ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Διπλωματική Εργασία

ΑΝΑΛΥΣΗ ΤΟΥ INTERNET OF THINGS

Καρύκας Παναγιώτης

Επιβλέπων : Σταμούλης Γεώργιος

Βόλος 2020

UNIVERSITY OF THESSALY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

DIPLOMA THESIS

ANALYSIS OF INTERNET OF THINGS

Karykas Panagiotis

Supervisor : Stamoulis Georgios

Volos 2020

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

«Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής».

Ο/Η Δηλών/ούσα

Καρύκας Παναγιώτης

Ημερομηνία 24/7/2020

ΠΕΡΙΛΗΨΗ

Ο τομέας του Internet of Things συνεχώς εξελίσσεται και μπαίνει στη ζωή μας όλο και περισσότερο, αφού οι τομείς δράσης του είναι σχεδόν απεριόριστοι και βοηθούν στην ανάπτυξη της καθημερινότητας μας. Μέσω της τεχνολογίας, είναι πλέον εφικτό να λαμβάνουμε πληροφορίες από συσκευές με αισθητήρες και αφού τις επεξεργαστούμε οδηγούμαστε σε χρήσιμα συμπεράσματα, ικανά να αναβαθμίσουν και να αυτοματοποιήσουν πολλές λειτουργίες. Στην παρούσα διπλωματική, αρχικά γίνεται μια εισαγωγή στον τομέα του IoT και παρουσιάζεται η χρονολογική του εξέλιξη. Στη συνέχεια, στο κεφάλαιο 2 αναφέρονται οι τρόποι συνδεσιμότητας των συσκευών που χρησιμοποιούνται και παρατίθενται μερικά πλεονεκτήματα αλλά και μειονεκτήματα που προκύπτουν από την εφαρμογή τους. Φτάνοντας στο κεφάλαιο 3, αναλύεται η αρχιτεκτονική των συστημάτων IoT και περιλαμβάνονται πληροφορίες τόσο για τις τεχνολογίες που χρησιμοποιούνται όσο και για τους τρόπους επικοινωνίας που υπάρχουν. Δεδομένου ότι δεν ακολουθείται μόνο ένας τρόπος από τους κατασκευαστές, δίνονται πληροφορίες για όλους τους σημαντικούς τύπους τεχνολογιών και πρωτοκόλλων που χρησιμοποιούνται. Προχωρώντας στο κεφάλαιο 4 παρατηρούμε τις εφαρμογές στις οποίες βρίσκει δράση ο τομέας του IoT, όπως είναι το έξυπνο σπίτι ή η έξυπνη μετακίνηση. Λαμβάνοντας όμως υπόψη τους κινδύνους που ελλοχεύουν, στο 5ο και τελευταίο κεφάλαιο αναλύουμε τις πιθανές επιθέσεις που μπορεί να δεχτεί ένα σύστημα IoT αλλά και τους πιθανούς τρόπους αντιμετώπισης ανάλογα με το επίπεδο στο οποίο γίνεται η επίθεση.

ABSTRACT

The field of Internet of Things is constantly evolving and entering in our lives increasingly, since its areas of action are almost unlimited and help to develop our daily lives. Through technology, it is now possible to receive information from devices with sensors and after processing them we end up to useful conclusions, able to upgrade and automate many functions. In the specific thesis, an introduction is made to the field of IoT and its chronological evolution is presented. Then, in chapter 2, the ways of connecting the devices that are used are mentioned and some advantages and disadvantages that result from their application are listed. Subsequently, at Chapter 3, the architecture of IoT systems is analyzed and information is provided on both the technologies used and the means of communication that exist. As not only one way is followed by the manufacturers, information is given on all the important types of technologies and protocols used. Moving on to Chapter 4, we look at applications in which the IoT sector is active, such as smart home or smart mobility. However, taking into consideration the dangers that lurk, in the 5th and last chapter we analyze the possible attacks that an IoT system can receive but also the possible ways of dealing with it depending on the level at which the attack takes place.

Κατάλογος εικόνων

ΚΕΦΑΛΑΙΟ 1 - ΕΙΣΑΓΩΓΗ

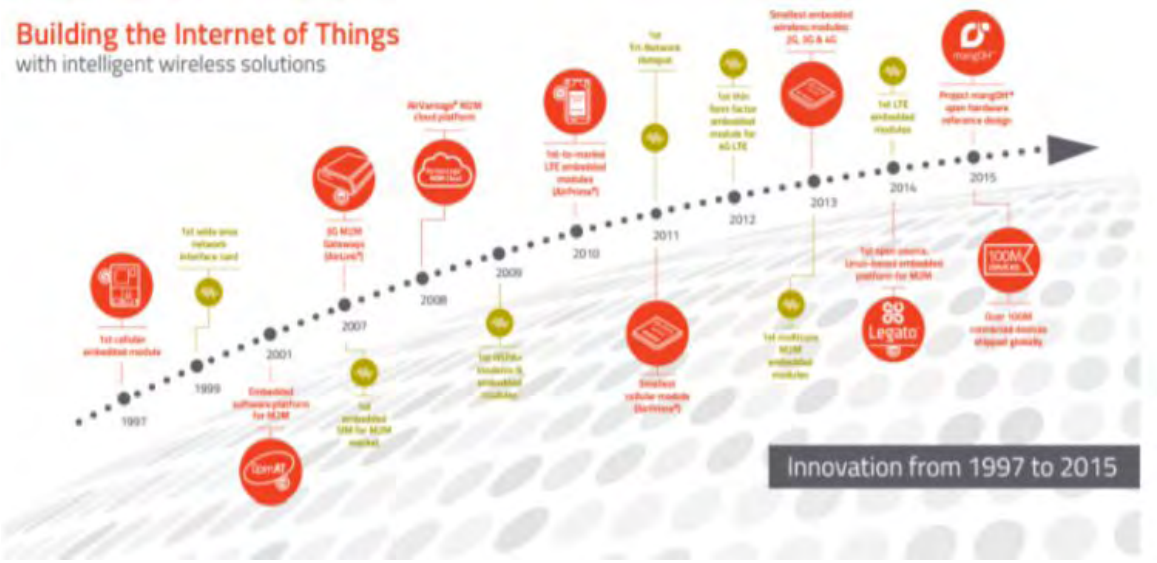
1.1 Εισαγωγή

Το “Διαδίκτυο των πραγμάτων” ή αλλιώς “Internet of Things” είναι το μονοπάτι για τον “έξυπνο κόσμο” αξιοποιώντας την πληροφορική και την τεχνολογία με στόχο τη διευκόλυνση των χρηστών. Αποτελείται από ένα δίκτυο συσκευών, αυτοκινήτων, κτιρίων και οποιουδήποτε αντικειμένου περιέχει ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικό, αισθητήρες καθώς και συνδεσιμότητα σε δίκτυο έτσι ώστε να μπορούν να αλληλεπιδράσουν και να ανταλλάξουν δεδομένα. Οι συσκευές και τα αντικείμενα αυτά συνδέονται με μια πλατφόρμα στην οποία υπάρχουν όλα τα δεδομένα που έχουν εκλάβει και κατάλληλες εφαρμογές αναλαμβάνουν τη διαχείρισή τους. Εκμεταλλεύονται τις χρήσιμες πληροφορίες και καταλήγουν σε συμπεράσματα μέσω των οποίων μπορούν να αυτοματοποιηθούν επαναλαμβανόμενες, χρονοβόρες ή ακόμα και επικίνδυνες εργασίες. Σαφώς, ο όγκος αυτών των πληροφοριών είναι τεράστιος και η σωστή αποθήκευσή του είναι μία πρόκληση, καθώς απαιτείται ασφάλεια και μεθοδικότητα. Κάποια από τα στοιχεία τα οποία συλλέγουν οι IoT συσκευές είναι πολύ προσωπικά, όπως συστήματα παρακολούθησης ή πληροφορίες υγείας, και συνεπώς η εμπιστοσύνη και η προστασία αυτών είναι απαραίτητη.

1.2 Ιστορική Αναδρομή

- Τα πρώτα βήματα της τεχνολογίας IoT τα είδαμε περίπου στο 1955, καθώς οι μηχανικοί μιας αμερικάνικης εταιρίας ήθελαν να βρουν έναν τρόπο για να αναγνωρίζουν το κάθε αντικείμενο ξεχωριστά. Έπειτα από αρκετούς πειραματισμούς κατάφεραν να δημιουργήσουν τα barcodes, μέσω των οποίων το κάθε αντικείμενο είχε ένα είδος ταυτότητας. Έπειτα επιστήμονες και μηχανικοί εξέλιξαν το επίπεδο όσον αφορά το hardware αλλά και τις κινητές φορητές συσκευές. Η πρώτη αξιοσημείωτη συσκευή ήταν του Edward Throrp και αποτελούνταν από ένα ρολόι το οποίο μπορούσε να προβλέψει τους κύκλους που έκαναν οι ρουλέτες στα καζίνα του Las Vegas.
- Ακολούθησαν κάποιες άλλες σημαντικές συσκευές όπως εκείνη του Hubet Upton το 1967 η οποία είχε σχήμα μυωπικών γυαλιών και βοηθούσε άτομα με ειδικές ανάγκες να διαβάζουν τα χείλη των υπολοίπων. Από αυτό εμπνεύστηκε η Google και επινόηση το project Google Glass.
- Το 1995 η Siemens δημιουργεί ένα ειδικό τμήμα για να ασχοληθεί με Machine-To-Machine βιομηχανικές εφαρμογές, καταφέρνοντας να μπορέσουν οι μηχανές να επικοινωνήσουν μεταξύ τους μέσω ασύρματων δικτύων.
- Το 1999 εγκαθιδρύεται στο MIT το Auto-Identification (Auto-ID) και ο David Brock ανακοίνωσε την εξέλιξη των Barcodes σε ένα πιο έξυπνο σύστημα για την αναγνώριση πληροφοριών. Αυτό είχε ως αποτέλεσμα τεχνολογίες όπως Bluetooth, RFID και άλλες ασύρματες να είναι ικανές να διαβάσουν και να γράψουν δεδομένα σε αντικείμενα μέσω του RFID tag.
- Το 2009 ο Kevin Ashton αναφέρει στο άρθρο του με τίτλο “That Internet of things thing” ότι το όνομα “Internet of Things” ξεκίνησε από εκείνον όταν το είχε χρησιμοποιήσει σε μία παρουσίασή του το 1999. Από τότε πολλά άρθρα και πολλοί επιστήμονες και όχι μόνο χρησιμοποιούσαν αυτή τη φράση για να αναφερθούν στο συγκεκριμένο θέμα.
- Στη συνέχεια, το Internet of Things άρχισε να εξελίσσεται ραγδαία και ακολούθησαν πολλά συνέδρια, παρουσιάσεις και μελέτες μέχρι σήμερα.

Στο παρακάτω σχήμα φαίνονται χρονολογικά κάποιες από τις πιο σημαντικές καινοτομίες στον τομέα του Internet of Things.



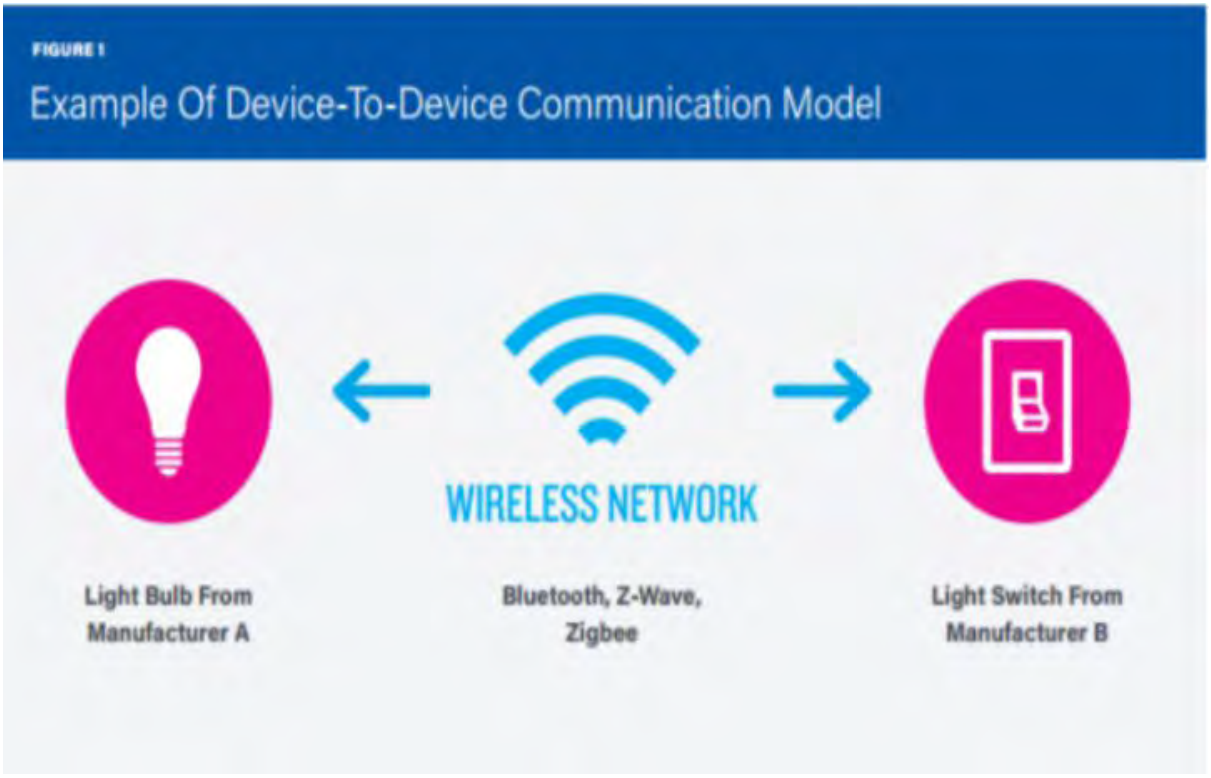
Εικόνα 1.1 Η χρονολογική εξέλιξη του Internet of Things

ΚΕΦΑΛΑΙΟ 2

2.1 Μοντέλα Συνδεσιμότητας

2.1.1 Device-To-Device

Το μοντέλο συνδεσιμότητας Device-To-Device αφορά δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν απευθείας η μία με την άλλη. Έχουν τη δυνατότητα να επικοινωνήσουν με πολλούς τύπους δικτύων, αλλά πιο συχνά χρησιμοποιούν πρωτόκολλα όπως το Bluetooth, το Z-Wave και το ZigBee. Σημαντική προϋπόθεση για να γίνει εφικτή η επικοινωνία αυτή μεταξύ των συσκευών είναι να έχουν επιλέξει οι κατασκευαστές τους το ίδιο πρωτόκολλο και όχι διαφορετικά ο καθένας. Χαρακτηριστικό παράδειγμα της χρήσης αυτού του μοντέλου είναι στα συστήματα οικιακού αυτοματισμού, τα οποία συνηθίζουν να μεταδίδουν μικρά πακέτα δεδομένων. Για παράδειγμα, οι οικιακές συσκευές που βρίσκονται σε ένα σπίτι, όπως θερμοστάτες, λαμπτήρες ή διακόπτες φωτισμού, δεν πρόκειται να μαζέψουν μεγάλο όγκο δεδομένων και έτσι είναι ιδανικές για τη χρήση αυτού του μοντέλου.[1]



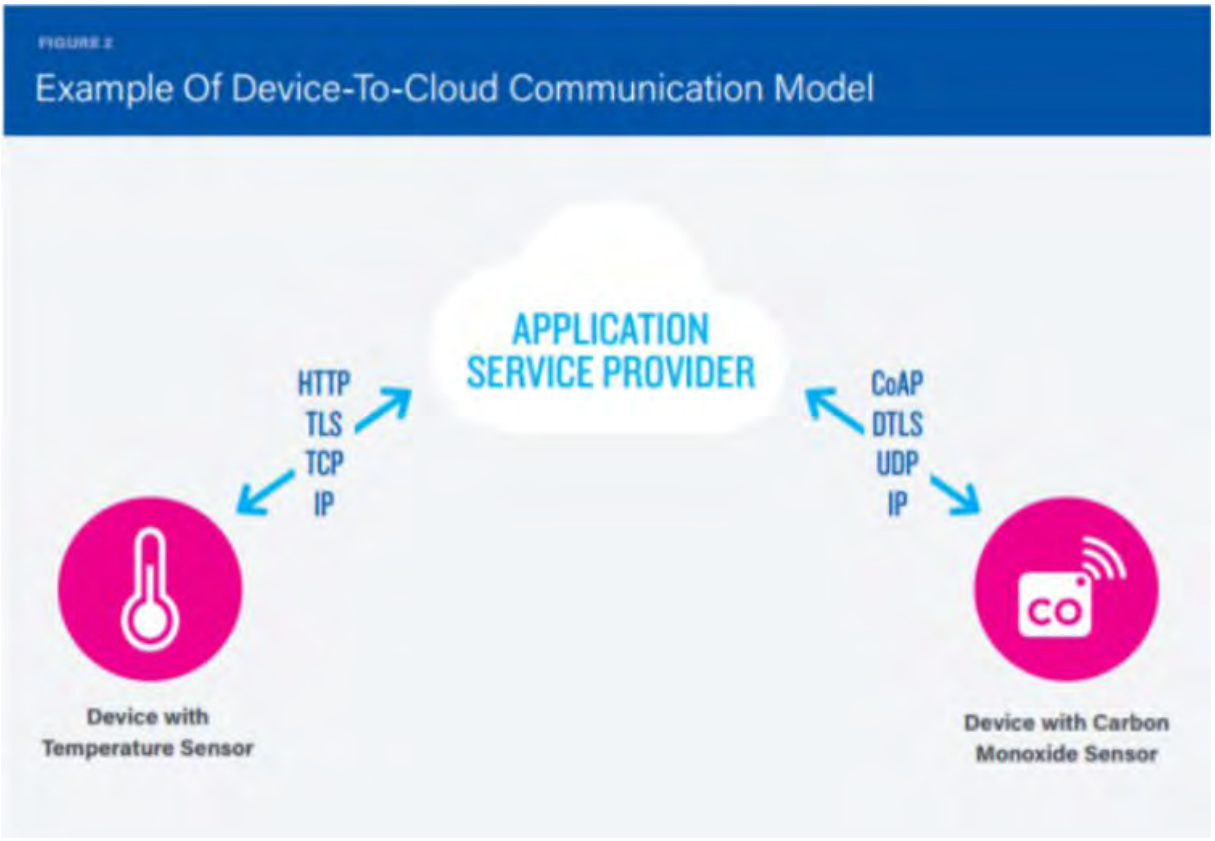
Εικόνα 2.1 Επικοινωνία με Device-To-Device μοντέλο

2.1.2 Device-To-Cloud

Σε αυτό το μοντέλο η συσκευή IoT συνδέεται απευθείας σε μια διαδικτυακή υπηρεσία Cloud και συνήθως είναι και τα δύο από τον ίδιο προμηθευτή. Έτσι γίνονται εφικτά και ο έλεγχος της κυκλοφορίας των μηνυμάτων αλλά και η ανταλλαγή πληροφοριών. Σαφώς είναι ένα πιο λειτουργικό μοντέλο και δίνει τη δυνατότητα στο χρήστη να αποκτήσει έλεγχο στις συσκευές του όχι μόνο ενσύρματα αλλά και ασύρματα.

Το μοντέλο αυτό χρησιμοποιείται τόσο στις έξυπνες τηλεοράσεις όσο και στο Learning Thermostat της Nest Labs. Όσον αφορά τις έξυπνες τηλεοράσεις, πραγματοποιείται μια διαδικτυακή σύνδεση με σκοπό να μεταδοθούν οι πληροφορίες με τα όσα ζητάει ο χρήστης στην τηλεόραση και να πραγματοποιηθούν. Στη δεύτερη περίπτωση, το Learning Thermostat είναι ένας “έξυπνος θερμοστάτης”, δηλαδή μόλις

δώσει ο χρήστης τις κατάλληλες πληροφορίες όσον αφορά τις ώρες και τις θερμοκρασίες που θα ήθελε στο σπίτι του, εκείνο αναλαμβάνει να κάνει τις ανάλογες αλλαγές έτσι ώστε να υπάρχει η επιθυμητή θερμοκρασία μέσα στο χώρο. Και στα δύο παραδείγματα καταλαβαίνουμε ότι το να χρησιμοποιείς τις συσκευές ακόμα και όταν δεν είσαι στο χώρο, είναι ένα καλό πλεονέκτημα και αυξάνονται οι δυνατότητές τους.[4]

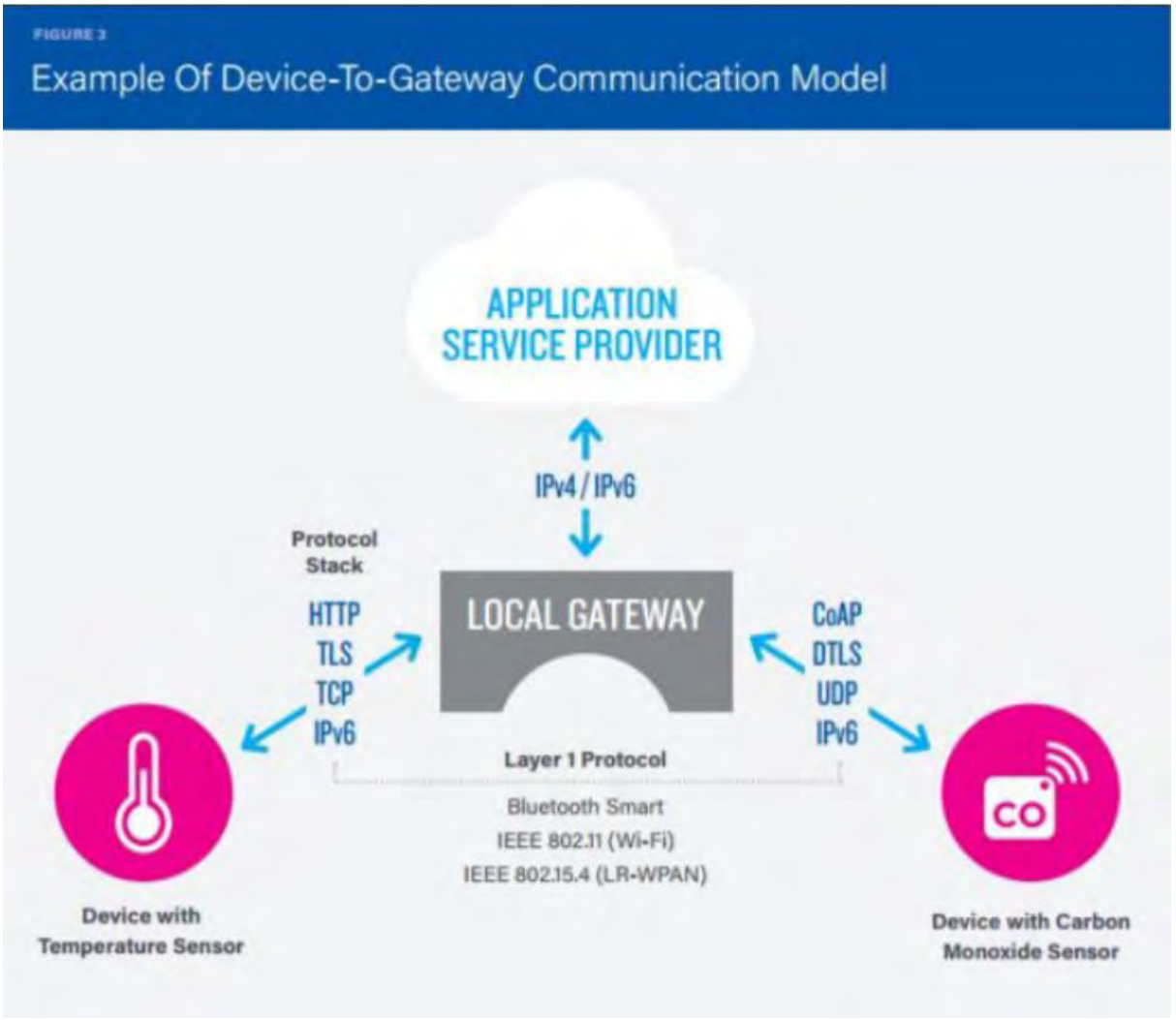


Εικόνα 2.2 - Επικοινωνία με Device-To-Cloud μοντέλο

2.1.3 Device-To-Gateway

Στο μοντέλο Device-To-Gateway οι IoT συσκευές συνδέονται στην υπηρεσία Cloud έχοντας ως μεσάζοντα μία ενδιάμεση συσκευή. Στην ενδιάμεση αυτή συσκευή υπάρχει ένα λογισμικό το οποίο εκτός από το ότι “ενώνει” τις συσκευές με το Cloud,

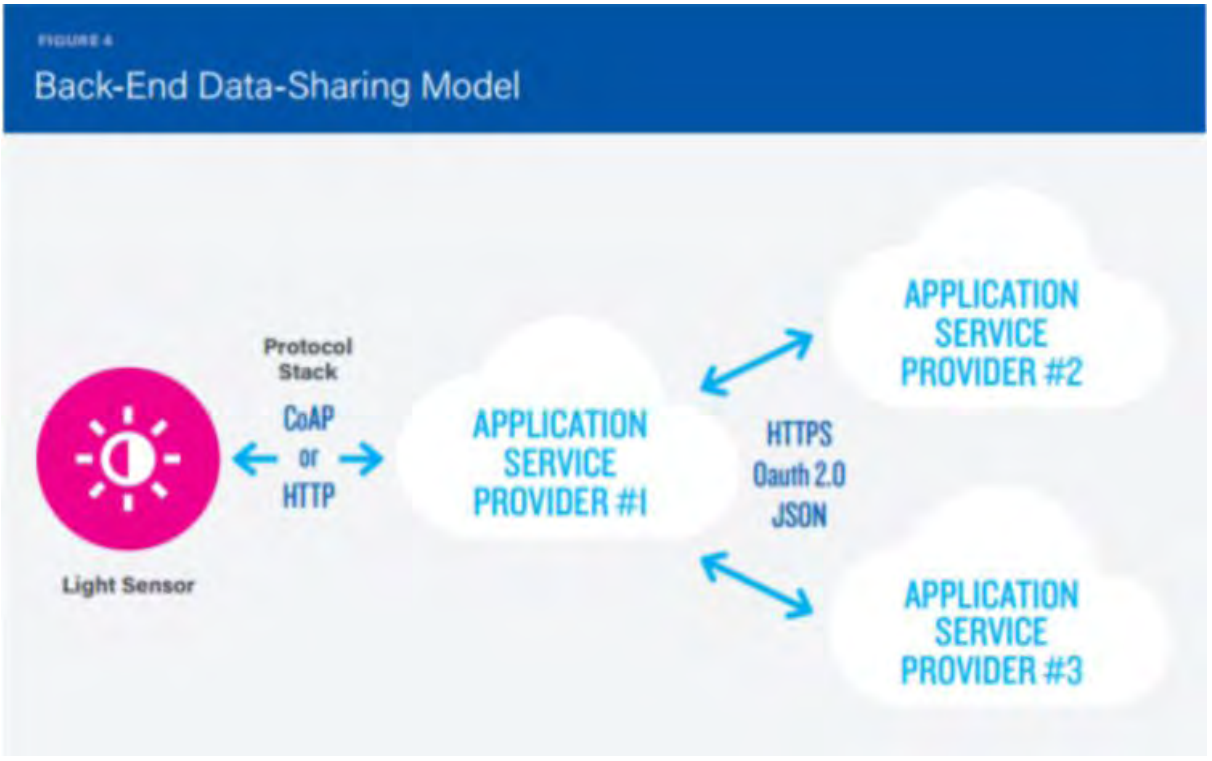
παρέχει ασφάλεια και μετάφραση δεδομένων ή πρωτοκόλλων. Μοντέλα τέτοιας μορφής συνηθίζεται να βλέπουμε στις συσκευές των καταναλωτών, για παράδειγμα ένα smartwatch. Λόγω του ότι είναι δύσκολο να συνδεθούν απευθείας στην Cloud υπηρεσία, συχνά χρησιμοποιούν ως ενδιάμεση συσκευή ένα smartphone.



Εικόνα 2.3 - Επικοινωνία με Device-To-Gateway μοντέλο

2.1.4 Back-End Data Sharing

Αυτό το μοντέλο αποτελεί μια επέκταση του μοντέλου Device-to-Cloud με τη διαφορά ότι για να συνδεθεί η IoT συσκευή στην Cloud υπηρεσία, μεσολαβεί μία άλλη συσκευή (π.χ. ένα smartphone). Σε αυτή τη συσκευή τρέχει το λογισμικό της εφαρμογής και δίνεται η δυνατότητα τα δεδομένα που συλλέγουν οι αισθητήρες να μπορούν να επεξεργαστούν και να αναλυθούν είτε από τους χρήστες είτε από εξουσιοδοτημένα τρίτα μέρη. Χρησιμοποιώντας αυτό το μοντέλο μπορεί κάποιος χρήστης να έχει εύκολη πρόσβαση σε δεδομένα από όλους τους αισθητήρες των συσκευών καθώς και να αξιοποιήσει τη φορητότητα των δεδομένων αυτών.



Εικόνα 2.4 - Επικοινωνία με Back-End Data-Sharing μοντέλο

2.2 Πλεονεκτήματα και Μειονεκτήματα του IoT

Το Internet of Things είναι μια τεχνολογία που μπορεί να δώσει απεριόριστες δυνατότητες στη σύγχρονη ζωή. Σχετίζεται με τη διαδικτυακή σύνδεση μεταξύ ηλεκτρονικών συσκευών και ανθρώπων με σκοπό την βέλτιστη λειτουργία των ικανοτήτων των συσκευών καθώς και την τεράστια διευκόλυνση στην καθημερινότητα των ίδιων των ατόμων. Προκειμένου να κατανοήσουμε καλύτερα την τεχνολογία αυτή είναι πολύ σημαντικό να αναφέρουμε παρακάτω κάποια από τα πολλά πλεονεκτήματα αλλά και μερικά μειονεκτήματα του IoT :

2.2.1 Πλεονεκτήματα του Internet of Things

1) **Παρακολούθηση**

Η πρόσβαση στις πληροφορίες γίνεται σαφώς ευκολότερη καθώς ο έλεγχος των δεδομένων πραγματοποιείται από οποιαδήποτε τοποθεσία μέσω ενός δικτύου που συνδέει τον χρήστη με τις συσκευές του. Με αυτόν τον τρόπο ο χρήστης παρακολουθεί με ακρίβεια τις τυχόν ελλείψεις των προϊόντων του καθώς αποκτά και πλήρη εικόνα της ποιότητας αυτών.

2) **Επικοινωνία**

Η επικοινωνία μεταξύ των συσκευών διευκολύνεται μέσω των εφαρμογών του συστήματος Internet of Things, η οποία καθιστά τις ηλεκτρονικές συσκευές πιο ικανές όσον αφορά την αποδοτικότητα τους και τη διατήρηση της συνδεσιμότητας τους. Επίσης προσφέρει αρκετές επιπλέον λειτουργίες και συμβάλλει στη μείωση της ανεπάρκειας.

3) **Αυτοματοποίηση**

Η αυτοματοποιημένη διαχείριση καθημερινών εργασιών δίχως την φυσική παρουσία ενός ατόμου και ο ακριβής έλεγχός τους, επιτυγχάνει μια πιο ποιοτική λειτουργία των συσκευών με σαφώς ταχύτερες διαδικασίες.

4) **Εξοικονόμηση Χρόνου**

Ο χρόνος που εξοικονομείται στον ανθρώπινο παράγοντα μέσω των συστημάτων παρακολούθησης των συσκευών διαδικτυακά είναι πολύ σημαντικός καθώς λιγοστεύει κατά πολύ την ατομική προσφορά και συμβάλλει σε ένα ανώτερο επίπεδο ζωής. Μέσω ενός IoT συστήματος μπορούν να εκτελεστούν επαναλαμβανόμενες εργασίες χωρίς την παρουσία του χρήστη.

5) **Αποταμίευση Χρημάτων**

Δεδομένου ότι οι συσκευές λειτουργούν στη μέγιστη απόδοσή τους ένα μεγάλο μέρος της ενέργειας εξοικονομείται. Επιπλέον, οι προειδοποιήσεις πιθανών δυσλειτουργιών που λαμβάνει ο χρήστης συμβάλλουν σημαντικά στην μείωση των εξόδων. Επιτρέποντας στις πληροφορίες που συλλέγονται, να ανταλλάσσονται μεταξύ των συσκευών και να επεξεργάζονται, καταλήγουμε σε σημαντικά συμπεράσματα και οφέλη.

2.2.2 Μειονεκτήματα του Internet of Things

1) **Ασφάλεια και Απόρρητο**

Λαμβάνοντας υπόψη ότι η σύνδεση μεταξύ των συσκευών πραγματοποιείται μέσω δικτύων υπάρχουν απεριόριστες πιθανότητες να προκύψουν διαρροές προσωπικών στοιχείων καθώς και παραβίαση ιδιωτικών πληροφοριών. Επιπλέον καθιστά εφικτή την πρόσβαση σε απόρρητα δεδομένα από παράνομους εισβολείς (χάκερς). Συμπεραίνουμε λοιπόν πως το IoT είναι ένα ελλειπές σύστημα όσον αφορά την ασφάλεια του προσωπικού απορρήτου.

2) **Πολυπλοκότητα**

Εφόσον πρόκειται για μια τεχνολογία που περιλαμβάνει πολλές διαφορετικές διαδικτυακές συνδέσεις, αυτόματα αυτό την καθιστά αρκετά σύνθετη. Μια μικρή μόνο βλάβη σε ένα από τα δίκτυα είναι αρκετή για να προκαλέσει δυσλειτουργία της συσκευής και μεγάλο ενδεχόμενο κατάρρευσης ολόκληρου του συστήματος.

3) **Συμβατότητα**

Καθότι αναφερόμαστε σε ένα πολύ νέο είδος τεχνολογίας, μέχρι στιγμής δεν υπάρχουν συγκεκριμένες προδιαγραφές για τις παροχές και τον τρόπο παρακολούθησης των συσκευών μέσω εφαρμογής αισθητήρων. Προκειμένου να επιλυθεί αυτό είναι απαραίτητο να δημιουργηθούν κάποια βιομηχανικά πρότυπα όπως για παράδειγμα το Bluetooth.

4) **Μείωση Θέσεων Εργασίας**

Ο αυτοματισμός πολλών λειτουργιών των συσκευών σταδιακά μας οδηγεί σε αντικατάσταση των φυσικών προσώπων από μηχανές. Η αξιοπιστία του ανθρώπινου παράγοντα υποκαθίσταται από την ίδια την τεχνολογία και αυτό θα έχει ως αποτέλεσμα την ελάττωση πολλών επαγγελμάτων.

ΚΕΦΑΛΑΙΟ 3 - ΑΡΧΙΤΕΚΤΟΝΙΚΗ

Όσον αφορά την αρχιτεκτονική του IoT δεν υπάρχει μόνο μία συγκεκριμένη που να χρησιμοποιείται από όλους. Διαφορετικές αρχιτεκτονικές επιλέγονται ανάλογα με τον σκοπό του καθενός και το τι θέλει να πετύχει. Η πιο βασική, η οποία παρουσιάστηκε στις αρχές των ερευνών αυτού του τομέα, είναι η three-Layer αρχιτεκτονική. Περιλαμβάνει τρία στάδια τα οποία είναι το perception επίπεδο (αντίληψης), το network επίπεδο (δικτύωσης) και το application επίπεδο (εφαρμογής). Η συγκεκριμένη ορίζει τη βασική ιδέα του Internet of Things αλλά δεν είναι σε όλες τις περιπτώσεις πλήρως αποδοτική με αποτέλεσμα να είναι στην ευχέρεια του καθενός ποιο μοντέλο αρχιτεκτονικής θα χρησιμοποιήσει. Παρακάτω θα δούμε την 3 επιπέδων (Three-Layer) αρχιτεκτονική.

3.1 Επίπεδα Αρχιτεκτονικής

3.1.1 Perception Layer (Επίπεδο Αντίληψης)

Η κύρια δουλειά ενός συστήματος IoT γίνεται σε αυτό το επίπεδο καθώς εδώ συλλέγονται οι πληροφορίες από τους αισθητήρες ή τις RFID ετικέτες. Στη συνέχεια μετατρέπονται σε ψηφιακά σήματα τα οποία μπορούν να μεταδοθούν μέσω του διαδικτύου ευκολότερα. Ωστόσο κάποια αντικείμενα ίσως να μην γίνονται αντιληπτά κατευθείαν. Για αυτό το λόγο, κάποια μικροτσίπ ενσωματώνονται σε αυτά τα αντικείμενα με σκοπό να τα κάνουν περισσότερο ανιχνεύσιμα και επεξεργάσιμα. Συνεπώς, καίριο ρόλο έχουν τόσο η νανοτεχνολογία, μέσω της οποίας κατασκευάζονται τσιπς αρκετά μικρά ώστε να χωράνε σε πολλά αντικείμενα της

καθημερινότητας, όσο και η τεχνητή νοημοσύνη που τα κάνει ικανά να επεξεργαστούν κατάλληλα τα δεδομένα που λαμβάνουν.[5]

3.1.2 Network Layer (Επίπεδο Μεταφοράς)

Το επίπεδο του διαδικτύου είναι υπεύθυνο για την επεξεργασία των δεδομένων που έχουν ληφθεί από το πρώτο στάδιο, εκείνο της αντίληψης. Ο ρόλος του είναι να μεταφέρει τις πληροφορίες στο επόμενο επίπεδο, το Application layer, μέσω διαφόρων τεχνολογιών του διαδικτύου όπως ενσύρματα ή ασύρματα αλλά και τοπικά δίκτυα. Τα κύρια μέσα για τη μεταφορά αυτή είναι το WiFi, το Bluetooth, 3G/4G, Zigbee κλπ. Επειδή μεγάλες ποσότητες δεδομένων μεταφέρονται από το δίκτυο είναι καίριας σημασίας να υπάρχει μια αξιόπιστη και δυναμική τεχνολογία μέσω της οποίας τα δεδομένα αυτά θα μπορούν να αποθηκευτούν και να επεξεργαστούν με ασφάλεια. Είναι ένα αρκετά ευαίσθητο επίπεδο από την άποψη ότι μπορεί να δεχθεί επίθεση από χάκερς και για αυτό το λόγο η ακεραιότητα των πληροφοριών θα πρέπει να διασφαλίζεται.

3.1.3 Application Layer (Επίπεδο Εφαρμογών)

Το επίπεδο των εφαρμογών είναι αυτό που χρησιμοποιεί τα επεξεργασμένα δεδομένα που προέρχονται από το επίπεδο του διαδικτύου. Αποτελεί το επίπεδο που είναι πιο κοντά στον τελικό χρήστη και μέσω αυτού ουσιαστικά γίνεται αντιληπτό στον άνθρωπο η χρησιμότητα και οι δυνατότητες του Internet of Things. Σαφώς, οι διάφοροι τομείς και οι εφαρμογές στα οποία εφαρμόζεται το IoT δεν έχουν τις ίδιες απαιτήσεις όσον αφορά τα δίκτυα, τις υποδομές και τις συνδεσιμότητες που χρησιμοποιούν. Στο επόμενο σχήμα διακρίνονται ενδεικτικά κάποια από τα χαρακτηριστικά των εφαρμογών αυτών.

	Smart Home	Smart Retail	Smart City	Smart Agriculture	Smart Water	Smart Transportation
Network size	Small	Small	Medium	Medium/large	Large	Large
Users	Very few (family)	Few (community)	Many (general public)	Few (landowners)	Few (government)	Large(general public)
Energy	Rechargeable battery	Rechargeable battery	Rechargeable battery, Energy harvesting	Energy harvesting	Energy harvesting	Rechargeable battery, Energy harvesting
Internet Connectivity	WiFi,3G,4G LTE backbone	WiFi,3G,4G LTE backbone	WiFi,3G,4G LTE backbone	WiFi, Satellite	Satellite, Microwave links	WiFi, Satellite
Data Management	Local server	Local server	Shared server	Local & shared servers	Shared server	Shared server
IoT devices	RFID,WSN	RFID,WSN	RFID,WSN	WSN	Single sensors	RFID,WSN, Single sensors
Bandwidth Requirement	Small	Small	Large	Medium	Medium	Medium / large
Examples	Aware Home	SAP future solutions	Smart Santander	Vineyards with Waspmotes	GBROOS	LocalMotion

Εικόνα 3.1 - Χαρακτηριστικά IoT εφαρμογών

3.2 Χαρακτηριστικά Αρχιτεκτονικών

Πολλές προκλήσεις και ανησυχίες βρίσκονται πίσω από ένα σύστημα IoT και δεν είναι εύκολο να μπουν στη καθημερινότητά μας εύκολα και γρήγορα οι εφαρμογές του. Κάποιες αρχιτεκτονικές που ενδεχομένως υπερτερούν από τις υπόλοιπες σε κάποιους τομείς, μπορεί να υστερούν σε κάποιους άλλους. Όλες έχουν τα αρνητικά και τα θετικά τους, ανάλογα με την οπτική μεριά του καθενός. Παρακάτω θα προσπαθήσουμε να συνοψίσουμε κάποια **χαρακτηριστικά,** τα οποία υπάρχουν στις αρχιτεκτονικές :

- **Κατανομή** : Τα δεδομένα που συλλέγονται σε ένα σύστημα Internet of Things είναι πιθανό να μην έρχονται όλα από την ίδια πηγή. Συνεπώς, θα πρέπει να κατανέμονται και να επεξεργάζονται με αποτελεσματικότητα και να χρησιμοποιούνται ανάλογα με τη χρησιμότητά τους.

- **Διαλειτουργικότητα** : Οι συσκευές από διαφορετικούς κατασκευαστές θα πρέπει να μπορούν να συνεργαστούν με τέτοιο τρόπο ούτως ώστε να φέρουν εις πέρας έναν κοινό στόχο. Συνεπώς, θα πρέπει να χρησιμοποιούνται πρωτόκολλα και συστήματα μέσω των οποίων οι συσκευές θα μπορούν να αλληλεπιδράσουν και να “βοηθηθούν” μεταξύ τους.

- **Επεκτασιμότητα** : Λαμβάνοντας υπόψη ότι ο αριθμός των συσκευών που συμβάλλουν και στέλνουν δεδομένα σε ένα κοινό δίκτυο μπορεί να είναι τεράστιος, θα πρέπει τα συστήματα που διαχειρίζονται αυτές τις πληροφορίες να είναι ικανά να αντιμετωπίσουν πολύ μεγάλους όγκους δεδομένων.

- **Έλλειψη πόρων** : Τόσο οι ενεργειακές όσο και οι υπολογιστικές δυνατότητες των συσκευών IoT δεν θα πρέπει να είναι σε έλλειψη.

- **Ασφάλεια** : Οι αισθητήρες και οι συσκευές IoT μπορούν να λαμβάνουν δεδομένα και πληροφορίες, τα οποία για κάποιους χρήστες ίσως είναι προσωπικά και δεν επιθυμούν να τα μοιραστούν. Μία συνεχόμενη καταγραφή μπορεί να αποτρέψει κάποιους χρήστες από το να εμπιστευτούν τα συστήματα, εκτός εάν υπάρχει πλήρη διασφάλιση και προστασία υπέρ τους.

3.3 Τεχνολογίες του IoT

3.3.1 Radio Frequency Identification (RFID)

Το RFID είναι ένα σύστημα μέσω του οποίου πραγματοποιείται ασύρματη ταυτοποίηση αντικειμένων χρησιμοποιώντας ραδιοκύματα. Ουσιαστικά πρόκειται για μία ηλεκτρονική “ετικέτα” που ταυτοποιεί το κάθε αντικείμενο και η ετικέτα αυτή χωρίζεται σε 2 κατηγορίες, την ενεργητική και την παθητική, ανάλογα με τον τύπο της εφαρμογής που χρησιμοποιείται. Οι ενεργητικές ετικέτες αποτελούνται από μια μπαταρία, δηλαδή έχουν τη δική τους παροχή ισχύος. Εκπέμπουν σήματα δεδομένων ανεξάρτητα από την απόσταση και είναι ικανές να επικοινωνούν στιγμιαία. Από την άλλη, οι παθητικές ετικέτες δεν παίρνουν ενέργεια από μπαταρία. Χρησιμοποιούν την ενέργεια από το ηλεκτρομαγνητικό πεδίο που δημιουργεί η κεραία της συσκευής ανάγνωσης. Το κύρια πλεονεκτήματα της τεχνολογίας RFID είναι η αξιοπιστία τους, το χαμηλό τους κόστος και η ακρίβειά τους. Για αυτό το λόγο είναι ιδιαίτερα επιθυμητή σε εφαρμογές που αφορούν τη ρομποτική, τη βιομηχανία, την παρακολούθηση ασθενών.[13]

3.3.2 Ασύρματα δίκτυα αισθητήρων (WSN)

Τα ασύρματα δίκτυα αισθητήρων αποτελούνται από κόμβους οι οποίοι συλλέγουν τις πληροφορίες από το περιβάλλον και επικοινωνούν μεταξύ τους. Με έναν αυτόνομο τρόπο λειτουργίας, καταφέρνουν να αξιοποιήσουν την επικοινωνία σε αρκετά καλά επίπεδα και να στείλουν τις πληροφορίες στο σταθμό βάσης. Απαραίτητη προϋπόθεση για να λειτουργήσουν σωστά είναι να συνεργαστούν μεταξύ τους κατάλληλα και μεθοδευμένα, έτσι ώστε να ομαδοποιήσουν τα στοιχεία που συλλέγονται από όλους τους κόμβους και να μην λειτουργεί ο καθένας ατομικά.

Δεδομένου όμως ότι οι κόμβοι αυτοί αποτελούνται από συσκευές με περιορισμένη ενέργεια, επεξεργαστές χαμηλής ισχύος και δεν μπορούν να αποθηκεύσουν μεγάλο όγκο δεδομένων, επηρεάζονται σε κάποιο βαθμό η σχεδίαση και η εφαρμογή των ασύρματων δικτύων αισθητήρων.[12]

Οι βασικές διαφορές που υπάρχουν ανάμεσα στα RFID συστήματα και στα ασύρματα δίκτυα αισθητήρων είναι οι εξής. Η πρώτη κατηγορία είναι κατάλληλη για να ανιχνεύσει αντικείμενα τα οποία δεν είναι εύκολα παρατηρήσιμα χρησιμοποιώντας βασικές τεχνολογίες αλλά όχι για να παρακολουθεί αντικείμενα. Εν αντιθέση, τα ασύρματα δίκτυα αισθητήρων βρίσκουν εφαρμογή σε περιπτώσεις που χρειάζεται να παρακολουθούνται καταστάσεις ή αντικείμενα και η εξίσου σημαντική τους ιδιότητα είναι το γεγονός ότι μπορούν να λειτουργήσουν ασύρματα, πράγμα πολύ χρήσιμο για τον τομέα του IoT.

3.3.3 Cloud Computing

Στη συγκεκριμένη τεχνολογία υπάρχει μία αριθμητικά μεγάλη ποσότητα διακομιστών, οι οποίοι συνδέονται σε μία cloud υπηρεσία και καταφέρνουν να δώσουν την άδεια στους χρήστες ούτως ώστε να χειρίζονται τις συσκευές τους από απόσταση όποτε εκείνοι το θελήσουν. Η δυνατότητά τους να αποθηκεύουν μεγάλους όγκους δεδομένων αλλά και να επεξεργάζονται τα δεδομένα που συλλέγονται από τους αισθητήρες, καθιστά την τεχνολογία αυτή πολύ χρήσιμη με σημαντικά οφέλη. Το χαμηλό της κόστος σε σχέση με την απόδοση και τις λειτουργίες που προσφέρει, την κατατάσσει στις αποδοτικότερες τεχνολογίες στον τομέα του IoT. Επίσης, τα αντίγραφα ασφαλείας που δημιουργούνται δίνουν τη δυνατότητα στους χρήστες να πραγματοποιήσουν μια ανάκτηση πληροφοριών σε περίπτωση που κάτι χαθεί. Οι εφαρμογές στην υπηρεσία Cloud ενσωματώνονται αυτόματα και δεν απαιτούνται ενέργειες από τους χρήστες για τη διασύνδεσή τους. Ωστόσο, παρά τα σημαντικά πλεονεκτήματα που μόλις αναφέραμε, υπάρχουν και μερικά μειονεκτήματα τα οποία θα πρέπει να λαμβάνονται υπόψη από τους χρήστες πριν επιλέξουν αυτήν την τεχνολογία. Το γεγονός ότι οι πληροφορίες που συλλέγονται είναι διαθέσιμες στο

διαδίκτυο μπορεί να κεντρίσουν το ενδιαφέρον σε εισβολείς και να πραγματοποιηθούν επιθέσεις με σκοπό την υποκλοπή τους. Ακόμα και τα διάφορα τεχνικά προβλήματα που μπορεί να προκύψουν ή η ελλιπής υποστήριξη σε συγκεκριμένες εφαρμογές μπορεί να προκαλέσουν ανησυχίες.[13]

Οι κατηγορίες στις οποίες θα μπορούσε να χωριστεί η υπηρεσία Cloud είναι οι εξής :

- **Private Cloud**
  Η λειτουργία εδώ γίνεται από έναν και μόνο χρήστη και δεν μπορεί να δοθεί πρόσβαση σε άλλα άτομα.

- **Public Cloud**
  Η δημόσια υπηρεσία του Cloud διαχειρίζεται από περισσότερους ανθρώπους και γίνεται διαθέσιμο από κάποιον τρίτο φορέα παροχής υπηρεσιών.

- **Community Cloud**
  Σε αυτή τη μορφή δίνεται πρόσβαση σε ομάδες οι οποίες έχουν τους ίδιους στόχους και ενδεχομένως επιθυμούν να συνεργαστούν για την επίτευξη του κοινού αποτελέσματος.

- **Hybrid Cloud**
  Ο συνδυασμός δύο ή περισσότερων από τις παραπάνω κατηγορίες οδηγεί στη δημιουργία του υβριδικού Cloud.

3.4 Επικοινωνία

Χρησιμοποιούνται διαφόρων ειδών τεχνολογίες ούτως ώστε να γίνει εφικτή η επικοινωνία μεταξύ των συσκευών, των αισθητήρων και του δικτύου σε ένα σύστημα IoT. Ο κάθε χρήστης επιλέγει την τεχνολογία που συμβάλλει πιο αποτελεσματικά στο να επιτευχθεί η λειτουργία που χρειάζεται αλλά και από το μέγεθος του δικτύου. Παρακάτω θα αναλύσουμε τις τεχνολογίες επικοινωνίας.

3.4.1 Επικοινωνία κοντινού πεδίου (NFC)

Το NFC χρησιμοποιείται για να επικοινωνήσουν οι κινητές συσκευές μεταξύ τους όταν όμως βρίσκονται σε απόσταση λίγων εκατοστών. Προσφέρει μια επικοινωνία ασύρματα και με μικρή εμβέλεια και η αλληλεπίδραση αυτή βασίζεται στην RFID τεχνολογία. Λειτουργεί στην ίδια ζώνη συχνοτήτων με το RFID και υπάρχουν δύο τρόποι λειτουργίας, ο ενεργός και ο παθητικός. Στον ενεργό και οι δύο συσκευές παράγουν μαγνητικά πεδία ενώ στον παθητικό μόνο η μία συσκευή δημιουργεί το πεδίο και η άλλη χρησιμοποιείται για τη μεταφορά των δεδομένων. Συνεπώς, το δεύτερο είδος λειτουργίας χρησιμεύει σε συσκευές με μπαταρία ούτως ώστε να βελτιστοποιήσουν τη διαχείριση της ενέργειας. Το βασικό πλεονέκτημα του NFC είναι ότι παρέχει ασφάλεια στις συναλλαγές και έτσι μηδενίζει το ρίσκο στις πληρωμές για παράδειγμα.

3.4.2 Wireless Sensor Networks (WSN)

Το μειονέκτημα κάποιων τεχνολογιών όπως για παράδειγμα το NFC, το RFID ή το Bluetooth είναι πως λειτουργούν όταν υπάρχουν κοντινές αποστάσεις. Σε αντίθεση με αυτές τις τεχνολογίες, το WSN αποτελείται από πολλούς κόμβους αισθητήρων συνδεδεμένους ασύρματα. Είναι σε θέση να αποθηκεύουν τα δεδομένα και μέσω των

συσκευών τα μεταφέρουν στην cloud υπηρεσία. Η επικοινωνία αυτή μπορεί να είναι είτε μοναδική είτε πολλαπλή, καθώς, παρόλο που οι αισθητήρες έχουν περιορισμένες δυνατότητες, οι κόμβοι των πυλών έχουν επαρκή ισχύ και πόρους επεξεργασίας.

3.4.3 Bluetooth

Η τεχνολογία Bluetooth έχει αναπτυχθεί και χρησιμοποιείται σε κινητά τηλέφωνα, φορητούς υπολογιστές, ασύρματα ακουστικά και φορητές συσκευές όπως το smartwatch. Η λειτουργία του επιτρέπει σε ψηφιακές ή αναλογικές συσκευές να δημιουργούν αυτόματα το ασύρματο δίκτυο μέσα σε μικρά πεδία. Συνεπώς παρέχει βοηθητικές συνδέσεις για συσκευές και κάνει την μεταξύ τους επικοινωνία εύκολα εφικτή.

3.4.4 Χαμηλής Ισχύος WiFi

Το WiFi χαμηλής ισχύος καταναλώνει λιγότερη ενέργεια από το κανονικό WiFi και μπορεί να μεταδώσει σε μεγαλύτερη απόσταση. Για αυτό το λόγο αναπτύχθηκε και χρησιμοποιείται στον τομέα του Internet of Things. Σε περιπτώσεις όπου οι συσκευές δεν έχουν ατελείωτη ενέργεια και οι αποστάσεις είναι μεγαλύτερες από τις εμβέλειες που μπορούν να μεταδώσουν άλλες τεχνολογίες, το Wifi χαμηλής ισχύος είναι κατάλληλο. Ωστόσο ο ρυθμός που στέλνονται τα δεδομένα είναι μικρότερος και έτσι δεν είναι χρήσιμο για ανταλλαγή δεδομένων.

3.4.5 Zigbee

Το Zigbee σχετίζεται με τη σχεδίαση του χαμηλής ισχύος ασύρματου δικτύου. Δημιουργήθηκε επειδή έχει μικρότερο κόστος και απλούστερη σύνδεση από άλλες διαθέσιμες τεχνολογίες. Έχει τη δυνατότητα να επικοινωνήσει με συσκευές μέχρι και

εκατό μέτρα μακριά και να στείλει δεδομένα με ρυθμό μετάδοσης 250 kb/s. Συνεπώς είναι αρκετά χρήσιμη για περιπτώσεις που δεν θέλουμε να έχουν υψηλό κόστος και ισχύ, όπως για παράδειγμα για την παρακολούθηση του σπιτιού μας.

3.5 Αισθητήρες και Ενεργοποιητές

Για να μπορέσει να συλλέξει δεδομένα και πληροφορίες ένα σύστημα IoT είναι απαραίτητη η χρήση κάποιων αισθητήρων. Ανάλογα με τις απαιτήσεις του χρήστη, χρησιμοποιούνται και οι κατάλληλοι αισθητήρες. Σημαντικό πλεονέκτημα των αισθητήρων είναι το γεγονός ότι καταλαμβάνουν μικρό μέγεθος, καταναλώνουν χαμηλή ενέργεια και έχουν μικρό κόστος. Αναγκάζονται όμως οι αισθητήρες αυτοί να έχουν χωρητικότητα στην μπαταρία τους και να είναι εύκολοι στη χρήση τους. Παρακάτω θα αναλύσουμε κάποιους τύπους αισθητήρων που χρησιμοποιούνται για τις εφαρμογές του Internet of Things.[3]

3.5.1 Αισθητήρες κινητού τηλεφώνου

Το κινητό τηλέφωνο στις μέρες μας έχει εξελιχθεί σε μεγάλο βαθμό και βρίσκεται στην καθημερινότητα των περισσότερων ανθρώπων. Έχει πολλές λειτουργίες και θεωρείται μια αρκετά εύχρηστη συσκευή. Για να λειτουργήσουν όμως οι εφαρμογές του χρειάζονται αισθητήρες οι οποίοι εμπεριέχονται μέσα σε αυτό και έτσι γίνεται δυνατή η μεταφορά και η επεξεργασία των δεδομένων. Σε ένα σύγχρονο κινητό τηλέφωνο οπωσδήποτε υπάρχει μία κάμερα και ένα μικρόφωνο, τα οποία είναι ισχυροί αισθητήρες καθώς μέσα από αυτά συλλέγονται τόσο πληροφορίες εικόνας όσο και ήχου. Με την επεξεργασία αυτών των δεδομένων μπορούν να δοθούν σημαντικές πληροφορίες και να φτάσουμε σε χρήσιμα συμπεράσματα. Ένας άλλος αισθητήρας επίσης πολύ γνωστός είναι το GPS. Μέσω αυτού ανιχνεύεται η τοποθεσία η οποία είναι απαραίτητη σε αρκετές εφαρμογές του IoT ούτως ώστε να

επιτύχουν το σκοπό τους. Πέρα από αυτούς τους αισθητήρες υπάρχουν κι άλλοι όπως το γυροσκόπιο, που ανιχνεύει τον προσανατολισμό του τηλεφώνου, ο αισθητήρας του φωτός, μέσω του οποίου ρυθμίζεται η φωτεινότητα της οθόνης, ή ο ανιχνευτής ταχύτητας.

3.5.2 Αισθητήρες για την υγεία

Ο τομέας της υγείας έχει αποκτήσει σημαντικά πλεονεκτήματα χάρη στην ανάπτυξη του Internet of Things. Χρησιμοποιώντας αισθητήρες δίνεται η δυνατότητα να παρακολουθείται η υγεία ενός ασθενή από τρίτους σε περιπτώσεις που δεν βρίσκονται σε κάποιο νοσοκομείο ή είναι μόνοι τους. Έτσι, ο γιατρός ή ο υπεύθυνος θα μπορεί να βλέπει την κατάσταση του ασθενούς ή πολλών ασθενών ταυτόχρονα και να επεμβαίνει όποτε χρειάζεται. Τέτοιοι αισθητήρες χρησιμοποιούνται για να μετρούν τους σφυγμούς, την καρδιά, τη θερμοκρασία του σώματος ή τα επίπεδα αναπνοής. Τα smartwatch για παράδειγμα έχουν τέτοιες λειτουργίες και μόλις συνδεθούν με τις εφαρμογές των κινητών τηλεφώνων δίνεται η δυνατότητα να επεξεργαστούν τα δεδομένα αυτά.

3.5.3 Περιβαλλοντικοί και χημικοί αισθητήρες

Οι περιβαλλοντικοί αισθητήρες έχουν ως στόχο να ανιχνεύουν κάποιες παραμέτρους στο φυσικό περιβάλλον όπως είναι η υγρασία, η θερμοκρασία, η πίεση ή η ρύπανση των υδάτων. Επίσης, οι χημικοί αισθητήρες ανιχνεύουν βιοχημικές και χημικές ουσίες. Και οι δύο τύποι αισθητήρων μπορούν να φανούν αρκετά χρήσιμοι για να μετριούνται η ποιότητα του αέρα σε μια πόλη ή διάφοροι ρύποι στο νερό.

3.5.4 Ενεργοποιητές

Οι ενεργοποιητές είναι κάποιες συσκευές οι οποίες μετατρέπουν μια ηλεκτρική ενέργεια σε κάποια άλλη μορφή, πιο χρήσιμη για τη λειτουργία που χρειάζεται. Κάποια παραδείγματα αυτής της μορφής είναι τα φώτα, τα ηχεία ή οι οθόνες. Ουσιαστικά είναι σαν ένα “αόρατο δάχτυλο” το οποίο μπορεί για παράδειγμα να ανάψει τα φώτα όταν του δοθεί η εντολή, να κλειδώσει πόρτες ή παράθυρα αλλά και να ειδοποιήσει τους χρήστες για θέματα ασφαλείας ή παραβίασης.

ΚΕΦΑΛΑΙΟ 4 - Εφαρμογές του IoT

Οι τομείς στους οποίους εφαρμόζεται το Internet of Things συνεχώς αναπτύσσονται και πληθαίνουν. Βελτιώσεις και καινοτομίες είναι απαραίτητες για το μέλλον του συγκεκριμένου τομέα, καθώς και οι έρευνες μέσω των οποίων αποκτούμε σημαντικές γνώσεις για την πορεία. Οι εφαρμογές του IoT “υπόσχονται” πως θα βελτιώσουν την ποιότητα ζωής των ανθρώπων και της κοινωνίας, καθώς υπάρχουν σε όλο και περισσότερους τομείς τους περισσότερους από τους οποίους θα αναπτύξουμε παρακάτω.

4.1 Έξυπνο σπίτι

Τα έξυπνα σπίτια σίγουρα γίνονται όλο και πιο δημοφιλή με το πέρασμα του χρόνου και μελλοντικά θα υπάρχουν σε εξαιρετικά μεγάλο βαθμό. Είναι πολλές οι “ευκολίες” και οι χρήσεις που μπορεί να προσφέρει ένα έξυπνο σπίτι, αρκεί να χρησιμοποιηθούν σωστά. Οι άνθρωποι συνεχώς έρχονται όλο και πιο κοντά με την τεχνολογία και συνηδειτοποιούν πως μπορούν να βελτιώσουν τόσο την ποιότητα ζωής τους όσο και την προστασία τους μέσω αυτής. Επίσης, η τεχνολογία ωριμάζει συνεχώς όσον αφορά τους αισθητήρες και τα ασύρματα δίκτυά τους και συνεπώς προσφέρει νέες λύσεις.[3]

Τα οφέλη σε ένα έξυπνο σπίτι προέρχονται από τους αισθητήρες, οι οποίοι είναι ικανοί να παρέχουν αυτοματοποιημένες υπηρεσίες στον χρήστη. Οι καθημερινές δουλειές οι οποίες επαναλαμβάνονται και μπορούν να προγραμματιστούν, μπορούν να αυτοματοποιηθούν και να τις αναλάβουν εξ ολοκλήρου ή έως ένα σημείο οι εφαρμογές του IoT. Ακόμα όμως και όσες επηρεάζονται από άλλους παράγοντες οι οποίοι χρειάζεται να λαμβάνονται υπόψη, μπορούν επίσης να εκτελεστούν από τις εφαρμογές αυτές. Συνήθως μέσω των αισθητήρων κίνησης λαμβάνονται ωφέλιμα

συμπεράσματα και επιλογές όπως η εξοικονόμηση ενέργειας γίνονται με πολύ πιο εύκολο τρόπο. Για παράδειγμα, μια εφαρμογή μπορεί να απενεργοποιεί τα φώτα και κάποιες συσκευές όταν οι αισθητήρες δεν ανιχνεύουν κίνηση στο χώρο και να τα θέτει ξανά σε λειτουργία μόλις επιστρέψει ο χρήστης. Άλλος πολύ ενδιαφέρον τρόπος που συμβάλλει στην εξοικονόμηση ενέργειας είναι να συλλέγουν δεδομένα οι αισθητήρες από το περιβάλλον. Ελέγχοντας τα επίπεδα της υγρασίας, της θερμοκρασίας ή του φωτός, μπορούν οι κατάλληλες εφαρμογές να κάνουν τις αντίστοιχες δράσεις ούτως ώστε να επιφέρουν τα επιθυμητά αποτελέσματα στο χώρο του σπιτιού. Θα μπορούσαν παραδείγματος χάριν να ενεργοποιούν αυτόματα το κλιματιστικό τις στιγμές που η θερμοκρασία πέφτει κάτω από την προκαθορισμένη ή όταν αυξάνεται η υγρασία.

Η χρησιμότητά τους όμως δεν σταματάει στις διάφορες διευκολύνσεις που μπορούν να προσφέρουν. Μπορούν να φανούν πολύ χρήσιμες και σε περιπτώσεις ασφαλείας για άτομα που ενδεχομένως δεν μπορούν να φροντίσουν πλήρως τον εαυτό τους, όπως για παράδειγμα κάποιον ηλικιωμένο. Χρησιμοποιώντας τους αισθητήρες μπορεί να γίνει αντιληπτή σε κάποιον απομακρυσμένο χρήστη η κατάσταση υγείας του ηλικιωμένου ή ενδεχομένως κάποια πτώση του. Σε τέτοιες περιπτώσεις η άμεση δράση κάποιου τρίτου ατόμου μπορεί να φανεί πλήρως βοηθητική αλλά και να αποτρέψει κάποια δυσμενή κατάσταση.

Δίνοντας όμως πολλές πληροφορίες για ένα σπίτι στους αισθητήρες και στις εφαρμογές που χρησιμοποιούνται, απαραίτητη κρίνεται η ασφάλεια και η προστασία των δεδομένων αυτών. Κανένας δεν θα ήθελε να φτάσουν στοιχεία του σπιτιού του σε κάποιον χάκερ ή σε έναν κλέφτη οι οποίοι θα εκμεταλλευτούν τις πληροφορίες υπέρ τους. Απαιτείται λοιπόν η εμπιστοσύνη μεταξύ των εφαρμογών του Internet of Things και των ανθρώπων που τις χρησιμοποιούν και για αυτό το λόγο σε περιπτώσεις κάποιας ανωμαλίας θα πρέπει να ενημερώνεται κατευθείαν ο χρήστης.

Εικόνα 4.1 - Έξυπνο σπίτι

4.2 Έξυπνη μετακίνηση

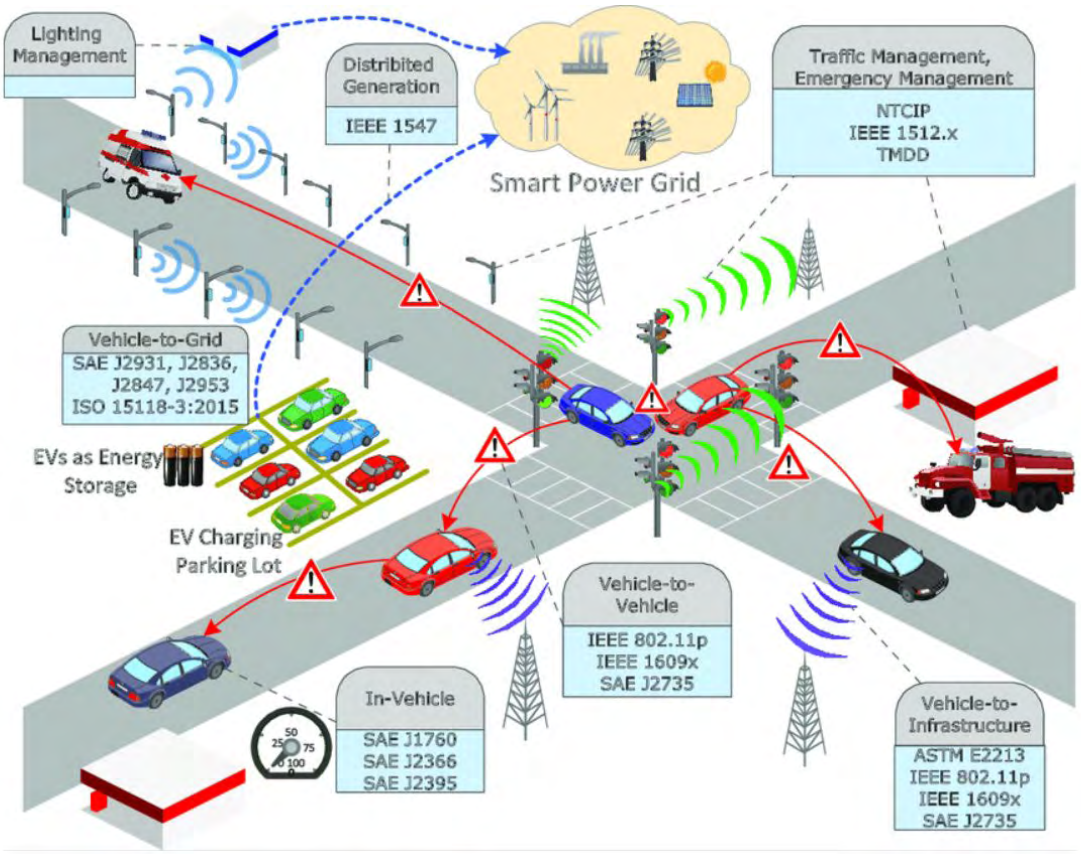
Η κυκλοφοριακή συμφόρηση στους δρόμους, η στάθμευση των αυτοκινήτων αλλά και η αποφυγή ατυχημάτων μπορούν να βελτιωθούν σε μεγάλο βαθμό με τη χρήση των εφαρμογών του IoT. Τεχνολογίες αισθητήρων όπως είναι το Gps, ανιχνευτές ταχύτητας αλλά και η χρήση RFID για την ταυτότητα του κάθε αυτοκινήτου μπορούν να οδηγήσουν σε χρήσιμα συμπεράσματα και να επιφέρουν σημαντικά οφέλη στην κυκλοφορία. Για να επιτευχθεί αυτό, θα πρέπει τα αυτοκίνητα να συνδεθούν μεταξύ τους σε ένα δίκτυο και μέσω των αισθητήρων θα μπορούν να γίνουν εκτιμήσεις ούτως ώστε να αποφευχθεί μια κυκλοφοριακή συμφόρηση. Επίσης, μελετώντας τα μοτίβα επισκεψιμότητας θα είναι εφικτές οι προβλέψεις για τις μελλοντικές συνθήκες κυκλοφορίας σε διαφορετικές περιοχές της πόλης.

Μέχρι σήμερα η ασφάλεια στους δρόμους κρίνεται καθαρά από τις οδηγικές συμπεριφορές των οδηγών. Έξυπνες εφαρμογές που έχουν προταθεί είναι ικανές να βοηθήσουν με σκοπό να γίνουν ασφαλέστερα τα προγράμματα οδήγησης. Παρακολουθώντας τις οδηγικές συμπεριφορές θα είναι σε θέση να ανιχνεύσουν πότε ένας οδηγός νιώθει υπνηλία και να του προτείνουν να ξεκουραστεί πριν συνεχίσει ή σύμφωνα με το ιστορικό του συγκεκριμένου οδηγού να καταλαβαίνουν αν οδηγεί φυσιολογικά ή υπάρχουν ανωμαλίες. Για παράδειγμα, τέτοια συμπεράσματα μπορούν να δοθούν μέσα από αισθητήρες για την ανίχνευση κίνησης των ματιών ή την ανίχνευση πίεσης των χεριών του στο τιμόνι.

Όσον αφορά τη στάθμευση, σε ένα έξυπνο σύστημα μεταφοράς δίνεται η δυνατότητα στο χρήστη μέσω του διαδικτύου να ελέγξει ποιες θέσεις είναι ελεύθερες και να πάει κατευθείαν εκεί. Με έναν τόσο απλό τρόπο θα μπορούσε να λυθεί το πρόβλημα που διαιωνίζει πολλούς οδηγούς σε περιοχές με περιορισμένες θέσεις στάθμευσης.

Οι έξυπνοι σηματοδότες είναι εκείνοι οι οποίοι ανιχνεύουν και επεξεργάζονται την κυκλοφορία στους γειτονικούς δρόμους και καθορίζουν αντίστοιχα τη λειτουργία τους. Βλέποντας πως σε μία διασταύρωση υπάρχει αυξημένη κίνηση προς μία κατεύθυνση, θα ήταν ωφέλιμο να παραμείνουν πράσινα και να ξαναγίνουν κόκκινα μόλις εμφανιστούν οδηγοί στην άλλη μεριά.

Τέλος, οι εφαρμογές ανίχνευσης ατυχημάτων θα μπορούσαν μέσω των ανιχνευτών ταχύτητας αλλά και των ακουστικών δεδομένων να καταλαβαίνουν πότε συμβαίνει ένα ατύχημα και να στέλνουν κατευθείαν ένα σήμα στο κοντινότερο νοσοκομείο.



Εικόνα 4.2 - Έξυπνη μετακίνηση

4.3 Έξυπνη ενέργεια

Το έξυπνο δίκτυο είναι ένα σύστημα που παρέχει την δυνατότητα στην τεχνολογία πληροφοριών και επικοινωνιών να παράγεται, να καταναλώνεται, να μεταδίδεται και να διανέμεται εύκολα στις μέρες μας. Αυτό που καθιστά έξυπνη την παραγωγή, μετάδοση και διανομή ηλεκτρικής ενέργειας, είναι το γεγονός ότι επιτρέπει στον καταναλωτή και τον προμηθευτή να αντιληφθεί καλύτερα τη ροή ισχύος και να κατανοήσει τη δυναμική τιμολόγηση, πράγμα που μπορεί να εξασφαλίσει πολλή ενέργεια.

Σε ένα τέτοιο δίκτυο, η παραγωγή και η ανάπτυξη της ενέργειας σε όλο το σύστημα πραγματοποιείται με την ύπαρξη αισθητήρων. Επομένως, το έξυπνο δίκτυο στην ουσία αποτελείται από μια σειρά μικροδικτύων προκειμένου να γίνεται σωστή επιτήρηση του συστήματος. Τα μικροδίκτυα αυτά, δημιουργούν μεγάλη ισχύ ώστε να διασφαλίσουν τις απαιτήσεις των τοπικών τοποθεσιών, να μεταφέρουν πίσω την πλεονάζουσα ενέργεια στο κεντρικό δίκτυο αλλά και να απαιτήσουν ενέργεια από αυτό, σε περίπτωση ελλειψης της.

Κάποιες από τις εφαρμογές IoT που υπάρχουν σε αυτά τα δίκτυα είναι η διαδικτυακή παρακολούθηση των γραμμών μεταφοράς με σκοπό να αποτρέψει πιθανές καταστροφές και να είναι αποδοτική η χρήση της ενέργειας στα έξυπνα σπίτια, εφόσον παρέχουν έναν έξυπνο μετρητή για να παρακολουθείται η κατανάλωση της ενέργειας.

Οι μετρητές αυτοί μελετούν και επεξηγούν τα πρότυπα κατανάλωσης ισχύος και σε κανονικούς αλλά και σε μέγιστους χρόνους φόρτωσης. Εν συνεχεία, οι πληροφορίες αυτές στέλνονται στον διακομιστή καθώς επίσης παραχωρούνται και στον χρήστη, ώστε να είναι εφικτή η ρύθμιση της παραγωγής σύμφωνα με τα πρότυπα κατανάλωσης. Τέλος, ο χρήστης έχει τη δυνατότητα να ρυθμίσει έτσι τη χρήση του προκειμένου να ελαττωθεί το κόστος και οι έξυπνες ηλεκτρικές συσκευές να χρησιμοποιήσουν τις πληροφορίες αυτές ούτως ώστε να λειτουργούν στις κατάλληλες ώρες.

4.4 Έξυπνη γεωργία

Στη γεωργική παραγωγή, σημαντικό ρόλο παίζουν η θερμοκρασία και η υγρασία του περιβάλλοντος. Αυτές οι δύο παράμετροι μπορούν να ελεγχθούν από τους αγρότες χρησιμοποιώντας αισθητήρες με σκοπό η παραγωγή να γίνει αρκετά πιο αποδοτική. Ένα παράδειγμα μιας τέτοιας εφαρμογής είναι και η αυτόματη άρδευση που ρυθμίζεται βάση των καιρικών συνθηκών.

Ακόμα μία σημαντική εφαρμογή που συμβάλλει στη βελτίωση της γεωργίας είναι και τα θερμοκήπια, στα οποία διάφορα στοιχεία όπως η θερμοκρασία, η υγρασία αλλά και οι πληροφορίες για το έδαφος μπορούν να μετρηθούν και να σταλούν στο δίκτυο για να επεξεργαστούν. Τα συμπεράσματα που προκύπτουν βοηθούν ώστε να αυξηθεί η ποιότητα και η απόδοση της παραγωγής. Επίσης, υπάρχει η δυνατότητα ανίχνευσης για τυχόν υπολείμματα φυτοφαρμάκων με τη χρήση ενός βιοαισθητήρα. Από τα δεδομένα που συλλέγονται, καταλήγουμε σε χρήσιμα συμπεράσματα όσον αφορά την ποσότητα, το σημείο και τη χρονική διάρκεια. Έτσι επιτυγχάνουμε μια πιο αποτελεσματική και ποιοτική καλλιέργεια. Επιπρόσθετα, τα αγροτικά προϊόντα θα μπορούν να συσκευάζονται σε κούτες οι οποίες θα αντιστοιχούν σε έναν κωδικό QR. Σαρώνοντας τον κωδικό αυτό οι καταναλωτές θα έχουν τη δυνατότητα να παρατηρήσουν την ποσότητα των φυτοφαρμάκων που υπάρχει σε αυτά πριν καν ακόμα τα αγοράσουν.

Ένα άλλο θέμα που απασχολεί αρκετά είναι η ρύπανση που προκαλούν τα οχήματα στην ατμόσφαιρα. Οι επιπτώσεις δεν είναι μικρές και έχουν προταθεί εφαρμογές για να τις μειώσουν. Μία από αυτές είναι σε θέση να συλλέγει πληροφορίες από την ατμόσφαιρα και να παρακολουθεί τα επίπεδα ρύπανσης. Θεωρώντας ότι τα οχήματα είναι εξοπλισμένα με RFID ετικέτες και οι δρόμοι με RFID αναγνώστες, θα είναι σε θέση να εντοπίσει τα οχήματα που προκαλούν την περισσότερη ρύπανση και να ληφθούν μέτρα ώστε να αντιμετωπιστούν.

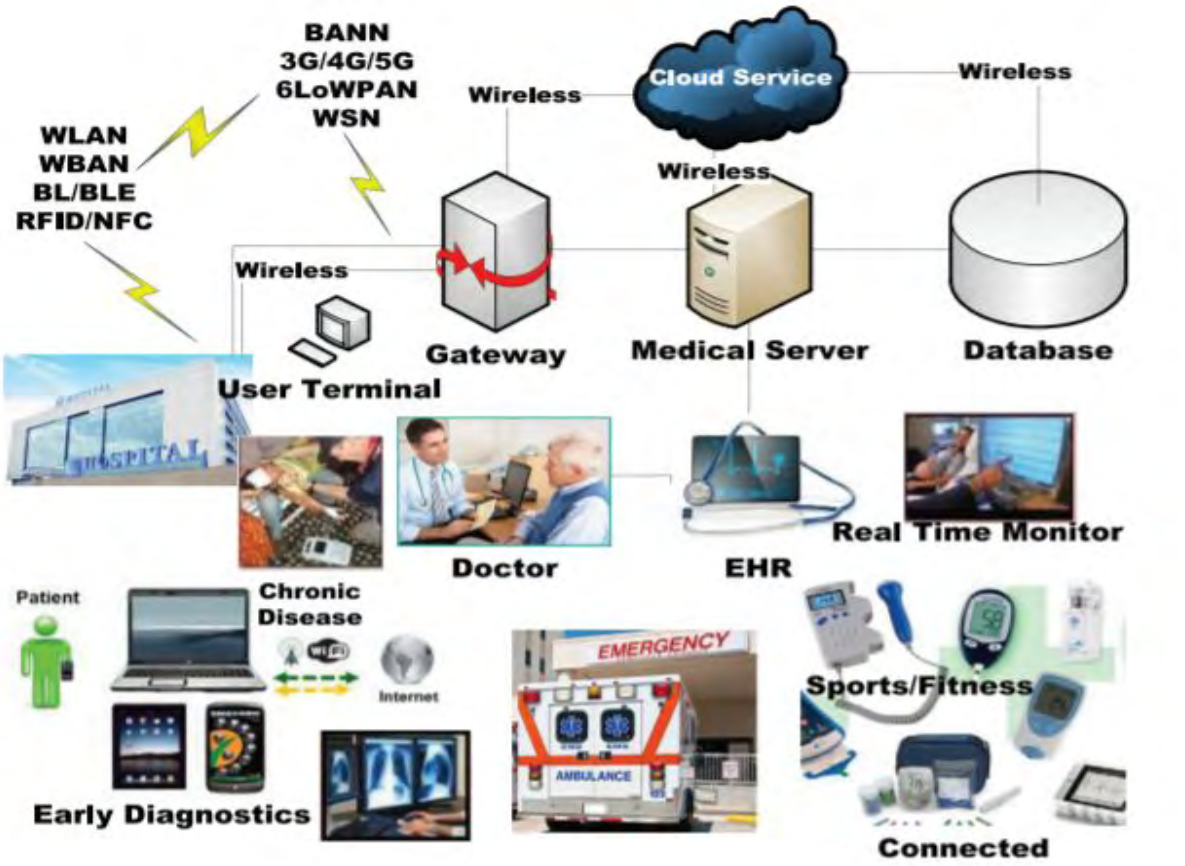
Εικόνα 4.3 - Απεικόνιση της έξυπνης γεωργίας

4.5 Έξυπνη Υγεία

Ο τομέας της υγείας θα μπορούσε να αποκομίσει τεράστια οφέλη από τη χρήση των Internet of Things συστημάτων και να μεταμορφώσει προς το καλύτερο τα συστήματα και τις μεθόδους που χρησιμοποιούνται. Αρχικά, μέσω των αισθητήρων που διαθέτουν και τις πληροφορίες που συλλέγονται, θα είναι σε θέση να

παρακολουθούν την υγεία ενός ασθενή και να βγάζουν συμπεράσματα για την πρόοδό του. Με το πέρας του χρόνου οι πληροφορίες αυτές θα γίνονται όλο και περισσότερες και μαζί με αυτές θα μεγαλώνει και η εμπειρία των γιατρών, καθώς θα μπορούν να έχουν στοιχεία για πολλές περιπτώσεις βοηθώντας τους να κρίνουν ποια θα είναι η κατάλληλη θεραπεία για τον επόμενο ασθενή. Επιπλέον, τους δίνεται η δυνατότητα να μπορούν να παρακολουθούν τους ασθενείς τους από απόσταση και σε πραγματικό χρόνο, δίνοντας έτσι τέλος σε περιπτώσεις που χρειάζεται να παραμείνει στο νοσοκομείο για παράδειγμα κάποιος ασθενής μόνο και μόνο επειδή χρειάζεται να παρακολουθείται η υγεία του. Συσκευές που μπορούν να μεταφερθούν θα λύσουν αυτό το πρόβλημα και θα μειώσουν τις επισκέψεις στα ιατρεία για απλούς ελέγχους, καθώς θα είναι εφικτό πολύ εύκολα από το σπίτι. Συνεπώς, καταλαβαίνουμε ότι ορισμένα έξοδα που χωρίς τη χρήση του IoT θεωρούνται απαραίτητα, θα μπορούν να περιοριστούν ή ακόμα και να σταματήσουν να υπάρχουν. Επιπρόσθετα, άνθρωποι όπως κάποιοι ηλικιωμένοι ή ασθενείς οι οποίοι αναγκάζονται να μένουν σε νοσοκομεία για μεγάλα χρονικά διαστήματα, με σκοπό να παρακολουθείται συνεχώς η υγεία τους, θα τους δοθεί επιτέλους η δυνατότητα να ζήσουν όπου εκείνοι επιθυμούν παίρνοντας απλά μαζί τους τον κατάλληλο εξοπλισμό.[12]

Μία επιπλέον λειτουργία που μπορεί να προστεθεί χρησιμοποιώντας την τεχνολογία του IoT είναι η αποτελεσματική διαχείριση των φαρμάκων. Σε δύσβατες περιοχές ή σε περιοχές που δεν πληρούν τις κατάλληλες συνθήκες για την αποθήκευση εμβολίων για παράδειγμα, υπάρχουν περιπτώσεις ανά τον κόσμο που οι άνθρωποι νοσούν εξαιτίας της ελλιπούς προσβασιμότητας. Πιο συγκεκριμένα, σε περιοχές της Αφρικής όπου το ρεύμα δεν είναι σταθερό έτσι ώστε να μπορούν να αποθηκεύσουν τα εμβόλια σε κάποιο ψυγείο με τη σωστή ψύξη, μπορεί να δοθεί λύση με τη χρήση ενός έξυπνου ψυγείου. Χρησιμοποιώντας την τεχνολογία μπορούμε να παρακολουθήσουμε από απόσταση αν ένα ψυγείο διατηρεί τη θερμοκρασία που απαιτείται έτσι ώστε να διατηρηθεί η ποιότητα του εμβολίου και να επέμβουμε στις περιπτώσεις που κάτι χρειάζεται άμεση επέμβαση. Στο παρακάτω σχήμα φαίνονται κάποιες από τις συσκευές αυτές που συμβάλλουν στη βελτίωση της υγείας χρησιμοποιώντας την τεχνολογία του Internet of Things.[17]



Εικόνα 4.4 - Απεικόνιση συστημάτων στην έξυπνη υγεία

ΚΕΦΑΛΑΙΟ 5 - ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ

5.1 Εισαγωγή

Το Internet of Things είναι ένας τομέας που μπορεί να προσφέρει στους χρήστες σχεδόν απεριόριστες δυνατότητες, απλοποιώντας πολλές λειτουργίες και κάνοντας τη ζωή μας πιο “εύκολη”. Μέσω των αισθητήρων που το αποτελούν και τις πληροφορίες που συλλέγουν, οδηγούμαστε σε χρήσιμα συμπεράσματα ή αναθέτουμε λειτουργίες αυτόματα στις συσκευές που το αποτελούν. Το γεγονός όμως ότι αυτός ο τεράστιος όγκος δεδομένων που συλλέγεται βρίσκεται στο διαδίκτυο, σημαίνει ότι θα πρέπει να καταφέρουμε να τον κρατήσουμε και ασφαλή. Όπως όλοι γνωρίζουμε το διαδίκτυο έχει προσφέρει πολλά θετικά στην εξέλιξη της τεχνολογίας, αλλά δεν παύουν να υπάρχουν και ορισμένα μειονεκτήματα. Τα μειονεκτήματα αυτά εμφανίζονται κυρίως σε περιπτώσεις στις οποίες δεν μπορούμε να διασφαλίσουμε την ασφάλεια των συστημάτων και δεχόμαστε ενδεχομένως κάποια επίθεση. Υπάρχουν κάποια βασικά χαρακτηριστικά τα οποία θα πρέπει να υπάρχουν σε όλα τα συστήματα του IoT έτσι ώστε να μπορέσουμε να κρατήσουμε ασφαλή τα δεδομένα μας, αλλά όπως η τεχνολογία της ασφάλειας αναπτύσσεται, έτσι ακριβώς αναπτύσσεται και η τεχνολογία της αντίθετης πλευράς, δηλαδή εκείνης των εισβολέων. Παρακάτω θα αναλύσουμε πιθανές επιθέσεις που παρατηρούνται στον τομέα του Internet of Things αλλά και πιθανούς τρόπους για να τις αποφύγουμε.

5.2 Βασικές απαιτήσεις ασφάλειας

- **Εμπιστευτικότητα**

Είναι αυτονόητο ότι στα συστήματα του IoT μπορεί να περιέχονται προσωπικά δεδομένα και ευαίσθητες πληροφορίες, τα οποία δεν θα έπρεπε να φτάσουν σε χέρια τρίτων. Όλες οι συσκευές που ανήκουν σε ένα τέτοιο σύστημα θα πρέπει να είναι έμπιστες για τον χρήστη και να διασφαλίζεται η χρήση τους μόνο από εκείνους. Ο τρόπος για να επιτευχθεί κάτι τέτοιο είναι η συμμετρική ή ασύμμετρη κρυπτογράφηση, μέσω της οποίας δεν δίνεται ο έλεγχος σε τρίτους. Η συγκεκριμένη απαίτηση είναι σημαντική στα συστήματα IoT καθώς σκεφτείτε για παράδειγμα να λάβει κάποιος διαρρήκτης όλα τα στοιχεία για τις συσκευές σε ένα σπίτι. Ενδεχομένως να μπορέσει να ξεκλειδώσει και να ελέγξει και εκείνος ότι βρίσκεται μέσα στο σπίτι και είναι συνδεδεμένο στο διαδίκτυο, με συνέπειες καταστροφικές για τους πραγματικούς χρήστες.

- **Ιδιωτικότητα**

Λαμβάνοντας υπόψη ότι το Internet of Things μπορεί να εφαρμοστεί σε πολλούς και διάφορους τομείς της καθημερινής μας ζωής, η ιδιωτικότητα των δεδομένων είναι ένα εξίσου βασικό κριτήριο. Συνεπώς θα πρέπει να διασφαλίζεται το γεγονός ότι μόνο οι “σωστοί” χρήστες θα πρέπει να έχουν πρόσβαση στα στοιχεία του συστήματος. Όσο χρησιμοποιούνται πρωτόκολλα για τον έλεγχο της πρόσβασης αλλά και για το λόγο για κάποια μεταφορά των δεδομένων, είναι δυνατό να τηρηθεί η ιδιωτικότητα του χρήστη. Επίσης αρκετά σημαντικό θεωρείται ο χρήστης και τα στοιχεία του να μην αντιστοιχίζονται σε τρίτους και η ανωνυμία του χρήστη να υπερισχύει.

- **Ακεραιότητα**

Στα πλαίσια του IoT, ανταλλάσσονται σημαντικά δεδομένα και με φορείς όπως κυβερνητικές αρχές, πάροχοι υπηρεσιών διαδικτύου (ISP) και ελεγκτικοί μηχανισμοί, οι οποίοι απαιτούν τα δεδομένα, κατά την αποθήκευση και τη μετάδοσή τους, να μην αλλοιώνονται ούτε από δόλο αλλά ούτε από σφάλμα.

Η ακεραιότητα των δεδομένων είναι πρωταρχικής σημασίας κατά το σχεδιασμό αξιόπιστων IoT συστημάτων. Αυτό επιτυγχάνεται με κώδικες αυθεντικοποίησης μηνύματος (MAC) που χρησιμοποιούν συναρτήσεις κατακερματισμού (hash functions). Η επιλογή των τεχνικών αυτών πάλι καθορίζεται από τις δυνατότητες των εκάστοτε συσκευών. Χαρακτηριστικό παράδειγμα που η ακεραιότητα των δεδομένων είναι εξ ’ορισμού αναγκαία αποτελεί το «έξυπνο» σπίτι το οποίο είναι συνδεδεμένο με ένα «έξυπνο» πλέγμα ηλεκτροδότησης. Σ ’αυτήν την περίπτωση η ηλεκτρονική και αυτόματη έκδοση των λογαριασμών δε συνάδει με πιθανή αλλοίωση στα δεδομένα της κατανάλωσης ηλεκτρικού ρεύματος

- **Διαθεσιμότητα**

Στο περιβάλλον ενός IoT συστήματος περιλαμβάνονται συσκευές οι οποίες λειτουργούν σαν κόμβοι με σκοπό να μεταφέρουν τις πληροφορίες και να καθιστούν εφικτή τη σύνδεση στο δίκτυο. Οι συσκευές αυτές συνήθως παρακολουθούν για παράδειγμα την κατανάλωση του ρεύματος ή τη μετάδοση εικόνων από τις κάμερες ασφαλείας. Τίθεται σκόπιμο όμως οι πληροφορίες αυτές να είναι προσβάσιμες από τους χρήστες οποιαδήποτε στιγμή εκείνοι θελήσουν. Δεδομένου ότι τα πρωτόκολλα ασφαλείας δεν μπορούν να εγγυηθούν για αυτή τη λειτουργία, απαιτούνται διάφορες τεχνικές αλλά και μετρήσεις έτσι ώστε να βεβαιωθεί το ποσοστό διαθεσιμότητας. Συνήθως τέτοιες συμφωνίες γίνονται ανάμεσα στους χρήστες και στους παρόχους.[8]

- **Αυθεντικότητα**

Καίριας σημασίας χαρακτηριστικό ενός συστήματος Internet of Things είναι η αυθεντικότητα των δεδομένων και η εγκυρότητα της πηγής από την οποία λαμβάνονται. Η ταυτότητα τόσο του δέκτη που δέχεται τις πληροφορίες όσο και του αποστολέα που τις στέλνει θα πρέπει να επαληθεύεται και να είναι

έμπιστη. Μέσω αλγορίθμων που περιλαμβάνονται σε ορισμένα πρωτόκολλα αυτό είναι δυνατό να επιτευχθεί.

- **Έλεγχος πρόσβασης**

  Οι μηχανισμοί που είναι υπεύθυνοι να ελέγχουν το ποιος έχει πρόσβαση στα διάφορα δεδομένα παίζουν καθοριστικό ρόλο σε ένα σύστημα IoT. Λαμβάνοντας υπόψη ότι οι συσκευές ενός τέτοιου συστήματος είναι πολλές και έχουν τη δυνατότητα να συλλέγουν ιδιωτικές και προσωπικές πληροφορίες, κρίνεται σκόπιμο να ελέγχεται και να ταυτοποιείται ο καθένας που ζητάει πρόσβαση σε αυτές. Οι άδειες χρήσης και οι λίστες ελέγχου πρόσβασης αναλαμβάνουν αυτό το ρόλο και γίνονται προσπάθειες ούτως ώστε να είναι όσο πιο ακριβείς και σωστοί γίνονται.[8]

- **Αξιοπιστία**

  Οι συσκευές του IoT έχουν ως σκοπό να συλλέξουν και να μεταφέρουν τα κατάλληλα δεδομένα έτσι ώστε να αξιοποιηθούν κατάλληλα και να καταλήξουμε σε χρήσιμα συμπεράσματα. Ακόμα και μια μικρή παραμόρφωση σε κάποιο στοιχείο θα μπορούσε να οδηγήσει σε ανεπιθύμητες καταστάσεις και συνεπώς να αλλοιωθεί το πολυπόθητο αποτέλεσμα. Για αυτό το λόγο, θα πρέπει να διασφαλίζεται η αξιοπιστία των δεδομένων και να είναι όλα έγκυρα. Αυτός ο ρόλος εκτελείται από ένα μηχανισμό ο οποίος στηρίζεται στην ανταλλαγή διαπιστευτηρίων πριν τη μετάδοση των πληροφοριών.

5.3 Κατηγοριοποίηση των πιθανών επιθέσεων

Οι επιθέσεις που μπορεί να υποστεί ένα σύστημα Internet of Things μπορούν να κατηγοριοποιηθούν στις εξής κατηγορίες : φυσική, μέσω του διαδικτύου, μέσω των εφαρμογών του συστήματος ή μέσω κρυπτογράφησης. Ο λόγος που τις κατηγοριοποιούμε είναι ότι χρησιμοποιούνται πολλές τεχνολογίες και πρωτόκολλα από την αρχή έως το τελικό στάδιο μιας λειτουργίας οπότε θα αναλύσουμε στο καθένα από αυτά τα στάδια τις πιθανές επιθέσεις που μπορεί να δεχθεί.

Παρακάτω φαίνονται στο σχήμα οι πιθανές επιθέσεις ανάλογα με το επίπεδο της αρχιτεκτονικής.

<table>
<tr><th>Physical Attacks</th><th>Network Attacks</th><th>Software Attacks</th><th>Encryption Attacks</th></tr>
<tr><td>Node Tampering</td><td>Traffic Analysis Attacks</td><td rowspan="2">Virus and Worms</td><td>Side Chanel Attacks</td></tr>
<tr><td>RF Interference</td><td>RFID Spoofing</td><td rowspan="5">Cryptanalysis Attacks:
a) Ciphertext Only Attack
b) Known Plaintext Attack
c) Chosen Plaintext or Ciphertext Attack</td></tr>
<tr><td>Node Jamming</td><td>RFID Cloning</td><td rowspan="2">Spyware and Adware</td></tr>
<tr><td>Malicious Node Injection</td><td>RFID Unauthorised Access</td></tr>
<tr><td>Physical Damage</td><td>Sinkhole Attack</td><td rowspan="2">Trojan Horse</td></tr>
<tr><td>Social Engineering</td><td>Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Sleep Deprivation Attack</td><td rowspan="2">Denial of Service</td><td rowspan="2">Malicious scripts</td><td rowspan="3">Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Routing Information Attacks</td></tr>
<tr><td rowspan="2">Malicious Code Injection on the Node</td><td rowspan="2">Denial of Service</td></tr>
<tr><td>Sybil Attack</td></tr>
</table>

Εικόνα 5.1 - Πιθανές επιθέσεις ανάλογα με το επίπεδο της αρχιτεκτονικής

5.3.1 Φυσικές επιθέσεις

Αυτές οι επιθέσεις αναφέρονται σε περιπτώσεις που ο επιτιθέμενος αλλάζει ή καταστρέφει κάποιο υλικό εξάρτημα του συστήματος ή κάποια λειτουργία του και συνεπώς βρίσκεται κοντά στο χώρο.

1. **Παραβίαση κόμβου**

Ο επιτιθέμενος μπορεί να καταστρέψει κάποιον κόμβο αισθητήρων ή να τον αλλάξει με έναν δικό του, ο οποίος όμως δεν θα έχει την ίδια λειτουργία. Επίσης, μπορεί να “κλέψει” κάποιες πληροφορίες από ένα εξάρτημα του συστήματος με αποτέλεσμα οι πληροφορίες αυτές να πάψουν να είναι απόρρητες προς τρίτους. Με αυτόν τον τρόπο, η παραβίαση του κόμβου θα προκαλέσει ανεπιθύμητες ενέργειες.

2. **Παρεμβολές RF σε RFID**

Στέλνοντας λανθασμένα σήματα ή σήματα θορύβου στην ίδια συχνότητα που χρησιμοποιούν τα RFID έχει ως αποτέλεσμα να παραμορφώνονται ή να αποκρύπτονται τα σωστά σήματα και έτσι οι τελικές πληροφορίες που λαμβάνονται από το σύστημα να είναι λανθασμένες.

3. **Μπλοκάρισμα σε κόμβο WSN**

Όπως και στην προηγούμενη περίπτωση, έτσι και εδώ είναι πιθανό να σταλούν λανθασμένα σήματα μέσω της ραδιοσυχνότητας και επομένως να πειραχτεί η συχνότητα των κόμβων με τους αισθητήρες. Αν επιτευχθεί κάτι τέτοιο θα έχει ως αποτέλεσμα να μπλοκαριστεί ο κόμβος και να μην καταφέρει να στείλει τα δεδομένα που θα έπρεπε.

4. **Παρεμβολή κακόβουλου κόμβου**

Μία προσθήκη ενός κακόβουλου κόμβου ανάμεσα σε δύο ήδη υπάρχοντες μπορεί να δώσει τη δυνατότητα στον “εχθρό” να συλλέγει και να ελέγχει όλες τις πληροφορίες που περνάνε από τους κόμβους αυτούς. Με αυτόν τον τρόπο αλλάζει η λειτουργία του συστήματος και επιφέρει αρνητικά αποτελέσματα.

5. **Φυσική ζημιά**

Ο αντίπαλος μπορεί να καταστρέψει με φυσικό τρόπο κάποια ή κάποιες συσκευές του IoT συστήματος με αποτέλεσμα να τεθούν εκτός λειτουργίας και να μην συλλέξουν ή μεταδώσουν τις πληροφορίες που θα έπρεπε. Για παράδειγμα αν μία κάμερα παρακολούθησης σπάσει, δεν θα είναι σε θέση να συνεχίσει τη λειτουργία της.

6. **Εξασθένηση της μπαταρίας**

Αρκετοί κόμβοι αισθητήρων είναι προγραμματισμένοι έτσι ώστε να σταματούν τη λειτουργία τους σε ορισμένες προκαθορισμένες στιγμές με σκοπό να παρατείνουν την ενέργεια της μπαταρίας τους. Ένα κακόβουλο λογισμικό μπορεί να τους θέσει σε πλήρη λειτουργία ανελλιπώς με αποτέλεσμα να μην εξοικονομούν τη μπαταρία που χρειάζεται και συνεπώς κάποια στιγμή θα αναγκαστούν να σταματήσουν αφού θα έχει τελειώσει η μπαταρία τους.

7. **Προσθήκη κακόβουλου λογισμικού**

Εισάγοντας έναν κακόβουλο κώδικα σε κάποιον κόμβο του συστήματος θα μπορούσε να δώσει πρόσβαση στον επιτιθέμενο όχι μόνο στον κόμβο αυτόν, αλλά και σε ολόκληρο το σύστημα. Για παράδειγμα, εισάγοντας ένα φλασάκι με τον κατάλληλο κώδικα σε ένα κόμβο θα μπορούσε να δοθεί ο έλεγχος σε κάποιον τρίτο.

5.3.2 Επιθέσεις στο δίκτυο

Τέτοιου είδους επιθέσεις δεν απαιτούν τη φυσική παρουσία του επιτιθέμενου όπως στις προηγούμενες περιπτώσεις, αλλά μπορούν να πραγματοποιηθούν από οποιοδήποτε μέρος με πρόσβαση στο διαδίκτυο.

1. **Απόκτηση κρυμμένων πληροφοριών**

   Μέσω διαφόρων εφαρμογών μπορεί ο εισβολέας να καταλάβει ορισμένα χαρακτηριστικά του συστήματος ακόμα και εάν δεν μπορεί να τα δει άμεσα. Έχοντας γνώση για τις τεχνολογίες που χρησιμοποιούνται και δοκιμάζοντας διάφορες τεχνικές, μπορεί να καταλήξει σε συμπεράσματα για το πώς ακριβώς λειτουργεί ένα συγκεκριμένο σύστημα IoT. Αυτό συνηθίζεται να συμβαίνει πριν από την κύρια επίθεση καθώς δίνει στον επιτιθέμενο σημαντικές πληροφορίες έτσι ώστε να μπορέσει να “ξεκλειδώσει” διάφορους κόμβους στην πορεία.

2. **Πλαστογράφηση RFID ετικέτας**

   Πλαστογραφώντας ένα RFID σήμα και στέλνοντάς το για να λάβει και να καταγράψει δεδομένα από το σύστημα, δίνει τη δυνατότητα στον χρήστη να μάθει τα αληθινά στοιχεία μέσα από το σήμα που θα του απαντήσει το σύστημα. Έτσι, θα είναι σε θέση στη συνέχεια να στέλνει έγκυρα για το σύστημα σήματα και να φαίνεται ότι όλα είναι φυσιολογικά.

3. **Κλωνοποίηση RFID**

   Αν καταφέρει ένας χρήστης να αντιγράψει τα δεδομένα από την κανονική RFID ετικέτα και τα μεταφέρει σε μία δικιά του, τότε το σύστημα δεν θα είναι σε θέση να καταλάβει ποια από τις δύο είναι η αξιόπιστη καθώς θα είναι ακριβώς ίδιες.

4. **Πρόσβαση RFID από τρίτους**

   Επειδή τα περισσότερα συστήματα RFID υστερούν στο να αποκλείουν την πρόσβαση σε χρήστες που δεν έχουν την άδεια, ο επιτιθέμενος μπορεί να αλλοιώσει τα δεδομένα στους κόμβους ή ακόμα και να διαγράψει κάποια προς όφελός του.

5. **Αλλαγή κατεύθυνσης**

Ο επιτιθέμενος μπορεί να δημιουργήσει μια “τρύπα” στους κόμβους WSN με αποτέλεσμα αντί τα δεδομένα να προωθούνται στον επόμενο κόμβο, να πέφτουν και να χάνονται.

6. **Παρεμβολή κόμβου**

Όπως και στις φυσικές επιθέσεις παραπάνω, έτσι και εδώ υπάρχει η περίπτωση να προστεθεί ένας κόμβος ανάμεσα σε δύο άλλους με αποτέλεσμα να ελέγχονται και να ρυθμίζονται από τον εισβολέα όλες οι πληροφορίες που ανταλλάσουν μεταξύ τους. Η διαφορά είναι ότι εδώ δεν χρειάζεται να βρίσκεται κάποιος σε κοντινή απόσταση έτσι ώστε να τοποθετήσει τον επιπλέον κόμβο, αλλά το πράττει μέσω του δικτύου.

7. **Άρνηση υπηρεσίας**

Αν ένας χρήστης στείλει μεγαλύτερο όγκο δεδομένων στο δίκτυο από αυτόν που μπορεί να διαχειριστεί, τότε το δίκτυο θα μπλοκάρει και δεν θα μπορέσει να συνεχίσει την φυσιολογική του λειτουργία.

8. **Δρομολόγηση πληροφοριών**

Σε αυτού του είδους την επίθεση ο εισβολέας, μέσω της πλαστογραφίας ή της τροποποίησης πληροφοριών που αφορούν τη δρομολόγηση, μπορεί να “μπερδέψει” το δίκτυο και να χειρίζεται είτε την κατεύθυνση των δεδομένων είτε να στέλνει λανθασμένα μηνύματα.

5.3.3 Επιθέσεις στο λογισμικό

Οι επιθέσεις στο λογισμικό είναι εκείνες που χρειάζονται περισσότερη προσοχή, καθώς ακόμα υπάρχουν αρκετές αδυναμίες και οι κακοπροαίρετοι χρήστες βρίσκουν την ευκαιρία να επιτεθούν.

1. **Μέσω "ψαρέματος"**

   Πλαστογραφώντας πληροφορίες ή στέλνοντας email που περιέχουν μολυσμένα στοιχεία μπορεί να λάβει σημαντικές πληροφορίες που θα οδηγήσουν στο να αποκτήσει πρόσβαση σε δεδομένα που δεν επιτρέπεται.

2. **Μέσω ιού**

   Στέλνοντας ένα κακόβουλο λογισμικό στο σύστημα μπορεί να δώσει τη δυνατότητα στον επιτιθέμενο να αποκτήσει πρόσβαση σε πληροφορίες και να παραβιάσει δεδομένα.

3. **Κακόβουλοι κώδικες**

   Από τη στιγμή που τα συστήματα του Internet of Things είναι συνδεδεμένα στο διαδίκτυο, είναι πιθανό ένας χρήστης να ξεγελαστεί και να εκτελέσει κακόβουλους κώδικες οι οποίοι θα επιφέρουν αρνητικά αποτελέσματα στη λειτουργία του συστήματος, όπως για παράδειγμα τον τερματισμό του.

4. **Άρνηση υπηρεσιών**

   Πραγματοποιώντας άρνηση υπηρεσίας ο επιτιθέμενος μπορεί να επηρεάσει ή ακόμα και να αποκλείσει τους πραγματικούς χρήστες σε ένα σύστημα, και συγκεκριμένα στο επίπεδο των εφαρμογών.

5.3.4 Κρυπτογράφηση

Οι συγκεκριμένες επιθέσεις αναφέρονται σε κρυπτογραφημένες πληροφορίες οι οποίες αποκαλύπτονται στον επιτιθέμενο μέσω των παρακάτω τεχνικών.

1. **Κρυπτανάλυση**

   Χρησιμοποιώντας κάποιες τεχνικές που βασίζονται σε παράγοντες όπως ο χρόνος ή τα σφάλματα, είναι πιθανό να δοθεί πρόσβαση στο κλειδί με το οποίο θα μπορεί στη συνέχεια να αποκρυπτογραφήσει πληροφορίες.

2. **Παρέμβαση ανάμεσα σε κανάλια**

   Ένας τρόπος για να επικοινωνούν με ασφάλεια δύο κανάλια μεταξύ τους είναι να ανταλλάξουν κλειδιά και έτσι να μην μπορεί κάποιος άλλος να συμβάλλει στη μεταξύ τους επικοινωνία. Όμως, είναι πιθανό ο επιτιθέμενος να μπει ανάμεσα στα δύο αυτά κανάλια και να λάβει εκείνος τα σήματα που στέλνουν. Απαντώντας στο καθένα ξεχωριστά, θα είναι σε θέση να μπερδέψει τους διαχειριστές των καναλιών και όσο εκείνοι θα νομίζουν ότι έχουν επικοινωνία με το ζητούμενο κανάλι, εκείνος θα λαμβάνει όλα τα μηνύματα για τον εαυτό του. Έτσι, η αποκρυπτογράφηση δεδομένων θα γίνει εφικτή.

5.4 Ασφάλεια στα επίπεδα αρχιτεκτονικής

Στον τομέα του Internet of Things περιλαμβάνονται πολλές πληροφορίες και δεδομένα, τα οποία κάποιες φορές μπορούν να κοινοποιηθούν σε όλους αλλά κάποιες άλλες είναι απαραίτητο να διατηρηθούν ακέραια και απόρρητα. Θέματα

όπως η ιδιωτικότητα, η διαχείριση των πληροφοριών και η αποθήκευσή τους αλλά και ο έλεγχος πρόσβασης χρειάζονται αρκετή προσπάθεια ώστε να καταφέρουμε να τηρηθούν και να μην παραβιάζονται. Τεχνικές όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές χρησιμοποιούνται με σκοπό να εξασφαλίσουν την εμπιστευτικότητα και την ιδιωτικότητα των πληροφοριών. Συστήματα όπως τα RFID αλλά και τα δίκτυα που συνδέουν τους ασύρματους αισθητήρες χρησιμοποιούν αυτές τις τεχνικές, καθώς έρχονται σε επαφή πολύ νωρίς με τα δεδομένα και είναι σημαντικό να καταφέρουν να τα κρατήσουν ασφαλή. Όταν οι πληροφορίες μεταδίδονται μπορεί να δεχτούν επιθέσεις και να γίνουν προσπάθειες υποκλοπής από τρίτους. Κάποιοι παράγοντες που βοηθούν τους επιτιθέμενους στο να ξεκλειδώσουν κάποιο σύστημα και να υποκλέψουν πληροφορίες, είναι η πολυπλοκότητα και η διαφορετικότητα των τεχνολογιών που χρησιμοποιούνται. Το γεγονός αυτό δυσκολεύει την επικοινωνία και τη συνεργασία των συσκευών και των δικτύων, με αποτέλεσμα να συμβαίνουν “αναταράξεις”, όπως μία συμφόρηση δεδομένων για παράδειγμα. Χωρίζοντας τα επίπεδα της αρχιτεκτονικής και αναλύοντας στο καθένα ξεχωριστά τους τρόπους αντιμετώπισης των πιθανών επιθέσεων, μπορεί να γίνει περισσότερο κατανοητό το τι χρειάζεται και συνεπώς να καταλήξουμε σε ένα πιο ασφαλές σύστημα.

5.4.1 Ασφάλεια στο επίπεδο της αντίληψης

Το επίπεδο της αντίληψης περιλαμβάνει τους αισθητήρες και τα δίκτυα των αισθητήρων. Μέσω των αισθητήρων συλλέγει τις πληροφορίες από το περιβάλλον και μέσω των δικτύων τις μεταφέρει στο επόμενο επίπεδο, αυτό του διαδικτύου.

5.4.1.1 Ασφάλεια στα RFID συστήματα

Το RFID είναι η τεχνολογία που αναγνωρίζει αυτόματα ένα αντικείμενο μέσω της κατάλληλης ετικέτας του και μας δίνει τις αντίστοιχες πληροφορίες. Υπάρχουν όμως αρκετά ζητήματα ασφαλείας.

- **Ενιαία κωδικοποίηση**

  Η κωδικοποίηση των ετικετών που χρησιμοποιούνται σε ένα RFID σύστημα δεν ακολουθεί κάποιο διεθνές πρότυπο και συνεπώς προκύπτουν προβλήματα και λάθη στην ανάγνωση των ετικετών αυτών. Για παράδειγμα είναι πιθανό είτε να διαβαστεί κάτι λάθος είτε να μην καταφέρει να το διαβάσει γενικότερα.

- **Συγκρούσεις ετικετών**

  Κάποιες φορές συμβαίνει να στέλνονται στους αναγνώστες πολλαπλές ετικέτες την ίδια στιγμή, με αποτέλεσμα να μην επιτυγχάνεται η ανάγνωση όλων ή μερικών από αυτές. Για αυτό το λόγο, είναι χρήσιμο να τοποθετούνται σε σειρά οι πληροφορίες που στέλνονται και να συλλέγονται ολόκληρες χωρίς να υπάρχουν επικαλύψεις.

- **Προστασία ιδιωτικότητας**

  Λόγω του χαμηλού κόστους των ετικετών οι πόροι που χρησιμοποιούνται είναι περιορισμένοι, όπως για παράδειγμα η χαμηλή χωρητικότητα αποθήκευσης και οι αδύναμες δυνατότητες υπολογισμών. Θα πρέπει να χρησιμοποιούνται αποτελεσματικές τεχνικές για να επιτυγχάνεται η ιδιωτικότητα, χωρίς όμως να έχουν υψηλές απαιτήσεις. Τα δεδομένα υψίστης σημασίας θα ήταν ωφέλιμο να αποθηκεύονται σε υψηλού επιπέδου βάσεις δεδομένων και όχι στους αποθηκευτικούς χώρους των αναγνωστών. Επίσης, η ιδιωτικότητα είναι σημαντικό να διασφαλίζεται και στα δεδομένα που αφορούν τοποθεσίες καθώς δεν θα θέλαμε να εντοπίζονται πληροφορίες με γεωγραφικές θέσεις.

- **Εμπιστευτικότητα**

  Η εμπιστοσύνη είναι ένας όρος πολύ σημαντικός για τα RFID συστήματα τόσο μεταξύ των ετικετών και των αναγνωστών όσο και μεταξύ των αναγνωστών και τους σταθμούς βάσης. Η ψηφιακή υπογραφή μπορεί να παίξει καθοριστικό ρόλο σε αυτόν τον τομέα έτσι ώστε να διασφαλίζεται η ακεραιότητα των δεδομένων που μεταδίδονται. Για να γίνει αυτό εφικτό χρειάζεται η χρήση της κρυπτογράφησης μέσω αλγορίθμων και συνεπώς διαθέσιμοι αποθηκευτικοί χώροι αλλά και επεξεργαστική ισχύ όσον αφορά τις ετικέτες. Όσο λιγότερες απαιτήσεις σε συνδυασμό με τα παραπάνω μπορούν να εξελίξουν τα συγκεκριμένα συστήματα.

5.4.1.2 Ασφάλεια στα Ασύρματα Δίκτυα Αισθητήρων (WSN)

Στα ασύρματα δίκτυα αισθητήρων υπάρχει μια δυναμική τεχνολογία δικτύου και πολλαπλά βήματα μετάδοσης. Εξαιτίας του χαμηλού τους κόστους υστερούν σε θέματα όπως η χωρητικότητα, οι ικανότητές τους για επεξεργασία και η εμβέλεια. Αυτά όμως τα κάνει πιο αδύναμα όσον αφορά την ασφάλεια. Ο ρόλος των δικτύων αυτών είναι να καταγράφουν τις πληροφορίες αλλά και να διασφαλίζεται η ακεραιότητα, ο χρόνος ανανέωσης αλλά και η ιδιωτικότητά τους. Οι πληροφορίες αυτές είναι πιθανός στόχος εισβολέων και για αυτό οι κρυπτογραφημένοι αλγόριθμοι, η σωστή διαχείριση των κλειδιών αλλά και η ύπαρξη εμπιστοσύνης ανάμεσα στους κόμβους είναι απολύτως απαραίτητα και θα τα αναλύσουμε παρακάτω.

- **Κρυπτογραφικοί αλγόριθμοι**

  Για να διασφαλιστεί η ασφάλεια στα ασύρματα δίκτυα αισθητήρων, η ύπαρξη της οποίας παίζει καθοριστικό ρόλο, χρειάζεται να χρησιμοποιηθούν κρυπτογραφικοί αλγόριθμοι. Οι αλγόριθμοι αυτοί μπορούν να χωριστούν σε

δύο κατηγορίες, εκείνους της συμμετρικής κρυπτογράφησης και εκείνους που χρησιμοποιούν δημόσια κλειδιά. Η αδυναμία όμως των αισθητήρων για υπολογιστικές λειτουργίες καθώς και οι περιορισμένοι αποθηκευτικοί χώροι καθιστούν δύσκολη τη λειτουργία της ασύμμετρης κρυπτογράφησης, αφού εκεί υπάρχει πολυπλοκότητα στους υπολογισμούς και κατανάλωση ενέργειας. Για αυτό λοιπόν, χρησιμοποιείται συχνά η συμμετρική κρυπτογράφηση χάρη στους απλούς και λίγους ποσοτικά υπολογισμούς που χρειάζεται. Αυτό δεν σημαίνει ότι και οι αλγόριθμοι συμμετρικής κρυπτογράφησης δεν έχουν προβλήματα. Υπάρχει πολυπλοκότητα στα πρωτόκολλα που χρησιμοποιούνται για την ανταλλαγή κλειδιών και σε συνδυασμό με τα προβλήματα εμπιστευτικότητας των κλειδιών δημιουργούνται προβλήματα. Αν παραβιαστεί ένας μόνο κόμβος, εξαιτίας της συνδεσιμότητας που υπάρχει θα βρεθούν σε κίνδυνο και τα κλειδιά του συστήματος. Επίσης, ανησυχίες δημιουργούν οι υψηλές ποσότητες ενέργειας που χρειάζονται οι αλγόριθμοι ούτως ώστε να γίνει η αυθεντικοποίηση των μηνυμάτων. Γίνεται κατανοητό λοιπόν, ότι οι αλγόριθμοι που χρησιμοποιούν την κρυπτογράφηση δημόσιου κλειδιού είναι πιο αποτελεσματικοί και επιλέγονται έναντι της συμμετρικής κρυπτογράφησης. Τόσο το ιδιωτικό κλειδί όσο και το δημόσιο του σταθμού βάσης βρίσκεται στην κατοχή του κόμβου, ενώ οι σταθμοί βάσεις κατέχουν τα δημόσια κλειδιά των κόμβων. Η επεκτασιμότητα επιτυγχάνεται χωρίς τη χρήση περίπλοκων πρωτοκόλλων για τη διαχείριση των κλειδιών και η εμπιστευτικότητα του δικτύου παραμένει ορατή.

Εν κατακλείδι, και οι δύο μορφές των αλγορίθμων έχουν τα θετικά τους στοιχεία αλλά δεν λύνουν πλήρως τα ζητήματα ασφαλείας που δημιουργούνται στα ασύρματα δίκτυα αισθητήρων. Οι κύριες διαφορές είναι ότι οι ασυμμετρικοί αλγόριθμοι μπορούν να παρέχουν ασφάλεια σε υψηλά επίπεδα αλλά αρκετές έρευνες απαιτούνται ακόμα για να γίνουν ένα ολοκληρωμένο σύστημα. Από την άλλη μεριά, η συμμετρική κρυπτογράφηση είναι σχετικά αναπτυγμένη αλλά υστερεί στον τομέα της ασφάλειας.

- **Διαχείριση των κλειδιών**

Η διαχείριση του κλειδιού είναι ένα αρκετά σημαντικό στοιχείο για τα ασύρματα δίκτυα αισθητήρων και διασφαλίζοντας την ασφάλεια σε αυτό, θα μπορούμε να λύσουμε και άλλα θέματα ασφαλείας που υπάρχουν. Εδώ περιλαμβάνονται η παραγωγή των κλειδιών, η διανομή τους, η αποθήκευσή τους και η καταστροφή τους. Η πιο σημαντική διαδικασία στη διαχείριση των κλειδιών είναι ο σχεδιασμός της διανομής τους σε όσους νόμιμα το δικαιούνται, χωρίς όμως να χρησιμοποιείται μεγάλος αριθμός πόρων και υψηλές απαιτήσεις. Η διανομή των κλειδιών μπορεί να κατηγοριοποιηθεί ως εξής. Αρχικά έχουμε την ευρεία διανομή τους σε όλο το δίκτυο, η οποία χρειάζεται αρκετή ενέργεια και τη χρησιμοποιούμε όταν χρειάζονται ανανέωση τα κλειδιά. Στη συνέχεια υπάρχει η ομαδική διανομή η οποία έχει ως όφελος περισσότερη ασφάλεια ανάμεσα στους κόμβους. Έπειτα έχουμε ανάμεσα στον κόμβο και στο σταθμό βάσης τη διανομή του κύριου κλειδιού και τέλος υπάρχει η διανομή μοιρασμένων κλειδιών στους κόμβους που είναι κοντά. Εξαιτίας της κατανάλωσης ενέργειας και άλλων παραγόντων, μοιράζεται το κλειδί μεταξύ των κόμβων για να βελτιωθεί η ασφάλεια στις μεταδόσεις και τις συνδέσεις που πραγματοποιούνται.

- **Ασφαλή πρωτόκολλα δρομολόγησης**

Μία ενδεχόμενη επίθεση στο στάδιο της δρομολόγησης ενός συστήματος IoT θα μπορούσε να προκαλέσει αρκετά προβλήματα ή ακόμα και να “διαλύσει” ολόκληρο το δίκτυο. Κάποια πρωτόκολλα τα οποία μπορούν να προσφέρουν ένα ικανοποιητικό ποσοστό ασφαλείας, δυστυχώς δεν μπορούν να χρησιμοποιηθούν στα ασύρματα δίκτυα επειδή η χωρητικότητα, η επεξεργαστική ισχύ και τα ενεργειακά αποθέματα του δικτύου είναι περιορισμένα. Μελέτες πάνω στις κρυπτογραφικές μεθόδους και τη διαχείριση των κλειδιών έχουν δείξει πως η ασφάλεια και η ακεραιότητα των δεδομένων μπορεί να διασφαλιστεί, αλλά η αυθεντικότητα των πληροφοριών που αφορούν τη δρομολόγηση μπορεί να επιτευχθεί μόνο με τη βοήθεια των κατάλληλων πρωτοκόλλων.

- **Εμπιστευτικότητα των κόμβων**

  Η μεταφορά των πληροφοριών ανάμεσα στους κόμβους και τους σταθμούς βάσης απαιτείται να πραγματοποιηθεί με πλήρη ασφάλεια και ακεραιότητα, καθώς σε διαφορετική περίπτωση μπορεί να καταρρεύσει ολόκληρο το δίκτυο. Οι περιορισμένοι πόροι στους κόμβους των αισθητήρων αλλά και ο συγκεκριμένος τρόπος επικοινωνίας που έχουν, είναι κάποια από τα ιδιαίτερα χαρακτηριστικά των δικτύων αυτών. Επίσης, οι κρυπτογραφικοί αλγόριθμοι από μόνοι τους δεν κρίνονται επαρκείς ούτως ώστε να διασφαλίσουν την ασφάλεια. Συνεπώς, ένα σύστημα το οποίο θα είναι ικανό να διαχειριστεί κατάλληλα τον τρόπο μετάδοσης των πληροφοριών ανάμεσα στους κόμβους βασισμένο στη διασφάλιση της εμπιστευτικότητας κρίνεται αναγκαίο. Μηχανισμοί με κύριο ρόλο την αξιολόγηση και την παραγωγή της εμπιστοσύνης μπορούν να συμβάλλουν σημαντικά στα δίκτυα αυτά. Δεδομένου ότι το σύστημα των αισθητήρων χρειάζεται τη βοήθεια όλων των κόμβων για τη συλλογή των δεδομένων, μπορεί να μην καταφέρει να λειτουργήσει αν ένας και μόνο κόμβος δεν συνεργαστεί. Τα αποτελέσματα μιας τέτοιας περίπτωσης θα είναι να φτάσουν λανθασμένα στοιχεία στους τελικούς χρήστες ή ακόμα και κάποιος κακόβουλος χρήστης να αποκτήσει πρόσβαση σε προσωπικά δεδομένα. Συνεπώς, οι κρυπτογραφικοί αλγόριθμοι χωρίς αυξημένες απαιτήσεις, τα πρωτόκολλα δρομολόγησης καθώς και το σύστημα που θα διαχειρίζεται την εμπιστοσύνη μεταξύ των κόμβων θα μπορέσουν να παρέχουν την ασφάλεια που ζητάμε.

5.4.1.3 Προβλήματα στην ετερογενή ενσωμάτωση

Τα συστήματα του Internet of Things στις μέρες μας επεξεργάζονται αρκετά μεγάλους όγκους δεδομένων και έχουν αρκετές λειτουργίες μέχρι να φτάσουν στο τελικό αποτέλεσμα που επιθυμεί ο χρήστης. Οι ανησυχίες όμως που προκύπτουν

οφείλονται στο γεγονός ότι δεν χρησιμοποιούνται από όλα τα συστήματα οι ίδιες τεχνολογίες και πρωτόκολλα. Αυτό οδηγεί σε ασυμβατότητες και δημιουργεί προβλήματα στα επόμενα στάδια, καθώς θα πρέπει να συμβαδίζουν οι τύποι των πληροφοριών μεταξύ τους ούτως ώστε να επεξεργάζονται όλες μαζί. Οι κύριες μέθοδοι που χρησιμοποιούνται για τη συλλογή δεδομένων είναι τα συστήματα RFID και τα ασύρματα δίκτυα. Οι δύο περιπτώσεις αυτές έχουν κάποιες διαφορές στις λειτουργίες τους και θα ήταν χρήσιμο να βρεθούν λύσεις για να βαδίζουν στην ίδια φιλοσοφία. Μέχρι στιγμής το συγκεκριμένο πρόβλημα δεν έχει λυθεί, παρόλο που έχουν γίνει προσπάθειες. Πιο συγκεκριμένα, τα RFID συστήματα διαχειρίζονται διαφορετικά την αποθήκευση των δεδομένων, την πρόσβαση αλλά και τον τρόπο με τον οποίο θα διασφαλιστεί η ασφάλεια. Βρίσκοντας τεχνικές έτσι ώστε να ομογενοποιηθούν οι τεχνολογίες των δύο συστημάτων και να μπορέσουν να λειτουργήσουν σαν να μην έχουν διαφορές, θα ωφελούσε σημαντικά το περιβάλλον του IoT.

5.4.2 Ασφάλεια στο επίπεδο μεταφοράς

Το επίπεδο μεταφοράς είναι εκείνο το οποίο συνδέει το επίπεδο της αντίληψης με εκείνο των εφαρμογών. Είναι το στάδιο δηλαδή στο οποίο μεταφέρονται οι πληροφορίες αφού έχουν συλλεχθεί και χρειάζονται επεξεργασία.

5.4.2.1 Δίκτυο πρόσβασης

Στο δίκτυο πρόσβασης γίνεται η επαφή με τα δεδομένα του προηγούμενου επιπέδου και αναλαμβάνει να διασφαλίσει την ασφάλειά τους σε τυχόν θέματα που δεν έχουν ήδη διευθετηθεί. Αποτελείται από το Wi-Fi, τα δίκτυα ad hoc καθώς και τα 3G και 4G. Σύμφωνα με τη δομή που έχει το καθένα από αυτά τα δίκτυα, μπορούν να χωριστούν

σε δύο κατηγορίες, εκείνα που δεν είναι απαραίτητο να υπάρχει σταθμός βάσης, όπως το ad hoc, και εκείνα που το θεωρούν αναγκαίο, όπως το WiFi και τα 3G,4G.

- **Δίκτυο WiFI**

  Το δίκτυο WiFi είναι σαφώς το πιο διαδεδομένο στις μέρες μας και χρησιμοποιείται από αμέτρητους ανθρώπους καθημερινά. Όσον αφορά τον τομέα του IoT, υπάρχουν οι εφαρμογές που χρησιμοποιούν τους φυλλομετρητές με στόχο να επιτευχθεί η περιήγηση στο διαδίκτυο καθώς και εφαρμογές που χρησιμοποιούνται για να ανταλλάξουν μηνύματα ηλεκτρονικού ταχυδρομείου και να διαχειριστούν τα αρχεία. Όντας ένα τόσο διαδεδομένο δίκτυο με δράση σχεδόν σε κάθε κτίριο, είναι λογικό οι κακόβουλοι χρήστες να προσπαθούν να το “χτυπήσουν” και χρησιμοποιούν τεχνικές όπως το “ψάρεμα” ή τις επιθέσεις άρνησης υπηρεσιών.[21] Συνεπώς, η ασφάλεια στο συγκεκριμένο δίκτυο θα πρέπει να διασφαλιστεί πλήρως και αυτό επιτυγχάνεται χρησιμοποιώντας τεχνικές όπως η κρυπτογράφηση και ο έλεγχος πρόσβασης. Η πρώτη περίπτωση επιτρέπει μόνο σε όσους χρήστες διαθέτουν το απαραίτητο κλειδί να συνδεθούν στο δίκτυο ενώ η δεύτερη επιτρέπει την είσοδο στους πιστοποιημένους χρήστες.

- **Δίκτυο ad hoc**

  Στα δίκτυα ad hoc δεν υπάρχει στήριξη σε κάποια σταθερή υποδομή. Ουσιαστικά είναι αυτοδιαχειριζόμενα, οργανώνονται μόνα τους και προσφέρουν χρήσιμα οφέλη στα συστήματα του τομέα μας. Επίσης οι κόμβοι του συγκεκριμένου δικτύου λειτουργούν αυτόνομα. Είναι όμως μια ακόμα κατηγορία ασύρματων δικτύων από την οποία δεν λείπουν οι επιθέσεις και οι υποκλοπές. Απειλές μπορεί να εμφανιστούν αρχικά στους κόμβους, οι οποίοι θα πρέπει να ελέγχουν και να αλληλεπιδρούν μόνο με όσους είναι πιστοποιημένοι έτσι ώστε να μην διαρρεύσουν πληροφορίες σε τρίτους. Ο τρόπος δόμησής τους δίνει “ευκαιρίες” σε κακόβουλους χρήστες να

καταφέρουν κάποια χτυπήματα όπως υποκλοπές και διαρροές και για αυτό το λόγο η διαχείριση των κλειδιών είναι ένα αρκετά σημαντικό κομμάτι για την αντιμετώπιση των επιθέσεων, όπως επίσης και η κρυπτογράφηση.

- **Δίκτυο 3G/4G**

  Τα λεγόμενα κυψελωτά δίκτυα μπορούν επίσης να χρησιμοποιηθούν σε ένα IoT περιβάλλον με τον κίνδυνο βέβαια, όπως και τα υπόλοιπα, να δεχθούν κάποια επίθεση. Η υποκλοπή προσωπικών δεδομένων και η απώλεια πακέτων πληροφοριών είναι οι συνηθισμένες περιπτώσεις επιθέσεων και μπορούν να αντιμετωπιστούν μέσω της κρυπτογράφησης αλλά και της σωστής διαχείρισης των κλειδιών. Ελέγχοντας την προέλευση των δεδομένων και διασφαλίζοντας ότι προέρχονται από έμπιστες πηγές, μειώνει τους κινδύνους που το απασχολούν. Ένα ακόμα σημαντικό πλεονέκτημα του συγκεκριμένου δικτύου είναι το γεγονός ότι μπορούν να χρησιμοποιήσουν τις κάρτες SIM των χρηστών για να ελέγξουν αν ένας χρήστης είναι έγκυρος ή υπάρχει κάποιος εισβολέας και να πράξουν ανάλογα.

5.4.2.2 Βασικό δίκτυο

Το βασικό δίκτυο είναι υπεύθυνο έτσι ώστε να μεταδοθούν τα δεδομένα χρησιμοποιώντας ως μέσο μετάδοσης το διαδίκτυο. Είναι λογικό λοιπόν, τα θέματα ασφαλείας που υπάρχουν στο διαδίκτυο να ταυτίζονται με αυτά του βασικού δικτύου. Λόγω του μεγάλου πλήθους διευθύνσεων που χρησιμοποιούνται σε ένα σύστημα Internet of Things, το πρωτόκολλο IPv4 δεν μπορεί να καλύψει όλες τις ανάγκες και να αντιστοιχίσει τους δικτυακούς αισθητήρες με τις διευθύνσεις τους. Συνεπώς, συνίσταται η χρήση του πρωτοκόλλου IPv6 στο οποίο η κατανάλωση ενέργειας δεν φτάνει σε υψηλά επίπεδα.

5.4.2.3 Τοπικά δίκτυα

Στον τομέα του Internet of Things, μία ενδεχόμενη διαρροή δεδομένων ή υποκλοπή μπορεί να προκαλέσει σοβαρά προβλήματα καθώς αφορά προσωπικά στοιχεία. Για το λόγο αυτό λοιπόν, η ασφάλεια είναι ακόμα πιο σημαντικό να διασφαλιστεί. Αυτό είναι εφικτό αρχικά αφαιρώντας από το σύστημά μας το κακόβουλο λογισμικό εφόσον υπάρχει, και δεύτερον χρησιμοποιώντας τεχνικές όπως η ύπαρξη κωδικών πρόσβασης και η συχνή ανανέωση του συστήματος. Επιπρόσθετα, μία άλλη πιθανή μορφή επίθεσης που συμβαίνει στα δίκτυα αυτά είναι εκείνη της άρνησης υπηρεσιών. Μηχανισμοί οι οποίοι μπορούν να ανιχνεύουν κακόβουλα λογισμικά και να διασφαλίζουν την ακεραιότητα των δεδομένων συμβάλλουν στην ασφάλεια των δικτύων αυτών.

Επίλογος

Συμπεραίνοντας από τις πληροφορίες που παρατέθηκαν, καταλαβαίνουμε ότι ο τομέας του Internet of Things θα παίξει καθοριστικό ρόλο στην εξέλιξη της κοινωνίας μας. Στα επόμενα χρόνια η δράση του θα είναι μεγαλύτερη και οι “έξυπνες” συσκευές θα υπάρχουν σε ολοένα και περισσότερα σπίτια ή μέρη. Σαφώς ο άνθρωπος θα πρέπει να προσαρμοστεί στα νέα δεδομένα και συστήματα έτσι ώστε να μπορέσει να απολαύσει τα οφέλη που προσφέρονται, καθώς κατά κάποιο τρόπο αλλάζουν τα έως τώρα δεδομένα και τη ζωή του ανθρώπου. Επίσης, οι τεχνολογίες που χρησιμοποιούνται συνεχώς εξελίσσονται και βελτιώνουν την απόδοση των συστημάτων αυτών. Δίνοντας την απαραίτητη προσοχή στα θέματα της ασφάλειας αλλά και στη σωστή χρήση, μπορούμε να ελαχιστοποιήσουμε τις αρνητικές παρενέργειες και να τα χρησιμοποιήσουμε προς όφελός μας. Υπάρχουν αρκετοί τύποι επιθέσεων όπως αναλύσαμε στο τελευταίο κεφάλαιο, αλλά επίσης υπάρχουν και αρκετοί τρόποι αντιμετώπισής τους. Ανάλογα με το σχεδιασμό ενός συστήματος IoT από τον κατασκευαστή του, κρίνεται και το ποσοστό ασφάλειας και λειτουργικότητάς του. Συνεπώς, οι λειτουργίες και τα οφέλη που μπορούμε να αποκομίσουμε χρησιμοποιώντας την “έξυπνη” τεχνολογία είναι πολύ σημαντικά, αρκεί να χρησιμοποιείται σωστά και κάτω από τις κατάλληλες προδιαγραφές.

Βιβλιογραφία

[1] Santosh Kulkarni and Sanjeev Kulkami, “Communication Models in Internet of Things: A Survey”, International Journal of Science Technology and Engineering, vol 3, May 2017

[2] Maria Rita Palattella, Mischa Dohler, Alfredo Grieco, Gianluca Rizzo, Johan Torsner, Thomas Engel and Latif Ladid, “Internet of Things in the 5G Era: Enablers, Architecture and Business Models”, 2015

[3] Pallavi Sethi and Smruti R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications”, Journal of Electrical and Computer Engineering, January 2017

[4] Tabassum Ara, Pritam Gajkumar Shah and M. Prabhakar, “Internet of Things Architecture and Applications : A Survey”, Indian Journal of Science and Technology, December 2016, DOI: 10.17485/ijst/2016/v9i45/106507

[5] Riyadh Abdmeziem, Djamel Tandjaoui and Imed Romdhani, “Architecting the Internet of Things: State of the Art”, August 2015, DOI: 10.1007/978-3-319-22168-7_3

[6] Siham Al Hinai and Ajay Vikram Singh, “Internet of Things: Architecture, Security challenges and Solutions”, IEEE, 2017, **DOI:** 10.1109/ICTUS.2017.8286004

[7] Miao Yun and Bu Yuxin, “Research on the Architecture and Key Technology of Internet of Things (loT) Applied on Smart Grid”, Advances in Energy Engineering, July 2010, DOI: 10.1109/ICAEE.2010.5557611

[8] Ankush B. Pawar and Shashikant Ghumbre, “A SURVEY ON IoT APPLICATIONS, SECURITY CHALLENGES AND COUNTERMEASURES”, International Conference on Computing, Analytics and Security Trend, 2016

[9] Maninder Jeet Kaur and Piyush Maheshwari , “Building Smart Cities Applications using IoT and Cloud-based Architectures”, IEEE, 2016

[10] Zeeshan Ali Khan and Ubaid Abbasi, “Evolution of Wireless Sensor Networks toward Internet of Things”, Emerging Communication Technologies Based on Wireless Sensor Networks, pp.179-200, 2016

[11] Saeedreza Arab, Hossein Ashrafzadeh and Amir Alidadi, “Internet of Things: Communication Technologies, Features and Challenges”, vol 6, 2018

[12] RIAZUL ISLAM, DAEHAN KWAK, HUMAUN KABIR, MAHMUD HOSSAIN AND KYUNG-SUP KWAK, “The Internet of Things for Health Care: A Comprehensive Survey”, IEEE, 2015

[13] Chen Yang, Weiming Shen and Xianbin Wang, “Applications of Internet of Things in manufacturing”, IEEE Computer Supported, doi:10.1109/cscwd.2016.7566069

[14] Himadri Nath Saha, Abhilasha Mandal and Abhirup Sinha, “Recent Trends in the Internet of Things”, IEEE 7th Annual Computing and Communication Workshop and Conference, 2017, DOI: 10.1109/CCWC.2017.7868439

[15] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer and Shahid Khan, “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges”, 10th International Conference on Frontiers of Information Technology, 2012

[16] Fadele Ayotunde Alabaa, Mazliza Othmana, Ibrahim Abaker Targio Hashema and Faiz Alotaibi, “Internet of Things security: A survey”, Journal of Network and Computer Applications, 2017

[17] Yazdan Ahmad Qadri, Ali Nauman, Yousaf Bin Zikria, Athanasios V. Vasilakos and Sung Won Kim, “The Future of Healthcare Internet of Things: A Survey of Emerging Technologies”, IEEE Communications Surveys & Tutorials, vol 22, 2020, **DOI:** 10.1109/COMST.2020.2973314

[18] Parul Datta and Bhisham Sharma, “A Survey on IoT Architectures, Protocols, Security and Smart City based Applications”, IEEE - 40222, July 2017

[19] Shadi Al-Sarawi, Mohammed Anbar, Kamal Alieyan and Mahmood Alzubaidi, “Internet of Things (IoT) Communication Protocols : Review”, 8th International Conference on Information Technology, 2017

[20] Somayya Madakam, R. Ramaswamy and Siddharth Tripathi, “Internet of Things (IoT): A Literature Review”, Journal of Computer and Communications, vol 3, 2015

[21] Xiaolin Jia, Quanyan Feng, Taihua Fan and Quanshui Lei, “RFID Technology and Its Applications in Internet of Things (IOT)”, IEEE, 2012

[22] Mauro Conti, Ali Dehghantanha, Katrin Franke and Steve Watson, “Internet of Things security and forensics: Challenges and opportunities”, Future Generation Computer Systems, pp 544-546, 2018

[23] Ioannis Andrea, Chrysostomos Chrysostomou and George Hadjichristofi, “Internet of Things: Security Vulnerabilities and Challenges”, 5 International Workshop on Smart City and Ubiquitous Computing Applications, 2015

[24] J. Sathish Kumar and Dhiren R. Patel, “A Survey on Internet of Things: Security and Privacy Issues”, International Journal of Computer Applications, vol 90, 2014

[25] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul and Imran Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures”, 10th International Conference for Internet Technology and Secured Transactions, DOI**:** 10.1109/ICITST.2015.7412116

[26] Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung, “THE INTERNET OF THINGS: NEW INTEROPERABILITY, MANAGEMENT AND SECURITY CHALLENGES”, International Journal of Network Security & Its Applications, vol 8, 2016

[27] Danai Chasaki and Christopher Mansour, “Security challenges in the internet of things”, Int. J. Space-Based and Situated Computing, Vol. 5, 2015

[28] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu and Dechao Qiu, “Security of the Internet of Things: perspectives and challenges”, Wireless Netw, 2017