεια θα αναφερθούμε στις δύο πιο ευάλωτες έξυπνες οικιακές συσκευές σύμφωνα με την εταιρεία Avira καθώς επίσης και στις μεθόδους με τις οποίες παραβιάστηκαν.

5.1 Μελέτη περίπτωσης Mirai Botnet

Μέσα στην ολοένα αυξανόμενη τάση της τεχνολογίας του IoT [37] πέρα από τις αμέτρητες δυνατότητες που δημιουργούνται, παράλληλα έχουν δημιουργηθεί κενά ασφαλείας και διάφορες αστοχίες ως προς την προστασία των δεδομένων. Αυτά τα κενά ασφαλείας σε συνδυασμό με τη συνεχή σύνδεση των συσκευών στο διαδίκτυο και τις σπάνιες αναβαθμίσεις των λογισμικών τους, δημιουργούν ένα εύκολο έδαφος σε διάφορους επιτήδειους hackers να εκμεταλλευτούν την έλλειψη ασφάλειας και προστασίας των συσκευών IoT και να κάνουν κακόβουλες επιθέσεις. Παρά το γεγονός πως οι συσκευές IoT συνήθως σχετίζονται και εξυπηρετούν απλές καθημερινές διεργασίες, με μικρή υπολογιστική ισχύ για την κάθε συσκευή. Ωστόσο σαν σύνολο η δυναμική τους είναι αρκετά μεγάλη. Οι επιτήδειοι χρησιμοποιούν αυτή την μεγάλη υπολογιστική ισχύ του δικτύου τους χρησιμοποιώντας τα botnet. Ο όρος botnet [38] δημιουργείται από τις λέξεις robot και network. Το botnet είναι ένα δίκτυο υπολογιστών το οποίο έχουν προσβάλει οι hackers με κακόβουλο λογισμικό. Σκοπός τους είναι η διενέργεια πράξεων στο διαδίκτυο χωρίς την άδεια και τη γνώση των θυμάτων. Όταν ένα bot κάνει επίθεση σε έναν υπολογιστή, ο χειριστής του μπορεί να πάρει τον έλεγχο της συσκευής καθώς και των υπόλοιπων συσκευών που βρίσκονται στο botnet.

Μία τέτοιου είδους επίθεση είναι και το Mirai Botnet, [39] ένα κακόβουλο λογισμικό που μολύνει έξυπνες συσκευές που λειτουργούν με επεξεργαστές ARC, μετατρέποντάς τες σε ένα δίκτυο από τηλεκατευθυνόμενα bots ή «ζόμπι». Αυτό το δίκτυο ρομπότ, που ονομάζεται botnet , χρησιμοποιείται συχνά για την εκτόξευση επιθέσεων DDoS . Συντομογραφία του κακόβουλου λογισμικού, είναι ένας γενικός όρος που περιλαμβάνει σκουλήκια υπολογιστών, ιούς, δούρειους ίππους, rootkits και λογισμικό υποκλοπής spyware. Μερικοί τύποι συσκευών που προσβλήθηκαν από το Mirai είναι δρομολογητές, DVRs, κάμερες, εκτυπωτές και δέκτες τηλεοπτικών καναλιών. Οι δημιουργοί του κακόβουλου λογισμικού Mirai το Σεπτέμβριο του 2016 ξεκίνησαν μια επίθεση DDoS στον ιστότοπο ενός ειδικού ασφαλείας, λίγο καιρό αργότερα κοινοποίησαν δημόσια τον πηγαίο κώδικα, ίσως για να καλύψουν τα ίχνη τους. Ο κώδικας αντιγράφηκε πολύ

γρήγορα από πολλούς άλλους επιτήδειους του διαδικτύου και πιθανολογείται ότι βρίσκεται πίσω από τη μαζική επίθεση που κατέστρεψε τον πάροχο υπηρεσιών καταχώρισης τομέα, Dyn, τον Οκτώβριο του 2016 όπου χρησιμοποιήθηκαν περίπου εκατό χιλιάδες συσκευές IoT που μολύνθηκαν με σκοπό την κατάρριψη του.

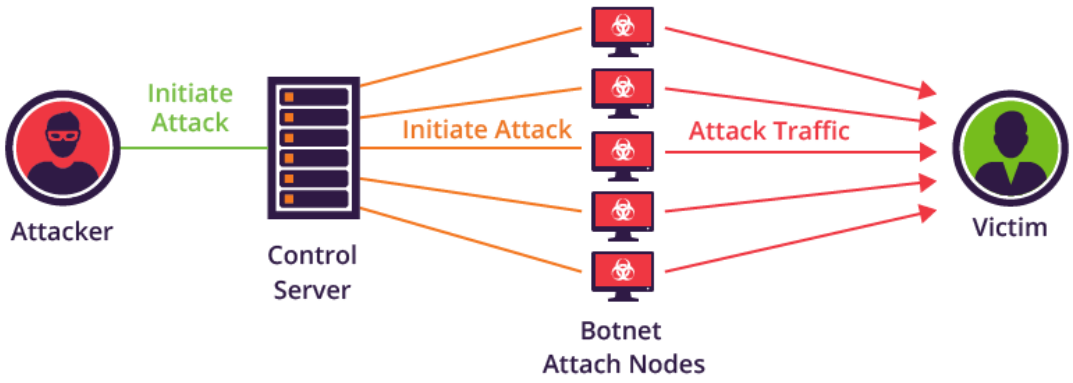


Εικόνα 20. Διαγραμματική απεικόνιση τρόπου λειτουργίας του Mirai Botnet

Πηγή: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

Το Mirai λειτουργεί σαρώνοντας το Διαδίκτυο για να εντοπίσει συσκευές IoT που λειτουργούν με βάση τον επεξεργαστή ARC. Αυτός ο επεξεργαστής εκτελεί μια έκδοση του λειτουργικού συστήματος Linux. Εάν ο προεπιλεγμένος συνδυασμός ονόματος χρήστη και κωδικού πρόσβασης δεν αλλάξει, το Mirai μπορεί να συνδεθεί στη συσκευή και να τη μολύνει. Οι δημιουργοί του Mirai είναι δύο νεαροί άνδρες ηλικίας 20 και 21 ετών οι οποίοι ίδρυσαν μια εταιρεία παροχής υπηρεσιών προστασίας από επιθέσεις DDoS. Ουσιαστικά στην περίπτωσή τους παρείχαν υπηρεσίες στους ίδιους οργανισμούς στους οποίους είχαν επιτεθεί με το κακόβουλο λογισμικό τους. Παρά το γεγονός ότι οι αρχικοί δημιουργοί εντοπίστηκαν, το λογισμικό Mirai παραμένει επικίνδυνο διότι ο πηγαίος κώδικας παραμένει και μεταλλάσσεται. Έχουν προέλθει από αυτό πολλές παραλλαγές όπως το Okiru, το Satori, το Masuta και το PureMasuta. Και το προσφάτως ανακαλυφθέν και ισχυρό στέλεχος με διάφορες ονομασίες όπως IoTrooper και Reaper το οποίο μπορεί να προσβάλει συσκευές IoT πολύ γρηγορότερα από το Mirai.

Η διαδικασία [40] που ακολουθείτε σε μια επίθεση botnet DDoS είναι απλή και συγκεκριμένη. Αρχικά ο εγκέφαλος τις επίθεσης δίνει εντολές και κατευθύνει τον κεντρικό server, ο κεντρικός server με τη σειρά του δρομολογεί εντολές επίθεσης σε κάθε μία από τις συνδεδεμένες έξυπνες συσκευές (μεμονωμένους κόμβους) στο δίκτυο. Έπειτα η επίθεση δρομολογείται από τις μολυσμένες συσκευές στον τελικό στόχο της επίθεσης. Όλη αυτή η διαδικασία απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 21. Διαγραμματική απεικόνιση επίθεσης Botnet

Πηγή: https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

Οι επιθέσεις botnet με το πέρασμα του χρόνου εξελίχθηκαν και τα κίνητρα δεν ήταν πια τα ίδια. Πλέον από την απλή αποστολή spam μηνυμάτων, οι hackers έχουν βρει τρόπους να εισπράττουν χρήματα με παράνομους τρόπους βασισμένοι σε εκβιασμούς όπως γίνεται και με τις επιθέσεις του Mirai Botnet. Με τη ραγδαία αύξηση του αριθμού των συσκευών IoT αυξάνεται σημαντικά και το πρόσφορο πεδίο δράσης των επιθέσεων botnet. Παρακολουθώντας τον τρόπο δράσης της επίθεσης διαπιστώνουμε πως εξελίσσονται ταυτόχρονα τρείς διαφορετικές ροές εργασιών. Η σάρωση, η μόλυνση και η επίθεση. Διαπιστώνουμε λοιπόν πως με αυτόν τον τρόπο η ταχύτητα με την οποία μπορεί να σαρώσει το διαδίκτυο αυξάνεται σχεδόν με εκθετική ανάπτυξη.

Εικόνα 22. Ροή εργασιών μόλυνσης

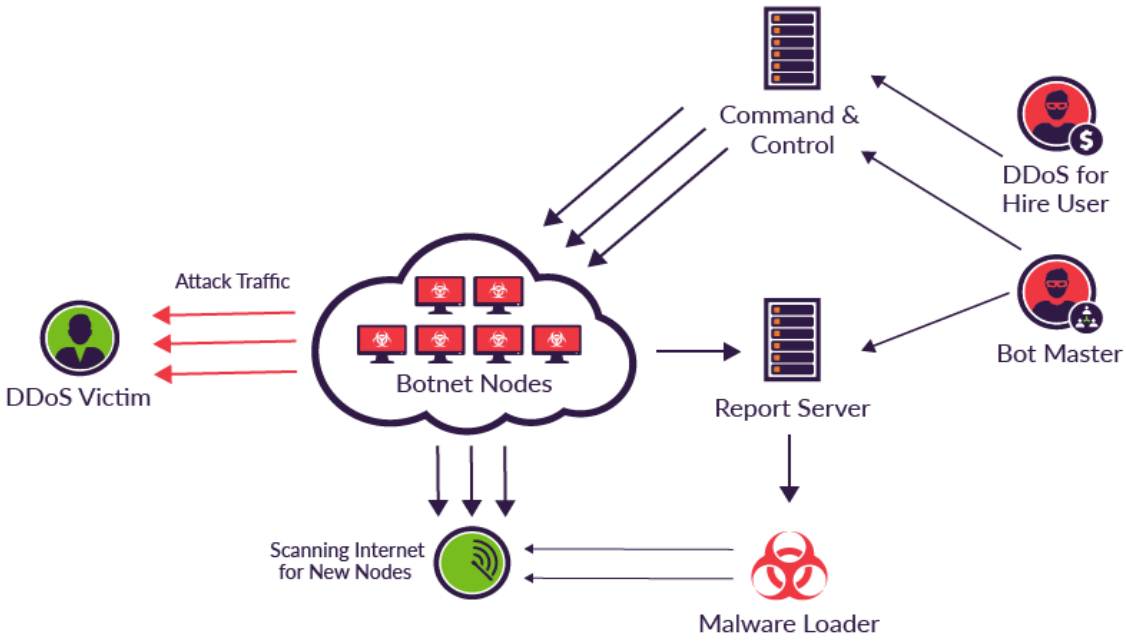
Πηγή: https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

Η ροή εργασιών της σάρωσης μπορεί να επιμερισθεί σε τρείς διαφορετικές λειτουργίες ενεργειών.

- Η πρώτη είναι η διερεύνηση στο διαδίκτυο για την εύρεση πιθανών στόχων (SYN Port Scan).
- Η δεύτερη είναι η εκτέλεση βασικών προτύπων (έλεγχοι ταυτότητας).
- Και η τελευταία είναι η αποστολή των αποτελεσμάτων σε έναν κεντρικό διακομιστή αναφορών (επιτυχής αναφορά). Έτσι κατά αυτόν τον τρόπο το κακόβουλο λογισμικό μολύνει της συσκευές IoT εντοπίζοντας πρώτα μέσω

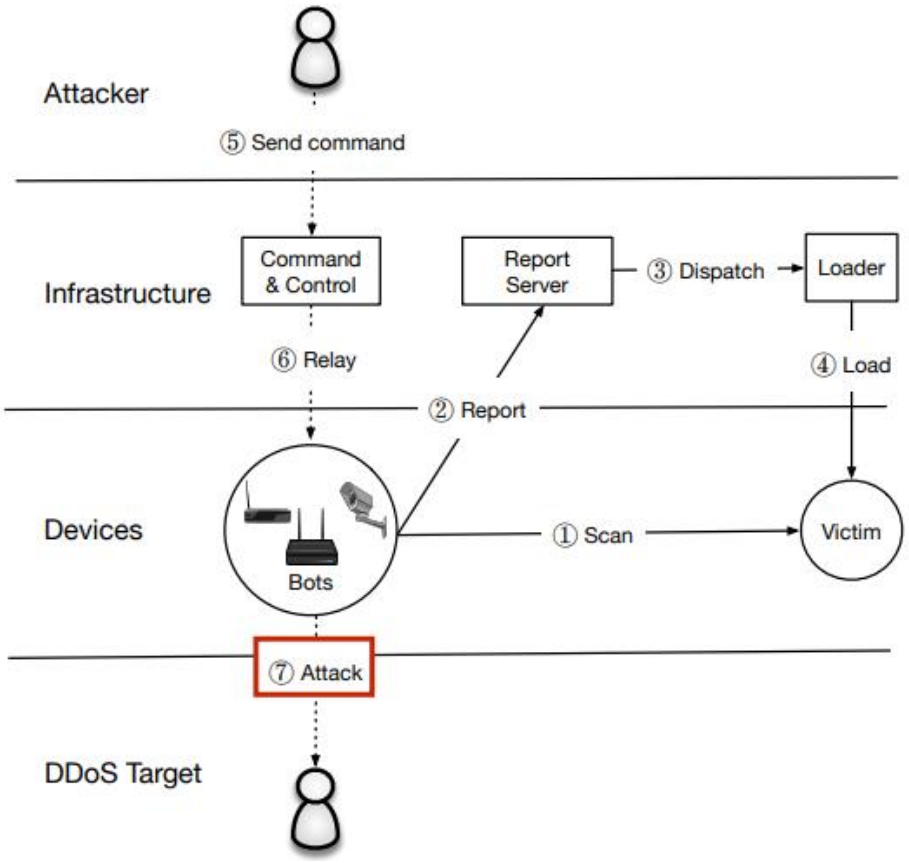
της σάρωσης την συσκευή. Στη συνέχεια μετά την επιτυχή σάρωση αποστέλλονται τα δεδομένα και διαχέεται η μόλυνση στο δίκτυο.

Είναι πολύ σημαντικό να αναφερθεί ότι ο κατανεμητής δεδομένων (loader) προσπαθεί να εντοπίσει την αρχιτεκτονική της κάθε συσκευής και να φορτώσει το αντίστοιχο συμβατό αρχείο. Στην συνέχεια με την εκτέλεση του αρχείου η συσκευή IoT είναι πλέον μέλος του Botnet και αρχίζει πλέον με τη σειρά της να πραγματοποιεί και αυτή τις ίδιες ενέργειες σάρωσης και επίθεσης σε άλλους κόμβους στο Botnet. Στα παρακάτω διαγράμματα ροής βλέπουμε αναλυτικά τη ροή που ακολουθείτε σε μια επίθεση. Αρχικά ο Bot Master στέλνει μια εντολή επίθεσης στον διακομιστή εντολών και ελέγχου. Στη συνέχεια ο διακομιστής στέλνει δεδομένα σε κάθε κόμβο στο Botnet τα οποία μολύνουν τους κόμβους και κάθε ένας από αυτούς δρομολογεί μια νέα επίθεση. Αξίζει να σημειωθεί σε αυτό το σημείο ότι κατά τη διάρκεια των επιθέσεων οι κόμβοι συνεχίζουν τις ενέργειες σάρωσης με αποτέλεσμα να μην σταματά ποτέ να αναζητά νέες συσκευές για να επιτεθεί και να μολύνει.



Εικόνα 23. Διαγραμματική απεικόνιση επίθεσης Mirai Botnet

Πηγή: https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack



Εικόνα 24. Διαγραμματική απεικόνιση επίθεσης Mirai Botnet

Πηγή: https://www.usenix.org/sites/default/files/conference/protected-files/usenixsecurity17_slides_ma_zane.pdf

Τέλος, το κακόβουλο λογισμικό λαμβάνει μέτρα ασφαλείας για να κάνει δύσκολο τον εντοπισμό του. Διαγράφεται από το σύστημα εκτελεσμένων αρχείων μόλις ολοκληρωθεί η δράση του κακόβουλου λογισμικού του. Διαγράφεται από τη διαδικασία εκτέλεσης και μετονομάζεται με νέο τυχαίο όνομα. Θα μπορούσαμε να πούμε πως το Mirai Botnet είναι ένα ιδιαίτερα σύνθετο και περίπλοκο πρόγραμμα κακόβουλου λογισμικού.

5.2 Μελέτη περιπτώσεων κοινών επιθέσεων ασφαλείας σε συσκευές IoT

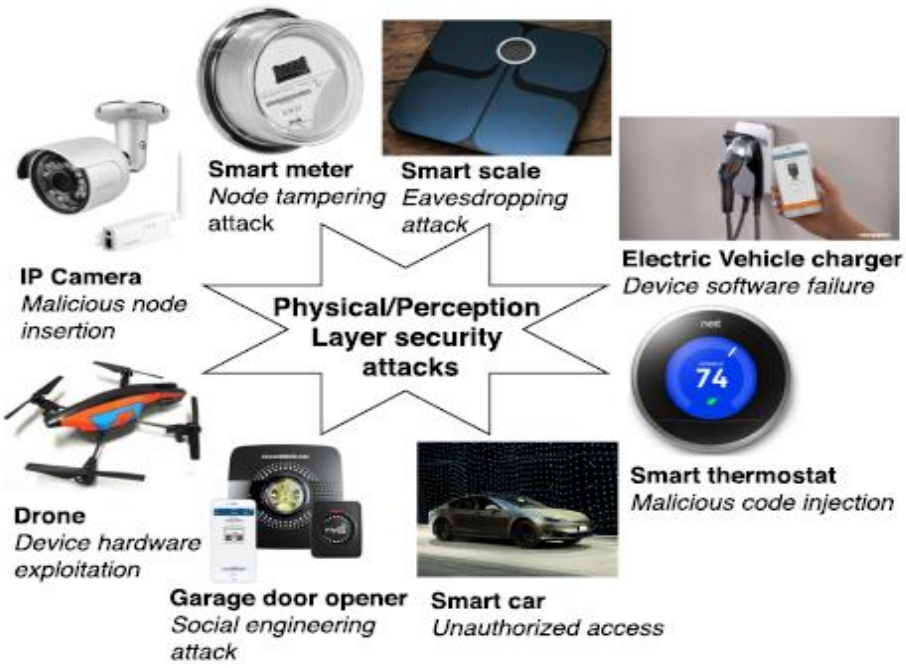
Με την ραγδαία ανάπτυξη [47] της τεχνολογίας του IoT έχει προκύψει η μεγάλη ανάγκη τα δεδομένα και οι πληροφορίες που μεταφέρονται να μην είναι ανιχνεύσιμα και εκτεθειμένα προς υποκλοπή από τρίτους με κακόβουλες προθέσεις. Ανεξάρτητα από το γεγονός αν οι πληροφορίες που διακινούνται και ανταλλάσσονται είναι απόρρητες, ιδιωτικές, εμπιστευτικές ή όχι. Είναι άμεση υποχρέωση των εταιρειών να ενημερώνουν αλλά και να ασφαλίζουν μέσω διαδικασιών ελέγχου τα προϊόντα τους από κοινές κακόβουλες επιθέσεις.

Ωστόσο είναι κατανοητό πως πάντα θα διατίθενται προς πώληση στην αγορά, συσκευές IoT χαμηλού κόστους και ποιότητας οι οποίες δεν θα διαθέτουν κανένα

απολύτως μηχανισμό ασφαλείας. Σε αυτή την περίπτωση έγκειται στον καταναλωτή να αποφασίσει για την επιλογή του.

Γενικότερα παρατηρείται ένας συμβιβασμός των κατασκευαστικών εταιρειών συσκευών IoT ως προς τα μέτρα ασφαλείας με σκοπό να διατηρήσουν την ανταγωνιστικότητά τους και να εισάγουν γρηγορότερα τα προϊόντα τους στην αγορά, αλλά και τη μείωση του συνολικού κόστους. Έτσι οι συσκευές IoT καταλήγουν να είναι εύκολοι στόχοι σε επιθέσεις και κακόβουλες ενέργειες όπως για παράδειγμα αναφέρει και η έρευνα των J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, και Y. Jin [48] τις σχετικές ευπάθειες που υπάρχουν απέναντι στον απλό καταναλωτή και γενικότερα στη βιομηχανία των συσκευών IoT. Μια άλλη έρευνα κατατάσσει το επίπεδο της αρχιτεκτονικής του IoT στην ζώνη υψηλότερου κινδύνου ως προς θέματα ασφαλείας, εξαιτίας του γεγονότος πως οι συσκευές αναπτύσσονται σε εχθρικά και απροστάτευτα περιβάλλοντα.

Επομένως, υπάρχει άμεση ανάγκη εκπαίδευσης των χρηστών και των απλών καταναλωτών. Θα πρέπει να επισημαίνονται και να γνωστοποιούνται οι πιθανοί κίνδυνοι που απειλούν την χρήση και την ομαλή λειτουργία των συσκευών IoT. Στη συνέχεια θα μελετήσουμε οκτώ περιπτώσεις κοινών επιθέσεων σε απλές συσκευές IoT καθώς και τρόπους με τους οποίους μπορούμε να αντιμετωπίσουμε την κάθε περίπτωση ξεχωριστά.



Εικόνα 25. Οκτώ κοινές επιθέσεις σε συσκευές IoT

Πηγή: https://ieeexplore.ieee.org/document/8977812

5.2.1 Αποτυχία στο λογισμικό της συσκευής

Σε αυτήν την περίπτωση ευπάθειας, οποιοδήποτε κενό ασφαλείας στο υλικολογισμικό ή και στο λογισμικό της συσκευής, μπορεί να αξιοποιηθεί από τους κακόβουλους που παραμονεύουν για να πραγματοποιήσουν μια σειρά από επιθέσεις. Όπως στην μελέτη περίπτωσης που θα αναφέρουμε και αφορά έναν φορτιστή ηλεκτρικού οχήματος (EV) από την εταιρεία Charge Point Inc.

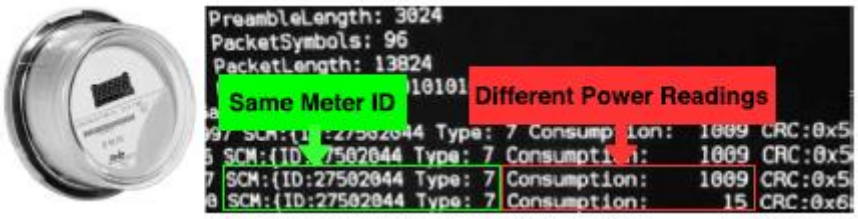
Επίθεση και συνέπειες: Η έρευνα σε αυτή την περίπτωση έδειξε πως ο κωδικός πρόσβασης του φορτιστή EV μπορεί να παρακαμφθεί στη φάση ελέγχου ταυτότητας. Αυτό δίνει τη δυνατότητα στους εισβολείς να καταφέρουν να έχουν πρόσβαση στη συσκευή ακόμη και αν εισάγουν λανθασμένους κωδικούς πρόσβασης. Με την πρόσβαση στο σύστημα της συσκευής μπορούν να βλάψουν με διάφορους τρόπους την λειτουργία και τα δεδομένα που μεταδίδονται. Επιπλέον αποδείχθηκε ότι μπορούν οι εισβολείς να τροποποιήσουν οποιοδήποτε αρχείο του συστήματος ή να εκτελέσουν οποιοδήποτε λειτουργικό σύστημα (OS) στο κέντρο ελέγχου της συσκευής. Με σκοπό οι εταιρείες να προσελκύσουν περισσότερους πελάτες IoT προσθέτουν συχνά νέες δυνατότητες στα προϊόντα τους όπως και στη περίπτωσή μας χωρίς να γίνονται οι απαραίτητοι έλεγχοι στην έκταση που απαιτείται. Εκμεταλλευόμενοι οι επιτιθέμενοι τα παραπάνω κενά ασφαλείας μπορούν να κερδίσουν πλήρως τον έλεγχο της συσκευής. Για παράδειγμα, στη περίπτωση του φορτιστή EV μπορούν να αλλάξουν τις λειτουργίες του, την ένταση του ρεύματος, ακόμη και να το απενεργοποιήσουν. Επίσης μπορούν να προκαλέσουν ακόμη και σωματικές βλάβες.

Αδυναμίες και μέτρα πρόληψης: Όπως αναφέραμε και προηγουμένως το βασικό τρωτό σημείο είναι κατά την ταυτοποίηση του χρήστη μέσω του κωδικού πρόσβασης, κατά την οποία ο εισβολέας μπορεί να εισβάλει ακόμη και με την εισαγωγή λανθασμένου κωδικού. Για να διασφαλιστεί ότι ένας επιτιθέμενος δεν θα εκμεταλλευτεί τα τρωτά σημεία που περιγράψαμε, θα πρέπει να τεθούν ίσως πρόσθετα τεκμήρια ταυτοποίησης με περεταίρω ελέγχους. Επίσης θα βοηθήσουν αρκετά τεχνικές επαλήθευσης και ανίχνευσης μη ασφαλούς χρήσης των λειτουργιών του λογισμικού.

5.2.2 Επίθεση παραβίασης κόμβων

Πρόκειται για μια επίθεση κατά την οποία ο εισβολέας υποκλέπτει τα χαρακτηριστικά στοιχεία του εξοπλισμού της συσκευής και παραποιεί χειροκίνητα το ηλεκτρονικό της κύκλωμα και τις ρυθμίσεις της. Μια τέτοια περίπτωση αποτελεί ο έξυπνος μετρητής Itron Centron CL200.

Επίθεση και συνέπειες: Ένα επιτυχημένο χακάρισμα του έξυπνου μετρητή μελετήθηκε και αναλύθηκε. Το πρωταρχικό κίνητρο της επίθεσης ήταν να αλλάξει το Device ID της συσκευής και να αντιγράψει τη ταυτότητα του μετρητή.



Εικόνα 26. Έξυπνος Μετρητής και ενδείξεις

Πηγή: https://ieeexplore.ieee.org/document/8977812

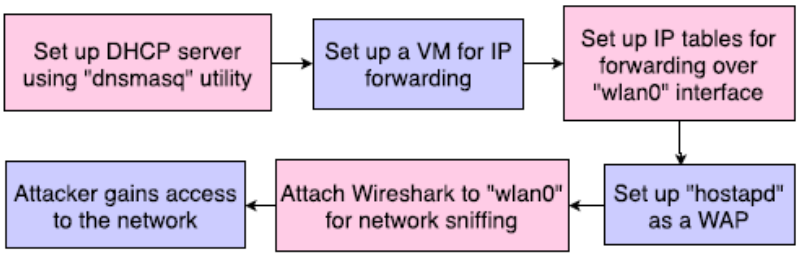
Στην εικόνα του μετρητή που βλέπουμε παραπάνω στις δύο τελευταίες ενδείξεις του αρχείου καταγραφής βλέπουμε τα δεδομένα από δύο διαφορετικές συσκευές που μοιράζονται το ίδιο αναγνωριστικό αλλά έχουν διαφορετικές τιμές κατανάλωσης ενέργειας που οδηγούν σε κλοπή ενέργειας. Τέτοιου είδους επιθέσεις πέρα από την κλοπή ενέργειας οδηγούν και σε άλλες οικονομικές και εμπορικές ζημιές.

Αδυναμίες και μέτρα πρόληψης: Το τσιπ EEPROM που διαθέτει αυτή η συσκευή, δεν προστατεύεται από επιθέσεις με παράνομη πρόσβαση ανάγνωσης ή εγγραφής δεδομένων. Το τσιπ μπορεί να προστατευτεί απέναντι σε τέτοιες ενέργειες με τεχνικές αντιπαραποίησης των αρχικών δεδομένων, ή με πιο απλές εναλλακτικές λύσεις που αφορούν το λογισμικό κρυπτογράφησης και λειτουργούν ως διαπιστευτήρια επιτρέποντας την τροποποίηση μόνο σε συσκευές που έχουν πιστοποιηθεί.

5.2.3 Επίθεση Υποκλοπής

Σε αυτή την περίπτωση επίθεσης η μεταφορά δεδομένων από τις συσκευές IoT που αποτελούν στόχο ανιχνεύονται από έναν <<ενδιάμεσο κακόβουλο>> man-in-the-middle (MITM) με δυνατότητα υποκλοπής χρήσιμων πληροφοριών δικτύου. Μια τέτοια περίπτωση είναι η έξυπνη ζυγαριά.

Επίθεση και συνέπειες: Αυτή η συσκευή στέλνει στατιστικά στοιχεία στον διακομιστή τύπου Fitbit μέσω ασύρματου δικτύου σημείου πρόσβασης (WAP) που επιτρέπει στον χρήστη να παρακολουθεί την πορεία της υγείας του μέσω ενός προφίλ φυσικής κατάστασης που είναι διαθέσιμο στο διακομιστή. Χρησιμοποιώντας το βασικό Kali Linux η Pen Test Partners πραγματοποίησε επίθεση τύπου MITM στη συσκευή. Εγκατέστησε έναν διακομιστή πρωτοκόλλου διαμόρφωσης δυναμικού κεντρικού υπολογιστή χρησιμοποιώντας το βοηθητικό πρόγραμμα dnsmasq, για την εκχώρηση έγκυρης IP διεύθυνση στη συσκευή. Στη συνέχεια έστησε πίνακες IP και μια εικονική μηχανή που προωθεί πακέτα IP πάνω από τη διεπαφή wlan0. Επίσης έστησε hostapd ως εικονικό WAP και κατέγραψε τη συσκευή σε αυτό. Χρησιμοποιώντας το Wireshark μπορεί να ανιχνεύσει τα πακέτα δεδομένων που μεταδίδονται από τη συσκευή. Στο παρακάτω διάγραμμα βλέπουμε τα βήματα της επίθεσης.



Εικόνα 27. Διάγραμμα επίθεσης MITM

Πηγή: https://ieeexplore.ieee.org/document/8977812

Αυτή η περίπτωση αποτελεί ένα ακόμη παράδειγμα πως υπάρχουν κακώς διαμορφωμένες συσκευές IoT που μπορούν να αποκαλύψουν ευαίσθητες πληροφορίες μέσω του δικτύου που αποτελεί μέρος του συστήματος. Αν και οι πληροφορίες που διαρρέουν μέσω αυτής της επίθεσης δεν είναι ιδιαίτερα σημαντικές, ο εισβολέας μπορεί να βρει το αναγνωριστικό συνόλου υπηρεσιών δικτύου (SSID). Κατά συνέπεια, αυτό επιτρέπει στον εισβολέα να αποκτήσει πρόσβαση στο οικιακό δίκτυο των χρηστών, το οποίο μπορεί να αποτελέσει τη βάση εκτόξευσης νέων επιθέσεων.

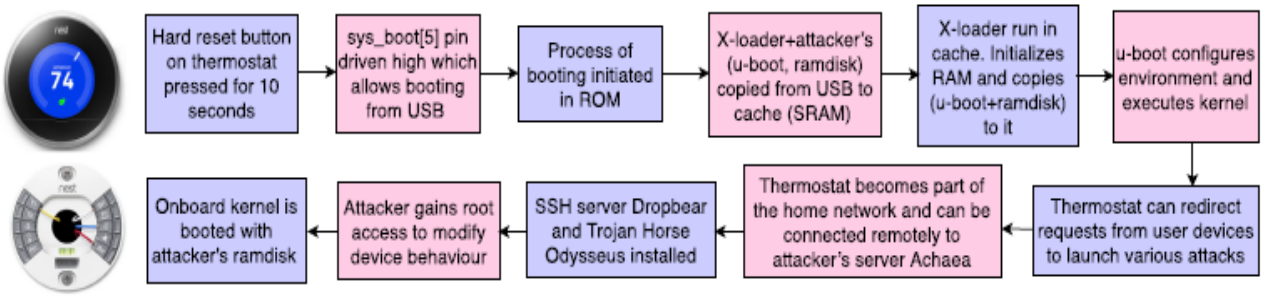
Αδυναμίες και μέτρα πρόληψης: Στην περίπτωση αυτή δεν υπάρχει κρυπτογραφημένο κανάλι επικοινωνίας μεταξύ του διακομιστή υποστήριξης και της συσκευής, επιτρέποντας επιθέσεις υποκλοπής. Με αυτόν τον τρόπο ο εισβολέας εμφανίζεται ως νόμιμη οντότητα και έχει πρόσβαση σε μη κρυπτογραφημένα δεδομένα που αποστέλλονται μέσω αυτού του οικιακού δικτύου, οδηγώντας σε πιθανή κλοπή προσωπικών πληροφοριών δικτύου. Συμβατικές τεχνικές κρυπτογράφησης δεδομένων που έχουν σχεδιαστεί για την ασφάλεια δικτύου γενικά δεν είναι αρκετά εύκολο να εφαρμοστούν σε συσκευές IoT με περιορισμένη μνήμη. Αυτό απαιτεί σχεδιασμό τεχνικών κρυπτογράφησης ειδικά σχεδιασμένο στα χαρακτηριστικά του IoT. Ακόμη και στις συσκευές χωρίς ιδιαίτερες ανάγκες κρυπτογράφησης, εφαρμόζοντας κρυπτογραφημένη επικοινωνία διασφαλίζεται το απόρρητο για άλλες οντότητες που αποτελούν μέρος του δικτύου.

5.2.4 Κακόβουλη εισβολή κώδικα

Αυτή είναι μια περίπτωση επίθεσης όπου η συσκευή IoT παραβιάζεται από την εισβολή κακόβουλου κώδικα μέσω εκτεθειμένου και μη ασφαλούς συνδεδεμένου λογισμικού που υπάρχει σε αυτήν. Όπως βλέπουμε στην επίθεση με στόχο τον έξυπνο θερμοστάτη της Google αποδείχθηκαν τα ευπαθή σημεία στη λειτουργία αυτής της συσκευής.

Επίθεση και συνέπειες: Πατώντας το κουμπί της ολικής επαναφοράς, θέτεται ο θερμοστάτης σε λειτουργία ενημέρωσης του υλικολογισμικού της συσκευής που δίνει τη δυνατότητα εκκίνησης από ένα USB stick που έχει τοποθετηθεί σε αντίστοιχη θήρα USB.

Αυτή τη λειτουργία εκμεταλλεύονται οι επιτιθέμενοι και εξασφαλίζουν πρόσβαση στη συσκευή. Αφού εξασφαλίσουν την πρόσβαση στη συσκευή εισάγουν το κακόβουλο λογισμικό Odysseus bypassing και γίνεται μέρος του οικιακού δικτύου. Ο θερμοστάτης λειτουργεί πλέον ως botnet για τον έλεγχο του συνόλου του οικιακού δικτύου. Στην παρακάτω εικόνα βλέπουμε τις δύο όψεις του θερμοστάτη και το διάγραμμα ροής της επίθεσης. Οι γενικότερες συνέπειες περιλαμβάνουν τη δημιουργία προφίλ από άτομα που παρακολουθούν παράνομα και αποκτούν τη δυνατότητα να τραβούν φωτογραφίες ή βίντεο παραβιάζοντας τις κάμερες και άλλες συσκευές του δικτύου.



Εικόνα 28. Έξυπνος θερμοστάτης και διάγραμμα ροής επίθεσης

Πηγή: https://ieeexplore.ieee.org/document/8977812

Αδυναμίες και μέτρα πρόληψης: Γενικότερα στην διαδικασία εκκίνησης της συσκευής, ένας εισβολέας προσπαθεί να εισβάλει στην κανονική διαδικασία εκκίνησης της συσκευής εκμεταλλευόμενος οποιαδήποτε ευπάθειά της στη διαδικασία αυτή. Έτσι ο χρήστης θα πρέπει να είναι πολύ προσεκτικός στη διαδικασία εκκίνησης για να αντιληφθεί έγκαιρα οποιαδήποτε ύποπτη κίνηση. Επίσης, ο επιτιθέμενος μπορεί να εκμεταλλευτεί την εκκίνηση του θερμοστάτη από τη συσκευή USB. Ο εισβολέας θα μπορούσε να εγκαταστήσει περαιτέρω κακόβουλο λογισμικό στη συσκευή αποκτώντας απομακρυσμένη πρόσβαση στη συσκευή και είσοδο στο οικιακό δίκτυο. Ένας τρόπος να αντιμετωπιστούν τέτοια φαινόμενα είναι να υπάρξουν επαρκείς μηχανισμοί ελέγχου ταυτότητας από το στάδιο της αρχικής εκτέλεσης του κώδικα. Αυτό απαιτεί την αντικατάσταση στους ενσωματωμένους επεξεργαστές με προσαρμοσμένο υλικό για να ενισχύσει την ασφαλή εκκίνηση της συσκευής. Επίσης πρακτικές για την προστασία των τελικών σημείων API όπως για παράδειγμα είναι η επικύρωση εισόδου, το φιλτράρισμα διεύθυνσης IP κ.α. μπορούν να εμποδίσουν τέτοιες επιθέσεις.

5.2.5 Μη εξουσιοδοτημένη πρόσβαση

Ένας εισβολέας μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή μία συσκευή IoT με πολλούς διαφορετικούς τρόπους που κυμαίνονται από την εκμετάλλευση τρωτών σημείων υλικού/λογισμικού σε παράνομες απόπειρες σύνδεσης. Η ακόλουθη μελέτη περίπτωσης για το Tesla Model S περιγράφει τον τρόπο που πραγματοποιείται μια τέτοια επίθεση.

Επίθεση και συνέπειες: Τα κέντρα εξυπηρέτησης Tesla και οι σταθμοί φόρτισης είναι εξοπλισμένοι με TeslaService WiFi SSID. Τα διαπιστευτήρια για την πρόσβαση αποθηκεύονται στο OtCarBrowser (ιστός της Tesla πρόγραμμα περιήγησης) ως μέρος της δυνατότητας αυτόματης σύνδεση. Πλαστογραφώντας αυτό το SSID, οι εισβολείς ανακατεύθυναν την κυκλοφορία από το πρόγραμμα περιήγησης στον τομέα τους. Το πρόγραμμα περιήγησης της Tesla βρέθηκε να περιέχει έναν αριθμό σφαλμάτων λογισμικού, τα οποία εκμεταλλεύτηκαν οι εισβολείς για να πραγματοποιήσουν την επίθεσή τους. Το Gateway είναι μία από τις μονάδες ελέγχου ECU που υπάρχουν στο εσωτερικό του οχήματος και είναι υπεύθυνη για τη μετάδοση των εντολών ελέγχου σε άλλες μονάδες ECU. Οι εισβολείς παρέκαμψαν το υλικολογισμικό Gateway και προγραμμάτισαν το προσαρμοσμένο υλικολογισμικό τους. Ευφυή και συνδεδεμένα οχήματα (ICV) όπως το Tesla Model S είναι εξοπλισμένα με ασύρματη επικοινωνία και τεχνολογίες που επιτρέπουν στα οχήματα να επικοινωνούν μεταξύ τους.

Αδυναμίες και μέτρα πρόληψης: Αρκετά τρωτά σημεία ασφαλείας ανακαλύφθηκαν στο Tesla Model S, τα οποία επέτρεψαν στον εισβολέα να χειριστεί εξ αποστάσεως το όχημα σε κατάσταση αναμονής αλλά και σε κατάσταση οδήγησης. Η μονάδα AppArmor μπορεί να ενισχυθεί με τέτοιο τρόπο έτσι ώστε να μην επιτρέπει διαρροές διεύθυνσης και με υποχρεωτικούς ελέγχους οι φάκελοι μπορούν να γίνουν απρόσιτοι στο πρόγραμμα περιήγησης με αυστηρούς κανόνες πρόσβασης. Επίσης μια αναβάθμιση σε νεότερη έκδοση Linux που χρησιμοποιεί η Tesla θα βελτιώσει αρκετά το θέμα της ασφάλειας. Οι κατασκευαστές συσκευών IoT πρέπει να διασφαλίσουν συσκευές χωρίς συνεχή σύνδεση στο Διαδίκτυο με τακτικές ενημερώσεις και επιδιορθώσεις γνωστών σφαλμάτων ασφαλείας, είτε μέσω ασφαλούς ενημέρωσης over-the-air (OTA) ή μέσω άλλων εναλλακτικών μηχανισμών. Αντί να χρησιμοποιείται ένα σταθερό κλειδί ασφαλείας, μπορεί με τη χρήση γεννήτριας τυχαίων αριθμών να εισάγονται διαφορετικά κλειδιά ασφαλείας ανά συνεδρία. Έτσι περιορίζονται οι μη εξουσιοδοτημένες είσοδοι σε οποιοδήποτε IoT υλικολογισμικό της συσκευής.

5.2.6 Επίθεση κοινωνικής μηχανικής

Εξάγοντας τις προσωπικές πληροφορίες των χρηστών, ο εισβολέας αποκτά πρόσβαση στα προφίλ των χρηστών στο οικιακό δίκτυο. Στη μελέτη περίπτωσης που ακολουθεί παρουσιάζεται η επίθεση σε έξυπνο σύστημα ανοίγματος γκαραζόπορτας.

Επίθεση και συνέπειες: Έχει αποδειχθεί ότι οι ευπάθειες των έξυπνων οικιακών συσκευών μπορούν να δώσουν τη δυνατότητα σε επιτήδειους να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα και να αποκτήσουν τον έλεγχο σε κλειδαριές θυρών και σε διάφορους αισθητήρες. Μετά από τη πρόσβαση στον λογαριασμό του χρήστη ο εισβολέας δεν είναι μόνο σε θέση να διαβάσει την κατάσταση της πόρτας πχ ανοιχτή ή κλειστή αλλά ακόμη και να την ανοίξει ή και να τη κλείσει. Ο εισβολέας μπορεί επίσης να προσθέσει κανόνες που να τον ειδοποιούν μέσω email όταν αλλάζει η κατάσταση της

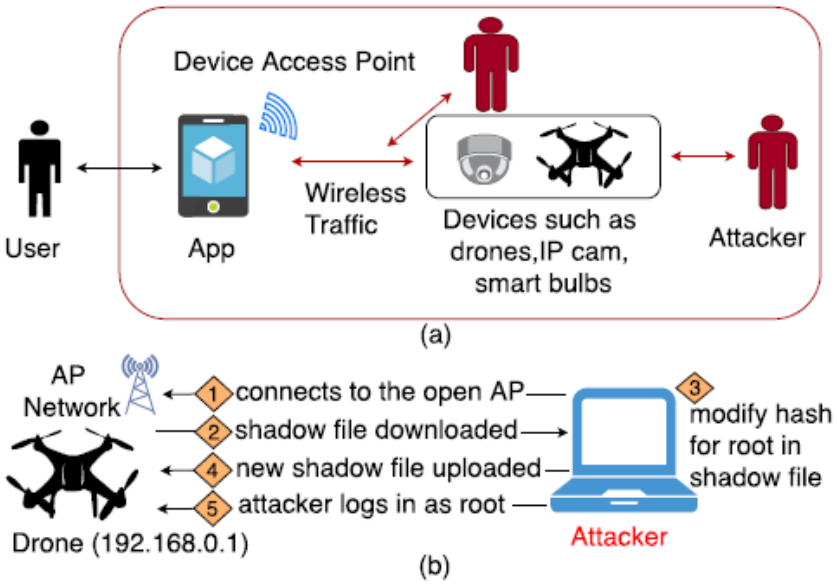
πόρτας. Ο επιτιθέμενος μπορεί επίσης να παρακολουθεί τα προφίλ των ενοίκων του σπιτιού και να μελετά τα ιστορικά στοιχεία χρήσης της γκαραζόπορτας.

Αδυναμίες και μέτρα πρόληψης: Έχοντας ισχυρούς κωδικούς πρόσβασης, μειώνονται σημαντικά οι πιθανότητες εισβολής στο σύστημα. Επίσης σημαντικές πληροφορίες, συμπεριλαμβανομένων και των διαπιστευτηρίων ελέγχου ταυτότητας και τα διακριτικά της συνεδρίας μπορούν να κλαπούν. Ουσιαστικά η ισχυρή προστασία με κωδικό πρόσβασης είναι το πρώτο και σημαντικότερο βήμα για την ασφάλεια της συσκευής IoT και των προσωπικών δεδομένων του κάθε χρήστη που έχει νόμιμη πρόσβαση στη συσκευή. Για την επιπλέον ενίσχυση της ασφάλειας μπορεί να χρησιμοποιηθεί μηχανισμός ελέγχου ταυτότητας.

5.2.7 Εκμετάλλευση υλικού συσκευών

Ανοιχτές θύρες και μη προστατευμένες διεπαφές υλικού αφήνονται ως κενά ασφαλείας από τους κατασκευαστές των συσκευών IoT και αποτελούν εύκολους στόχους για τους επιτιθέμενους που αποκτούν τον έλεγχο αυτών των συσκευών. Σε αυτού του είδους την επίθεση θα δούμε την επίθεση σε ένα drone Parrot AR 2.0 Quadcopter.

Επίθεση και συνέπειες: Σε ένα πρόσφατο πείραμα από ερευνητές κάνοντας σάρωση σε ένα δίκτυο Linux ανοιχτού κώδικα. Το βοηθητικό πρόγραμμα Mapper αποκάλυψε ανοιχτές θύρες στο drone (π.χ. πρωτόκολλο μεταφοράς αρχείων θύρας 21(FTP) και θύρα 23-Telnet). Τέτοιες πληροφορίες μπορούν να αξιοποιηθούν με σκοπό τη διεξαγωγή επιθέσεων στις συσκευές όπως φαίνεται και στο παρακάτω σχήμα.



Εικόνα 29. Επίθεση σε Drone

Πηγή: https://ieeexplore.ieee.org/document/8977812

Χρησιμοποιώντας μια συμβατή εφαρμογή για κινητά μπορεί κάποιος να συνδεθεί στη συσκευή – στόχο μέσω του ανοιχτού σημείου πρόσβασης (AP) μέσω κακόβουλου

FTP. Τα αρχεία μπορούν στη συνέχεια να φορτωθούν στο σύστημα αρχείων του εισβολέα ή μπορεί να πραγματοποιηθεί επιβλαβής ενημέρωση υλικολογισμικού, καθιστώντας το drone μη λειτουργικό. Χρησιμοποιώντας μια ανώνυμη σύνδεση FTP ο εισβολέας μπορεί να κατεβάσει τον κωδικό πρόσβασης και να τον μεταβάλλει. Ένα συμβατικό drone μπορεί να μεταδίδει ζωντανά παράνομα βίντεο από τη γύρω περιοχή, έτσι καταπατούνται προσωπικά δεδομένα των χρηστών. Επίσης ένας εισβολέας μπορεί από απόσταση να απενεργοποιήσει και να καταρρίψει ένα ιπτάμενο drone με κακούς σκοπούς.

Αδυναμίες και μέτρα πρόληψης: Τα AP των drone διατηρούνται ως επί το πλείστον ανοιχτά, και ως εκ τούτου είναι επιρρεπή σε επιθέσεις hacking. Τέτοιου είδους AP πρέπει να αναβαθμιστεί σε τεχνολογία WPA2 και να προστατεύεται χρησιμοποιώντας ισχυρούς κωδικούς πρόσβασης, επιτρέποντας μόνο περιορισμένο αριθμό εγγεγραμμένων χρηστών για σύνδεση με αυτούς. Εάν οι θύρες βοηθητικού δικτύου είναι όπως το FTP και το Telnet στο drone τότε θα είναι πάντα εκτεθειμένα και ευάλωτα σε επιθέσεις. Διεπαφές υλικού, όπως δράση κοινής δοκιμής, ομάδα (JTAG), γενικός σειριακός δίαυλος (USB) και οι σειριακές θύρες, χρησιμοποιούνται συνήθως από κατασκευαστές συσκευών IoT για να διευκολύνουν τον επακόλουθο εντοπισμό σφαλμάτων και την υποστήριξη υπηρεσιών. Ωστόσο, αυτές οι διεπαφές είναι ένα δίκοπο μαχαίρι, διότι μπορούν να χρησιμοποιηθούν και για κακόβουλες δραστηριότητες. Ως εκ τούτου, οι κατασκευαστές θα πρέπει να διασφαλίσουν το ενδεχόμενο ότι αυτές οι διεπαφές έχουν περιορισμούς πρόσβασης και είναι κατάλληλα ασφαλισμένες. Τα νεότερα προϊόντα θα πρέπει να σχεδιάζονται με διεπαφές τηρώντας τα τρέχοντα βιομηχανικά πρότυπα, κατά τη σταδιακή κατάργηση προϊόντων με παρωχημένες διεπαφές.

5.2.8 Εισαγωγή κακόβουλου κόμβου

Σε αυτού του είδους την επίθεση ένα bot λογισμικό – κακόβουλου κόμβου εισάγεται στο δίκτυο δημιουργώντας μια ψεύτικη ταυτότητα ενός γνήσιου κόμβου με σκοπό την πλαστοπροσωπία. Παρακάτω θα περιγράψουμε ένα σχετικά πρόσφατο χακαρισμένο σύστημα κάμερας (IP Edimax).

Επίθεση και συνέπειες: Αυτό το σύστημα κάμερας αποτελείται από τρία διαφορετικά στοιχεία, την IP κάμερα, το χειριστήριο που είναι ουσιαστικά μια εφαρμογή κινητού που επικοινωνεί με την κάμερα και τον διακομιστή αναμετάδοσης εντολών. Κάθε κάμερα πρέπει να εγγραφεί στο διακομιστή του δικτύου πριν γίνει μέρος του. Η επίθεση ξεκινά από μια δημόσια συσκευή IoT που έχει ήδη μολυνθεί από το κακόβουλο λογισμικό (π.χ.Mirai) που λειτουργεί ως bot λογισμικού και επεκτείνεται και στις υπόλοιπες συσκευές του δικτύου.

Επίθεση και συνέπειες: Οι πρώτοι έξι χαρακτήρες στη διεύθυνση MAC των 12 χαρακτήρων υποδεικνύει τον κατασκευαστή και μπορεί με ευκολία να προβλεφτεί. Ο επιτιθέμενος χρησιμοποιεί δυναμική επίθεση και προσπαθεί να βρει τον κωδικό πρόσβασης της κάμερας. Σε αυτό το σύστημα χρησιμοποιείται το σχήμα Base64 για την

κωδικοποίηση πληροφοριών ελέγχου ταυτότητας, ο εισβολέας μπορεί εύκολα να ανακαλύψει τον κωδικό πρόσβασης. Διότι δεν χρησιμοποιείται μυστικό κλειδί σε αυτό το σχήμα, και έτσι ο οποιοσδήποτε γνωρίζει τις λειτουργίες κωδικοποίησης Base64 μπορεί να το χακάρει. Υπάρχει μια διαρκώς αυξανόμενη ανάγκη για ταυτοποίηση μεταξύ των συσκευών IoT. Μια ισχυρή συμμετρική κρυπτογράφηση κλειδιού μπορεί να χρησιμοποιηθεί ως τεχνική ασφαλείας, μόνο όπου ο διακομιστής και η αρχική συσκευή γνωστοποιούν το κοινόχρηστο μυστικό κλειδί.

5.3 Οι συσκευές IoT με τις περισσότερες παραβιάσεις στα έξυπνα σπίτια

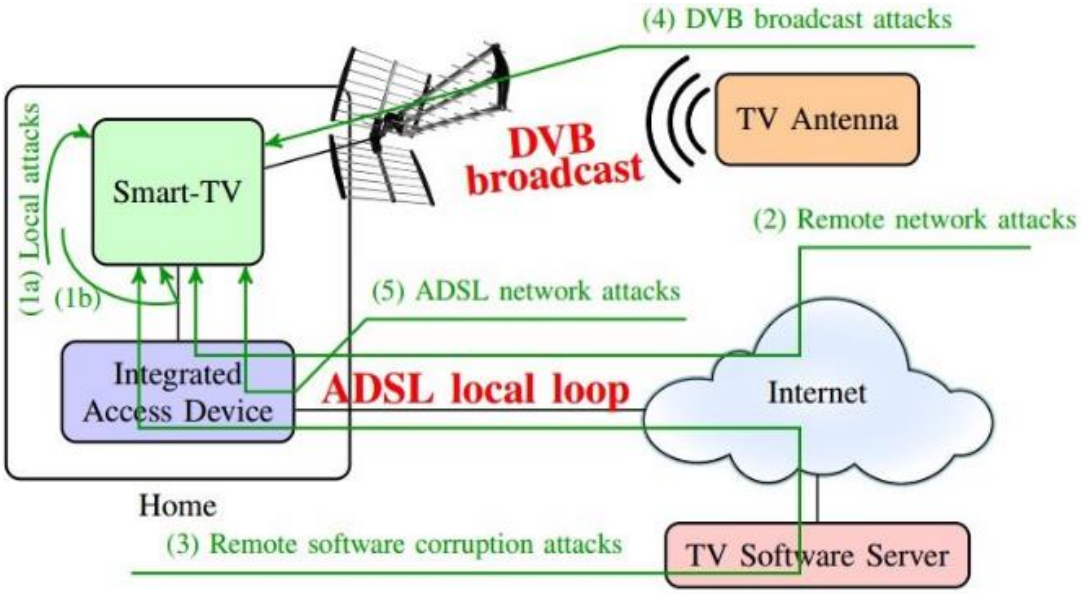
Σύμφωνα με την εταιρεία Avira [42] οι δύο έξυπνες συσκευές με τις περισσότερες παραβιάσεις τα τελευταία χρόνια είναι οι έξυπνες τηλεοράσεις και τα έξυπνα οικιακά ηχεία. Τα περισσότερα έξυπνα σπίτια διαθέτουν ολοκληρωμένα συστήματα ψυχαγωγίας τα οποία είναι συνδεδεμένα σε δίκτυο Wi-Fi παράλληλα με άλλες συσκευές που αφορούν την ασφάλεια και γενικότερα την καθημερινή λειτουργία του σπιτιού. Σύμφωνα με την γερμανική εταιρεία Statista ο ρυθμός αύξησης των συνδεδεμένων κατοικιών είναι 12 % κάθε χρόνο και το ποσοστό έξυπνων σπιτιών στις ΗΠΑ αναμένεται να αγγίξει το 53,5 % έως το 2023 σε σχέση με το 33,2 % που ήταν το 2021. Στις ΗΠΑ υπάρχουν περίπου 42,2 εκατομμύρια έξυπνα σπίτια.

5.3.1 Επιθέσεις σε έξυπνες τηλεοράσεις

Στα πλαίσια την πανδημίας του covid 19, ενώ τα μέτρα που λήφθηκαν εμπόδισαν τις εταιρείες να έχουν άμεση επαφή και επικοινωνία με τους καταναλωτές και τους λάτρεις της τεχνολογίας, η ανάπτυξη και η εξέλιξη της τεχνολογίας θα λέγαμε ότι επιταχύνθηκε. Οι εταιρείες εργάστηκαν με έντονο ρυθμό για να καλύψουν τις αυξημένες ανάγκες των καταναλωτών που προέκυψαν λόγω του μεγάλου διαστήματος που χρειάστηκε να μείνουν στο σπίτι τους. Παρά το γεγονός ότι οι έξυπνες τηλεοράσεις αναπτύχθηκαν και προωθήθηκαν ιδιαίτερα τα προηγούμενα χρόνια, στην περίοδο της πανδημίας οι πωλήσεις τους ξεπέρασαν κατά πάρα πολύ το προσδοκώμενο. Οι εταιρείες προώθησης και παραγωγής τους προσπάθησαν με κάθε τρόπο την τελευταία περίοδο να εξελίξουν και να διαφοροποιήσουν τα προϊόντα τους.

Η τεχνολογία που υπάρχει πίσω από την επόμενη γενιά έξυπνων οικιακών συσκευών είναι ιδιαίτερα εντυπωσιακή, ωστόσο δεν πρέπει να ξεχνάμε ότι η νέες τεχνολογίες φέρνουν επίσης νέες προκλήσεις και πιθανούς κινδύνους για την ασφάλεια στο διαδίκτυο και γενικότερα στο κυβερνοχώρο. Κατά γενικό κανόνα κάθε συσκευή που έχει τη δυνατότητα να συνδεθεί στο διαδίκτυο, διατρέχει το κίνδυνο να παραβιαστεί ακόμη και η πιο απλή οικιακή συσκευή. Έτσι και οι έξυπνες τηλεοράσεις οι οποίες διαθέτουν ενσωματωμένα προγράμματα περιήγησης τα οποία αποτελούν σε πολλές περιπτώσεις μια πύλη για να εισβάλει το κακόβουλο λογισμικό που συνήθως διαδίδεται στο διαδίκτυο.

Στην παρακάτω εικόνα [44] περιγράφεται διαγραμματικά πως η Smart TV μπορεί να δεχθεί επίθεση με διαφορετικούς τρόπους από διαφορετικά μονοπάτια. Και αριθμούνται τα ευάλωτα σημεία που υπάρχουν.



Εικόνα 30. Ευπάθειες δικτύου Smart TV Home

Πηγή: https://www.researchgate.net/publication/320044280_Detection_and_Prevention_of_Non-PC_Botnets

1) Οι προεπιλεγμένοι κωδικοί πρόσβασης μέσω των οποίων έχουν πραγματοποιηθεί αρκετές από τις επιθέσεις σε IoT.

2) Ο τοπικός βρόχος, οι περισσότερες επιθέσεις Smart TV ή επιθέσεις σε άλλες συνδεδεμένες συσκευές συμβαίνουν λόγω της ευπάθειας του τοπικού βρόχου στην οποία η γραμμή κόβεται φυσικά και το νέο ADSL και το DSLAM εγκαθίστανται στο δίκτυο. Η επίθεση που γίνεται έμμεσα με χρήση κατεστραμμένων υλικολογισμικών ή κακόβουλων εφαρμογών είναι πιο συνηθισμένη, καθώς η Smart TV έχει παρόμοιες μεθόδους επίθεσης με αυτές που γίνονται και σε προσωπικούς υπολογιστές. Όπως φαίνεται από την εικόνα, οι τοπικοί βρόχοι ADSL μπορεί να είναι επικίνδυνοι καθώς ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στην Smart TV και να θέσει σε κίνδυνο το απόρρητό της ή ακόμη και να εγκαταστήσει κακόβουλο λογισμικό.

3) Το πρωτόκολλο UPnP, αυτό το πρωτόκολλο χρησιμοποιείται για να ειδοποιεί, ανακαλύπτει και να ελέγχει συσκευές. Αυτό το πρωτόκολλο είναι ανεξάρτητο από οποιοδήποτε λειτουργικό σύστημα και γλώσσες προγραμματισμού. Υπάρχει σε κάθε συσκευή δικτύου, κάτι που βοηθά στην ομαλή ανακάλυψη άλλων συσκευών στο δίκτυο. Χρησιμοποιείται για σύνδεση δικτύου, κοινή χρήση δεδομένων κ.λπ. Έπειτα από έρευνα που έγινε, διαπιστώθηκε ότι το πρωτόκολλο ήταν ευάλωτο στη διαδικασία

εκτέλεσης απομακρυσμένου κώδικα και σε άλλα σημεία που αφορούν στο πρωτόκολλο.

4) Η Θύρα 7547, οι κατασκευές των δρομολογητών Zyxel - speedportetc αφήνουν τη θύρα TCP ανοιχτή στο εξωτερικό δίκτυο, αυτό σημαίνει πως είναι ευάλωτη σε επιθέσεις με βάση τα TR-064 και TR-069 protocol. Αυτό συμβαίνει συνήθως σε δρομολογητές που χρησιμοποιούν CWMP (πρωτόκολλο που βασίζεται σε κείμενο). Η θύρα 7547 χρησιμοποιείται για την παροχή επικοινωνίας μεταξύ εξοπλισμού χώρων πελατών και διακομιστών που μπορούν να ρυθμιστούν αυτόματα. Αναγνωρίστηκε για πρώτη φορά από το ιστολόγιο Reverse Engineering το οποίο βρήκε ότι τα μόντεμ ERID 1000 ήταν ευάλωτα. Το ελάττωμα έχει διαπιστωθεί στην επιλογή απομακρυσμένης διαχείρισης που είναι ενεργοποιημένη και η όψη προς το Διαδίκτυο είναι ευάλωτη σε hacks. Ακόμη, οποιοσδήποτε μπορεί να έχει πρόσβαση στους δρομολογητές Netgear μπορεί να το μετατρέψει σε πιθανά botnets.

5) Η ευπάθεια IP κάμερας, ανακαλύφθηκε ότι υπάρχει ευπάθεια στις κάμερες συσκευών IoT που έχουν ενεργοποιημένες IP από εταιρείες όπως Forscam, Vstarcam κ.λπ. Η αδυναμία υπάρχει στο διακομιστή web goahead που χρησιμοποιείται από τις αναφερόμενες εταιρείες. Ουσιαστικά επιτρέπει σε έναν εισβολέα να δημιουργήσει παραμορφωμένο αίτημα HTTP το οποίο θα δώσει πρόσβαση στη συνδιάλεξη μέσω αρχείου με κωδικό πρόσβασης σύνδεσης.

Το 2016 οι τηλεοράσεις Android της LG επηρεάστηκαν από μια έκδοση του ransomware Cyber.Police (FLocker) ή αλλιώς γνωστό και ως Frantic Locker ή Dogspectus. Η επίθεση αρχικά έγινε σε μία από τις τελευταίες γενιές έξυπνων τηλεοράσεων LG που διέθεταν το Google TV, μια πλατφόρμα έξυπνης τηλεόρασης που αναπτύχθηκε από τη Google μαζί με την Intel, τη Sony και τη Logitech. Στη συνέχεια το 2018 το σκουλήκι ADB.Miner στόχευσε έξυπνες τηλεοράσεις που βασίζονται σε Android και τις κατέλαβε με στόχο την πληρωμή των χάκερς με κρυπτονομίσματα. Οι χρήστες που κατεβάζουν λογισμικό μέσα από ανεπίσημες πηγές εκτίθενται σε ακόμη περισσότερους κινδύνους. Επιπρόσθετα, η ενσωματωμένη κάμερα και το μικρόφωνο κινδυνεύουν να χρησιμοποιηθούν από τους κυβερνοεγκληματίες για κατασκοπεία χρηστών.

5.3.2 Επιθέσεις σε έξυπνα οικιακά ηχεία

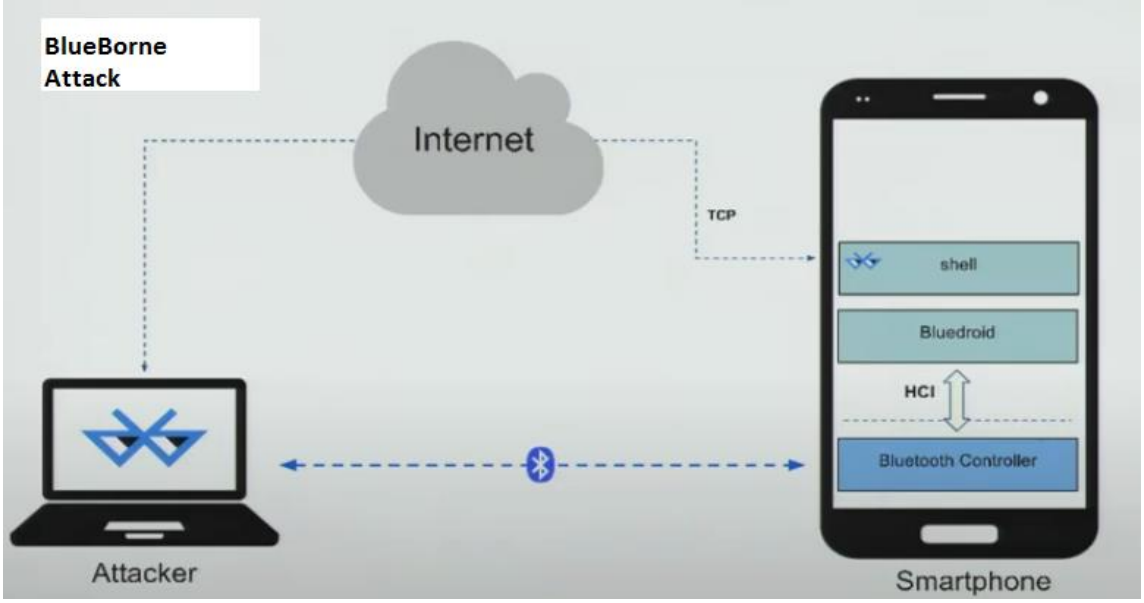
Σε μία άλλη περίπτωση έχουμε επίθεση σε έξυπνα οικιακά ηχεία όπως το Amazon Echo ή το Google Home τα οποία ενέχουν πολλούς κινδύνους για την ασφάλεια και το απόρρητο. Από ευπάθειες ασφαλείας που εκμεταλλεύονται τη σύνδεση Bluetooth, όπως το BlueBorne, μέχρι και κακόβουλα λογισμικά ενσωματωμένα σε εφαρμογές. Οι εγκληματίες του κυβερνοχώρου μπορούν να εκμεταλλευτούν τις ευπάθειες στα πρωτόκολλα επικοινωνίας, στις διεπαφές και τις εφαρμογές ιστού ή στο υλικολογισμικό.

Εικόνα 31. Νέα μορφή επίθεσης σε συνδεδεμένες συσκευές BlueBorne

Πηγή: https://www.secnews.gr/165906/blueborne-lenovo-argoporhmenh-kukloforia/

Το BlueBorne [43] απειλεί μεγάλα λειτουργικά συστήματα κινητών, επιτραπέζιων υπολογιστών και συσκευών IoT, συμπεριλαμβανομένων των Android, iOS, Windows και Linux, και των συσκευών που τα χρησιμοποιούν. Το BlueBorne μπορεί να εξαπλωθεί μέσω του αέρα και να επιτεθεί σε συσκευές μέσω Bluetooth. Επιτρέπει στους εισβολείς να αναλαμβάνουν τον έλεγχο της συσκευής, να έχουν πρόσβαση σε εταιρικά δεδομένα και δίκτυα και να διαδίδουν κακόβουλο λογισμικό πλευρικά σε γειτονικές συσκευές. Τέτοιου είδους επιθέσεις μπορούν να χρησιμοποιηθούν για τη διεξαγωγή μεγάλου εύρους επιθέσεων, συμπεριλαμβανομένης της απομακρυσμένης εκτέλεσης κώδικα καθώς και των επιθέσεων Man-in-The-Middle.

Η συγκεκριμένη μέθοδος επίθεσης έχει πολλές προεκτάσεις που μπορούν να έχουν καταστροφικό αποτέλεσμα όταν συνδυαστούν. Μεταδιδόμενο στον αέρα το BlueBorne στοχεύει το πιο αδύναμο σημείο στην άμυνα των δικτύων και ιδιαίτερα το σημείο που κανένα μέτρο ασφαλείας δεν προστατεύει. Η εξάπλωση από συσκευή σε συσκευή μέσω του αέρα το καθιστά ιδιαίτερα μολυσματικό. Επιπρόσθετα, δεδομένου ότι η διαδικασία Bluetooth έχει υψηλά προνόμια σε όλα τα λειτουργικά συστήματα, η εκμετάλλευσή της παρέχει ουσιαστικά πλήρη έλεγχο της συσκευής.



Εικόνα 32. Επίθεση BlueBorne

Πηγή: https://www.youtube.com/watch?v=NBAqzGtz9ts

Όλες αυτές οι δυνατότητες είναι εξαιρετικά χρήσιμες στους χάκερς, το BlueBorne μπορεί να χρησιμοποιηθεί για κατασκοπεία στο κυβερνοχώρο, κλοπή δεδομένων, ransomware, ακόμη και δημιουργία μεγάλων botnets από συσκευές IoT όπως το γνωστό Mirai Botnet. Αυτή η μέθοδος επίθεσης ξεπερνά τις δυνατότητες των άλλων ειδών επιθέσεων διότι διεισδύει σε ασφαλή δίκτυα που είναι αποσυνδεδεμένα από οποιοδήποτε άλλο δίκτυο ακόμη και από το διαδίκτυο.

Τέλος, σε αντίθεση με τα παραδοσιακά κακόβουλα προγράμματα ή επιθέσεις, ο χρήστης δεν χρειάζεται να κάνει κλικ σε έναν σύνδεσμο ούτε να κατεβάσει ένα αμφισβητούμενο αρχείο. Η επίθεση BlueBorne δεν απαιτεί αλληλεπίδραση με τον χρήστη, είναι συμβατή με όλες τις εκδόσεις λογισμικού και δεν απαιτεί προϋποθέσεις ή διαμορφώσεις εκτός από το να είναι ενεργό το Bluetooth. Σε αντίθεση με την κοινή παρανόηση, οι συσκευές με δυνατότητα Bluetooth αναζητούν συνεχώς εισερχόμενες συνδέσεις από οποιεσδήποτε συσκευές, και όχι μόνο από αυτές με τις οποίες έχουν γίνει σύζευξη. Αυτό σημαίνει ότι μια σύνδεση Bluetooth μπορεί να δημιουργηθεί χωρίς καθόλου σύζευξη των συσκευών. Αυτό καθιστά το BlueBorne μία από τις πιο ευρείες πιθανές επιθέσεις που έχουν βρεθεί τα τελευταία χρόνια και επιτρέπει σε έναν εισβολέα να χτυπήσει εντελώς απαρατήρητα.

Επίσης οι ερευνητές του Check Point κατάφεραν να χακάρουν το Amazon Alexa, την τεχνητή νοημοσύνη που τροφοδοτεί τη μεγάλη γκάμα έξυπνων οικιακών ηχείων της Amazon. Στέλνοντας έναν κακόβουλο σύνδεσμο σε έναν χρήστη – στόχο, οι ερευνητές κατάφεραν να έχουν πρόσβαση σε όλες τις προσωπικές πληροφορίες της συσκευής, συμπεριλαμβανομένων των τραπεζικών δεδομένων, να εξαγάγουν το ιστορικό

φωνητικής αναζήτησης και να κάνουν αλλαγές στις λειτουργίες της συσκευής. Αυτό κατέστη δυνατό με την εκμετάλλευση ευπαθειών σε ορισμένους υποτομείς Amazon Alexa που ήταν επιρρεπείς σε εσφαλμένη ρύθμιση παραμέτρων κοινής χρήσης πόρων μεταξύ προέλευσης (CORS) και σε δέσμες ενεργειών μεταξύ τοποθεσιών (XSS).

5.4 Επίθεση από χάκερς σε λαμπτήρες της εταιρείας Philips

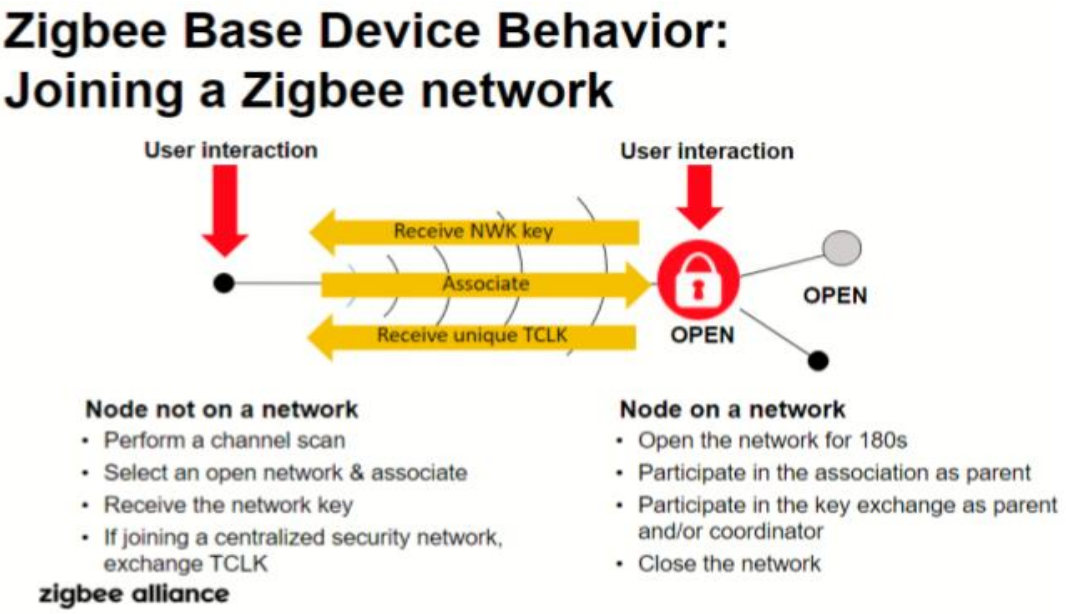
Έχει γίνει ευρέως γνωστό πως οι έξυπνοι λαμπτήρες της σειράς Hue της δημοφιλούς εταιρείας Philips έχουν παραβιαστεί από χάκερς οι οποίοι εκμεταλλεύτηκαν κενά ασφαλείας στο σύστημα τους. Οι έξυπνοι λαμπτήρες Philips Hue IoT [45] είναι ασύρματες συσκευές που έχουν σχεδιαστεί για να δημιουργούν ατμοσφαιρικό φωτισμό, και ενεργοποιείται με τη χρήση Bluetooth, ενεργοποιείται ως γέφυρα και λειτουργεί με την ασύρματη τεχνολογία Zigbee light link. Η συσκευή επίσης έχει τη δυνατότητα να ελέγχεται από εφαρμογές που επιτρέπουν φωνητικές εντολές, και λειτουργίες συγχρονισμού με πολυμέσα.

Εικόνα 33. Έξυπνοι λαμπτήρες Philips Hue

Πηγή: https://www.philips-hue.com/el-gr#lights_and_accessories

Για το χειρισμό ενός έξυπνου λαμπτήρα Philips Hue, ένας χρήστης μπορεί να επιλέξει μέσα από πολλές εφαρμογές για κινητές συσκευές που βρίσκονται σε διάφορα καταστήματα εφαρμογών όπως είναι το Google Play Store. Υποθετικά, ένας χρήστης θα πραγματοποιήσει λήψη εγκατάσταση και εκτέλεση της συμβατής συσκευής ελέγχου. Με όλη αυτή τη διαδικασία αρχίζει η εμπλοκή τρίτων πέρα από την επίσημη εταιρεία κατασκευής και ξεκινά μια ελεύθερη αδειοδότηση συμβατότητας του λογισμικού σε πλαίσια εμπιστοσύνης μεταξύ της εταιρείας και τρίτων διαμεσολαβητών. Αυτό δημιουργεί ένα τεράστιο κενό ασφαλείας που προκύπτει από τις εφαρμογές των τρίτων. Πρέπει να αναφέρουμε ότι ο έξυπνος λαμπτήρας μπορεί να συνδεθεί και να ελέγχεται μέσω Bluetooth και WiFi.

Ο έξυπνος λαμπτήρας ενεργοποιείται από το πρωτόκολλο Zigbee, το οποίο είναι ένα πρωτόκολλο επικοινωνίας μικρής εμβέλειας που βασίζεται στο Πρότυπο IEEE 203.15.4. το Zigbee χρησιμοποιείται σε συσκευές που μεταφέρουν δεδομένα σπάνια με χαμηλό ρυθμό σε περιορισμένη περιοχή σε εμβέλεια 10–100 m. «Το πρότυπο IEEE προσφέρει τη δυνατότητα να αναγνωρίζει μοναδικά κάθε συχνότητα σε ένα δίκτυο ως καθώς και τη μέθοδο και τη μορφή επικοινωνίας μεταξύ αυτών των ραδιοφώνων, αλλά δεν προσδιορίζει πέρα από ένα σύστημα σύζευξης επικοινωνιών, μια τοπολογία δικτύου, σχήματα δρομολόγησης ή μηχανισμοί ανάπτυξης και επιδιόρθωσης δικτύου.»



Εικόνα 34. Διάγραμμα λειτουργίας του Zigbee

Πηγή: https://www.researchgate.net/profile/Junibel-De-La-Cruz/publication/354674719_Philips_Hue_Bulb_IoT_App_Security/links/61458c70a595d06017d44988/Philips-Hue-Bulb-IoT-App-Security.pdf

Σε απόσταση πάνω από 100 μέτρα, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν την έλλειψη ελέγχου ταυτότητας του συστήματος Bluetooth, και ανιχνεύουν το δίκτυο και υποκλέπτουν τα χαρακτηριστικά της υπηρεσίας που μεταφέρονται από το χρήστη στον έξυπνο λαμπτήρα. Επίσης, η έλλειψη κρυπτογράφησης της υπηρεσίας Bluetooth επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε πληροφορίες και δεδομένα. Ως αποτέλεσμα αυτού ο εισβολέας μπορεί να πραγματοποιήσει μια επίθεση επανάληψης και να αποκτήσει πρόσβαση τόσο στη συσκευή όσο και στον χρήστη και να εκμεταλλευτεί περαιτέρω τις πληροφορίες της IP και της λειτουργίας της συσκευής. Ουσιαστικά ο εισβολέας μπορεί να αποκτήσει πρόσβαση στο σύστημα του οικιακού αυτοματισμού του χρήστη ή να εξαπολύσει επίθεση άρνησης υπηρεσίας σε διασυνδεδεμένες συσκευές.

Τέλος,[46] η ίδια η εταιρεία Philips στον επίσημο ιστότοπο της κάνει αναφορά σε θέματα ασφαλείας των προϊόντων Hue, και αναφέρει πως δεσμεύεται για την ασφάλεια των προϊόντων της. Επίσης αναφέρει πως διαθέτει σημαντικούς πόρους προκειμένου να εντοπίσει και να περιορίσει ευπάθειες στον τομέα της ασφάλειας. Ακόμη σημειώνει το γεγονός πως συνεργάζεται με ερευνητές στον τομέα της ασφάλειας και άλλους χρήστες για να διορθώνει και να ενημερώνει τυχόν ευπάθειες και ζητά από τους καταναλωτές της σε περίπτωση που έχουν εντοπίσει κάποια ευπάθεια να επικοινωνήσουν μέσω αντίστοιχου προγράμματος αποκάλυψης. Επιπλέον δίνει συμβουλές και οδηγίες προστασίας στους χρήστες με έμφαση να διατηρούν το σύστημα ενημερωμένο με την τελευταία έκδοση του λογισμικού και να πραγματοποιούν λήψη εφαρμογών μόνο από τα επίσημα καταστήματα εφαρμογών iOS και Android.

Συμπεράσματα

Ολοκληρώνοντας αυτή την εργασία, θα θέλαμε να αναφέρουμε συμπερασματικά το γεγονός πως ο τομέας της τεχνολογίας που σχετίζεται με το IoT είναι αναμφίβολα στο επίκεντρο των νέων δεδομένων της τεχνολογίας, επηρεάζοντας σημαντικά τόσο την επιχειρηματικότητα, την παγκόσμια οικονομία όσο και κοινωνικά ζητήματα αλλά και την καθημερινή ζωή. Η δυναμική του είναι τόσο μεγάλη που πέρα από τις συσκευές που χρησιμοποιούνται σε καθημερινά ζητήματα όπως τις οικιακές συσκευές ή τα συστήματα ασφαλείας, ψυχαγωγίας και πληθώρας άλλων παρόμοιων σε έξυπνα σπίτια ή κτίρια, βλέπουμε καθημερινά όλο και περισσότερες εφαρμογές ιδιαίτερα εξειδικευμένες να δίνουν λύσεις και να προσφέρουν καινοτομίες σε πάρα πολλούς τομείς όπως την ιατρική, τη γεωργία, τη βιομηχανία γενικότερα ακόμη και σε πολλά κοινωνικά ζητήματα κοινής ωφέλειας.

Ωστόσο, μελετώντας τεχνικά τη λειτουργία και την αρχιτεκτονική του IoT από την αρχή της δημιουργίας του έως και σήμερα, διαπιστώσαμε πως μαζί με την ραγδαία εξέλιξη του παρουσιάζονται ζητήματα τα οποία αφορούν ευαίσθητα θέματα όπως είναι η προστασία των προσωπικών δεδομένων και γενικότερα θέματα ασφάλειας. Μελετώντας περιπτώσεις κυβερνοεπιθέσεων όπως το Mirai Botnet που το 2016 προσέβαλε μαζικά αμέτρητες έξυπνες συσκευές IoT αλλά και πολλές άλλες περιπτώσεις που είχαν ως αποτέλεσμα υποκλοπές δεδομένων και οικονομικούς εκβιασμούς. Οι χάκερς συνήθως εκμεταλλεύονται κενά ασφαλείας των συστημάτων IoT και δημιουργούν όλο και περισσότερα προβλήματα στους χρήστες μέσω κυβερνοεπιθέσεων.

Βασιζόμενοι σε όλα τα παραπάνω που αναφέραμε, ως μελλοντική πρόταση επέκτασης της εργασίας, θεωρούμε ιδιαίτερα ενδιαφέρουσα την μελέτη και την έρευνα γύρω από τους μηχανισμούς ασφαλείας προστασίας σε θέματα κυβερνοεπιθέσεων απέναντι στη τεχνολογία του IoT. Η ανάπτυξη και ιδιαίτερα η αποτελεσματικότητα αυτών των μηχανισμών θεωρούμε πως είναι αναγκαία και θα πρέπει να συμβαδίζει με την ταχύτητα εξέλιξης του IoT με σκοπό να περιοριστούν όσο το δυνατόν περισσότερο οι κακόβουλες επιθέσεις. Ακόμη, θεωρούμε ιδιαίτερα σημαντικό να υπάρξει ολοκληρωμένη ενημέρωση γενικότερα στους χρήστες του IoT για τα κενά ασφαλείας που ενδεχομένως υπάρχουν σε κάποιες εφαρμογές, καθώς επίσης και αντίστοιχη ενημέρωση στο ευρύ κοινό για τα μέτρα που μπορεί να λάβει και τους μηχανισμούς ασφαλείας που καλύπτουν αυτά τα κενά και τους κινδύνους που ενέχουν.

Βιβλιογραφία

[1] Radouan Ait Mouha, Internet of Things (IoT), Journal of Data Analyssis and Information Processing, Vol.9 No.2, April 21, 2021

[2] http://www.itech4u.gr/tech/hands-on/item/7262-internet-of-things-se-apla-ellinika/7262-internet-of-things-se-apla-ellinika
[Πρόσβαση 12 04 2022]

[3] https://el.wikipedia.org/wiki/Διαδίκτυο_των_πραγμάτων
[Πρόσβαση 12 04 2022]

[4] https://datatracker.ietf.org/doc/html/rfc7452
[Πρόσβαση 14 04 2022]

[5] https://www.spoudase.gr/arthra/ti-einai-to-internet-if-things-iot/
[Πρόσβαση 14 04 2022]

[6] https://dspace.lib.uom.gr/bitstream/2159/20157/4/PapastathopoulouAlexandraMsc2017.pdf [Πρόσβαση 16 04 2022]

[7] http://repository.library.teiwest.gr/xmlui/bitstream/handle/123456789/7125/CLOUD%20COMPUTING..pdf?sequence=1&isAllowed=y
[Πρόσβαση 18 04 2022]

[8] https://www.csc.com.gr/cloud-computing/
[Πρόσβαση 18 04 2022]

[9] https://en.wikipedia.org/wiki/Cloud_computing [Πρόσβαση 18 04 2022]

[10] https://link.springer.com/search?facet-creator=%22Alessandro+Bassi%22
[Πρόσβαση 27 04 2022]

[11] https://www.ijaiem.org/Volume5Issue2/IJAIEM-2016-02-20-18.pdf
[Πρόσβαση 27 04 2022]

[12] https://www.iot-a.eu/public/ [Πρόσβαση 28 04 2022]

[13] https://ciksiti.com/el/chapters/6169-top-20-most-remarkable-iot-applications-in-today-s-world [Πρόσβαση 28 04 2022]

[14] https://apothesis.eap.gr/handle/repo/42086
[Πρόσβαση 01 05 2022]

[15] http://demo.daidalos.teipir.gr/smart-home/
[Πρόσβαση 01 05 2022]

[16] https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2018/ssceg2018/Presentation%20and%20Bio/Session4_John.pdf
[Πρόσβαση 02 05 2022]

[17] http://www.iep.edu.gr/images/IEP/EPISTIMONIKI_YPIRESIA/Epist_Monades/B_Kyklos/Tee/2016/GEpal/2016_GEpal_SecSy_studentbook.pdf
[Πρόσβαση 06 05 2022]

[18] https://www.electrodomi.gr/el/upiresies/eksupna-ktiria-knx
[Πρόσβαση 06 05 2022]

[19] http://users.sch.gr/jabatzo/files/yliko/live%20ebooks/syst_elegxou_asfaleias_2018_final/_3.html [Πρόσβαση 07 05 2022]

[20] https://dspace.lib.ntua.gr/xmlui/bitstream/handle [Πρόσβαση 07 05 2022]

[21] http://conta.uom.gr/conta/ekpaideysh/metaptyxiaka/technologies_diktywn/ergasies/2019/SMART%20BUILDINGS.pdf [Πρόσβαση 07 05 2022]

[22] https://manifest.gr/giati-afto-to-ktirio-ine-to-pio-exypno-ston-kosmo-2/
[Πρόσβαση 08 05 2022]

[23] http://www.imm.dtu.dk/~cdje/SmartHouseWebSite/projects.html#classification
[Πρόσβαση 20 05 2022]

[24] https://www.home-biology.gr/ilektromagnitikes-aktinovolies/aktinovolies-ipsilon-sixnotiton/eksypno-spiti-kai-eksypnes-syskeves#ti-aktinovolia-ekpempoun-oi-eksypnes-syskeves
[Πρόσβαση 20 05 2022]

[25] https://www.researchgate.net/figure/The-layered-architectures-of-IoT-three-four-and-five-layers_fig6_327272757
[Πρόσβαση 27 05 2022]

[26] https://www.iarc.who.int/wp-content/uploads/2018/07/pr208_E.pdf
[Πρόσβαση 04 06 2022]

[27] https://guardian.ng/business-services/communication/cell-phone-wireless-radiation-classified-group-1-carcinogenic-to-humans/
[Πρόσβαση 04 06 2022]

[28] https://www.europarl.europa.eu/doceo/document/A-6-2009-0089_EL.html?redirect [Πρόσβαση 04 06 2022]

[29] https://pedion24.gr/electromagnetic-radiation/ [Πρόσβαση 07 06 2022]

[30] https://researcharchive.lincoln.ac.nz/handle/10182/4006
[Πρόσβαση 20 06 2022]

[31] https://www.researchgate.net/publication/3236246_RFID_security_and_privacy_A_research_survey [Πρόσβαση 21 06 2022]

[32] https://web.archive.org/web/20131124235452/http://hackerspace.lifehacker.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382
[Πρόσβαση 22 06 2022]

[33] https://www.webopedia.com/definitions/dos-attack/
[Πρόσβαση 22 06 2022]

[34] https://www.webopedia.com/definitions/flooding/ [Πρόσβαση 22 06 2022]

[35] https://hellanicus.lib.aegean.gr/bitstream/handle/11610/18539/IoT%20Security%20Thesis.pdf?sequence=1
[Πρόσβαση 22 06 2022]

[36] https://open.library.ubc.ca/soa/cIRcle/collections/ubctheses/24/items/1.0401501
[Πρόσβαση 22 06 2022]

[37] Michele De Donno, Nicola Dragoni, Alberto Giaretta, and Angelo Spognardi. Ddoscapable iot malwares: Comparative analysis and mirai investigation. Security and Communication Networks, 2018(Article ID 7178164), February 2018. URL https: //doi.org/10.1155/2018/7178164.

[38] https://www.secnews.gr/189228/botnet-prostasia-epitheseis/
[Πρόσβαση 07 07 2022]

[39] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
[Πρόσβαση 10 07 2022]

[40] https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/
[Πρόσβαση 15 07 2022]

[41] https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis
[Πρόσβαση 15 07 2022]

[42] https://www.avira.com/en/blog/these-are-the-two-most-hacked-devices-in-smart-homes
[Πρόσβαση 31 07 2022]

[43] https://www.armis.com/research/blueborne/
[Πρόσβαση 31 07 2022]

[44] https://www.researchgate.net/publication/320044280_Detection_and_Prevention_of_Non-PC_Botnets
[Πρόσβαση 31 07 2022]

[45] https://www.researchgate.net/profile/Junibel-De-La-Cruz/publication/354674719_Philips_Hue_Bulb_IoT_App_Security/links/61458c70a595d06017d44988/Philips-Hue-Bulb-IoT-App-Security.pdf
[Πρόσβαση 04 08 2022]

[46] https://www.philips-hue.com/el-gr/support/security-advisory
[Πρόσβαση 04 08 2022]

[47] https://ieeexplore.ieee.org/document/8977812
[Πρόσβαση 08 09 2022]

[48] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, και Y. Jin, '' Ανάλυση ασφαλείας σε καταναλωτές και βιομηχανίες Συσκευών IoT'', In Proc. 21st Asia South Pacific Des. Autom. Conf., 2016