



INTERNET OF THINGS

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΤΗΣ

ΣΤΑΡΟΥΛΑΣ ΤΡΑΪΦΟΡΟΥ



ΕΠΙΒΛΕΠΩΝ: Σταυρούλα Δαφνά
Εργαστηριακός Συνεργάτης

ΜΑΙΟΣ 2019

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

Υπογραφή:

.....

Σταυρούλα Τραϊφόρου

Περίληψη

Στην παρούσα πτυχιακή εργασία θα μελετηθεί και θα παρουσιασθεί το «Internet of Things» το οποίο παρουσιάζει ενδιαφέρον στον τομέα της σύγχρονης τεχνολογίας. Το διαδίκτυο των πραγμάτων είναι ένα είδος νευρωνικού δικτύου το οποίο είναι ένα δίκτυο επικοινωνίας που μπορούν να συνδέονται πολλές έξυπνες συσκευές μεταξύ τους. Τα τελευταία χρόνια το Διαδίκτυο των Πραγμάτων (Internet of Things, IoT) έχει σημειώσει μεγάλη επίδραση στον ερευνητικό χώρο. Είναι χωρίς αμφιβολία η επερχόμενη τάση σε ότι αφορά την εξέλιξη του διαδικτύου.

Τα επόμενα χρόνια το IoT αναμένεται να ενώσει διαφορετικές τεχνολογίες και να δημιουργήσει νέες εφαρμογές. Ταυτόχρονα θα αλλάξει τον τρόπο με τον οποίο εργαζόμαστε και ζούμε ανοίγοντας νέες ευκαιρίες για ανάπτυξη και καινοτομία καθώς επίσης θα κάνουν την ζωή μας εύκολη. Ο στόχος της πτυχιακής εργασίας είναι να μελετήσουμε και να παρουσιάσουμε κάποιες από τις τεχνολογίες γενικής εφαρμογής, των μοντέλων επικοινωνίας, των πρωτοκόλλων και των θεμάτων εφαρμογής του Internet of Things

Λέξεις Κλειδιά:

Internet of Things, Έξυπνο, Δίκτυο, Cloud, Τεχνολογίες, Επικοινωνία.

Abstract

The focus of this thesis is to study and present the field of the Internet of Things. The Internet of Things is a type of neural network more specifically a communication network that has the ability to connect many smart devices. In recent years the Internet of Things has had a major impact in the research community. There is no doubt that in the years to come IoT will be the evolution of the Internet.

In years to come the Internet of Things will unite different technologies and create new applications. At the same time it will revolutionize the way we work and live and create new opportunities for growth and innovation as well as making daily life easier. The aim of this dissertation is to study and present some general application technologies, communication models and protocols of the Internet of Things.

Keywords

Internet of Things, Smart, Network, Cloud, Technologies, Communication.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά τη κα. Δαφνά Σταυρούλα που ανέλαβε να με βοηθήσει και να οριστεί ως νέος επιβλέπων για την εκπόνηση της πτυχιακής μου εργασίας.

Επίσης ένα μεγάλο ευχαριστώ στους γονείς μου για τη βοήθεια τους όλα αυτά τα χρόνια των σπουδών μου. Και στον άντρα μου για την υπομονή που έδειξε κατά τη διάρκεια της υλοποίησης της εργασίας.

Σπάρτη, Μάιος 2019

Σταυρούλα Τραιφόρου

Περιεχόμενα

Περίληψη.....	5
Abstract.....	7
Ευχαριστίες.....	9
Κατάλογος Εικόνων.....	13
Πρόλογος.....	15
ΚΕΦΑΛΑΙΟ 1- ΕΙΣΑΓΩΓΗ.....	17
1.1 Εισαγωγή.....	17
1.2 Τι είναι το Internet of Things.....	17
1.3 Διάρθρωση της Εργασίας.....	18
ΚΕΦΑΛΑΙΟ 2- ΤΟ INTERNET OF THINGS.....	19
2.1 Ιστορική Αναδρομή.....	19
2.2 Συνδεσιμότητα.....	22
2.3 Σύνοψη των Μοντέλων.....	28
ΚΕΦΑΛΑΙΟ 3- ΤΕΧΝΟΛΟΓΙΕΣ ΤΟΥ ΙοΤ- ΜΟΝΤΕΛΟ ARM.....	29
3.1 Τεχνολογίες.....	29
3.2 Ασφάλεια και Ιδιωτικότητα.....	36
3.3 Αρχιτεκτονική του ΙοΤ.....	41
3.2 Το Μοντέλο ARM.....	41
3.3 Οφέλη του Μοντέλου ARM.....	43
3.4 Διαδικασία Ανάπτυξης του Μοντέλου ARM.....	44
ΚΕΦΑΛΑΙΟ 4 - ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΙοΤ.....	46
4.1 Έξυπνη Πόλη.....	46
4.2 Έξυπνη Ενέργεια.....	49
4.3 Έξυπνη Μεταφορά.....	51
4.4 Έξυπνο Σπίτι-Κτίριο.....	52
4.5 Έξυπνη Βιομηχανία.....	54
4.6 Έξυπνη Λιανική.....	55
4.7 Έξυπνη Γεωργία-Εκτροφή.....	56
ΚΕΦΑΛΑΙΟ 5- ΤΟ ΙοΤ ΣΤΟ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ.....	57
5.1 Το Internet of Medical Things (IoMT).....	57
5.2 Οφέλη του IoMT.....	58

5.3	Εφαρμογές του ΙοMT	59
5.4	Αρχιτεκτονική των ΙοMT Συστημάτων	61
5.5	Ασφάλεια των ΙοMT Συστημάτων	62
	Βιβλιογραφία	66

Κατάλογος Εικόνων

Εικόνα 1: Internet of Things ¹³	17
Εικόνα 2: Smart Glasses ¹⁴	19
Εικόνα 3: Device-to-Device ¹⁵	23
Εικόνα 4: Device-to-Cloud ¹⁶	25
Εικόνα 5: Device-to-Gateway.....	26
Εικόνα 6: Data Sharing ¹⁷	27
Εικόνα 7: RFID system ¹⁸	30
Εικόνα 8: Wireless Communication ¹⁹	31
Εικόνα 9: Cloud Computing Model ²⁰	32
Εικόνα 10: ARM model ²¹	42
Εικόνα 11: Smart City ²²	47
Εικόνα 12: Smart Grid ²³	50
Εικόνα 13: Internet of Vehicles ²⁴	51
Εικόνα 14: Smart Home ²⁵	53
Εικόνα 15: Smart Factory ²⁶	54
Εικόνα 16: Smart Service ²⁷	55
Εικόνα17: Internet of Medical Things ²⁸	59

Πρόλογος

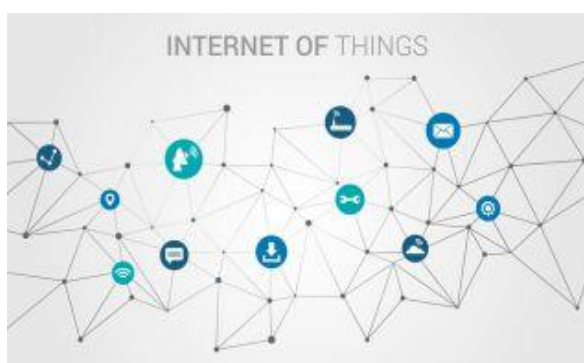
Η παρούσα Πτυχιακή εργασία με τίτλο «Internet of Things» εκπονήθηκε στα πλαίσια του προγράμματος σπουδών, για τη λήψη του πτυχίου από το Τ.Ε.Ι. ΠΕΛΟΠΟΝΝΗΣΟΥ του τμήματος Μηχανικών Πληροφορικής Τ.Ε. (Έδρα: Σπάρτη) της σχολής Τεχνολογικών Εφαρμογών.

Σκοπός της πτυχιακής εργασίας είναι να γίνει μία μελέτη και μία επισκόπηση των τεχνολογιών γενικής εφαρμογής, μοντέλων επικοινωνίας, των πρωτοκόλλων και των θεμάτων εφαρμογής του Internet of Things.

ΚΕΦΑΛΑΙΟ 1- ΕΙΣΑΓΩΓΗ

1.1 Εισαγωγή

Ο όρος Διαδίκτυο των πραγμάτων (IoT) χρησιμοποιήθηκε για πρώτη φορά το 1999 από τον Kevin Ashton για να περιγράψει ένα σύστημα στο οποίο τα αντικείμενα του φυσικού κόσμου θα μπορούσαν να συνδεθούν με το Internet μέσω αισθητήρων χρησιμοποιώντας ταυτοποίηση με τεχνολογία ραδιοσυχνοτήτων RFID (Radio Frequency Identification). Σήμερα ο όρος IoT χρησιμοποιείται για να περιγράψει ένα δίκτυο επικοινωνίας οικιακών συσκευών, αυτοκινήτων και διάφορων άλλων συσκευών που ενσωματώνουν ηλεκτρονικά μέσα ώστε να μπορούν να συνδεθούν με το δίκτυο, αλλά και μεταξύ τους, και να ανταλλάζουν δεδομένα.



Εικόνα 1: Internet of Things¹³

1.2 Τι είναι το Internet of Things

Το Internet of Things (IoT) ονομάζουμε ένα δίκτυο φυσικών αντικειμένων, συσκευών, οχημάτων, κτιρίων αλλά και άλλων αντικειμένων τα οποία περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά, αισθητήρες και διαδικτυακή δυνατότητα σύνδεσης, κάτι που επιτρέπει σε αυτά τα αντικείμενα να συλλέγουν και να ανταλλάσσουν δεδομένα. Το IoT επιτρέπει στα αντικείμενα αυτά να ελέγχονται απομακρυσμένα μέσω μιας δικτυακής υποδομής δημιουργώντας ευκαιρίες αλληλεπίδρασης του φυσικού κόσμου με τα υπολογιστικά συστήματα. Αυτό έχει ως αποτέλεσμα τη βελτίωση της αποτελεσματικότητας των συσκευών αυτών, της ακρίβειας αλλά και τη μείωση του κόστους. Επιπλέον το IoT στηρίζεται σε τεχνολογία που συμπεριλαμβάνει αισθητήρες και ενεργοποιητές τα οποία αποτελούν μέρος των καθημερινών έξυπνων συστημάτων όπως τα έξυπνα σπίτια και τα έξυπνα οχήματα. Κάθε αντικείμενο αναγνωρίζεται ξεχωριστά από το ενσωματωμένο υπολογιστικό σύστημα και μπορεί να λειτουργεί τόσο αυτόνομα όσο και σε συνεργασία με την υπόλοιπη διαδικτυακή υποδομή.

1.3 Διάρθρωση της Εργασίας

Η εργασία έχει προγραμματιστεί ως εξής:

Στο **2^ο κεφάλαιο**, αφού γίνεται μια ιστορική αναδρομή στο Internet of Things, αναλύονται οι βασικές λειτουργίες συνδεσιμότητας και τα μοντέλα τα οποία εφαρμόζονται.

Στο **3^ο κεφάλαιο** αναλύονται οι τεχνολογίες που χρησιμοποιούνται για την ανάπτυξη ενός IoT μοντέλου, η αρχιτεκτονική στην οποία βασίζεται το IoT αλλά και τα απαραίτητα μέτρα ασφάλειας όσο αφορά τη χρήση του.

Στο **4^ο κεφάλαιο** γίνεται αναφορά στις εφαρμογές όπου χρησιμοποιείται ένα IoT μοντέλο.

Λόγω του σημαντικού ρόλου του IoT στο τομέα της Υγείας. Στο **5^ο κεφάλαιο** γίνεται μια ειδική αναφορά σε αυτό και στην ανάπτυξη του Internet of Medical Things (IoMT).

Συμπεράσματα της εργασίας αναφέρονται στο **6^ο κεφάλαιο**¹.

¹“Overview of the Internet of Things”, June 2012, ITU

4. https://en.wikipedia.org/wiki/Internet_of_things. IoT. *Wikipedia*.

ΚΕΦΑΛΑΙΟ 2- ΤΟ INTERNET OF THINGS

Το κεφάλαιο αυτό αρχικά έχει ως σκοπό να δώσει μια ιστορική αναδρομή στο πως αναπτύχθηκε η τεχνολογία πάνω στην οποία στηρίχτηκε η επιστήμη του Διαδικτύου των Πραγμάτων (Internet of Things), ξεκινώντας δειλά το 1950 με χρήση των πρώτων barcodes έως τη σημερινή εποχή των έξυπνων συσκευών. Επιπλέον δίνεται έμφαση στη συνδεσιμότητα τέτοιων συσκευών και στα βασικά μοντέλα που έχουν αναπτυχθεί και πάνω στα οποία στηρίζεται η τεχνολογία του IoT.

2.1 Ιστορική Αναδρομή

Η τεχνολογία αυτή αναπτύχθηκε βίαια στα πρόθυρα της νέας γενιάς του IoT, για να επιτρέψει την ασύγχρονη επικοινωνία αυτών των συσκευών, όμως το IoT άρχιζε να υφίσταται σαν μια αόριστη σκέψη ήδη από το 1950.

- Οι μηχανικοί της IBM είχαν την ανάγκη να ορίσουν ταυτότητες σε κάθε αντικείμενο και μηχανήμα που χρησιμοποιούσαν στην επιχείρηση . Η διαρκής ενασχόληση και οι πειραματισμοί με γραμμικά σχήματα, οδήγησαν στην ανακάλυψη των barcodes. Νέοι πειραματισμοί από μηχανικούς και επιστήμονες ακολούθησαν σε επίπεδο hardware και κινητών φορητών συσκευών τις οποίες μπορείς να φοράς στον καρπό σου (wearables). Η πρώτη και αξιοσημείωτη συσκευή του Edward O. Thorp το 1955 ο οποίος κατασκεύασε ένα ρολόι το οποίο πρόβλεπε τους κύκλους που έκαναν οι ρουλέτες στα καζίνα του Las Vegas μέσα από περίπλοκους αλγορίθμους.
- Το 1967 από τον Hubert Upton δημιουργήθηκε η πρώτη συσκευή σε σχήμα μυωπικών γυαλιών η οποία βοηθούσε τα άτομα με ειδικές ανάγκες να διαβάζουν τα χείλια των ανθρώπων .Το 2011 η εταιρία Google χρησιμοποιώντας την ιδέα του Hubert επινόησε και δημιούργησε το project Google Glass.



Εικόνα 2: Smart Glasses¹⁴

- Τρία χρόνια μετά, το 1970, δημιουργήθηκε το δίκτυο ARPANET για την επικοινωνιακή ανταλλαγή δεδομένων ανάμεσα στις στρατιωτικές βάσεις των ΗΠΑ. Στάλθηκε το πρώτο μήνυμα απομακρυσμένων υπολογιστών αποτελώντας το πρώτο δίκτυο που σήμανε νέα εποχή δικτύωσης, και το ξεκίνημα της εποχής του Internet.
- Το 1982 ήταν η γενιά του Internet και του πρωτόκολλου TCP/IP, το οποίο έγινε πρότυπο. Με το πρωτόκολλο TCP/IP ξεκινά μια νέα εποχή, ενός παγκόσμιου ιστού με δίκτυα που ενώνονται μεταξύ τους, για να δημιουργηθεί το διαδίκτυο όπως το ξέρουμε σήμερα.
- Η τεχνολογία του RFID που θα χρησιμοποιηθεί κατά κόρων στην εποχή του Internet of Things, είναι η τεχνολογία που μας επιτρέπει την ασύρματη αλλά παθητική ανάγνωση και εγγραφή δεδομένων σε συσκευές. Η τεχνολογία αυτήν δημιουργήθηκε τον Ιανουάριο του 1973 από τον Mario Cardullo και όμως η ευρεία χρήση του RFID, κυρίως στον επιχειρησιακό κλάδο ξεκίνησε το 2013 με την πολυεθνική Inditex, να χρησιμοποιεί την τεχνολογία μαζικά σε όλα τα καταστήματα της, και εν συνεχεία με άλλες επιχειρήσεις να ασπάζονται το όραμα του Internet of Things.
- Μια δεκαετία μετά, αναπτύχθηκε η σκέψη επικοινωνίας «Machine to Machine» από φοιτητές του Πανεπιστημίου Carnegie Mellon της Pennsylvania. Εγκατέστησαν μηχανισμούς για την παρακολούθηση θερμοκρασίας από τερματικούς υπολογιστές, στα μηχανήματα αυτόματων πολιτών που υπήρχαν στο Πανεπιστήμιο.
- Το 1995 η Siemens ανακοίνωσε το πρώτο chip το οποίο μέσω δικτύου GSM επιτρέπει βιομηχανικά συστήματα να επικοινωνούν μεταξύ τους ασύρματα και να εκτελούν εντολές, ενώ η IEEE ξεκίνησε το πρώτο διεθνές φόρουμ για τα wearable computers.
- Το 1999 το MIT δημιουργεί το πρώτο κέντρο ερευνών με σύγχρονα συστήματα για έρευνες και μέσα σε 2 χρόνια ο David Brock ανακοίνωσε την εξέλιξη των Barcodes σε ένα νέο σύστημα ποιο έξυπνων τρόπων ανάγνωσης πληροφοριών. Αυτός ο τρόπος θα επέτρεπε τις τεχνολογίες RFID, Bluetooth και άλλες ασύρματες τεχνολογίες να τροποποιήσουν, διαβάσουν και να γράψουν δεδομένα σε αντικείμενα, μέσω ενός RFID tag. Αυτό το νέο σύστημα ονομάστηκε EPC (Electronic Product Code). Ένα χρόνο μετά έγινε το πρώτο υπερσύγχρονο δίκτυο ανάπτυξης και standardizing του Internet of Things.

- Το 2000 ο υπάλληλος της IBM Andy Stanford και ο υπάλληλος Arlen Nipper της εταιρίας Eurotech δημιούργησαν το πρώτο πρωτόκολλο επικοινωνίας Machine to Machine, για συσκευές οι οποίες είναι διασυνδεδεμένες με τον ιστό. Το πρωτόκολλο ονομάστηκε από τους ίδιους MQ Telemetry Transport (MQTT), και ήταν ένα σημαντικό βήμα προς την ενίσχυση της ιδέας για το IoT.
- Το 2005 μέλη από το πρόγραμμα Interaction Design Institute Ivrea κατασκεύασαν την πλατφόρμα του Arduino, για μια φτηνή λύση μικροελεγκτή που προορίζονταν για τους φοιτητές.
- Το 2008 η ομάδα IPSO συντάχθηκε με σκοπό να διαδώσουν το πρωτόκολλο IP σε όλα τα μελλοντικά σχέδια και προτάσεις του Internet of Things. Πλέον η IPSO έχει πάνω από 50 εταιρικά μέλη για την διάδοση του πρωτοκόλλου προς το μέλλον.
- Δύο χρόνια μετά, η τεχνολογία του Bluetooth αναβαθμίζεται και έρχεται στην αγορά ένα νέο standard με ονομασία Smart Bluetooth ή αλλιώς Bluetooth Low Energy (BLE), επιτρέποντας νέες εφαρμογές και συνδεδεμένες συσκευές στους τομείς της υγείας, άθλησης, και home entertainment να ενταχθούν στον κόσμο του IoT .
- Το 2010 πληροφορίες που διέρρευαν σχετικά με τ' ότι η υπηρεσία της Google, Street View φωτογραφούσε 360 μοιρών φωτογραφίες και αποτύπωνε γειτονιές και δρόμους σε ηλεκτρονική μορφή, αλλά επίσης είχε αποθηκευμένους τόνους δεδομένων των δικτύων WiFi των ανθρώπων σε αυτές τις περιοχές. Οι άνθρωποι συζητούσαν αυτή την πληροφορία σαν την αρχή μιας νέας στρατηγικής της Google. Την ίδια χρονιά, η κινεζική κυβέρνηση ανακοίνωσε ότι θα κάνει το IoT να αποτελεί στρατηγική προτεραιότητα στο πενταετές σχέδιο τους.
- Ενώ το 2011, η Gartner, η εταιρεία έρευνας της αγοράς που εφηύρε την περίφημη «διαφημιστική εκστρατεία του κύκλου για τις αναδυόμενες τεχνολογίες» περιλαμβάνεται ένα νέο στη λίστα της: «To Internet of Things».
- Το επόμενο έτος, το θέμα της μεγαλύτερης ευρωπαϊκής διαδικτυακής διάσκεψης LeWeb ήταν το «Internet of Things». Ταυτόχρονα δημοφιλή περιοδικά που εστιάζουν στην τεχνολογία όπως το Forbes, το Fast Company, και το Wired άρχισαν να χρησιμοποιούν το IoT στο λεξιλόγιό τους για να περιγράψουν το νέο αυτό φαινόμενο. Την ίδια χρονιά το πρωτόκολλο του IP

άλλαξε versioning και με την νέα έκτη έκδοση του υποστηρίζει περισσότερες συσκευές γρηγορότερες, αποδοτικότερες σε θέματα διασύνδεσης και με την υπόσχεση ότι μπορεί να υποστηρίξει των καλπάζοντας ρυθμό ζήτησης για διευθύνσεις έως το 2128.

- Τον Οκτώβριο του 2013, η IDC δημοσίευσε μια έκθεση που αναφέρει ότι το IoT θα στοίχιζε \$8.900 δισεκατομμύρια στην αγορά το 2020 και ο όρος Internet of Things έφτασε στη μαζική συνειδητοποίηση της αγοράς, όταν η Google ανακοίνωσε την αγορά της Nest για \$3,2 δις μια εταιρία που κατασκεύαζε συσκευές για το IoT καθώς την ίδια στιγμή το Consumer Electronics Show (CES) στο Λας Βέγκας πραγματοποιήθηκε υπό το θέμα του IoT.
- Το 2014 η Apple ανακοίνωσε το HealthKit & HomeKit, δυο πλατφόρμες ανάπτυξης υλοποιήσεων και την υποστήριξη της πλατφόρμας από τις νέες συσκευές, με σκοπό η ιδέα του έξυπνου σπιτιού & τρόπο ζωής να έρθει πιο κοντά στο σήμερα. Επίσης η τεχνολογία iBeacon έφερε νέα πρότυπα στην αγορά των καταστημάτων και της πώλησης.

Όπως φαίνεται από τις πιο πάνω ιστορικές αναδρομές, τα σημεία κλειδιά για την ανάπτυξη του Internet of Things ήταν η τεχνολογία του RFID και συναφείς τεχνολογίες διευθυνσιοδότησης -που αναπτύχθηκαν πρώτα στο κέντρο Auto ID Lab - καθώς και οι δυνατότητες του IPv6 θα επιτρέψουν κάθε αντικείμενο να έχει την δικιά του ξεχωριστή IP διεύθυνση, και αυτά τα αντικείμενα να «εισέλθουν» στο κόσμο του IoT².

2.2 Συνδεσιμότητα

Όπως αναφέρθηκε το IoT έχει ως βάση τη σύνδεση διάφορων μικρών συσκευών ή οχημάτων με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης τόσο μεταξύ τους όσο και με το κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά δεδομένα με στόχο να προσφέρουν περισσότερες υπηρεσίες.

Το IoT απεικονίζεται ως μια σειρά από νέα ανεξάρτητα ενσωματωμένα συστήματα διαστάσεων μικροσίπ, smart συσκευές, real time systems, συστήματα συγκέντρωσης όλων των πληροφοριών σε μεγάλες βάσεις δεδομένων, που

² Bassi, Alessandro, και συν. *Enabling Things o Talk: Designing IOT solutions with the IOT Architectural Reference Model*. New York : Springer, 2013.

λειτουργούν με δικές τους υποδομές και χρησιμοποιούν το διαδίκτυο για τη σύνδεσή τους.

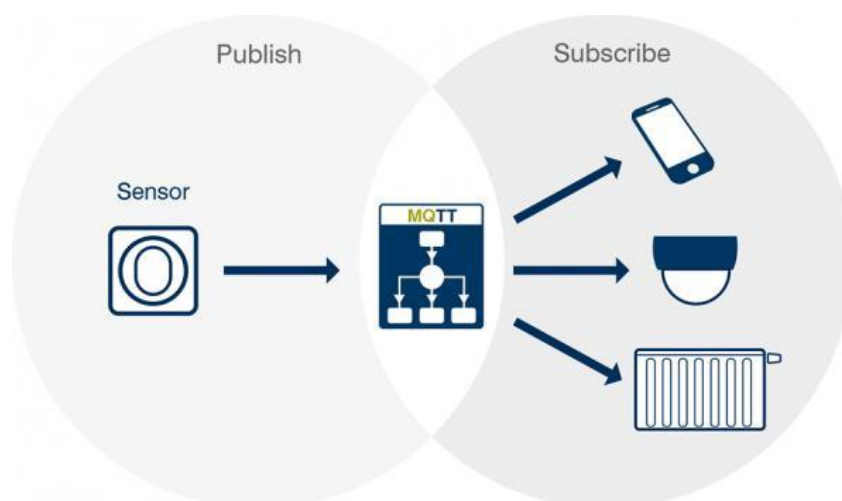
Τα τρία κύρια μέρη ενός IoT είναι:

1. Οι συσκευές που συλλέγουν πληροφορίες οπουδήποτε και οποιαδήποτε στιγμή χρησιμοποιώντας RFID τεχνολογία, αισθητήρες και κώδικα.
2. Τα δίκτυα επικοινωνιών που συνδέουν τις συσκευές αυτές.
3. Τα υπολογιστικά συστήματα και οι εφαρμογές που επεξεργάζονται όσα δεδομένα ρέουν από και προς τις συσκευές αυτές.

Η συνδεσιμότητα των τριών αυτών μερών του IoT πραγματοποιείται με τέσσερις τρόπους δικτύωσης.

2.2.1 Μοντέλο Device-to-Device

Το μοντέλο επικοινωνίας device to device αντιπροσωπεύει δυο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους, και όχι μέσω ενδιάμεσου server εφαρμογών. Αυτές οι συσκευές επικοινωνούν μέσω πολλών τύπων δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Internet, χρησιμοποιώντας πρωτόκολλα όπως Bluetooth, 40 Z-Wave ή ZigBee³.



Εικόνα 3: Device-to-Device¹⁵

Τα μοντέλα αυτά, device-to-device δίνουν την δυνατότητα στις συσκευές που στηρίζονται σε ένα συγκεκριμένο πρωτόκολλο επικοινωνίας να επικοινωνούν και να ανταλλάσσουν μηνύματα μεταξύ τους. Το device-to-device χρησιμοποιείται ευρέως σε εφαρμογές όπως τα συστήματα οικιακού αυτοματισμού, που συνήθως

³“Definition of Cloud Computing” Mell, Peter and Grace, Tim, NIST 2009

χρησιμοποιούν μικρά πακέτα δεδομένων πληροφοριών για την επικοινωνία μεταξύ συσκευών και χαρακτηρίζονται από χαμηλό ρυθμό μετάδοσης δεδομένων.

Οικιακές IoT συσκευές όπως λαμπτήρες, διακόπτες φωτισμού, θερμοστάτες και κλειδαριές στις πόρτες συνήθως στέλνουν μικρές ποσότητες πληροφοριών μεταξύ τους.

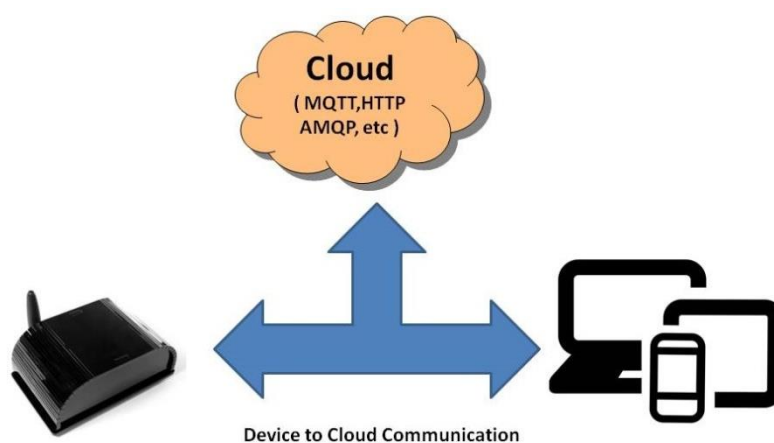
Όμως αυτή η προσέγγιση του μοντέλου επικοινωνίας device-to-device απεικονίζει πολλές από τις προκλήσεις της διαλειτουργικότητας. Αυτές οι συσκευές έχουν συχνά άμεση σχέση μεταξύ τους και έχουν συνήθως ενσωματωμένη ασφάλεια, αλλά χρησιμοποιούν επίσης μοντέλα δεδομένων για συγκεκριμένες συσκευές που απαιτούν περεταίρω προσπάθειες ανάπτυξης από τις κατασκευαστές τους. Αυτό σημαίνει ότι οι κατασκευαστές να πρέπει να επενδύσουν στην αναπτυξιακή προσπάθεια για την υλοποίηση συσκευών με συγκεκριμένες μορφές δεδομένων και όχι ανοιχτές προσεγγίσεις που επιτρέπουν τη χρήση τυποποιημένων μορφών δεδομένων. Από τη πλευρά του χρήστη, αυτό σημαίνει ότι τα πρωτόκολλα επικοινωνίας του μοντέλου device-to-device δεν είναι συμβατά, αναγκάζοντάς τον να επιλέξει μια οικογένεια συσκευών που χρησιμοποιούν ένα κοινό πρωτόκολλο. Για παράδειγμα, η οικογένεια των συσκευών που χρησιμοποιούν τα πρωτόκολλα Z-Wave δεν είναι συμβατή με την οικογένεια συσκευών που χρησιμοποιούν το πρωτόκολλο ZigBee⁴.

⁴ Machine to Machine, https://en.wikipedia.org/wiki/Machine_to_machine. s.l. : Wikipedia.

2.2.2 Μοντέλο Device-to-Cloud

Σε αυτό το μοντέλο, η IoT συσκευή συνδέεται απευθείας σε μια διαδικτυακή υπηρεσία cloud όπως ένας πάροχος υπηρεσιών εφαρμογής, ώστε να ανταλλάσσει δεδομένα και να διαχειρίζεται την κίνηση μηνυμάτων.

Αυτό το μοντέλο συχνά εκμεταλλεύεται υπάρχοντες μηχανισμούς επικοινωνίας όπως η παραδοσιακή ενσύρματη Ethernet ή Wi-Fi συνδέσεις για να εγκαταστήσει μια σύνδεση μεταξύ της συσκευής και του δικτύου IP, το οποίο συνδέεται τελικά με υπηρεσία cloud.



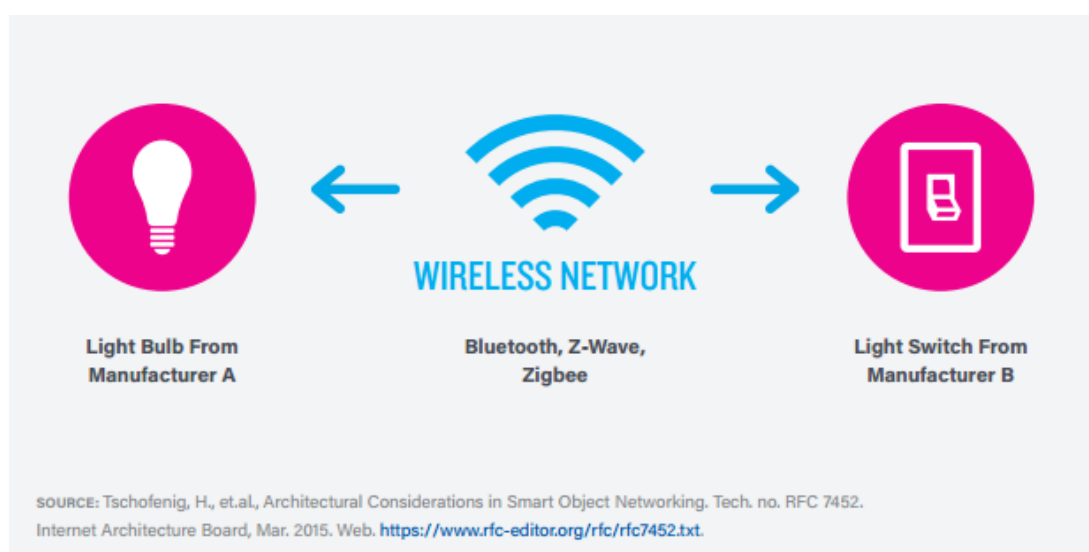
Εικόνα 4: Device-to-Cloud¹⁶

Το επικοινωνιακό αυτό μοντέλο χρησιμοποιείται από κάποιες γνωστές καταναλωτικές IoT συσκευές όπως η SmartTV της Samsung και το Learning Thermostat της Nest Labs. Στην δεύτερη περίπτωση, η συσκευή μεταδίδει δεδομένα σε μια cloud βάση δεδομένων όπου τα δεδομένα μπορούν να χρησιμοποιηθούν για να αναλύσουν την κατανάλωση οικιακής ενέργειας. Επιπλέον αυτή η σύνδεση με το cloud δίνει τη δυνατότητα στον χρήστη να αποκτήσει εξ αποστάσεως πρόσβαση στον θερμοστάτη του μέσω ενός smartphone ή μέσου του ιστού και επίσης υποστηρίζει αναβαθμίσεις λογισμικού για τον θερμοστάτη. Παρομοίως με την τεχνολογία SmartTV η τηλεόραση χρησιμοποιεί μια διαδικτυακή σύνδεση για να μεταδίδει πληροφορίες προβολών του χρήστη στη Samsung για ανάλυση και να ενεργοποιεί τις διαδραστικές λειτουργίες αναγνώρισης ομιλίας που διαθέτει η τηλεόραση. Σε αυτές τις περιπτώσεις το μοντέλο Device-to-Cloud προσθέτει αξία στον χρήστη επεκτείνοντας τις δυνατότητες της συσκευής πέρα από τα εγγενή της χαρακτηριστικά.

Παρόλα αυτά, προκλήσεις στη διαλειτουργικότητα μπορούν να προκληθούν όταν γίνεται προσπάθεια ενοποίησης συσκευών οι οποίες είναι φτιαγμένες από διαφορετικούς κατασκευαστές. Συχνά η συσκευή και η υπηρεσία cloud είναι από το ίδιο προμηθευτή. Αν χρησιμοποιούνται πρωτόκολλα δεδομένων βιομηχανικής ιδιοκτησίας μεταξύ της συσκευής και της υπηρεσίας cloud, ο ιδιοκτήτης ή ο χρήστης της συσκευής ίσως να δεσμεύεται από συγκεκριμένη υπηρεσία cloud, περιορίζοντας ή αποτρέποντας τη χρήση εναλλακτικών πάροχων υπηρεσιών. Αυτό αναφέρεται ως «κλείδωμα προμηθευτών» (vendor lock-in), ένας όρος που περικλείει άλλες όψεις της σχέσης με το πάροχο όπως η ιδιοκτησία και η πρόσβαση στα δεδομένα. Ταυτόχρονα οι χρήστες μπορούν να είναι σίγουροι ότι συσκευές που είναι σχεδιασμένες για τη συγκεκριμένη πλατφόρμα μπορούν να ενσωματωθούν.

2.2.3 Μοντέλο Device-to-Gateway

Στο μοντέλο Device-to-Gateway η συσκευή συνδέεται μέσω μιας υπηρεσίας ALG ως αγωγός για να επιτευχθεί μια σύνδεση με την υπηρεσία cloud. Διαθέτει λογισμικό εφαρμογής, το οποίο δρα ως διαμεσολαβητής μεταξύ της συσκευής και της υπηρεσίας cloud και παρέχει ασφάλεια και άλλες λειτουργίες όπως δεδομένα ή μετάφραση πρωτόκολλων.



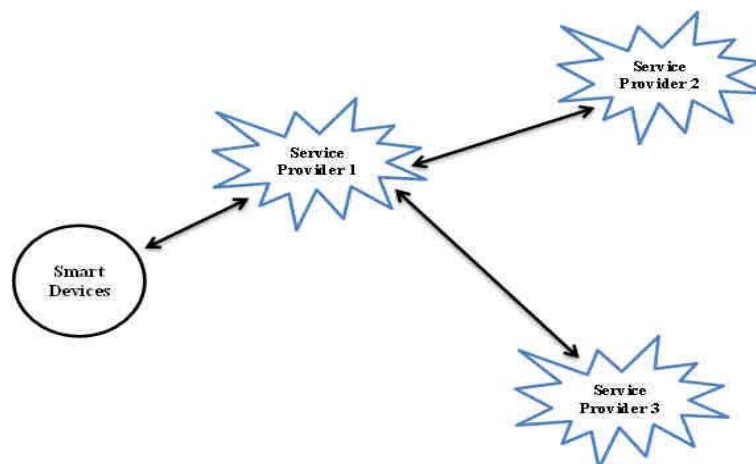
Εικόνα 5: Device-to-Gateway

Αυτό το μοντέλο βρίσκει εφαρμογή σε συσκευές καταναλωτών. Οι συσκευές που χρησιμοποιούν αυτό το μοντέλο επικοινωνίας είναι τα smartphones, τα οποία τρέχουν εφαρμογές για να επικοινωνήσουν με τις IoT συσκευές και να μεταφέρουν δεδομένα σε μια υπηρεσία cloud. Οι συσκευές αυτές δεν έχουν τη δυνατότητα να συνδεθούν απευθείας με μια υπηρεσία cloud οπότε βασίζονται συχνά σε εφαρμογές των smartphones οι οποίες λειτουργούν ως μεσάζοντες.

Άλλη μορφή αυτού του μοντέλου επικοινωνίας αποτελούν οι συσκευές «Hub» σε εφαρμογές οικιακού αυτοματισμού. Τα «Hub» είναι συσκευές που λειτουργούν ως Gateway μεταξύ των μεμονωμένων IoT συσκευών και μιας υπηρεσίας cloud, αλλά ταυτόχρονα μπορούν να γεφυρώσουν το χάσμα της διαλειτουργικότητας μεταξύ των IoT συσκευών. Παράδειγμα αυτού του μοντέλου αποτελεί το Hub SmartThings που είναι μια αυτόνομη συσκευή Gateway που έχει εγκατεστημένους Z-Wave και ZigBee πομποδέκτες για να μπορεί να επικοινωνεί και με τις δυο οικογένειες συσκευών. Έπειτα συνδέεται με την υπηρεσία cloud Smart Things, επιτρέποντας στον χρήστη να αποκτήσει πρόσβαση στις συσκευές χρησιμοποιώντας μόνο μια εφαρμογή smartphone και μια σύνδεση στο Internet. Μειονέκτημα αυτής της προσέγγισης αποτελεί η απαραίτητη ανάπτυξη του συστήματος και του λογισμικού εφαρμογών πράγμα που το κάνει πολύπλοκο και μεγάλου κόστους.

2.2.4 Μοντέλο Back-End Data Sharing

Το μοντέλο αυτό αναφέρεται σε μια αρχιτεκτονική επικοινωνίας η οποία επιτρέπει στους χρήστες να εξάγουν και να αναλύσουν τα δεδομένα του έξυπνου αντικειμένου από μια υπηρεσία cloud, σε συνδυασμό με δεδομένα από άλλες πηγές. Αποτελεί επέκταση του μοντέλου Device-to-Cloud η οποία επιτρέπει στις συσκευές να ανεβάζουν δεδομένα μόνο για έναν πάροχο υπηρεσιών εφαρμογής. Το μοντέλο αυτό επιτρέπει τα δεδομένα που συλλέγονται να συγκεντρώνονται και να αναλύονται. Παράδειγμα χρήσης ενός τέτοιου μοντέλου αποτελεί ένας εταιρικός χρήστης ο οποίος θέλει να συγκεντρώσει και να αναλύσει δεδομένα που παράγονται από όλους τους αισθητήρες IoT. Η χρήση αυτού του μοντέλου θα επιτρέψει στην εταιρία να έχει εύκολη πρόσβαση και ανάλυση των δεδομένων που παράγονται από όλο το φάσμα των συσκευών στο κτίριο. Επιπρόσθετα επιτρέπει και διευκολύνει την ανάγκη για φορητότητα των δεδομένων.



Εικόνα 6: Data Sharing¹⁷

Η αρχιτεκτονική του μοντέλου αυτού είναι μια προσέγγιση για την επίτευξη της διαλειτουργικότητας μεταξύ back-end συστημάτων. Παρ' όλα αυτά το μοντέλο επικοινωνίας αυτό είναι τόσο αποτελεσματικό όσο τα υποκείμενα σχέδια του IoT συστήματος⁵.

2.3 Σύνοψη των Μοντέλων

Τα τέσσερα αυτά βασικά μοντέλα επιδεικνύουν στρατηγικές σχεδιασμού που χρησιμοποιούνται για να επιτρέψουν στις IoT συσκευές να επικοινωνήσουν και η χρήση των μοντέλων αυτών επηρεάζεται σε μεγάλο βαθμό από τη φύση των ίδιων των συσκευών. Στην περίπτωση Device-to-Gateway, το κύριο χαρακτηριστικό αποτελεί η ικανότητα να ξεπεραστούν οι περιορισμοί που υπάρχουν στην συνδεσιμότητα των IoT συσκευών. Αυτό σημαίνει πως η διαλειτουργικότητα των συσκευών αποτελεί βασικός παράγοντας στο σχεδιασμό και στην ανάπτυξη των συστημάτων IoT.

Σε τρία από τα τέσσερα μοντέλα επικοινωνίας οι συσκευές συνδέονται με μια υπηρεσία ανάλυσης δεδομένων σε περιβάλλον cloud. Με αυτό τον τρόπο οι χρήστες και οι πάροχοι υπηρεσιών μπορούν να χρησιμοποιήσουν με μεγαλύτερη ευκολία το σύνολο των δεδομένων, μπορούν να έχουν καλύτερη ανάλυση δεδομένων, οπτικοποίηση των δεδομένων και ανάπτυξη τεχνολογιών πρόβλεψης.

Με άλλα λόγια όσο καλύτερη η αρχιτεκτονική επικοινωνίας τόσο μεγαλύτερη η αξία που προσφέρεται στον τελικό χρήστη, ανοίγοντας δυνατότητες χρήσης των πληροφοριών με νέους τρόπους. Παρόλο που ο χρήστης έχει πολλά οφέλη από αυτά τα μοντέλα επικοινωνίας, θα πρέπει να σημειωθεί πως ενισχύεται και η τεχνολογική καινοτομία και η εμπορική ανάπτυξη. Νέα προϊόντα και υπηρεσίες μπορούν να σχεδιαστούν και να επωφεληθούν από IoT ροές δεδομένων που δεν υπήρχαν στο παρελθόν ενισχύοντας έτσι περαιτέρω καινοτομία.

⁵Mell, Peter και Grace, Tim. *Definition of Cloud Computing*. s.l. : NIST, 2009.

ΚΕΦΑΛΑΙΟ 3- ΤΕΧΝΟΛΟΓΙΕΣ ΤΟΥ ΙoT- **ΜΟΝΤΕΛΟ ARM**

Στο τρέχων κεφάλαιο γίνεται αναφορά στις τεχνολογίες πάνω στην οποία βασίζεται το IoT, δηλαδή η τεχνολογία πάνω στην οποία στηρίζεται η συνδεσιμότητα τους. Τεχνολογίες όπως ραδιοσυχνότητες RFID, ασύρματες τεχνολογίες Wi-Fi είναι κάποιες από τις οποίες στηρίζεται η επικοινωνία των έξυπνων συσκευών και αυτό το κεφάλαιο έχει ως σκοπό τη καλύτερη κατανόησή τους.

Επιπλέον το δεύτερο κομμάτι του κεφαλαίου δίνει έμφαση σε θέματα ασφάλειας που προκύπτουν με τη χρήση τέτοιων τεχνολογιών. Γίνεται αναφορά στα πρωτόκολλα ασφαλείας που θα πρέπει να τηρηθούν και στα θέματα ιδιωτικότητας.

Στο τέλος του κεφαλαίου αναλύεται η αρχιτεκτονική ενός συστήματος IoT, και δίνεται έμφαση στη βασική αρχιτεκτονική στην οποία στηρίζεται το μοντέλο ARM.

3.1 Τεχνολογίες

Η ανάπτυξη υπολογιστικών συστημάτων όπου τα ψηφιακά «πράγματα» μπορούν να αλληλοεπιδρούν με άλλα «πράγματα» για τη συλλογή δεδομένων οδήγησε στην ανάγκη για εύρεση και συνδυασμό νέων και αποτελεσματικών τεχνολογιών, οι οποίες έχουν την δυνατότητα να κάνουν τα πράγματα να εντοπίζονται και να επικοινωνούν μεταξύ τους. Οπότε, όλα καθοδηγούνται από τις νέες δυνατότητες ψηφιακής ανίχνευσης, τα ενσωματωμένα συστήματα πληροφορικής και επικοινωνιών που συνδέονται μέσω RFID (αναγνώρισης ραδιοσυχνοτήτων), ασύρματων δικτύων αισθητήρων (WSN), micro-chips, barcodes, QR (Quick Response) κωδικούς, Bluetooth, Wi-Fi, Beacons, Big Data, Analytics και Business Intelligence.

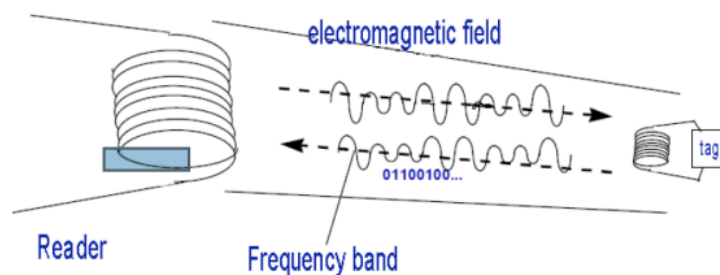
3.1.1 RFID- Ταυτοποίηση μέσω Ραδιοσυχνοτήτων

Το θεμέλιο του IoT είναι η τεχνολογία ανίχνευσης της συσκευής. Προς το παρόν η συλλογή πληροφοριών σε αυτό το σύστημα πραγματοποιείται από ηλεκτρονικές ετικέτες και αισθητήρες. Το IoT χρησιμοποιεί ευρέος φάσματος τεχνολογίες που στέλνουν σήμα σε ένα ευρύ φάσμα συχνοτήτων όπως η RFID.

Αποτελεί τη πιο βασική τεχνολογία του IoT για την αναγνώριση, τον προσδιορισμό και τη σύνδεση των «πραγμάτων». Είναι ένα μικροσίπ πομποδέκτης μαζί με ραδιοκύματα παρόμοιο με μία ετικέτα το οποίο θα μπορούσε να είναι είτε ενεργητικό είτε και παθητικό, ανάλογα με τον τύπο της εφαρμογής που

χρησιμοποιείται. Οι ενεργητικές ετικέτες αποτελούνται από μια μπαταρία, που λειτουργεί σαν παροχή ισχύος, εκπέμποντας συνεχώς σήματα δεδομένων, ενώ οι παθητικές ετικέτες δεν έχουν κάποια τροφοδοσία και απορροφούν ενέργεια από το ηλεκτρομαγνητικό πεδίο που δημιουργεί η κεραία της συσκευής ανάγνωσης. Το RFID σύστημα αποτελείται από ετικέτες/ αναμεταδότες, ένα πρόγραμμα ανάγνωσης και λογισμικό υποστήριξης. Ανάλογα με τον τύπο της εφαρμογής, οι συχνότητες RFID διαίρουνται σε τέσσερις διαφορετικές περιοχές συχνοτήτων :

- Χαμηλής συχνότητας (135kHz ή λιγότερο)
- Υψηλής συχνότητας (13.56 MHz)
- Ultra-High συχνότητα (862 MHz, 928MHz)
- Συχνότητα μικροκυμάτων (2,4GHz)⁶



Εικόνα 7: RFID system¹⁸

Το βασικό πλεονέκτημα της τεχνολογίας RFID αποτελεί το χαμηλό της κόστος, γεγονός που επιτρέπει την εξάπλωσή της. Έχει σημειώσει ιδιαίτερη απήχηση σε τομείς όπως αυτός της Ρομποτικής και στο κλάδο της Βιομηχανίας.

3.1.2 Ασύρματες Τεχνολογίες

Θα παρουσιαστούν οι τεχνολογίες δικτύου που μπορούν να βοηθήσουν στην μεγάλης κλίμακας ανάπτυξη του IoT. Εφόσον η κάθε συσκευή ενδέχεται να χρειάζεται να επικοινωνήσει με άλλες σε οποιαδήποτε απόσταση και με διαφορετικό μέσο επικοινωνίας, υπάρχουν συγκεκριμένες κατάλληλες τεχνολογίες αναλόγως των αποστάσεων:

⁶Forge, Simon. Radio Spectrum for the Internet of Things. INFO. Emerald Group Publishing, 2016, Τόμ. 18.

- BAN (Body Area Network), μερικά μέτρα PAN (Personal Area Network), από 10 έως 100 m
- LAN (Local Area Network), μερικά km MAN (Metropolitan Area Network), 10 έως 100 km
- WAN (Wide Area Network), 1000 km GAN (Global Area Network).



Εικόνα 8: Wireless Communication¹⁹

Οι ασύρματες τεχνολογίες (με τα πρωτόκολλα) για το IoT που έχουν αναπτυχθεί είναι οι ακόλουθες: ZigBee , WiMax , WiFi, UWB και Flash OFDM κυψελωτά συστήματα:

Το ZigBee είναι μια ασύρματη τεχνολογία που αναπτύχθηκε για να καλύψει τις ανάγκες για χαμηλό κόστος, χαμηλή ισχύς των ασύρματων δικτύων αισθητήρων. Το ZigBee στοχεύει στις εφαρμογές ραδιοσυχνότητας (RF) που απαιτούν ένα χαμηλό ρυθμό μεταφοράς δεδομένων, μεγάλη ζωή μπαταριών, και εξασφαλισμένη δικτύωση. Το WiMAX αποκαλείται η τεχνολογία ασύρματης δικτύωσης η οποία λειτουργεί με παρεμφερή τρόπο με το Wi-Fi, ωστόσο με πολύ μεγαλύτερη εμβέλεια. Συγκεκριμένα, ενώ το Wi-Fi εξασφαλίζει εμβέλεια επικοινωνίας μέχρι 100 μέτρα, το WiMax φθάνει τα 35 χιλιόμετρα ή και παραπάνω.

Η UWB τεχνολογία μπορεί γενικά να οριστεί σαν μια οποιαδήποτε ασύρματη μεταβίβαση που καταλαμβάνει ένα μήκος κύματος με συχνότητα 1,5 GHz. Είναι μια νέα μορφή της ασύρματης τεχνολογίας που βασίζεται σε μεταβίβαση χαμηλής ισχύος και κωδικοποιημένες ωθήσεις σε περιβάλλον μικρής απόστασης. Η UWB τεχνολογία χρησιμοποιείται σε εμπορικές και βιομηχανικές εφαρμογές για τον καθορισμό αποστάσεων ανάμεσα σε αντικείμενα, στην ανίχνευση αντικειμένων και καταστάσεων δια μέσου οικοδομών, σε συστήματα ασφαλείας και σε ιατρικά συστήματα.

Η ανακάλυψη των Flash OFDM κυψελωτών ραδιοσυστημάτων βελτίωσε τις ασύρματες επικοινωνίες, αφού προσέφερε χρήση περισσότερων καναλιών, επικάλυψη ραδιοσυχνοτήτων, ενώ πομποί και δέκτες χρειαζόταν πλέον λιγότερη ισχύ για την λειτουργία τους, κάτι που σήμαινε μικρότερο κόστος, βάρος και μέγεθος, καθώς και λιγότερες παρεμβολές. Η βασική ιδέα είναι ότι η γεωγραφική περιοχή που καλύπτει το σύστημα επικοινωνίας, χωρίζεται σε κυψέλες. Κάθε κυψέλη χρησιμοποιεί ένα σύνολο συχνοτήτων που μπορεί να χρησιμοποιούν και άλλες κοντινές κυψέλες αλλά όχι οι γειτονικές της.

3.1.3 Cloud Computing

Πρόκειται για μια έξυπνη τεχνολογία υπολογιστών με την οποία μεγάλος αριθμός servers συγκλίνουν σε μία πλατφόρμα cloud, η οποία επιτρέπει την κατανομή των πόρων μεταξύ τους και την πρόσβαση στα πράγματα οποιαδήποτε στιγμή και από οποιοδήποτε μέρος. Το cloud computing είναι το πιο σημαντικό μέρος του IoT, το οποίο δεν συνδέει μόνο τους διακομιστές, αλλά αναλύει και τις χρήσιμες πληροφορίες που λαμβάνονται από τους αισθητήρες παρέχοντας υψηλή ικανότητα αποθήκευσης.



Εικόνα 9: Cloud Computing Model₂₀

Το cloud μοντέλο αποτελείται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα παροχής υπηρεσιών, και τέσσερα μοντέλα ανάπτυξης:

- Private Cloud: Η υποδομή αυτή λειτουργεί αποκλειστικά και μόνο για έναν χρήστη και η διαχείρισή της μπορεί να γίνεται από τον ίδιο τον οργανισμό.
- Community Cloud: Η υποδομή αυτή μοιράζεται μεταξύ πολλών οργανισμών και υποστηρίζει μια συγκεκριμένη κοινότητα που έχει κοινές ανησυχίες και σκοπό. Η διαχείρισή της γίνεται από τον ίδιο τον οργανισμό.

- Public Cloud: Η υποδομή διατίθεται σε ευρύ κοινό και ανήκει σε έναν οργανισμό που πουλά υπηρεσίες cloud.
- Hybrid Cloud: Η υποδομή αυτή αποτελεί σύνθεση δυο ή περισσότερων clouds (private, community ή public) τα οποία παραμένουν μοναδικές οντότητες αλλά συνδέονται με τυποποιημένη ή αποκλειστική τεχνολογία που επιτρέπει τη μεταφορά δεδομένων και εφαρμογών.

Υπάρχουν και αντίστοιχα διάφορα μοντέλα παροχής υπηρεσιών που προσφέρουν διαφορετικές δυνατότητες. Συνοπτικά αναφέρονται παρακάτω:

- Cloud Service as a Software (SAAS): Ο καταναλωτής έχει τη δυνατότητα να χρησιμοποιεί τις εφαρμογές του παρόχου που τρέχουν στην υποδομή του. Οι εφαρμογές αυτές είναι προσβάσιμες από διάφορες client συσκευές μέσω ενός interface, όπως ένα πρόγραμμα περιήγησης Web. Ένα παράδειγμα αποτελεί το Google Drive και οι εφαρμογές του μπορούν να τρέξουν απ' ευθείας σε αυτό. Ο καταναλωτής δεν έχει τον έλεγχο ή τη διαχείριση της υποδομής παρά μόνο κάποιων user-specific ρυθμίσεων παραμετροποίησης εφαρμογών.
- Cloud Platform as a Service (PAAS): Ο καταναλωτής έχει τη δυνατότητα να αναπτύσσει πάνω στην cloud υποδομή εφαρμογές που έχει δημιουργήσει ή εφαρμογές που έχει αποκτήσει. Και πάλι δεν έχει τον έλεγχο ή τη διαχείριση της υποδομής αλλά έχει τον έλεγχο των εφαρμογών που έχουν αναπτυχθεί.
- Storage as a Service (STAAS): Υπάρχει πάροχος αποθηκευτικού χώρου online ο οποίος το νοικιάζει έναντι κάποιας αμοιβής. Παράδειγμα τέτοιας υποδομής αποτελεί το Drop box.
- Hardware as a Service (HAAS): Έναντι κάποιας αμοιβής ο προμηθευτής παρέχει hardware που χρειάζεται ένας χρήστης όπως web servers, μνήμη CPU, αποθηκευτικό χώρο και ότι άλλο μπορεί να χρειαστεί σε επίπεδο hardware.
- Database as a Service (DAAS): Υπάρχει μια online υπηρεσία που παρέχει βάση δεδομένων η οποία μπορεί να χρησιμοποιηθεί για web application. Η αμοιβή είναι ανάλογη της χρήσης, οπότε όσο περισσότερος κόσμος χρησιμοποιεί την εφαρμογή τόσο μεγαλύτερο το κόστος.
- Cloud Infrastructure as a Service (IAAS): Η δυνατότητα που προσφέρεται στο χρήστη είναι να μπορεί να δεσμεύσει προς χρήση επεξεργαστική ισχύ, αποθηκευτικά μέσα, δίκτυα και άλλους υπολογιστικούς πόρους όπου μπορεί να αναπτυχθεί λογισμικό το οποίο περιλαμβάνει λειτουργικά συστήματα και εφαρμογές. Ο καταναλωτής δεν έχει τον έλεγχο της χρησιμοποιημένης cloud υποδομής αλλά έχει τον έλεγχο των λειτουργικών συστημάτων που έχει αναπτύξει.

3.1.4 Τεχνολογίες Δικτύου

Οι τεχνολογίες αυτές έχουν παίξει σημαντικό ρόλο στην επιτυχία του IoT δεδομένου ότι είναι υπεύθυνες για την σύνδεση μεγάλου αριθμού πραγμάτων, προσφέροντας ένα γρήγορο και αποτελεσματικό δίκτυο. Για ευρύ φάσμα δίκτυο συνήθως χρησιμοποιούνται τα 3G, 4G κ.λπ. ενώ για ένα δίκτυο επικοινωνίας μικρής εμβέλειας χρησιμοποιούνται τεχνολογίες όπως Bluetooth, WiFi κ.α. Παρακάτω αναλύονται οι σημαντικότερες εξ αυτών⁷:

3.1.4.1 Δίκτυο Ασύρματων Αισθητήρων- Wireless Sensor Network (WSN)

Ιδιαίτερα σημαντική τεχνολογία του IoT αποτελεί το Δίκτυο ασύρματων αισθητήρων (Wireless Sensor Network (WSN)). Το WSN αποτελείται από ένα μεγάλο αριθμό μικροσκοπικών κόμβων αισθητήρων, με δυνατότητα ανίχνευσης των «πραγμάτων». Ο ρόλος των αισθητήρων είναι η παροχή ακατέργαστων πληροφοριών για επεξεργασία, μετάδοση, ανάλυση και ανατροφοδότηση πληροφοριών. Οι κόμβοι συλλέγουν και προωθούν τα δεδομένα στο σταθμό βάσης για την από κοινού παρακολούθηση των «πραγμάτων». Στα ασύρματα δίκτυα αισθητήρων υπάρχουν ένας ή περισσότεροι σταθμοί βάσης και αρκετοί κόμβοι αισθητήρων. Η βασική σύνθεση του κόμβου δικτύου αισθητήρων περιλαμβάνει τη μονάδα επεξεργασίας, τη μονάδα επικοινωνίας και τη μονάδα ενέργειας. Ο σταθμός βάσης χρησιμεύει ως επεξεργαστής δεδομένων που συνδέει το δίκτυο αισθητήρων με τον εξωτερικό κόσμο.

3.1.4.2 Beacon Technology

Εξίσου σημαντική η οποία αποτελείται από μικρές ασύρματες συσκευές/ μικροπομπού που μεταδίδουν συνεχώς ένα απλό ραδιοφωνικό σήμα. Όταν η κινητή συσκευή ανιχνεύει το σήμα Beacon, διαβάζει τον αριθμό αναγνώρισης του πομπού (ID), υπολογίζει την απόσταση από το πομπό και με βάση αυτά τα δεδομένα, ενεργοποιεί την εφαρμογή του κινητού. Πρόκειται για μια Real-time επικοινωνία με τους χρήστες. Προσφέρει άμεση και σε πραγματικό χρόνο πρόσβαση στις παρεχόμενες υπηρεσίες οποιαδήποτε στιγμή.

⁷Mell, Peter και Grace, Tim. *Definition of Cloud Computing*. s.l. : NIST, 2009.

3.1.4.3 Επικοινωνία Κοντινού Πεδίου (NFC)

Μία άλλη τεχνολογία το NFC (Near field communication) ή αλλιώς «επικοινωνία κοντινού πεδίου» που δημιουργήθηκε από τις εταιρείες Nokia, Philips και Sony και αποτελεί μια ασύρματη τεχνολογία διασυνδεσιμότητας η οποία επιτρέπει την ανταλλαγή πληροφοριών ανάμεσα σε συσκευές όπως smartphones και tablets. Η λειτουργία του NFC είναι αρκετά απλή, αρκεί να πλησιάσουν μεταξύ τους δύο συσκευές που υποστηρίζουν NFC για να αλληλεπιδράσουν και να ανταλλάξουν πληροφορίες σε αντίθεση με τις τεχνολογίες Bluetooth και WiFi στις οποίες προϋπόθεση για την επικοινωνία των συσκευών αποτελεί η εδραίωση της σύνδεσης (ενεργοποίηση-ανακάλυψη-σύζευξη). Το πλαίσιο λειτουργίας της NFC τεχνολογίας ορίζει δύο τρόπους λειτουργίας τον ενεργό, κατά τον οποίο και οι δύο συσκευές παράγουν ένα RF σήμα μέσω του οποίου πραγματοποιείται η μεταφορά των δεδομένων, και τον παθητικό, κατά τον οποίο μόνο η μία συσκευή παράγει RF σήμα ενώ η άλλη συσκευή λειτουργεί ως «στόχος» μεταφέροντας τα δεδομένα στην πρώτη χωρίς να τροφοδοτείται από εξωτερική πηγή ενέργειας. Σε εφαρμογές όπως η λιανική η τεχνολογία NFC χρησιμοποιείται ⁸, όπου μια συσκευή NFC μπορεί να λειτουργεί ως scanner διαβάζοντας πληροφορίες από RFID ετικέτες, σε οποιουδήποτε είδους πληρωμές και ως επαγγελματική κάρτα, για την ανταλλαγή των στοιχείων των επαφών που είναι καταχωρημένες στις συσκευές μας.

3.1.4.3 Narrow Band IoT

Για τη διασύνδεση συσκευών στο IoT χρησιμοποιήθηκαν τα δίκτυα κινητής τηλεφωνίας. Με τη περαιτέρω ανάπτυξη του “Internet of Things”, το πρόβλημα που εμφανίστηκε είναι ότι τα υπάρχοντα δίκτυα κινητής τηλεφωνίας δεν μπορούσαν να υποστηρίξουν την ταυτόχρονη σύνδεση στο διαδίκτυο χιλιάδων συσκευών που είναι στον ίδιο χώρο, ενώ η κατανάλωση ενέργειας είναι αρκετά μεγάλη. Γι’ αυτό το λόγο επινοήθηκε η Narrow-Band IoT (NB-IoT). Πρόκειται για μία τεχνολογία σύνδεσης συσκευών μέσω δικτύων κινητής επικοινωνίας όπου η κατανάλωση ενέργειας κινείται σε πολύ χαμηλά επίπεδα, επιτρέποντας την ταυτόχρονη σύνδεση στο διαδίκτυο μεγάλου αριθμού συσκευών.

⁸ https://en.wikipedia.org/wiki/Narrowband_IoT

3.2 Ασφάλεια και Ιδιωτικότητα

Το περιβάλλον ενός συστήματος Internet of Things θα πρέπει να δομηθεί με τέτοιο τρόπο ώστε να διασφαλίζει την ασφάλεια και να παρέχει ευκολία στη χρήση. Αφού σε ένα σύστημα IoT κάθε έξυπνο αντικείμενο έχει τη δυνατότητα να συνδέεται με κάποιο άλλο έξυπνο αντικείμενο δημιουργούνται θέματα ασφαλείας και ιδιωτικότητας. Όσο πιο αυτόνομο είναι ένα αντικείμενο τόσες περισσότερες πρωτοβουλίες μπορεί να πάρει και αναδύονται περισσότερα θέματα με την ασφάλεια. Οι βασικές αρχές που θα πρέπει να διασφαλιστούν είναι:

- Εμπιστευτικότητα
- Ιδιωτικότητα
- Ακεραιότητα
- Διαθεσιμότητα
- Αυθεντικότητα
- Αξιοπιστία
- Έλεγχος Πρόσβασης

Στην επόμενη ενότητα γίνεται αναφορά σε αυτές τις αρχές⁹.

3.2.1 Βασικές Απαιτήσεις Ασφάλειας

- Εμπιστευτικότητα

Οι υπηρεσίες IoT μπορεί να εμπεριέχουν ευαίσθητα δεδομένα και πληροφορίες. Γι' αυτό το λόγο θα πρέπει να είναι διασφαλισμένα σχετικά με τους χρήστες που τα διαχειρίζονται. Η εμπιστευτικότητα μπορεί να επιτευχθεί μέσω συμμετρικής ή ασύμμετρης κρυπτογράφησης.

- Ιδιωτικότητα

Όπως έχει ήδη αναφερθεί το σύστημα IoT εμπεριέχει προσωπικά δεδομένα των χρηστών. Θα πρέπει να χρησιμοποιούνται τεχνικές στις ροές πληροφοριών (Information Flow Control) ώστε να δίνουν τη δυνατότητα στα μεταδιδόμενα δεδομένα να χαρακτηρίζονται ως προς το λόγο μεταφοράς τους και με αυτό τον τρόπο να προστατεύονται τα προσωπικά δεδομένα του χρήστη. Παράλληλα μπορούν να χρησιμοποιηθούν πρωτόκολλα ελέγχου πρόσβασης και τεχνικές που βοηθούν στην προστασία της ανωνυμίας.

⁹Li, Shancang, Tryfonas, Theo και Li, Honglei. The Internet of Things: A Security Point of View. *Internet Research*. Emerald Group Publishing, 2016, Τόμ. 26.

- Ακεραιότητα

Στα πλαίσια του IoT μεταδίδονται σημαντικά δεδομένα με φορείς όπως κυβερνητικές αρχές και πάροχοι υπηρεσιών διαδικτύου οπότε είναι απαραίτητης σημασίας η ακεραιότητα των δεδομένων ώστε να μην αλλοιώνονται. Αυτό επιτυγχάνεται με συναρτήσεις κατακερματισμού και κώδικες αυθεντικοποίησης μηνύματος.

- Διαθεσιμότητα

Σε ένα IoT περιβάλλον θα υπάρχουν κόμβοι που λειτουργούν ως εξυπηρετητές/διακομιστές. Σε αυτή τη περίπτωση θα πρέπει οι πληροφορίες αυτές να είναι ανά πάσα στιγμή διαθέσιμες στους χρήστες. Αυτό συνήθως αποτελεί αντικείμενο συμφωνιών σε επίπεδο υπηρεσιών μεταξύ χρηστών και παρόχων.

- Αυθεντικότητα

Σχετίζεται με την επαλήθευση ταυτότητας κάποιου χρήστη. Αυτό όμως θα πρέπει να επιτυγχάνεται από τις δυο πλευρές. Ο αποδέκτης των δεδομένων θα πρέπει να είναι σίγουρος για τη ταυτότητα του αποστολέα και την αυθεντικότητα της πηγής αλλά και ο πάροχος των δεδομένων οφείλει να ταυτοποιεί τον αποδέκτη της πληροφορίας. Μπορούν να χρησιμοποιηθούν αλγόριθμοι αυθεντικοποίησης.

- Αξιοπιστία

Θα πρέπει τα συστήματα IoT να εξασφαλίζουν την αξιοπιστία που παρέχουν. Αυτό περιλαμβάνει και τα σωστά δεδομένα τα οποία θα πρέπει να ανανεώνονται συστηματικά και μεταδίδονται σωστά.

- Έλεγχος Πρόσβασης

Οι μηχανισμοί ελέγχου πρόσβασης αναλαμβάνουν να υλοποιούν μοντέλα για τη διασφάλιση της εξουσιοδοτημένης πρόσβασης σε δεδομένα και πόρους, λαμβάνοντας αποφάσεις βάσει ενός μοντέλου ελέγχου πρόσβασης. Το βασικό στοιχείο που χρησιμοποιείται είναι οι λίστες ελέγχου πρόσβασης που καθορίζουν τα δικαιώματα των χρηστών και ταυτόχρονα υπάρχει ένας έλεγχος πρόσβασης που στηρίζεται στο ρόλο των χρηστών.

3.2.2 Ασφάλεια στην Αρχιτεκτονική

Εκτός από θέματα ασφάλειας που προκύπτουν από τα δίκτυα αισθητήρων το διαδίκτυο και τις κινητές επικοινωνίες δημιουργούνται και θέματα ασφάλειας που προκύπτουν με την αποθήκευση των δεδομένων. Τα RFID συστήματα έρχονται πρώτα σε επαφή με τις εκάστοτε πληροφορίες και για αυτό το λόγο χρησιμοποιούνται τεχνικές όπως οι ψηφιακές υπογραφές και η κρυπτογράφηση για να επιτευχθεί η εμπιστευτικότητα. Ανασταλτικός παράγοντας που προκύπτει κατά τη μετάδοση δεδομένων είναι η πολυπλοκότητα των δικτύων και των τεχνολογιών. Προκύπτουν πολυπλοκότητες που δυσχεραίνουν την ανάπτυξη εμπιστοσύνης στις επικοινωνίες των IoT κόμβων.

Μια αρχιτεκτονική IoT χωρίζεται σε τρία επίπεδα: Επίπεδο Αντίληψης, Επίπεδο Μεταφοράς και Επίπεδο Εφαρμογών. Για να επιτευχθεί ασφάλεια θα πρέπει να γίνει σαφές το αντικείμενο που κάθε φορά θα πρέπει να διασφαλιστεί ανάλογα με το επίπεδο αρχιτεκτονικής στο οποίο βρίσκεται¹⁰.

3.2.3 Ασφάλεια στο Επίπεδο Αντίληψης

Το επίπεδο αυτό είναι υπεύθυνο για τη συλλογή πληροφοριών και συμπεριλαμβάνονται οι τεχνολογίες RFID και WSN.

- RFID

Η τεχνολογία RFID που χρησιμοποιείται ευρέως βρίσκεται αντιμέτωπη με μια σειρά από προβλήματα:

- Ενιαία Κωδικοποίηση
Εάν δεν υπάρχει ενιαία κωδικοποίηση προκύπτουν ζητήματα ανάγνωσης από τον RFID αναγνώστη.
- Συνωστισμός Δεδομένων
Όταν υπάρχει συνωστισμός δεδομένων δημιουργείται μια σύγχυση κατά τη διαδικασία ανάγνωσης με αποτέλεσμα η μη επίτευξή της. Θα πρέπει να χρησιμοποιούνται τεχνικές κατά των συγκρούσεων (Anti-collision) των δεδομένων που θα τα τοποθετεί σε σειρά.

¹⁰**Stergiou, Christos, και ουν.** Secure Integration of IoT and Cloud Computing. *Future Generation Computer Systems*. Elsevier, 2018, Τόμ. 78, 3.

- Ιδιωτικότητα
Η ανάγκη για χαμηλού κόστους συστημάτων RFID οδήγησε στο περιορισμό των υπολογιστικών τους πόρων. Θα πρέπει να βρεθούν αξιόπιστες λύσεις σε θέματα ιδιωτικότητας που δεν θα απαιτούν μεγάλη επεξεργαστική ισχύ. Μπορεί να είναι φυσικές είτε να στηρίζονται σε κωδικούς.
- Διαχείριση Εμπιστευτικότητας
Εδώ η ψηφιακή υπογραφή μπορεί να αποτελέσει σημαντικό ρόλο στη διασφάλιση της εμπιστευτικότητας των δεδομένων. Εδώ χρησιμοποιούνται αλγόριθμοι και πρωτόκολλα κρυπτογραφίας.

- WSN

Τα δίκτυα αισθητήρων WSN πάσχουν σε θέματα επεξεργαστικών ικανοτήτων, χωρητικότητας και εμβέλειας. Αφού είναι υπεύθυνα για τη συλλογή δεδομένων, αυτά τα δεδομένα μπορεί να είναι εκτεθειμένα σε πιθανές υποκλοπές, αλλοιώσεις περιεχομένου και παράνομη αναδρομολόγηση. Αυτό επηρεάζει σημαντικά ένα IoT σύστημα. Τα προβλήματα που θα πρέπει να αντιμετωπιστούν:

- Αλγόριθμοι Κρυπτογραφίας
Η κρυπτογράφηση μπορεί να δώσει λύση αφού τα ασύρματα δίκτυα αισθητήρων απαιτούν υψηλό επίπεδο ασφαλείας. Βέλτιστη λύση αποτελούν οι συμμετρικοί αλγόριθμοι κρυπτογράφηση αφού σε αντίθεση με τους ασύμμετρους δεν απαιτούν ιδιαίτερους πόρους.
- Διαχείριση Κλειδιών
Όταν αναφερόμαστε σε διαχείριση κλειδιών εννοούμε τη παραγωγή τους, τη διανομή τους, την αποθήκευσή τους, την ανανέωσή τους και την καταστροφή τους. Η διανομή του κλειδιού στους νόμιμους αποδέκτες θα πρέπει να έχει στόχο να μην είναι απαιτητική σε πόρους. Έρευνες σε αυτό το τομέα προσανατολίζονται στην ανάπτυξη αλγορίθμων που θα συνδυάζουν τη φιλοσοφία των συμμετρικών ασύμμετρων κρυπτοσυστημάτων, αξιοποιώντας ταυτόχρονα τα πλεονεκτήματά τους για την ασφαλή διαχείριση κλειδιού.
- Πρωτόκολλα για Ασφαλή Δρομολόγηση
Υπάρχουν περιορισμοί σε ενεργειακά αποθέματα, χωρητικότητα και επεξεργαστική ισχύ που δεν επιτρέπουν την εφαρμογή παραδοσιακών πρωτοκόλλων δρομολόγησης στα ασύρματα δίκτυα. Για να εξασφαλιστεί η αυθεντικότητα και η ακεραιότητα των δεδομένων πρέπει να εξειδικευτούν οι έρευνες σε πρωτόκολλα που μπορούν να εστιάσουν σε θέματα ενεργειακής κατανάλωσης.

- Διαχείριση Εμπιστοσύνης των Κόμβων
Ο μοναδικός τρόπος επικοινωνίας κόμβων και σταθμών βάσης καθιστούν τα συστήματα WSN ευάλωτα σε επιθέσεις. Για αυτό το λόγο θα πρέπει, εκτός από κρυπτογραφικούς αλγόριθμους, να αναπτυχθεί ένα σύστημα διαχείρισης εμπιστοσύνης των κόμβων. Αυτό περιλαμβάνει μηχανισμούς μέτρησης λαθών, τυποποίηση σχέσεων εμπιστοσύνης και τη τακτική ανανέωσή τους.
- Πρόβλημα Ετερογένειας
Σε ένα περιβάλλον IoT υπάρχει μεγάλος όγκος δεδομένων που πρέπει να συλλεχθεί, να επεξεργαστεί και να αποθηκευτεί. Τα δεδομένα αυτά όμως συλλέγονται με διαφορετικούς τρόπους και διαφορετικά πρωτόκολλα. Άρα πρέπει πρώτα να ομογενοποιηθούν τα δεδομένα, οπότε προκύπτουν ζητήματα συμβατότητας.

Ασφάλεια στο Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς περιλαμβάνει τη μετάδοση των πληροφοριών και την αποθήκευσή τους για χρήση σε εφαρμογές ανωτέρου επιπέδου. Βασικό ζήτημα ασφάλειας είναι στο ζήτημα στο επίπεδο του Wi-Fi.

Στα πλαίσια του IoT, οι εφαρμογές Wi-Fi που χρησιμοποιούνται περιλαμβάνουν browsers για τη περιήγηση στο διαδίκτυο και εφαρμογές ανταλλαγής μηνυμάτων ηλεκτρονικού ταχυδρομείου. Η έννοια της ασφάλειας κατέχει σημαντική θέση. Για να αντιμετωπιστούν αυτά τα θέματα ασφαλείας χρησιμοποιούνται έλεγχοι πρόσβασης και μηχανισμοί κρυπτογράφησης του δικτύου. Ο έλεγχος πρόσβασης αφορά ώστε μόνο πιστοποιημένοι χρήστες έχουν πρόσβαση στο διαδίκτυο ενώ η κρυπτογράφηση διασφαλίζει πως μόνο ο αποδέκτης που έχει πρόσβαση στο κλειδί θα έχει και τη δυνατότητα αποκρυπτογράφησης των δεδομένων. Τα πρωτόκολλα WPA/WPA2 χρησιμοποιούνται ως μέθοδοι κωδικοποίησης.

Ασφάλεια στο Επίπεδο Εφαρμογών

Αυτό το επίπεδο υποστηρίζει όλα τα είδη επιχειρηματικών λειτουργιών, κάνει έξυπνους υπολογισμούς, επεξεργάζεται τα εισερχόμενα δεδομένα και συνεισφέρει στη λήψη αποφάσεων. Ταυτόχρονα μπορεί να φιλτράρει και τα κακόβουλα δεδομένα.

Ο όγκος των δεδομένων που θα κληθεί να υποστηρίξει είναι μεγάλος οπότε πρέπει να έχει μεγάλα αποθέματα αποθηκευτικού χώρου και να μπορεί γραμμικά να επεκταθεί η χωρητικότητά του. Το λογισμικό θα πρέπει να διαχειριστεί εισερχόμενα μηνύματα που μπορεί να έχουν ένα χρόνο ζωής.

3.3 Αρχιτεκτονική του IoT

Το 2009 μετά από συζήτηση αρκετών χρόνων σχετικά με τις βασικές έννοιες του IoT, μια ομάδα ερευνητών από περισσότερες από 20 μεγάλες βιομηχανικές εταιρίες και ερευνητικά ιδρύματα ένωσαν τις δυνάμεις τους για να τεθούν τα θεμέλια για μια κοινή αρχιτεκτονική για το Internet of Things, και έτσι δημιουργήθηκε το IoT-Architecture (IoT-A).

Από τεχνική άποψη ήταν σαφές ότι οι υπάρχουσες λύσεις δεν επαρκούσαν για να καλυφθούν οι απαιτήσεις κλιμάκωσης ενός μελλοντικού IoT, τόσο από άποψη της επικοινωνίας μεταξύ των έξυπνων συσκευών και όσο από άποψη διαχείρισης των σύνθετων υπηρεσιών. Επιπλέον το IoT περιλαμβάνει πολλά διαφορετικά μοντέλα διακυβέρνησης τα οποία είναι συχνά ασύμβατα. Αυτό οδηγεί σε μια κατάσταση όπου η προστασία της ιδιωτικής ζωής και της ασφάλειας αντιμετωπίζονται ανά περίπτωση και ανά νομοθεσία, κατασκευάζοντας λύσεις στα υπάρχοντα σχέδια κάτι το οποίο παρεμποδίζει τη δυνατότητα μεταφοράς, τη διαλειτουργικότητα και την ανάπτυξη. Έγινε σαφές ότι σε αυτόν τον τομέα υπάρχει ανάγκη για κοινό έδαφος.

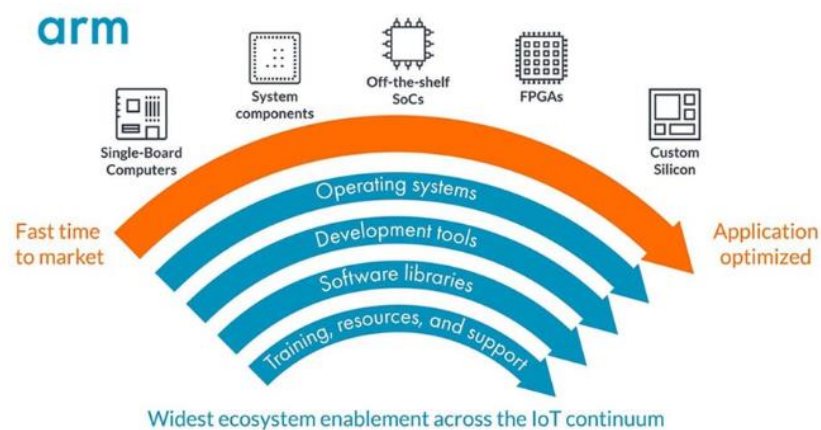
Η κεντρική απόφαση του έργου IoT-A ήταν να στηρίξει το έργο της σχετικά με τη τρέχουσα κατάσταση, αντί να εφαρμοστεί μια καθαρή προσέγγιση. Αυτό είχε σαν αποτέλεσμα να σχηματιστεί το Αρχιτεκτονικό Μοντέλο Αναφοράς (ARM). Δεν είναι δυνατόν πλέον να δημιουργηθούν αρχιτεκτονικές μόνο μέσω ενός εργαστηρίου χωρίς την επαφή με τον πραγματικό κόσμο. Το IoT-A αναγνώρισε αυτή τη πραγματικότητα και με τη βοήθεια των τελικών χρηστών νέες απαιτήσεις έχουν συλλεχθεί και εισαχθεί στην κύρια διαδικασία του νέου μοντέλου αρχιτεκτονικής.

3.2 Το Μοντέλο ARM

Το μοντέλο IoT-A ARM αποτελείται από τέσσερα βασικά μέρη:

1. Το όραμα, το οποίο συνοψίζει το σκεπτικό για τη δημιουργία ενός αρχιτεκτονικού μοντέλου αναφοράς για το IoT. Εξετάζει το πώς μπορεί να χρησιμοποιηθεί το αρχιτεκτονικό πρότυπο αναφοράς, την μεθοδολογία που εφαρμόζεται στη μοντελοποίηση της αρχιτεκτονικής, τα επιχειρηματικά σενάρια και την ομάδα που αποτελείται από τα ενδιαφερόμενα μέλη.
2. Τα επιχειρηματικά σενάρια, που ορίζονται ως απαιτήσεις από τα ενδιαφερόμενα μέρη και είναι οι οδηγοί του έργου της αρχιτεκτονικής. Ένα συγκεκριμένο παράδειγμα της αρχιτεκτονικής αναφοράς μπορεί να επικυρωθεί μέσα από επιλεγμένα επιχειρηματικά σενάρια. Η ανάλυση των απαιτήσεων και των ανησυχιών των ενδιαφερόμενων μερών συμβάλλει στη κατανόηση των πτυχών του αρχιτεκτονικού μοντέλου αναφοράς.
3. Το IoT Μοντέλο Αναφοράς (Reference Model), το οποίο παρέχει το υψηλότερο επίπεδο αφαίρεσης για τον ορισμό του IoT-A Αρχιτεκτονικού

μοντέλου αναφοράς. Παράγει τη κοινή κατανόηση του τομέα IoT. Περιλαμβάνει μια γενική συζήτηση σχετικά με τον τομέα IoT, ένα IoT Μοντέλο Τομέα (IoT Domain model) ως περιγραφή υψηλού επιπέδου, ένα IoT Μοντέλο Πληροφοριών (IoT Information Model) που εξηγεί πως πρόκειται να διαμορφωθούν πληροφορίες του IoT και ένα IoT Μοντέλο Επικοινωνίας (IoT Communication Model) ώστε να γίνουν κατανοητές οι λεπτομέρειες που αφορούν την επικοινωνία μεταξύ πολλών ετερογενών IoT συσκευών.



Εικόνα 10: ARM model¹¹

4. Η IoT Αρχιτεκτονική Αναφοράς(IoT Reference Architecture) , αποτελεί ένα σημείο αναφοράς για τη δημιουργία συμβατών αρχιτεκτονικών IoT. Παρέχει απόψεις και προοπτικές για διαφορετικές αρχιτεκτονικές πτυχές του IoT. Η δημιουργία της Αρχιτεκτονικής Αναφοράς επικεντρώνεται σε αφηρημένα σύνολα των μηχανισμών και όχι σε αρχιτεκτονικές εφαρμογών. Όσο αφορά τους οργανισμούς αποτελεί σημαντική πτυχή για τη συμμόρφωση των τεχνολογιών τους με τα διεθνή πρότυπα έτσι ώστε να διασφαλίζεται η διαλειτουργικότητα μεταξύ των οργανισμών. Έτσι κάθε ενδιαφερόμενος μπορεί να δημιουργήσει νέες επιχειρήσεις που θα λειτουργούν σε συνεργασία με τις ήδη υπάρχουσες¹¹.

¹¹Bassi, Alessandro, και ου. *Enabling Things o Talk: Designing IOT solutions with the IOT Architectural Reference Model*. New York : Springer, 2013.

3.3 Οφέλη του Μοντέλου ARM

Η χρήση του μοντέλου IoT-A ARM έχει πολλά πλεονεκτήματα τα οποία σημαντικότερα παρατίθενται παρακάτω:

1. Γνωστική Ενίσχυση

Κατά τη διάρκεια ανάπτυξης προϊόντος η αναφορά σε κάποιο αρχιτεκτονικό μοντέλο έχει τετραπλή σημασία. Πρώτον με τη χρήση του μοντέλου όσοι εμπλέκονται στην ανάπτυξη μπορούν να συνεννοούνται αφού υπάρχει κοινή γλώσσα επικοινωνίας.

Δεύτερον, η υψηλού επιπέδου άποψη ενός τέτοιου μοντέλου έχει εκπαιδευτική αξία από τη στιγμή που παρέχει ένα περίγραμμα αλλά και συνολική εικόνα του τομέα, οπότε όποιος θα θελήσει να ασχοληθεί με αυτό το πεδίο θα μπορεί να βοηθηθεί στη κατανόηση των ιδιαιτεροτήτων και πολυπλοκοτήτων του IoT

Τρίτον το μοντέλο αναφοράς θα μπορεί να βοηθήσει τους επικεφαλής ενός IoT project να οργανώσουν τις εργασίες αλλά και τις ομάδες που θα συμμετέχουν στο έργο.

Τέταρτον το μοντέλο αναφοράς έχει ως στόχο την αναγνώριση των ανεξαρτήτων κομματιών ενός IoT συστήματος, το οποίο θα μπορεί να παρέχει σημαντικές πληροφορίες όσο αφορά τα συστατικά του συστήματος, την αρχιτεκτονική κ.α.

2. Μοντέλο Αναφοράς σαν κοινή βάση

Για να είναι αποτελεσματική η καθιέρωση μιας κοινής βάσης θα πρέπει να περιλαμβάνει τον ορισμό των IoT οντοτήτων και να περιγράφει την αλληλεπίδραση και τις σχέσεις μεταξύ αυτών. Το αρχιτεκτονικό μοντέλο αναφοράς παρέχει αυτή τη κοινή βάση για το πεδίο IoT. Οποιαδήποτε ομάδα στοχεύει στο να αναπτύξει ένα IoT συμβατό σύστημα με το IoT-A θα πρέπει να ακολουθεί κανόνες που ορίζονται από το μοντέλο αναφοράς.

3. Δημιουργία Αρχιτεκτονικών

Επιπλέον πλεονέκτημα στην χρήση του IoT-A ARM αποτελεί η δημιουργία παρόμοιων αρχιτεκτονικών για εξειδικευμένα συστήματα. Αυτό επιτυγχάνεται με τη δυνατότητα υποστήριξης εργαλείων, το οποίο έχει σαν πλεονέκτημα την αυτοματοποίηση της διαδικασίας αλλά και το γεγονός ότι αυτή η αρχιτεκτονική θα παρέχει διαλειτουργικότητα στα συμπληρωματικά IoT συστήματα.

4. Εντοπισμός Διαφορών

Χρησιμοποιώντας κανείς τα εργαλεία που προαναφερθήκανε, οι τυχόν διαφορές στις παραγόμενες αρχιτεκτονικές αποδίδονται στις ιδιαιτερότητες κάθε περίπτωσης. Με την εφαρμογή του IoT-A ARM, είναι διαθέσιμες οι προβλέψεις της πολυπλοκότητας του συστήματος. Αυτό καθιστά την αξιολόγηση του συνολικού έργου ευκολότερη. Επιπλέον το IoT-A ARM καθορίζει μια σειρά από τακτικές και σχεδιάζει επιλογές για την ικανοποίηση των ποιοτικών απαιτήσεων του συστήματος. Με αυτό τον τρόπο μπορεί να χρησιμοποιηθεί για να προβλεφθεί αν δυο παραγόμενες αρχιτεκτονικές θα διαφέρουν και αν ναι σε ποια σημεία.

5. Συγκριτική Αξιολόγηση

Εξίσου σημαντικό πλεονέκτημα. Ενώ το μοντέλο αναφοράς καθορίζει τη γλώσσα που θα χρησιμοποιηθεί στο σύστημα, η αρχιτεκτονική αναφοράς δηλώνει τις ελάχιστες λειτουργικές απαιτήσεις για αυτό το σύστημα. Με την τυποποίηση της περιγραφής και της παραγγελίας και της οριοθέτησης των στοιχείων που αποτελούν το σύστημα παρέχει ένα υψηλό επίπεδο διαφάνειας και συγκρισιμότητας στη διαδικασία της συγκριτικής αξιολόγησης.

3.4 Διαδικασία Ανάπτυξης του Μοντέλου ARM

Η διαδικασία ανάπτυξης του ARM αποτελείται από μια κύρια διαδικασία, την παραγωγή της, και εντός αυτής της παραγωγής οι δυο βασικές ενέργειες είναι η μοντελοποίηση τομέα το οποίο έχει σαν αποτέλεσμα το Μοντέλο Αναφοράς και η λειτουργική μοντελοποίηση, η οποία αποτελεί τον κύριο συντελεστή στην Αρχιτεκτονική Αναφοράς. Η τελευταία διαδικασία λαμβάνει πληροφορίες από τη διαδικασία συλλογής απαιτήσεων, η οποία με τη σειρά της λαμβάνει πληροφορίες από τα ενδιαφερόμενα μέρη και τις έρευνες που διενέργησαν κατά τα πρώτα στάδια του IoT-A.

Το προσχέδιο της διαδικασίας ARM αξιολογείται από τα ενδιαφερόμενα μέρη του έργου, τις δραστηριότητες επίδειξης, καθώς και τα τεχνικά πακέτα εργασίας. Η αξιολόγηση χρησιμεύει ως πρώτη ύλη για την αναθεώρηση της ARM. Πέρα από αυτό παρέχεται στο χρήστη της ARM πρακτικές για την εφαρμογή ειδικών αρχιτεκτονικών, που είναι προς το όφελος του χρήστη και επιπλέον παρέχει δευτερεύον όφελος για τη παροχή πολύτιμων πληροφοριών για την ίδια παραγωγή του ARM. Ακολουθώντας τις κατευθυντήριες γραμμές για τη μετατροπή του ARM σε μια συγκεκριμένη αρχιτεκτονική, αποκαλύπτονται τα πιθανά κενά.

Επιπλέον η εφαρμογή βέλτιστων πρακτικών εμβαθύνει στην κατανόησή μας για τον τομέα IoT και παρέχει καθοδήγηση σχετικά με το ποιες πτυχές του χρειάζονται ενίσχυση.

Το IoT μοντέλο ακολουθεί σπειροειδή σχεδιασμό, το οποίο είναι συνυφασμένο με την αναπτυξιακή διαδικασία του ARM . Επιλέχθηκε πρώτον επειδή κάθε νέα επανάληψη της διαδικασίας αυξάνει τη σταθερότητα της ARM και δεύτερον λόγω των πολλαπλών βημάτων η διάδοση της ARM ξεκινά πολύ νωρίς μέσα στο project. Τρίτον αυτή η προσέγγιση συντονίζει την αλληλεπίδραση της δραστηριότητας της αρχιτεκτονικής μέσα στο IoT-A με εκείνη των άλλων δραστηριοτήτων, η οποία αναμένεται να ενισχύσει την αποτελεσματικότητα της εν λόγω ανταλλαγής.

ΚΕΦΑΛΑΙΟ 4 - ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΙοΤ

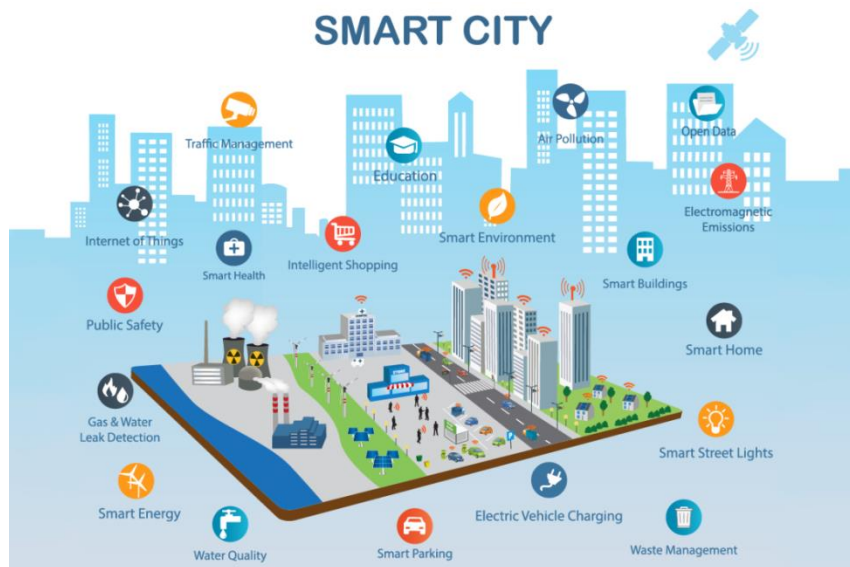
Σε αυτό το κεφάλαιο παρουσιάζονται διάφορες εφαρμογές του ΙοΤ, οι οποίες είναι σημαντικές και αναγνωρισμένες. Οι εφαρμογές του ΙοΤ απευθύνονται στις ανάγκες τις κοινωνίας και τις εξελίξεις σε ευρείας εφαρμογής τεχνολογίας και σε αυτό το κεφάλαιο γίνεται αναφορά στα βασικά πεδία εφαρμογής του όπως το σπίτι, πόλη, μεταφορά, βιομηχανία, αγροτική και λιανική επιχείρηση. Αναφέρονται σε εφαρμογές που έχουν επιλεχθεί από την IERC (European Research Cluster on The Internet of Things).

4.1 Έξυπνη Πόλη

Μια έξυπνη πόλη ορίζεται ως μια πόλη που παρακολουθεί, ελέγχει και προσπαθεί να προσαρμόσει υποδομές, συμπεριλαμβανομένων των δρόμων, γέφυρες, σήραγγες, σιδηροδρομικές/υπόγειες διαβάσεις, αεροδρόμια, λιμάνια, επικοινωνίες, νερό, ενέργεια ακόμα και μεγάλα κτίρια μπορεί να βελτιστοποιήσει καλύτερα τους πόρους της, να προγραμματίσει δραστηριότητες προληπτικής συντήρησής της και να παρακολουθεί τις πτυχές της ασφάλειας μεγιστοποιώντας παράλληλα τις υπηρεσίες προς τους πολίτες της. Χρησιμοποιώντας αισθητήρες και συστήματα παρακολούθησης μπορούμε να συλλέξουμε δεδομένα και με τα δεδομένα αυτά να γίνεται αξιολόγηση. Με αυτό τον τρόπο βελτιώνεται και ενισχύεται η οργάνωση και διαχείριση μιας πόλης.

Στο μέλλον οι έξυπνες πόλεις θα διαθέτουν συστήματα και υποδομές με τα οποία θα μπορούν να παρακολουθούν τις δικές τους καταστάσεις και θα πραγματοποιούν αυτό-επισκευές. Θα μπορεί να βελτιωθεί το φυσικό περιβάλλον, όπως ο αέρας, το νερό και οι πράσινες περιοχές αφού θα παρακολουθούνται με τέτοιο τρόπο ώστε να δημιουργείται μια ενισχυμένη διαβίωση και ένα περιβάλλον που θα είναι καθαρό, αποτελεσματικό και ασφαλές¹²

¹²Hammi, Badis, και ουν. Internet of Things (IoT) Technologies for Smart Cities. *IET Journals*. 2015.



Εικόνα 11: Smart City²²

Βασικές τεχνολογίες όπως έξυπνη μέτρηση, ασύρματα δίκτυα αισθητήρων, ανοιχτές πλατφόρμες, ευρυζωνικές υπηρεσίες υψηλής ταχύτητας και το cloud computing αποτελούν βασικά δομικά στοιχεία της υποδομής μιας έξυπνης πόλης. Υπάρχει Ευρωπαϊκό σχέδιο που έχει δημιουργηθεί για τις έξυπνες πόλεις (European Smart City Project) που στηρίζεται στα παρακάτω έξι χαρακτηριστικά:

- Έξυπνη Διακυβέρνηση: Αφορά τη χρήση τεχνολογίας για τη διευκόλυνση και το καλύτερο σχεδιασμό στη διαδικασία λήψης κυβερνητικών αποφάσεων. Οι τεχνολογίες σε επίπεδο υλικού, λογισμικού και υποδομής θα είναι αυτές που θα παράγουν την απαιτούμενη διαλειτουργικότητα και θα τροφοδοτήσουν με τα απαραίτητα δεδομένα τους αρμόδιους φορείς. Οι κυβερνήσεις θα μπορούν να παρέχουν την απαιτούμενη διαφάνεια στους πολίτες καθώς θα κοινοποιούνται οι διαδικασίες λήψης αποφάσεων προάγοντας έτσι δημοκρατικές διαδικασίες. Προς αυτή τη κατεύθυνση συμβάλλουν σημαντικά οι πλατφόρμες κοινωνικής δικτύωσης αλλά και οι πλατφόρμες ηλεκτρονικής διακυβέρνησης.
- Έξυπνη Κινητικότητα: Οι σύγχρονες πόλεις στηρίζονται σε συστήματα μετακίνησης αγαθών και ανθρώπων που δεν είναι βιώσιμο. Έρευνες και αναλύσεις αναδεικνύουν την ανάγκη αναθεώρησης του τρόπου με τον οποίο μετακινούνται οι πολίτες σε μια πόλη. Ο όρος έξυπνη κινητικότητα αναφέρεται στα ολοκληρωμένα συστήματα μεταφορών και εφοδιαστικών αλυσίδων που στηρίζονται σε τεχνολογίες ICT (Information and Communications Technology). Πιο συγκεκριμένα ένα βιώσιμο, ασφαλές και διασυνδεδεμένο σύστημα μέσω μαζικής μεταφοράς το οποίο θα περιλαμβάνει: Λεωφορεία, Τραμ, Μετρό, Τρένα, Ποδήλατα και Αυτοκίνητα.

- Έξυπνη Οικονομία: Αφορά κυρίως το ηλεκτρονικό εμπόριο και το ηλεκτρονικό επιχειρείν. Οι ανάπτυξη που παρέχουν τα ηλεκτρονικά μέσα στις αγοροπωλησίες αγαθών προωθεί την οικονομική ευρωστία σε αστικό επίπεδο.
- Έξυπνο Περιβάλλον: Αναφέρεται στα πλέγματα ενέργειας (Energy Grids) στηριζόμενα σε δομές ICT, στον έλεγχο της προκαλούμενης μόλυνσης αλλά και στην ανοικοδόμηση και ανακαίνιση των κτιρίων δίνοντας έμφαση στην μείωση του ενεργειακού αποτυπώματος. Αστικές υπηρεσίες όπως ο φωτισμός των δρόμων, τα αποχετευτικά συστήματα, η διαχείριση των αποβλήτων αποτελούν τομείς που έχουν ανάγκη υλοποίησης εφαρμογών IoT.
- Έξυπνοι Άνθρωποι-Έξυπνη Ζωή: Σε ένα IoT περιβάλλον θα δίνεται δυνατότητα στους κατοίκους μιας πόλης να έχουν πρόσβαση στο κοινωνικό και πολιτικό γίνεσθαι.

Για να μπορούν να εφαρμοστούν τα παραπάνω θα πρέπει να ληφθούν υπόψη κάποιες ερευνητικές προκλήσεις. Μερικές από αυτές αναφέρονται παρακάτω:

- Ένα από τα σημαντικότερα εμπόδια αποτελεί το γεγονός ότι σε μια πόλη η κάθε δημόσια υπηρεσία είναι υπεύθυνη για τη δική της περιοχή. Αυτή η παραδοσιακή οργάνωση θα πρέπει να ξεχαστεί για τις ανάγκες δημιουργίας μιας έξυπνης πόλης.
- Θα πρέπει να δημιουργηθούν αλγόριθμοι και συστήματα για να περιγραφούν οι πληροφορίες που δημιουργούνται από τους αισθητήρες σε διαφορετικές εφαρμογές, επιτρέποντας ταυτόχρονα την ανταλλαγή πληροφοριών μεταξύ των διάφορων υπηρεσιών της πόλης.
- Μηχανισμοί για την αποδοτικότητα του κόστους ανάπτυξης και συντήρησης των έργων αυτών.
- Εξασφάλιση αξιόπιστων μετρήσεων από τους αισθητήρες και σωστή βαθμονόμηση των αισθητήρων αυτών.
- Αλγόριθμοι και πρωτόκολλα χαμηλής ενέργειας.
- Αλγόριθμοι για ανάλυση και επεξεργασία των δεδομένων που θα αποκτηθούν από τη πόλη.
- Εγκατάσταση και ενσωμάτωση του IoT σε μεγάλη κλίμακα.

4.2 Έξυπνη Ενέργεια

Εξαιτίας της όλο και αυξανόμενης ανάγκης για αλλαγή πολιτικής στην κατανάλωση ενέργειας θα πρέπει να αναπτυχθούν ευέλικτα ηλεκτρικά δίκτυα τα οποία θα βασίζονται σε ανανεώσιμες πηγές ενέργειας.

Οι λειτουργίες των δικτύων αυτών θα πρέπει να βασίζονται σε έξυπνες συσκευές και σε στοιχεία υποδομής τα οποία θα βασίζονται σε μεγάλο βαθμό σε IoT, και συγκεκριμένα σε ηλεκτρονικό πλέγμα ενέργειας (grid). Θα πρέπει αυτό το ενεργειακό πλέγμα να ελέγχει ηλεκτρονικά: την παραγωγή, την αποθήκευση αλλά και τη διανομή της ενέργειας αυτής. Τα μελλοντικά δίκτυα ενέργειας θα πρέπει να αποτελούνται από ενεργειακές πηγές μικρής και μεσαίας απόδοσης που θα μπορούν να συνδυαστούν με μονάδες ηλεκτρικής ενέργειας. Τέτοιες πηγές ενέργειας θα είναι τα φωτοβολταϊκά, τα ορυκτά καύσιμα, οι ανεμογεννήτριες κ.τ.λ. .

Μεγάλη πρόκληση αποτελεί ο σχεδιασμός και η ανάπτυξη της υποδομής ενεργειακών συστημάτων τα οποία θα είναι σε θέση να στηρίζεται στις ανάγκες των χρηστών μέσω επικοινωνίας διπλής κατεύθυνσης ώστε η προσφορά να σχετίζεται με τη ζήτηση. Απαιτούνται αισθητήρες που θα μπορούν να καταγράφουν τις ανάγκες σε πραγματικό χρόνο ώστε οι καταναλωτές να μπορούν να διαχειρίζονται τα ενεργειακά αποθέματα. Παραδείγματος χάρη τα κλιματιστικά με τη βοήθεια του ενεργειακού πλέγματος θα μπορεί να ρυθμίσει την κατάλληλη θερμοκρασία. Ηλεκτρικές συσκευές θα μπορούν να λειτουργούν βραδινές ώρες για χαμηλότερη κατανάλωση ενέργειας.

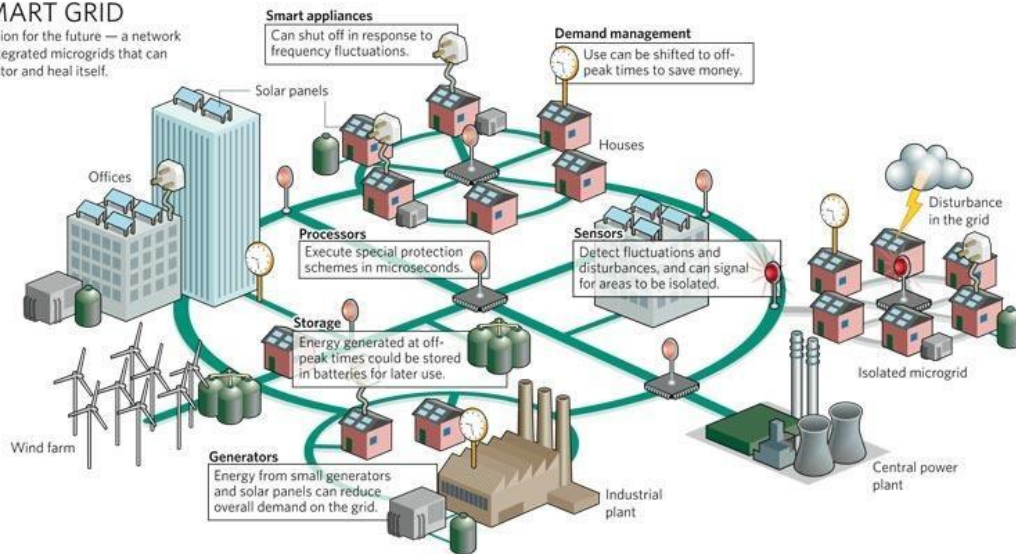
Θέμα το οποίο θα πρέπει να ληφθεί υπόψη θα είναι και τα δίκτυα μετάδοσης της πληροφορίας ώστε να παρέχει ασφάλεια. Το έξυπνο πλέγμα θα μπορεί να λειτουργεί σαν ένα άλλο Διαδίκτυο όπου τα πακέτα ενέργειας θα λειτουργούν σαν πακέτα δεδομένων. Με τη βοήθεια των αισθητήρων θα μπορεί να βρεθεί η βέλτιστη διαδρομή αυτών των πακέτων ώστε να μην βάλει σε κίνδυνο την ακεραιότητά τους.

Με αυτό τον τρόπο εισάγεται μια καινούργια έννοια στο χώρο της ενέργειας: Internet of Energy. Το Διαδίκτυο της ενέργειας ορίζεται ως μια δικτυακή υποδομή, που στηρίζεται σε διαλειτουργικούς δέκτες, αναμεταδότες και πρωτόκολλα επικοινωνίας, τα οποία θα επιτρέπουν την ισορροπία μεταξύ παγκόσμιων ενεργειακών απαιτήσεων και την κατά τόπους παραγωγή και αποθήκευση αυτής σε πραγματικό χρόνο¹³.

¹³Vermesan, Ovidiu και Friess, Peter. Internet of Things Applications. *AIOTI WGOI-IERC*. 2015.

SMART GRID

A vision for the future — a network of integrated microgrids that can monitor and heal itself.



Εικόνα 12: Smart Grid²³

Το Internet of Energy (IoE) παρέχει μια καινοτόμο ιδέα για τη διανομή ενέργειας, την αποθήκευση, την παρακολούθηση του δικτύου και την επικοινωνία. Θα επιτρέπει μονάδες ενέργειας να μεταφερθούν, όταν και όπου θα είναι αναγκαίο. Η παρακολούθηση της κατανάλωσης ενέργειας θα μπορεί πραγματοποιηθεί σε όλα τα επίπεδα από τις τοπικές συσκευές μέχρι εθνικό και διεθνές επίπεδο. Οι έξυπνοι μετρητές (smart meters) θα μπορούν να παρέχουν πληροφορίες στον χρήστη σχετικά με τη στιγμιαία κατανάλωση ενέργειας, δίνοντας δυνατότητα εξάλειψης συσκευών που καταναλώνουν μεγάλο ποσό ενέργειας. Επιπλέον θα μπορεί να δώσει συμβουλές για τη βελτιστοποίηση της ατομικής κατανάλωσης ενέργειας. Η σύνδεση με τους έξυπνους μετρητές θα βασίζεται σε WSN δίκτυα αισθητήρων.

Μακροπρόθεσμα η ηλεκτροκίνηση θα γίνει ένα σημαντικό στοιχείο των έξυπνων δικτύων ηλεκτρικής ενέργειας. Τα ηλεκτρικά οχήματα θα λειτουργούν ως φορτία ενέργειας και ταυτόχρονα ως κινητές αποθήκες ενέργειας συνδεδεμένα με σε IoT στοιχεία. Τα οχήματα αυτά θα είναι σε θέση να ενεργούν ως πηγές ενέργειας αναλόγως με τη κατάσταση φόρτισης, το χρονοδιάγραμμα χρήσης τους και της τιμής της ενέργειας η οποία θα εξαρτάται από την αφθονία της ενέργειας στο δίκτυο.

Για να επιτευχθούν όμως όλα τα παραπάνω που έχουν αναφερθεί θα πρέπει να ξεπεραστούν κάποια εμπόδια. Παρακάτω παρατίθενται κάποιες ερευνητικές προκλήσεις:

- Απόλυτα ασφαλή επικοινωνία μεταξύ στοιχείων δικτύου.
- Αντιμετώπιση επεκτασιμότητας και των προτύπων διαλειτουργίας
- Εξοικονόμηση ενέργειας και αξιόπιστοι αισθητήρες/ενεργοποιητές.
- Τεχνολογίες που εξασφαλίζουν ανωνυμία δεδομένων για ασφάλεια ιδιωτικότητας.
- Αποφυγή υπερφόρτισης του δικτύου επικοινωνίας λόγω μαζικής χρήσης.

- Μοντέλα και μεθόδους σχεδιασμού που προσφέρουν αξιόπιστη σύνδεση ετερογενών συστημάτων.
- Συστήματα που υποστηρίζουν την αυτό-ίαση και τον περιορισμό των ζημιών καθώς και ανάπτυξη στρατηγικών για τη διαχείριση της αποτυχίας.
- Τα δίκτυα της ηλεκτρικής ενέργειας θα πρέπει να είναι σε θέση να αντιδράσουν σωστά και γρήγορα σε αυξομειώσεις στην παροχή ηλεκτρικής ενέργειας από ανανεώσιμες πηγές ενέργειας.

4.3 Έξυπνη Μεταφορά

Η σύνδεση των οχημάτων με το Internet δημιουργεί ένα πλήθος νέων δυνατοτήτων και εφαρμογών κάνοντας τη μεταφορά ευκολότερη και ασφαλέστερη. Συνδέεται η έννοια του Δικτύου Οχημάτων (Internet of Vehicles) με την έννοια του Διαδικτύου Ενέργειας (Internet of Energy) οι οποίες αποτελούν τις μελλοντικές τάσεις για έξυπνες μεταφορές και κινητικότητα.



Εικόνα 13: Internet of Vehicles²⁴

Παρακάτω παρατίθενται κάποια σενάρια εφαρμογής του IoT στο πλαίσιο της αυτοκινητοβιομηχανίας:

- Θα πρέπει να δημιουργηθούν συστήματα για τη φόρτιση των ηλεκτρονικών συστημάτων και θα πρέπει να οριστεί εάν αυτή η φόρτιση θα ελέγχεται από ένα σύστημα εντός του οχήματος ή όχι.
- Ευέλικτη τιμολόγηση της ηλεκτρικής ενέργειας.
- Θα πρέπει το IoT να αποτελεί αναπόσπαστο μέρος του ελέγχου και της διαχείρισης του οχήματος. Ήδη σήμερα ορισμένες λειτουργίες των συστημάτων πλοήγησης παρακολουθούνται σε απευθείας σύνδεση με ένα κέντρο εξυπηρέτησης επιτρέποντας να καταστεί δυνατή η προληπτική

συντήρηση του οχήματος, η απομακρυσμένη διάγνωση, η υποστήριξη και έγκυρη διαθεσιμότητα ανταλλακτικών. Για αυτό το σκοπό τα δεδομένα από τους αισθητήρες συλλέγονται από μια έξυπνη μονάδα και στέλνονται μέσω διαδικτύου στο κέντρο εξυπηρέτησης.

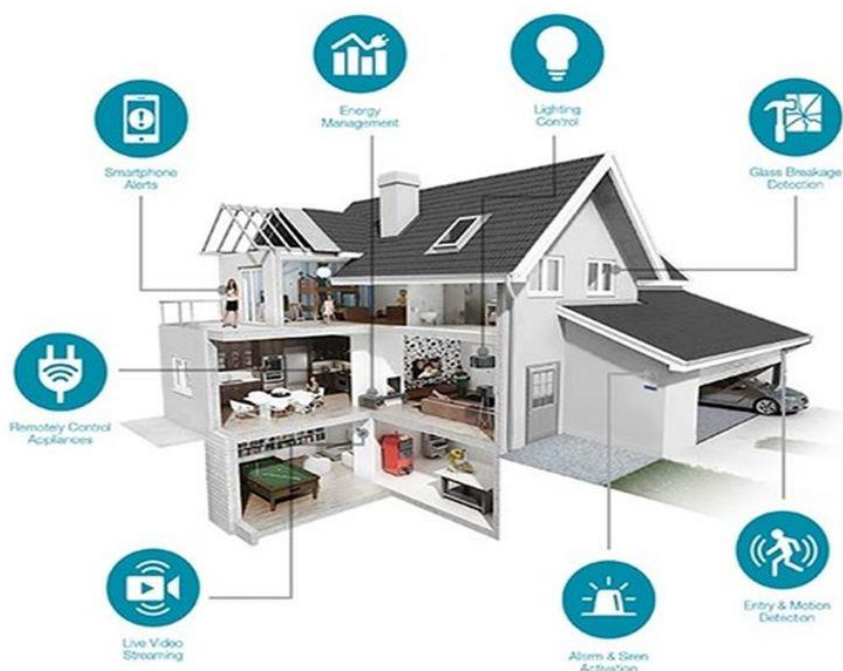
- Το IoT βοηθά σημαντικά στη βελτίωση του προβλήματος κυκλοφορίας. Τα αυτοκίνητα θα πρέπει να είναι σε θέση να οργανωθούν προκειμένου να αποφευχθεί η κυκλοφοριακή συμφόρηση. Αυτό θα μπορεί να γίνει σε συνεργασία με την υποδομή του ελέγχου της κυκλοφορίας και του συστήματος διαχείρισης έξυπνης πόλης. Επίσης για τη μείωση του αριθμού τροχαίων ατυχημάτων θα πρέπει να υπάρχει επικοινωνία μεταξύ των οχημάτων και των υποδομών ώστε να αναπτυχθούν οι καλύτεροι μηχανισμοί οδικής βοήθειας.
- Δημιουργούνται νέα σενάρια μεταφορών, δηλαδή οι αυτοκινητοβιομηχανίες πια θα παίζουν ρόλο ως πάροχοι κινητικότητας και όχι αποκλειστικά σαν κατασκευαστές.
- Αυτόνομη διασύνδεση και οδήγηση με τις υποδομές μια έξυπνης πόλης. Τα αυτόνομα αυτοκίνητα βρίσκονται ακόμα σε πρόωρη φάση αλλά θα πρέπει εξειδικευμένες τεχνολογίες να βοηθούν τα οχήματα να κατανοήσουν το περιβάλλον γύρω τους.

Τα παραπάνω σενάρια δεν είναι ανεξάρτητα το ένα από το άλλο αλλά αντιθέτως συνδυάζονται και δείχνουν το πλήρες δυναμικό τους. Τα έξυπνα συστήματα θα πρέπει να συλλέγουν πληροφορίες από το χρήστη, προορισμό και χρονοδιάγραμμα, κατάσταση οχήματος, θέση χρήση ενέργειας αλλά ταυτόχρονα να αλληλεπιδρά με εξωτερικά συστήματα. Το Internet of Vehicles (IoV) θα βασίζεται σε έξυπνους αισθητήρες που θα βρίσκονται σε οδικές υποδομές και στις υποδομές ελέγχου της κυκλοφορίας και θα μπορούν να συλλέγουν πληροφορίες σχετικά με το δρόμο, τη κατάσταση της κυκλοφορίας, της καιρικές συνθήκες κ.α. Για αυτό το λόγο οι αισθητήρες θα πρέπει να είναι σε θέση να αποδώσουν αξιόπιστες πληροφορίες. Επιπλέον θα πρέπει να αντιμετωπιστούν και τα προβλήματα που θα προκύψουν από το μεγάλο ποσό δεδομένων που θα συλλεχθεί και να βελτιστοποιηθούν οι μηχανισμοί οργάνωσης αυτών των πληροφοριών.

4.4 Έξυπνο Σπίτι-Κτίριο

Η άνοδος του ρόλου του Wi-Fi στην οικία έχει προκύψει εξαιτίας της δικτυωμένης φύσης των όλο και αναπτυσσόμενων οικιακών ηλεκτρικών ειδών, όπου ηλεκτρικές συσκευές έχουν αρχίσει και γίνονται μέρος του IP δικτύου στο σπίτι. Πολλοί οργανισμό στοχεύουν στο να εξοπλίσουν τα σπίτια με τεχνολογία που επιτρέπει στους καταναλωτές να χρησιμοποιούν μια μόνο συσκευή και να ελέγχουν με αυτήν τις υπόλοιπες. Η λύση σε αυτά τα προβλήματα βρίσκεται στην περιβαλλοντική παρακολούθηση, την διαχείριση ενέργειας, την υποβοηθούμενη διαβίωση, την

άνεση και την ευκολία. Βασίζονται σε ανοιχτές πλατφόρμες και χρησιμοποιείται ένα δίκτυο έξυπνων αισθητήρων για τη παροχή πληροφοριών σχετικά με την ενεργειακή κατάσταση του σπιτιού. Αυτοί οι αισθητήρες παρακολουθούν συστήματα όπως η παραγωγή ενέργειας και μέτρηση της θέρμανσης, ο εξαερισμός και ο κλιματισμός, ο φωτισμός και η ασφάλεια. Οι πληροφορίες που συλλέγονται επεξεργάζονται και διατίθενται μέσα από μια σειρά συσκευών, που θα έχουν πρόσβαση οι καταναλωτές, όπως οθόνες αφής και κινητά τηλέφωνα. Οι υπηρεσίες δικτύωσης παρέχουν απευθείας σύνδεση υπηρεσίας streaming ή αναπαραγωγής του δικτύου ενώ ταυτόχρονα ελέγχεται και η λειτουργικότητά του.



Εικόνα 14: Smart Home 25

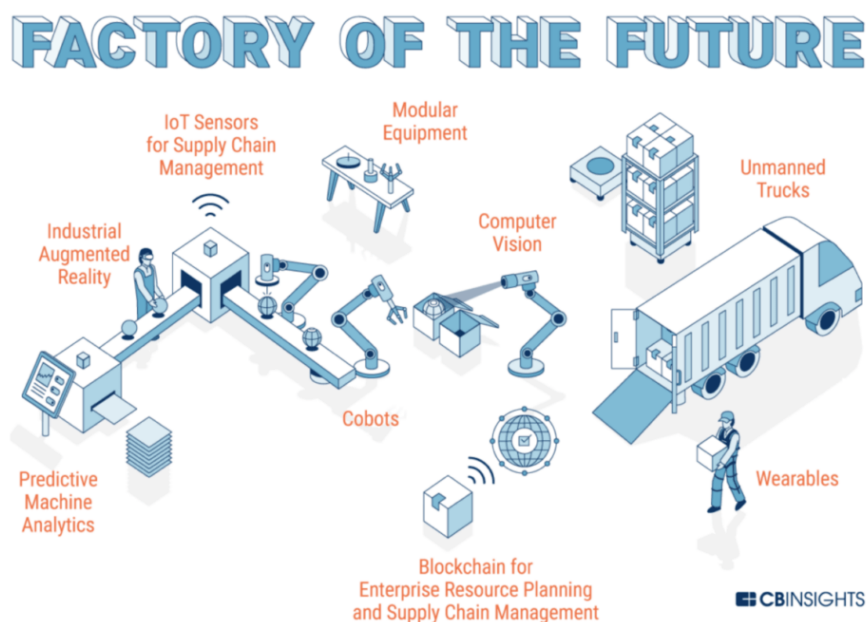
Υπάρχουν και πολλές εταιρίες που εξετάζουν το ενδεχόμενο να δημιουργηθούν πλατφόρμες που θα ενσωματώνουν την αυτοματοποίηση κτιρίων με την ψυχαγωγία, την παρακολούθηση της υγείας, την παρακολούθηση της κατανάλωσης ενέργειας και γενικότερα να επιτυγχάνεται η επίβλεψη των κτιρίων μέσω ασύρματων αισθητήρων. Οι συσκευές θα χρησιμοποιούν αισθητήρες για τη συλλογή πληροφοριών σχετικά με τις συνθήκες λειτουργίας. Επιπρόσθετα θα χρησιμοποιείται σύστημα cloud όπου θα αποθηκεύονται και θα αναλύονται δεδομένα που διαφέρουν. Με αυτό τον τρόπο ο καταναλωτής θα μπορεί να παίζει μεγαλύτερο ρόλο στη διαχείριση του σπιτιού του.

Η αξιοποίηση της τεχνολογίας αισθητήρων δικτύου θα διευκολύνουν την έξυπνη διαχείριση της ενέργειας στα κτίρια αυξάνοντας ταυτόχρονα και τις ανέσεις του καταναλωτή, μειώνοντας την ενεργειακή ζήτηση. Τα πλεονεκτήματα θα σημειώνονται και στο τομέα του περιβάλλοντος αλλά ταυτόχρονα θα

παρατηρηθούν και οικονομικά οφέλη από την εισαγωγή της εν λόγω έξυπνης διαχείρισης μέσα στο σπίτι. Θα επιτευχθούν και άλλα θετικά αποτελέσματα όπως η απλοποίηση του ελέγχου του κτιρίου, η τοποθέτηση παρακολούθησης, η παροχή πληροφοριών για τον εξοπλισμό και τον έλεγχο του κτιρίου. Επιπλέον η χρήση του Internet σε συνδυασμό με συστήματα διαχείρισης ενέργειας παρέχουν πρόσβαση σε πληροφορίες που αφορούν την ενεργειακή κλάση των κτιρίων και συστημάτων ελέγχου από έναν φορητό υπολογιστή ή ένα smartphone.

4.5 Έξυπνη Βιομηχανία

Ο ρόλος του IoT θα γίνει πιο εξέχων στο να δίνει πρόσβαση σε συσκευές και σε μηχανές, πράγμα που θα επιτρέψει στις τεχνολογίες Internet να διεισδύσουν περισσότερο σε ψηφιοποιημένα συστήματα παραγωγής. Το IoT θα μπορεί να επικεντρωθεί στη παραγωγή, συνδέοντας το εργοστάσιο με ένα νέο φάσμα εφαρμογών. Αυτό το φάσμα εφαρμογών θα έχει να κάνει με σύνδεση του εργοστασίου με έξυπνο δίκτυο, το διαμοιρασμό της εγκατάστασης παραγωγής ως υπηρεσία ή τη μεγαλύτερη ευελιξία και ελαστικότητα στο πλαίσιο της παραγωγής των ίδιων συστημάτων. Από την άλλη θα βελτιστοποιηθεί ο ποιοτικός έλεγχος μιας εργοστασιακής μονάδας σε όλα τα σημεία της παραγωγής.



Εικόνα 15: Smart Factory²⁶

Ένα πρώτο βήμα στη δημιουργία ενός έξυπνου εργοστασίου θα μπορούσε να πραγματοποιηθεί δίνοντας πρόσβαση στους σημερινούς εξωτερικούς φορείς όπως προμηθευτές και διακινητές, με σκοπό να αλληλεπιδράσουν με ένα σύστημα IoT

σύστημα παραγωγής. Μια αρχιτεκτονική βασισμένη σε ένα IoT, θα επιτρέπει στους παραπάνω φορείς να εκτελούν τις υπηρεσίες τους σε πολλαπλών βαθμίδων συστήματα παραγωγής. Η καινοτομία στο χώρο της εφαρμογής θα μπορούσε να αυξηθεί με το ίδιο βαθμό μεγέθους όπως οι ενσωματωμένες εφαρμογές ή Apps. Οι επιχειρήσεις θα μπορούν να κάνουν χρήση του τεράστιου ποσού των διαθέσιμων δεδομένων, των business analytics, των υπηρεσιών cloud, της κινητικότητας των επιχειρήσεων και πολλά άλλα για να βελτιωθεί ο τρόπος που διεξάγονται. Αυτές οι τεχνολογίες περιλαμβάνουν big data and business analytics, υπηρεσίες cloud, ενσωματωμένη τεχνολογία, δίκτυα αισθητήρων/ τεχνολογίας ανίχνευσης, RFID, GPS, M2M, κινητικότητα, ασφάλεια και τεχνολογία αναγνώρισης ταυτότητας, ασύρματο δίκτυο και ταυτοποίηση.

4.6 Έξυπνη Λιανική

Το IoT διευκολύνει και δίνει λύσεις και στο τομέα του εμπορίου. Με τη χρήση του IoT οι καταναλωτές θα μπορούν να δημιουργήσουν μια εξατομικευμένη εμπειρία, όπου θα μπορεί να συνδεθεί κάποιος οποιαδήποτε στιγμή με οποιαδήποτε συσκευή. Θα μπορεί να γίνετε προσαρμογή στις προτιμήσεις των καταναλωτών πράγμα που θα βοηθήσει και τους λιανοπωλητές.

Οι λιανοπωλητές θα πρέπει αναπτύξουν έξυπνες συνδεδεμένες συσκευές για όλες τις δραστηριότητές τους, όπου θα πρέπει να συνδεθούν τα πάντα, από τη παρακολούθηση των αποθεμάτων μέχρι και την διαφήμιση και με αυτό τον τρόπο θα αποκτηθεί ορατότητα στις εργασίες και θα μπορούν οι λιανοπωλητές να ανταποκρίνονται σε αλλαγές στη συμπεριφορά καταναλωτών. Και εδώ θα πρέπει να χρησιμοποιηθούν αισθητήρες, συσκευές σάρωσης και άλλες τεχνολογίες IoT. Η πληροφορία που θα συλλέγεται θα δώσει στους λιανοπωλητές μια πραγματική κατανόηση το πώς συνδέονται μεταξύ τους τα προϊόντα, οι πελάτες, οι εργαζόμενοι και άλλοι εξωτερικοί παράγοντες.



Εικόνα 16: Smart Service27

4.7 Έξυπνη Γεωργία-Εκτροφή

Οι κανονισμοί για τη δυνατότητα ανίχνευσης των αγροτικών ζώων και τις κινήσεις τους απαιτούν τη χρήση τεχνολογιών όπως IoT, ώστε να καθιστά δυνατή η ανίχνευση των ζώων σε πραγματικό χρόνο. Σε πολλές χώρες οι κυβερνήσεις δίνουν επιδοτήσεις ανάλογα με τον αριθμό των ζώων, και έτσι ο προσδιορισμός του αριθμού είναι πολλές φορές δύσκολος και υπάρχει πιθανότητα απάτης. Έξυπνα συστήματα αναγνώρισης μπορούν να βοηθήσουν στην ελαχιστοποίηση αυτής της απάτης. Με την εφαρμογή αυτών των συστημάτων αναγνώρισης, οι ασθένειες των ζώων μπορεί να ελεγχθούν, να ερευνηθούν και να προλαμβάνονται. Η επίσημη αναγνώριση των ζώων σε εθνικό και διεθνές εμπόριο έχει ήδη καθιερωθεί και έτσι η ταυτοποίηση των ζώων που έχουν εμβολιαστεί ή ελέγχονται από επίσημο οργανισμό ελέγχου ασθενειών είναι επίσης δυνατή. Τα δείγματα αίματος και ιστού μπορεί να προσδιοριστούν με ακρίβεια και η κατάσταση της υγείας των ζώων μπορεί να επίσης να πιστοποιηθεί από ένα σύστημα IoT.

Οι γεωργοί θα είναι σε θέση να παραδίδουν τις καλλιέργειες απευθείας στους καταναλωτές όχι μόνο σε μικρή περιοχή αλλά και σε ευρύτερη. Αυτό θα μπορεί να αλλάξει την αλυσίδα εφοδιασμού, η οποία προς το παρόν απαρτίζεται κυρίως από μεγάλες εταιρίες τώρα, σε μια πιο άμεση, μικρότερη αλυσίδα μεταξύ παραγωγών και καταναλωτών.

ΚΕΦΑΛΑΙΟ 5- ΤΟ ΙοΤ ΣΤΟ ΤΟΜΕΑ ΤΗΣ ΥΓΕΙΑΣ

Στο τρέχων κεφάλαιο γίνεται μια ειδική αναφορά σε έναν τομέα εφαρμογής του ΙοΤ, στο τομέα της Ιατρικής. Γίνεται μια ειδική αναφορά, σε αυτό που ονομάζεται ΙοΜΤ (Internet of Medical Things) και στην αρχιτεκτονική πάνω στην οποία αναπτύχθηκε και στηρίζεται. Επιπλέον γίνεται και εδώ μια αναφορά στα θέματα ασφάλειας και ιδιωτικότητας που προκύπτουν με την χρήση τέτοιων μοντέλων.

5.1 Το Internet of Medical Things (IoMT)

Το Internet of Medical Things (IoMT) προσφέρει αλληλεπίδραση μεταξύ μηχανών και επεμβατικές λύσεις σε πραγματικό χρόνο, που θα μπορεί να μεταμορφώσει ριζικά την παροχή υγειονομικής περίθαλψης, την οικονομική προσιτότητα και την αξιοπιστία. Επιπλέον, η αυξανόμενη συμμετοχή των ασθενών στη λήψη αποφάσεων θα ενισχύσει τη συμμόρφωση των υπηρεσιών υγειονομικής περίθαλψης. Παρέχοντας ατομικά δεδομένα με γνώμονα τη θεραπευτική αγωγή και βελτιστοποιημένες συσκευές σύμφωνα με τη φυσιολογία του ανθρώπου, το ΙοΜΤ θα προωθήσει τη προσωπική φροντίδα και το υψηλό βιοτικό επίπεδο¹⁴.

Το ΙοΜΤ προσφέρει τεράστια οφέλη στην υγειονομική περίθαλψη. Μπορεί να παίξει καθοριστικό ρόλο σε ένα ευρύ φάσμα των συσκευών υγειονομικής περίθαλψης όπως για παράδειγμα την απομακρυσμένη παρακολούθηση των ζωτικών σημείων στα νοσοκομεία και το πιο σημαντικό στο σπίτι. Η απομακρυσμένη παρακολούθηση φέρει τεράστια οφέλη όχι μόνο στη μείωση του κόστους υγειονομικής περίθαλψης αλλά και στη πρόληψη ασθενειών. Σε πολλές περιπτώσεις η υγειονομική περίθαλψη γίνεται όλο και πιο δαπανηρή, καθώς οι ασθενείς πρέπει να μείνουν στο νοσοκομείο για όλη τη διάρκεια της θεραπείας τους, λόγω της έλλειψης των συσκευών με δυνατότητα εξ αποστάσεως παροχής των πληροφοριών για την υγεία τους ασθενούς σε εξουσιοδοτημένους επαγγελματίες υγείας. Χρησιμοποιώντας ΙοΤ συλλέγονται πληροφορίες για την υγεία του ασθενούς και τη διαβίβασή του σε πραγματικό χρόνο για τους επαγγελματίες του τομέα υγείας, όχι μόνο θα μειωθεί το κόστος των υπηρεσιών περίθαλψης αλλά θα επιτρέπει την αντιμετώπιση θεμάτων υγείας πριν γίνουν κρίσιμα.

Τα τελευταία χρόνια έχει προσελκύσει μεγάλο ερευνητικό ενδιαφέρον για την αντιμετώπιση του ΙοΤ στο τομέα της υγειονομικής περίθαλψης. Κατά συνέπεια

¹⁴Islam, S.M. Riazul, και συν. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*. 2015, Τόμ. 3.

υπάρχουν πολλές εφαρμογές και υπηρεσίες. Η ερευνητικές τάσεις του IoT με βάση την υγειονομική περίθαλψη περιλαμβάνουν αρχιτεκτονικές δικτύων και πλατφορμών, νέες υπηρεσίες και εφαρμογές, τη διαλειτουργικότητα και ασφάλεια.

5.2 Οφέλη του IoMT

Βασικά πλεονεκτήματα των εφαρμογών IoMT στο τομέα της υγείας είναι:

1. Μείωση του κόστους περίθαλψης, αφού η υγεία των ασθενών μπορεί να ελεγχθεί σε πραγματικό χρόνο, αποφεύγοντας άσκοπες επισκέψεις σε γιατρούς.
2. Βελτιωμένα αποτελέσματα ασθενών. Αφού βασίζεται στη περιεκτική γνώση που έχει συγκεντρωθεί από προηγούμενα κρούσματα και έρευνες, οι φροντιστές και οι γιατροί μπορούν να χρησιμοποιήσουν ιατρική βασισμένη σε συγκεκριμένα στοιχεία για τη βελτίωση της υγείας των ασθενών.
3. Τα δεδομένα δίνονται σε πραγματικό χρόνο και έχουν ως αποτέλεσμα την έγκαιρη φροντίδα.
4. Διαχείριση νόσου σε πραγματικό χρόνο. Οι ασθενείς θα μπορούν να θεραπεύονται προληπτικά πριν επιδεινωθεί η κατάστασή τους. Αυτό δεν βοηθά μόνο στην υγεία των ασθενών αλλά μειώνει και το κόστος περίθαλψης. Μετατοπίζεται η έμφαση από θεραπεία σε ευεξία με αποτέλεσμα της βελτίωσης της ποιότητας ζωής.
5. Βελτιωμένη εμπειρία του χρήστη. Όσο αφορά τους ασθενείς και το ιατρικό προσωπικό, το IoMT καθιστά πιθανό να έχουν μια πλουσιότερη και πιο στενή εμπλοκή μεταξύ τους. Η αυτοματοποίηση της συλλογής δεδομένων καθιστά τη συλλογή δεδομένων με ακρίβεια, εγκαίρως και με ελάχιστη ανθρώπινη παρέμβαση, οπότε όλα τα ενδιαφερόμενα μέλη έχουν καλύτερη οπτική σε σχέση με τη κατάσταση.

5.3 Εφαρμογές του ΙοMT

Οι ιατρικές συσκευές μπορούν να τροποποιηθούν σε συσκευές ΙοMT έτσι ώστε να μπορούν να ανιχνεύουν δεδομένα σε πραγματικό χρόνο για τη παρακολούθηση των ασθενών. Οι συσκευές ΙοMT υπάρχουν σε διάφορες μορφές όπως οι έξυπνες συσκευές (wearable), ιατρικές συσκευές οικιακής χρήσης, συσκευές περίθαλψης και smartphone εφαρμογές υγειονομικής περίθαλψης, οι οποίες είναι σε θέση να επικοινωνούν με ιατρικό προσωπικό σε απομακρυσμένες περιοχές. Εκτός από τη χρησιμότητά τους στη διαχείριση της υγείας, χρησιμοποιούνται για πρόληψη ασθενειών. Ορισμένοι τομείς του ΙοMT είναι:

1. Απομακρυσμένη φροντίδα και παρακολούθηση

Τα δεδομένα από τις συσκευές δικτύου καταχωρούνται σε μια κεντρική βάση που βρίσκεται στο γραφείο του γιατρού. Η συγκέντρωση και επεξεργασία των δεδομένων του ασθενή επιτρέπουν την αυτοματοποίηση της υγειονομικής περίθαλψης, αναλύοντας νέα δεδομένα σε σχέση με τα προηγούμενα και αποφασίζοντας τη μελλοντική πορεία για τη διαχείριση του ασθενή. Τα έξυπνα συστήματα βοηθούν τους παρόχους υπηρεσιών να μεταθέσουν καθήκοντα της δρομολόγησης, της διαχείρισης και της παρακολούθησης σε μηχανές ΙοMT. Επιπλέον η εξ αποστάσεως παρακολούθηση οδηγεί σε μείωση του ποσοστού εγκατάλειψης του μέλους και την αύξηση της παραγωγικότητας των πόρων υγειονομικής περίθαλψης. Το σύστημα Body-Guardian Heart αποτελεί από τα πιο γνωστά συστήματα που χρησιμοποιούνται για τη παρακολούθηση καρδιακής λειτουργίας.



Εικόνα17: Internet of Medical Things²⁸

2. Διαχείριση χρόνιων ασθενών

Οι συσκευές IoMT προσφέρουν πολλά υποσχόμενες εναλλακτικές λύσεις για την αντιμετώπιση των χρόνιων νοσημάτων όπως η υπέρταση, καρδιακή ανεπάρκεια και ο διαβήτης. Οι συσκευές που χρησιμοποιούνται για τη παρακολούθηση παραμέτρων όπως η αρτηριακή πίεση, επίπεδα σακχάρου στο αίμα, το βάρος και οι συγκεντρώσεις ηλεκτρολυτών μέσα στο σώμα. Τα στοιχεία που επεξεργάζονται γίνετε με μεγάλη προσοχή και μπορεί να χρησιμοποιηθούν για μελλοντικές αλλαγές στην θεραπεία. Επίσης τα στοιχεία που συλλέγονται παρουσιάζουν μεγάλο ενδιαφέρον για μελέτες επιδημιολογίας.

3. Ευεξία και προσωπική φροντίδα

Οι συσκευές IoMT έχουν διευκολύνει την εποπτεία της υγείας με σύστημα παρακολούθησης για τη διατροφή, τη σωματική δραστηριότητα και τη ποιότητα ζωής. Καινοτόμες συσκευές (wearable) παρακολουθούν συνεχή δεδομένα σχετικά με τη δραστηριότητα των ασθενών. Επιπλέον οι απομακρυσμένες δυνατότητες δικτύωσης των συσκευών αυτών παρέχουν βοήθεια από εμπειρογνώμονες σε καταστάσεις έκτακτης ανάγκης.

4. Απομακρυσμένη παρέμβαση

Τα δεδομένα που λαμβάνουν σε πραγματικό χρόνο από τους αισθητήρες επιτρέπουν στους γιατρούς να διαχειριστούν φάρμακα και να αξιολογήσουν τη κατάσταση σε περίπτωση ανάγκης.

5. Διαχείριση Φαρμάκων

Οι RFID (Αναγνώριση μέσω ραδιοσυχνότητων) ετικέτες, που βασίζονται σε IoMT τεχνολογίες, διαχειρίζονται τα προβλήματα διαθεσιμότητας και το κόστος προμήθειας των φαρμάκων. Αυτό περιλαμβάνει τη προσθήκη ετικετών στις συσκευασίες φαρμάκων, οι οποίες επιτρέπουν στους κατασκευαστές να εξασφαλίζουν τη ποιότητα εφοδιαστικής αλυσίδας. Έχουν ανακαλυφθεί και τα λεγόμενα «έξυπνα» χάπια τα οποία βοηθούν στη παρακολούθηση των δόσεων του φαρμάκου.

5.4 Αρχιτεκτονική των IoMT Συστημάτων

Η αρχιτεκτονική των IoMT συστημάτων αποτελείται από τρία μέρη-στρώματα: τοπικές συσκευές, συνδεσιμότητα και ανάλυση δεδομένων και λύσεων. Τα στρώματα αυτά παρουσιάζονται παρακάτω.

5.4.1 Συσκευές

Η αποκεντρωμένη νοημοσύνη αποτελεί βασικό στοιχείο του IoMT. Πρωταρχικός στόχος είναι να φτιαχτεί μια ιατρική συσκευή με έξυπνες δυνατότητες ελέγχου, που βοηθά στην επεξεργασία των δεδομένων λειτουργίας, εκτός από τον κεντρικό διακομιστή και σε τοπικό επίπεδο. Οι συσκευές αυτές είναι ενσωματωμένες με αισθητήρες για τη μέτρηση λειτουργικών παραμέτρων, μετατροπείς που παράγουν ψηφιακές εισόδους, ελεγκτές για τη λήψη αποφάσεων σε πραγματικό χρόνο βάση στοιχείων που λαμβάνονται από τους μετατροπείς, και διασυνδέσεις δικτύου με σκοπό να μοιράζονται δεδομένα με άλλες μηχανές. Παράδειγμα τέτοιων συσκευών είναι wearable συσκευές παρακολούθησης, τα εμφυτεύματα και οι φορητές διαγνωστικές συσκευές. Τέτοιες συσκευές είναι ικανές να αποκτήσουν σε πραγματικό χρόνο, ποιοτικά, βιομετρικά δεδομένα από το σώμα του ασθενούς και να τα μεταδώσουν κάτω από ένα ασφαλές περιβάλλον σε υψηλότερο επίπεδο αρχιτεκτονικής. Κωδικοποιητές, ενεργοποιητές και συσκευές κρυπτογράφησης εκτελούν μετασχηματισμούς δεδομένων και τα μεταφέρουν σε επόμενο στρώμα¹⁵.

5.4.2 Συνδεσιμότητα

Αυτό το επίπεδο επικεντρώνεται στη συλλογή δεδομένων από τη συσκευή δικτύου και αποθηκεύει σε προκαθορισμένες αποθήκες δεδομένων. Οι τεχνολογίες σε αυτό το επίπεδο δεν είναι κατάλληλη για παρακολούθηση του ασθενούς, αφού βασικός σκοπός τους είναι η ασφαλής μεταφορά ιατρικών δεδομένων και η διαχείριση μεγάλου όγκου δεδομένων διασφαλίζοντας ταυτόχρονα τη ποιότητα.

¹⁵Catarinucci, Luca, και ούκ. An IoT-Aware Architecture for Smart Helathcare Systems. *IEEE Internet of Things Journal*. 2015, Τόμ. 2, 6.

5.4.3 Ανάλυση Δεδομένων

Ο κεντρικός διακομιστής συλλέγει δεδομένα από πολλαπλές συσκευές μέσω του δικτύου και των βασικών εξαρτημάτων του. Ο διακομιστής, διαθέτει ενσωματωμένους αλγόριθμους οι οποίοι αναλύουν τα δεδομένα λειτουργίας σε πραγματικό χρόνο, παρέχοντας γνώσεις και συμπεράσματα. Αυτά τα δεδομένα βοηθούν σημαντικά τη διαγνωστική ικανότητα, τη πρόβλεψη της νόσου και την εφαρμογή προληπτικών μέτρων. Η αξιολόγηση των δεδομένων από διαφορετικές πηγές επιτρέπει λύσεις υγειονομικής περίθαλψης, όπως η εξ αποστάσεως παρακολούθηση ασθενών, οι παρεμβάσεις αλλά και η διαχείριση χρόνιων ασθενειών.

5.5 Ασφάλεια των ΙοΜΤ Συστημάτων

Στα επόμενα χρόνια, στο τομέα τη ιατρικής αναμένεται η ευρεία εξάπλωση του ΙοΤ μέσω νέων συσκευών και εφαρμογών ηλεκτρονικής υγείας. Οι εφαρμογές και οι συσκευές περίθαλψης θα επεξεργάζονται ιδιωτικές πληροφορίες και προσωπικά δεδομένα υγείας. Επιπλέον θα συνδέονται με παγκόσμια δίκτυα πληροφοριών και θα υπάρχει πρόσβαση σε αυτά ανά πάσα στιγμή. Για αυτό το λόγο είναι σημαντικό να εντοπιστούν και να αναλυθούν τα ιδιαίτερα χαρακτηριστικά της ασφάλειας του ΙοΤ.

5.5.1 Απαιτήσεις Ασφάλειας

Για επίτευξη ασφαλών υπηρεσιών, θα πρέπει να επικεντρωθεί κανείς στις ακόλουθες απαιτήσεις:

1. **Εμπιστευτικότητα**
Το οποίο εξασφαλίζει την αδυναμία πρόσβασης των ιατρικών πληροφοριών σε μη-εξουσιοδοτημένους χρήστες, και εμπιστευτική αλληλογραφία να μην αποκαλύπτει το περιεχόμενο σε τρίτους.
2. **Ακεραιότητα**
Εξασφαλίζει ότι τα ληφθέντα ιατρικά δεδομένα δεν έχουν αλλοιωθεί κατά τη μεταφορά τους. Επίσης δεν θα πρέπει να τεθεί σε κίνδυνο η ακεραιότητα των ήδη αποθηκευμένων δεδομένων.
3. **Έλεγχος Ταυτότητας**
Επιτρέπει στη συσκευή ΙοΤ να εξασφαλίζει την ταυτότητα του ομότιμου με τον οποίο επικοινωνεί.

4. Διαθεσιμότητα
Εξασφαλίζει την ικανότητα επιβίωσης των υπηρεσιών υγειονομικής περιθαλψής ΙοΤ σε εξουσιοδοτημένα μέρη όταν χρειάζεται.
5. Ανανέωση Δεδομένων
Επειδή κάθε δίκτυο περιέχει κάποιες χρονικά μεταβαλλόμενες μετρήσεις υπάρχει ανάγκη να διασφαλιστεί ότι κάθε μήνυμα είναι ανανεωμένο. Αυτό σημαίνει ότι κάθε σύνολο δεδομένων είναι πρόσφατο.
6. Εξουσιοδότηση
Διασφαλίζει ότι μόνο εξουσιοδοτημένοι κόμβοι είναι προσβάσιμοι για υπηρεσίες δικτύου ή πόρων.
7. Ελαστικότητα
Αν κάποιες, μεταξύ των συνδεδεμένων συσκευών υγείας παραβιαστούν, τότε ένα σύστημα ασφαλείας θα πρέπει να εξακολουθεί να προστατεύει το δίκτυο/ συσκευή /πληροφορίες.
8. Ανοχή σε σφάλματα
Θα πρέπει ένα σύστημα ασφαλείας να παρέχει τις αντίστοιχες υπηρεσίες ασφαλείας, ακόμα και με τη παρουσίαση σφάλματος.
9. Αυτό-Θεραπεία
Μια ιατρική συσκευή σε ένα δίκτυο ΙοΤ μπορεί να χαλάσει και να βγει εκτός λειτουργίας. Θα πρέπει οι συνεργαζόμενες συσκευές να παρέχουν ένα ελάχιστο επίπεδο ασφάλειας.

ΚΕΦΑΛΑΙΟ 6-ΕΠΙΛΟΓΟΣ

Τα τελευταία χρόνια βλέπουμε πως το IoT έχει μπει καλά στη ζωή μας σημειώνοντας ταυτόχρονα σημαντική πρόοδο. Με τη συγκεκριμένη εργασία αναφερθήκαμε στα χαρακτηριστικά και στις τεχνολογίες του IoT αλλά και που βρίσκει εφαρμογή.

Τα επόμενα χρόνια οι τεχνολογίες που έχουν να κάνουν με το IoT θα ωριμάσουν γεγονός που ευνοεί την όλο και μεγαλύτερη χρήση του στη καθημερινότητα. Παρόλα αυτά οι προκλήσεις που θα έχει να αντιμετωπίσει η τεχνολογία αυτή θα είναι αρκετές και σύνθετες. Η διασφάλιση της ασφάλειας, της αξιοπιστίας, της ανθεκτικότητας και σταθερότητας των εφαρμογών και υπηρεσιών του IoT είναι κρίσιμα ζητήματα τα οποία θα πρέπει να αντιμετωπιστούν ώστε οι χρήστες να εμπιστεύονται το περιβάλλον τους. Εάν οι πληροφορίες των χρηστών δεν είναι ασφαλείς δημιουργούνται ζητήματα έλλειψης εμπιστοσύνης με συνέπεια την απροθυμία χρήσης μιας πλατφόρμας IoT. Για αυτό το λόγο η ασφάλεια των συσκευών και υπηρεσιών αποτελεί σημαντικό σημείο συζήτησης.

Επιπλέον θα πρέπει να τηρηθεί ένα νομικό πλαίσιο κατά τη χρήση του IoT που αφορά τη προστασία προσωπικών δεδομένων. Τον Απρίλη του 2016 εκδόθηκε τέτοιος κανονισμός από την Ευρωπαϊκή Ένωση.

Βιβλιογραφία

1. **Bassi, Alessandro, και ουυ.** *Enabling Things o Talk: Designing IOT solutions with the IOT Architectural Reference Model*. New York : Springer, 2013.
2. **Mell, Peter και Grace, Tim.** *Definition of Cloud Computing*. s.l. : NIST, 2009.
3. *Machine to Machine*. https://en.wikipedia.org/wiki/Machine_to_machine. s.l. : Wikipedia.
4. https://en.wikipedia.org/wiki/Internet_of_things. IoT. *Wikipedia*.
5. **Vermesan, Ovidiu και Friess, Peter**. Internet of Things Applications. *AIOTI WGOI-IERC*. 2015.
6. **Hammi, Badis, και ουυ.** Internet of Things (IoT) Technologies for Smart Cities. *IET Journals*. 2015.
7. **Li, Shancang, Tryfonas, Theo και Li, Honglei**. The Internet of Things: A Security Point of View. *Internet Research*. Emerald Group Publishing, 2016, Τόμ. 26.
8. **Forge, Simon**. Radio Spectrum for the Internet of Things. *INFO*. Emerald Group Publishing , 2016, Τόμ. 18.
9. **Alsaadi, E. και Tubaishat, A**. Internet of Things: Features, Challenges and Vulnerabilities. *International Journal of Advanced Computer Science and Information Technology*. 2015, Τόμ. 4.
10. **Catarinucci, Luca, και ουυ.** An IoT-Aware Architecture for Smart Helathcare Systems. *IEEE Internet of Things Journal*. 2015, Τόμ. 2, 6.
11. **Islam, S.M. Riazul, και ουυ.** The Internet of Things for Health Care: A Comprehesive Survey. *IEEE Access*. 2015, Τόμ. 3.
12. **Stergiou, Christos, και ουυ.** Secure Integrationof IoT and Cloud Computing. *Future Generation Computer Systems*. Elsevier, 2018, Τόμ. 78, 3.
13. <https://www.itproportal.com/features/next-big-things-in-iot-predictions-for-2020/>
14. <https://upskill.io/resources/blog/the-history-of-upskill-as-told-by-smart-glasses/>
15. <https://chipsnwafers.electronicsforu.com/2016/12/28/mqtt/>
16. <http://blog.isecurion.com/2017/05/11/iot-communication-protocols/>
17. https://www.researchgate.net/figure/Back-End-Data-Sharing-Model-10_fig1_301693195

18. https://www.researchgate.net/figure/RFID-tag-and-reader_fig1_275352749?fbclid=IwAR0t9QSR4-ZAAd2get-yPTGgX5RCIMbICyfbQqetKnk9G9Be3xazDEG4Sfs
19. <https://thosedays.be/thoughts/understanding-connectivity-for-internet-of-things>
20. <http://www.justscience.in/articles/hardware-software-borderline-cloud-computing/2018/01/22>
21. <https://community.arm.com/iot/b/blog/posts/the-arm-internet-of-things-iot-continuum>
22. <https://es.dreamstime.com/stock-de-ilustraci%C3%B3n-concepto-de-la-ciudad-y-internet-elegantes-de-cosas-image71616987>
23. <https://blog.phoenixcontact.com/marketing-sea/2017/04/smart-grids-how-automation-empowers-the-future-of-electricity/>
24. <https://www.unique-creations.biz/blog/internet-of-things-iot-enabled-vehicles/>
25. <http://homesecuritywithoutmonitoringfeesgasa.blogspot.com/2017/11/smart-home-iot.html>
26. <https://www.cbinsights.com/research/briefing/factory-of-the-future-manufacturing/>
27. <https://blogs.vmware.com/industry-solutions/2018/06/12/the-smart-store/>
28. <https://www.aumcore.com/blog/2018/12/11/what-is-the-internet-of-medical-things-and-what-is-its-impact-on-healthcare/>
29. https://en.wikipedia.org/wiki/Narrowband_IoT

