ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ & ΠΛΗΡΟΦΟΡΙΚΗΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΤΗΛΕΜΑΤΙΚΗ ΚΑΙ ΝΕΕΣ ΥΠΗΡΕΣΙΕΣ

INTERNET OF THINGS

ΚΥΡΙΑΚΗ – ΗΛΕΚΤΡΑ ΖΑΡΑΦΕΤΑ

Α.Μ. 5759

ΔΙΔΑΣΚΩΝ: ΧΡΗΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΑΤΡΑ 2018

ΠΕΡΙΕΧΟΜΕΝΑ

ΑΚΡΩΝΥΜΙΑ

- **IoT:** Internet of Things
- **RFID:** Radio Frequency Identification
- **GSM:** Global System for Mobile communications
- **EPC:** Electronic Product Code
- **MQTT:** MQ Telemetry Transport
- **BLE:** Bluetooth Low Energy
- **CES:** Consumer Electronics Show
- **USB:** Universal Serial Bus
- **MAC:** Message Authentication Code
- **IDC:** International Data Corporation
- **DDoS:** Distributed Denial of Service
- **IP:** Internet Protocol
- **IPv6**: Internet Protocol version 6
- **WSN**: Wireless sensor network
- **UID**: Universal Identification

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 ΟΡΙΣΜΟΙ

Οι ορισμοί του Internet of Things (IoT) ποικίλλουν. Αυτό που χαρακτηρίζει το IoT είναι ότι αποτελείται από "έξυπνα" (δηλαδή εξοπλισμένα με υπολογιστή) "πράγματα" (δηλαδή συσκευές) που συνδέονται μεταξύ τους και με βάσεις δεδομένων (δηλαδή servers) ώστε να παρέχουν πλήθος υπηρεσιών που αξιοποιούν και βασίζονται στα δεδομένα που παρέχουν οι συσκευές που έχουν στην κατοχή τους και χρησιμοποιούν οι καταναλωτές καθημερινά-[1]. Ένας απλουστευμένος ορισμός είναι ότι αποτελεί μια εφαρμογή αισθητήρων, τεχνολογίας πληροφοριών και δικτυακών τεχνολογιών για τη σύνδεση δισεκατομμυρίων συσκευών σε όλο τον κόσμο. Με τη διασύνδεση αυτή επιτρέπεται η ανάπτυξη νέων «έξυπνων» εφαρμογών, η εξαγωγή στατιστικών δεδομένων και η ανάπτυξη νέων επιχειρηματικών μοντέλων που θα έχουν ως αποτέλεσμα έναν καθαρότερο και πιο βιώσιμο τρόπο ζωής-[2]. Ουσιαστικά, το "Διαδίκτυο των Πραγμάτων" είναι ένα εγχείρημα, μία ιδέα, που έχει την βάση του στην σύνδεση διάφορων μικρών και μεγάλων συσκευών ή και οχημάτων με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης (tablets, τηλέφωνα, ηχεία, wearables, κάμερες, αισθητήρες, λευκές συσκευές, αυτοκίνητα και αναρίθμητες άλλες συσκευές) τόσο μεταξύ τους όσο και με τον κατασκευαστή, για να λαμβάνουν και να μεταδίδουν σχετικά δεδομένα με στόχο να προσφέρουν περισσότερες υπηρεσίες και πρόσθετη αξία-[3].

1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Το 1950 το Internet of Things άρχισε να υφίσταται ως μια αόριστη σκέψη. Πέντε χρόνια μετά, έκανε την εμφάνισή της η πρώτη συσκευή του Edward O. Throrp, η οποία ήταν ένα ρολόι το οποίο πρόβλεπε τους κύκλους που έκαναν οι ρουλέτες στα καζίνα του Las Vegas μέσα από περίπλοκους αλγορίθμους. Το 1967 ο Hubet Upton δημιούργησε την πρώτη συσκευή σε σχήμα μυωπικών γυαλιών, η οποία βοηθούσε τα άτομα με ειδικές ανάγκες να διαβάζουν τα χείλια των ανθρώπων και το 2011 η Google δημιούργησε το project Google Glass με στοιχεία από αυξημένη πραγματικότητα. Επίσης, με την δημιουργία του δικτύου ARPANET, 1970, για την επικοινωνία και ανταλλαγή δεδομένων ανάμεσα στις στρατιωτικές βάσεις των ΗΠΑ, στάλθηκε το πρώτο μήνυμα απομακρυσμένων υπολογιστών. Ήταν το πρώτο δίκτυο που σήμανε το ξεκίνημα της εποχής του Internet.

Το 1982 αποτελεί τη γενιά του Internet και του πρωτοκόλλου TCP/IP. Με το πρωτόκολλο αυτό ξετυλίγεται μια νέα εποχή, ενός παγκόσμιου ιστού, και δίκτυα που ενώνονται μεταξύ τους, για να δημιουργηθεί το διαδίκτυο. 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 αυτή δημιουργήθηκε το 1973 από τον Mario Cardullo και η ευρεία χρήση του RFID ξεκίνησε το 2013 με την πολυεθνική Inditex να χρησιμοποιεί την τεχνολογία μαζικά σε όλα τα καταστήματα της. Δέκα χρόνια μετά αναπτύχθηκε η σκέψη επικοινωνίας «machine to machine» από φοιτητές του Πανεπιστημίου Carnegie Mellon της Pennsylvania, οι οποίοι εγκατέστησαν μηχανισμούς για την παρακολούθηση θερμοκρασίας από τερματικούς υπολογιστές στα μηχανήματα αυτόματων πωλητών 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. Τέσσερα χρόνια μετά στο MIT δημιουργείται 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 πιο έξυπνων τρόπων ανάγνωσης πληροφοριών. Αυτός ο τρόπος θα επέτρεπε στις τεχνολογίες RFID, Bluetooth και σε

άλλες ασύρματες τεχνολογίες να τροποποιήσουν, να διαβάσουν και να γράψουν δεδομένα σε αντικείμενα μέσω ενός RFID tag. Αυτό το νέο σύστημα ονομάστηκε Electronic Product Code (EPC). Ο Ashton, ο οποίος δούλευε στην βελτιστοποίηση της εφοδιαστικής αλυσίδας, ήθελε να προσελκύσει την προσοχή της διοίκησης με μια νέα τεχνολογία που ονομάζεται RFID. Ένα χρόνο μετά το Auto ID Center μετονομάστηκε σε Auto ID Labs και έγινε το πρώτο υπερσύγχρονο δίκτυο ανάπτυξης και standardizing του Internet of Things, το οποίο όνομα ανακοινώθηκε από τον Kevin Ashton μέσα στο Auto ID Center.

Το 2000 ο υπάλληλος της IBM, Andy Stanforf, και ο υπάλληλος της εταιρίας Eurotech, Arlen Nipper, 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 αποτέλεσε ένα σημαντικό βήμα για την ενίσχυση της ιδές του Internet of Things. Στη συνέχεια, τα μέλη από το πρόγραμμα Interaction Design Institute Ivrea κατασκευάσανε το 2005 την πλατφόρμα του Arduino για μια φτηνή λύση μικροελεγκτή που προοριζόταν για τους φοιτητές. Το 2008 συντάχθηκε η ομάδα IPSO με σκοπό να διαδώσουν το πρωτόκολλο IP σε όλα τα μελλοντικά σχέδια και προτάσεις του Internet of Things. Πλέον η IPSO λεχει πάνω από 50 εταιρικά μέλη για την διάδοση του πρωτοκόλλου προς το μέλλον. Μετά από δύο χρόνια, η τεχνολογία Bluetooth αναβαθμίζεται και εμφανίζεται 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 Internet of Things. Η Gartner, η εταιρεία έρευνας της αγοράς που εφηύρε την περίφημη «διαφημιστική εκστρατεία του κύκλου για τις αναδυόμενες τεχνολογίες», περιλαμβάνει το 2011 στη λίστα της: «Το Internet of Things»

Αξιοσημείωτο είναι ότι το 201 το θέμα της μεγαλύτερης ευρωπαϊκής διαδικτυακής διάσκεψης LeWeb ήταν το Internet of Things. Επίσης, 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 αυτό το φαινόμενο. Την ίδια χρονιά το πρωτόκολλο του IP άλλαξε versioning και με την νέα έκτη έκδοσή του υποστηρίζει περισσότερες συσκευές, γρηγορότερες και αποδοτικότερες σε θέματα διασύνδεσης. Το 2013 η IDC δημοσίευσε μια έκθεση που

αναφέρει ότι το IoT θα στοιχίζει $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 δισεκατομμύρια, η οποία κατασκεύαζε συσκευές για το IoT. Την ίδια στιγμή το Consumer Electronics Show (CES) στο Las Vegas πραγματοποιήθηκε υπό το θέμα του IoT. Τέλος, την επόμενη χρονιά η Apple ανακοίνωσε το HealthKit & HomeKit, δύο πλατφόρμες ανάπτυξης υλοποιήσεων, και την υποστήριξη της πλατφόρμας από τις νέες συσκευές, με σκοπό η ιδέα του έξυπνου σπιτιού και τρόπου ζωής να έρθει πιο κοντά στο σήμερα. Επίσης, η τεχνολογία iBeacon έφερε νέα πρότυπα στην αγορά των καταστημάτων και της πώλησης.

ΚΕΦΑΛΑΙΟ 2: ΛΕΙΤΟΥΡΓΙΑ ΚΑΙ ΠΑΡΑΔΕΙΓΜΑΤΑ

2.1 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ INTERNET OF THINGS

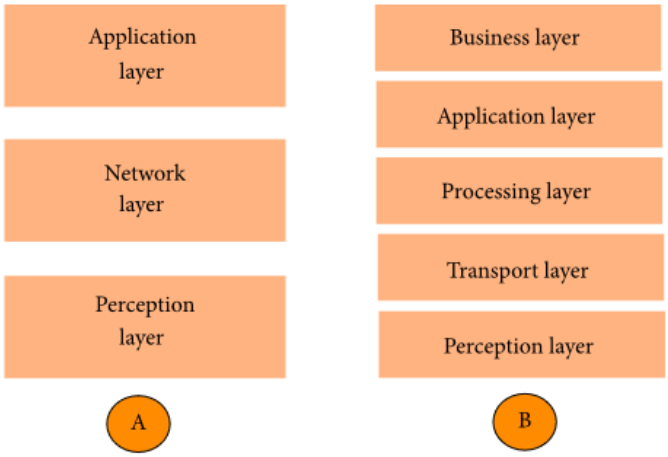
Συσκευές και αντικείμενα με ενσωματωμένους αισθητήρες συνδέονται με μία πλατφόρμα IoT, η οποία ενσωματώνει δεδομένα από τις διάφορες συσκευές και εφαρμόζει αναλυτικά στοιχεία ώστε να μοιράζονται τις πιο πολύτιμες πληροφορίες με εφαρμογές που έχουν δημιουργηθεί για την αντιμετώπιση συγκεκριμένων αναγκών.

Αυτές οι πλατφόρμες IoT έχουν την δυνατότητα να εντοπίζουν ακριβώς ποιές πληροφορίες είναι χρήσιμες καθώς και ποιές μπορούν να αγνοηθούν. Οι χρήσιμες αυτές πληροφορίες μπορούν να χρησιμοποιηθούν για την ανίχνευση μοτίβων, τη διατύπωση συστάσεων και την ανίχνευση πιθανών προβλημάτων πριν συμβούν-[5].

2.2 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ INTERNET OF THINGS

Δεν υπάρχει μία ευρέως αποδεκτή αρχιτεκτονική για το Internet of Things, ωστόσο έχουν προταθεί διαφορετικές αρχιτεκτονικές από διάφορους ερευνητές και οι οποίες παρουσιάζονται παρακάτω.

Η πιο βασική αρχιτεκτονική είναι η **αρχιτεκτονική τριών επιπέδων** (σχήμα 1Α), η οποία αποτελείται από τα επίπεδα αντίληψης, δικτύου και εφαρμογών.



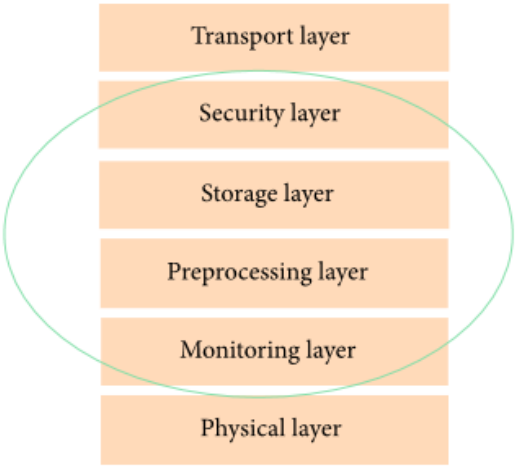
Σχήμα 1: Αρχιτεκτονική του IoT (Α: τριών επιπέδων) (Β: πέντε επιπέδων)

Το επίπεδο αντίληψης είναι το φυσικό επίπεδο, το οποίο διαθέτει αισθητήρες για την ανίχνευση και τη συλλογή πληροφοριών σχετικά με το περιβάλλον. Αισθάνεται μερικές φυσικές παραμέτρους ή εντοπίζει άλλα έξυπνα αντικείμενα στο περιβάλλον. Το επίπεδο δικτύου είναι υπεύθυνο για την σύνδεση με άλλα έξυπνα πράγματα, συσκευές δικτύου και διακομιστές. Τα χαρακτηριστικά του χρησιμοποιούνται για τη μετάδοση και την επεξεργασία δεδομένων αισθητήρων. Τέλος, το τρίτο επίπεδο, το επίπεδο εφαρμογής, είναι υπεύθυνο για την παροχή συγκεκριμένων υπηρεσιών εφαρμογής στον χρήστη. Ορίζει διάφορες εφαρμογές στις οποίες μπορεί να αναπτυχθεί το Internet of Things, για παράδειγμα έξυπνα σπίτια, έξυπνες πόλεις και έξυπνη υγεία.

Η αρχιτεκτονική τριών επιπέδων ορίζει την κύρια ιδέα του Internet of Things, αλλά δεν αρκεί για την έρευνα στο IoT, διότι η έρευνα συχνά επικεντρώνεται σε λεπτότερες πτυχές του IoT. Γι 'αυτό, προτείνονται και αρχιτεκτονικές με περισσότερες στρώσεις. Μία από αυτές είναι η **αρχιτεκτονική πέντε επιπέδων** (σχήμα 1Β), η οποία περιλαμβάνει επιπλέον τα επίπεδα επεξεργασίας και

επιχειρήσεων. Ο ρόλος των επιπέδων αντίληψης και εφαρμογής είναι ο ίδιος με αυτόν στην αρχιτεκτονική τριών επιπέδων. Το επίπεδο μεταφοράς μεταφέρει τα δεδομένα αισθητήρων από το επίπεδο αντίληψης στο επίπεδο επεξεργασίας και αντίστροφα μέσω δικτύων όπως ασύρματα, 3G, LAN, Bluetooth, RFID και NFC. Το επίπεδο επεξεργασίας αποθηκεύει, αναλύει και επεξεργάζεται μεγάλο όγκο δεδομένων που προέρχονται από το επίπεδο μεταφοράς. Μπορεί να διαχειρίζεται και να παρέχει ένα ποικίλο σύνολο υπηρεσιών προς τα κάτω επίπεδα και χρησιμοποιεί πολλές τεχνολογίες όπως βάσεις δεδομένων, cloud computing και μεγάλες μονάδες επεξεργασίας δεδομένων. Τέλος, το επίπεδο επιχειρήσεων διαχειρίζεται ολόκληρο το σύστημα του Internet of Things, συμπεριλαμβανομένων των εφαρμογών, των μοντέλων επιχειρήσεων και κερδών και του ιδιωτικού απορρήτου των χρηστών.

Σε ορισμένες αρχιτεκτονικές συστημάτων η επεξεργασία δεδομένων πραγματοποιείται μέσω των cloud υπολογιστών. Μια τέτοια αρχιτεκτονική κρατά το σύννεφο στο κέντρο, οι εφαρμογές βρίσκονται πάνω από αυτό και το δίκτυο έξυπνων πραγμάτω από κάτω. Η αρχιτεκτονική **cloud computing** παρέχει μεγάλη ευελιξία, δυνατότητα κλιμάκωσης και προσφέρει υπηρεσίες όπως η πλατφόρμα, το λογισμικό και η αποθήκευση. Οι προγραμματιστές μέσω του cloud μπορούν να παρέχουν εργαλεία αποθηκεύσης, εργαλεία λογισμικού, εξόρυξη δεδομένων, εργαλεία εκμάθησης μηχανών και εργαλεία οπτικοποίησης. Τον τελευταίο καιρό παρουσιάζεται μια κατεύθυνση προς μια άλλη αρχιτεκτονική του συστήματος, η οποία ονομάζεται fog computing. Στην αρχιτεκτονική **fog computing** οι αισθητήρες και οι πύλες δικτύου αποτελούν μέρος της επεξεργασίας δεδομένων και των αναλύσεων. Όπως φαίνεται στο σχήμα 2 η αρχιτεκτονική αυτή εισάγει επίπεδα παρακολούθησης, προεπεξεργασίας, αποθήκευσης και αφάλειας ανάμεσα στο επίπεδο μεταφοράς και στο φυσικό επίπεδο.

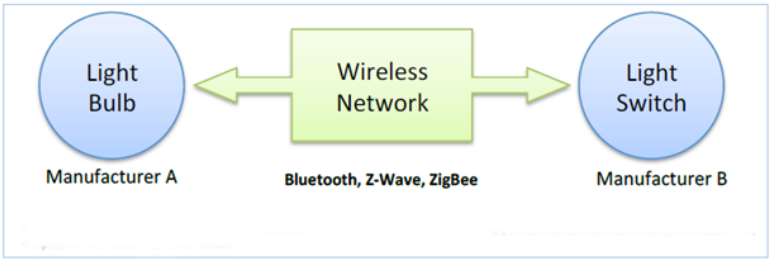


Σχήμα 2: Αρχιτεκτονική Fog μιας έξυπνης IoT πόλης

Το επίπεδο παρακολούθησης παρακολουθεί την ισχύ, τους πόρους, τις ανταποκρίσεις και τις υπηρεσίες. Το επίπεδο προεπεξεργασίας εκτελεί φιλτράρισμα, επεξεργασία και ανάλυση δεδομένων αισθητήρων. Το επίπεδο προσωρινής αποθήκευσης παρέχει λειτουργίες αποθήκευσης όπως αναπαραγωγή, διανομή και αποθήκευση δεδομένων. Τέλος, το επίπεδο ασφάλειας εκτελεί κρυπτογράφηση/αποκρυπτογράφηση και διασφαλίζει την ακεραιότητα και το απόρρητο των δεδομένων. Η παρακολούθηση και η προεπεξεργασία πραγματοποιούνται στην άκρη του δικτύου πρίν από την αποστολή δεδομένων στο cloud-[6].

2.3 ΜΟΝΤΕΛΑ ΤΟΥ INTERNET OF THINGS

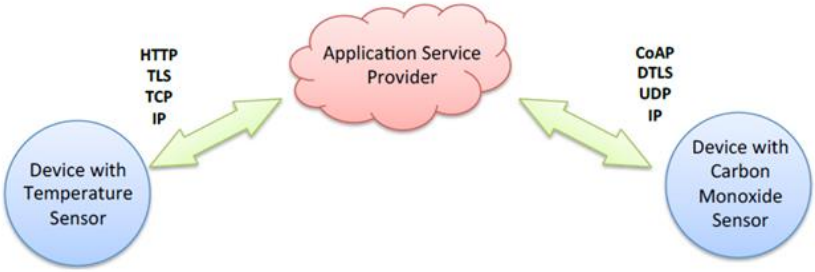
Τα μοντέλα του Internet of Things μπορούν να κατηγοριοποιηθούν σε δύο υποκατηγορίες, οι οποίες ονομάζονται μοντέλα συνδεσιμότητας και μοντέλα αναφοράς. Όσον αφορά τα μοντέλα συνδεσιμότητας, υπάρχουν τα μοντέλα Device – to – Device, Device – to – Cloud, Device – to – Gateway και Backend Data Sharing. Η επικοινωνία Device – to – Device (Σχήμα 3) αντιπροσωπεύει δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους. Μπορούν να επικοινωνούν μέσω πολλών τύπων δικτύων, συμπεριλαμβανομένων των δικτύων IP ή του Internet, αλλά συνήθως χρησιμοποιούνται τα πρωτόκολλα Bluetooth, Z – Wave και ZigBee. Αυτό το μοντέλο χρησιμοποιείται στα συστήματα οικιακής αυτοματοποίησης για τη μεταφορά μικρών πακέτων δεδομένων πληροφοριών μεταξύ συσκευών με σχετικά χαμηλό ρυθμό μετάδοσης δεδομένων. Αυτά μπορεί να είναι λαμπτήρες, θερμοστάτες και κλειδαριές πόρτας που στέλνουν μικρές ποσότητες πληροφοριών μεταξύ τους. Το device – to – device είναι δημοφιλές μεταξύ των φορητών συσκευών Internet of Things όπως μια συσκευή heart monitor συνδεδεμένη με ένα smartwatch όπου τα δεδομένα δεν είναι απαραίτητο να μοιράζονται με πολλούς ανθρώπους. Υπάρχουν πολλά πρότυπα που αναπτύσσονται γύρω από το Device – to – Device, όπως το Bluetooth Low Energy, το οποίο είναι δημοφιλές μεταξύ των φορητών και wearable συσκευών διότι οι χαμηλές απαιτήσεις ισχύος του σημαίνει ότι οι συσκευές θα μπορούσαν να λειτουργήσουν για μήνες ή χρόνια με μία μπαταρία. Επίσης, η μικρότερη πολυπλοκότητά του μπορεί να μειώσει το μέγεθος και το κόστος του-[7].



Σχήμα 3: Επικοινωνία Device – to – Device -[8]

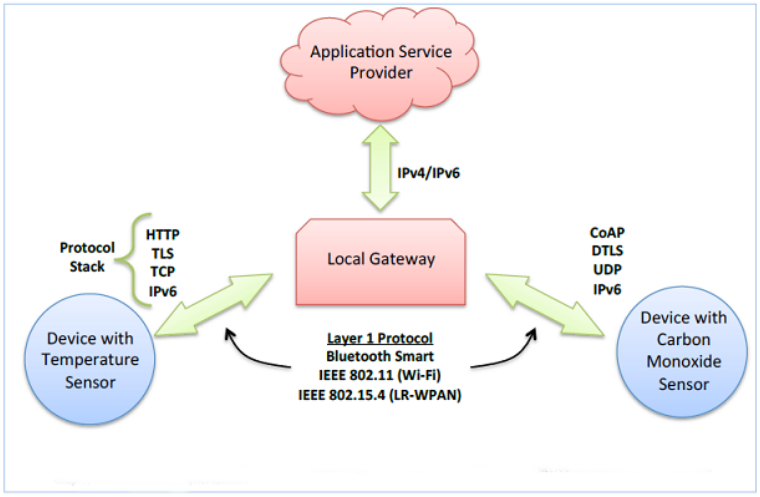
Η επικοινωνία Device – to – Cloud (Σχήμα 4) περιλαμβάνει μία συσκευή Internet of Things που συνδέεται απευθείας με μια υπηρεσία cloud στο Internet, όπως

ένας πάροχος υπηρεσιών εφαρμογών για την ανταλλαγή δεδομένων και την κυκλοφορίας μηνυμάτων ελέγχου. Συνήθως χρησιμοποιούνται παραδοσιακές ενσύρματες συνδέσεις Ethernet ή Wi – Fi, αλλά μπορεί να χρησιμοποιεί και κυψελοειδή τεχνολογία. Η συνδεσιμότητα cloud επιτρέπει στον χρήστη να αποκτήσει απομακρυσμένη πρόσβαση σε μια συσκευή και υποστηρίζει επίσης την προώθηση ενημερώσεων λογισμικού στη συσκευή. Μια περίπτωση χρήσης για το βασισμένο στην κυψελίδα μοντέλο Device – to – Cloud είναι μια έξυπνη ετικέτα που παρακολουθεί ένα σκυλί ενώ ο ιδιοκτήτης δεν είναι κοντά του-[7].



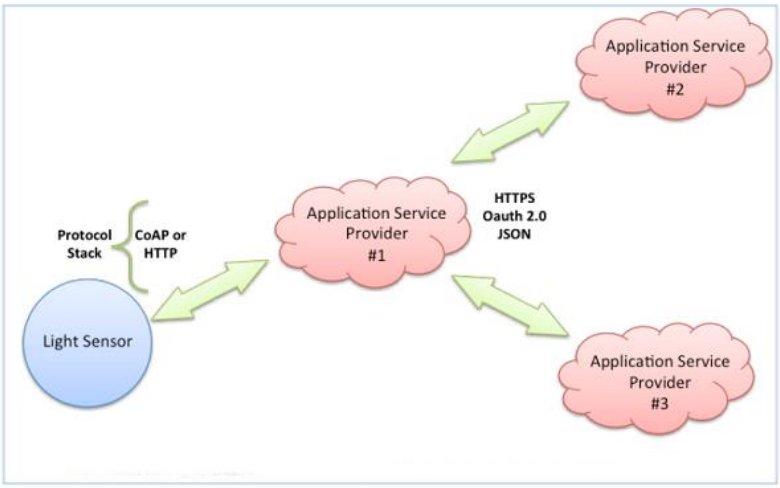
Σχήμα 4: Επικοινωνία Device – to – Cloud -[8]

Στο μοντέλο Device – to – Gateway (Σχήμα 5) οι συσκευές Internet of Things συνδέονται με μια ενδιάμεση συσκευή για πρόσβαση σε cloud υπηρεσία. Αυτό το μοντέλο συχνά περιλαμβάνει λογισμικό εφαρμογών που λειτουργεί σε μια τοπική συσκευή πύλης που ενεργεί ως μεσάζων ανάμεσα σε μια συσκευή Internet of Thins και μια cloud υπηρεσία. Αυτή η πύλη θα μπορούσε να παρέχει ασφάλεια και άλλες λειτουργίες, όπως δεδομένα ή μετάφραση πρωτοκόλλου. Αν η application – layer πύλη είναι ένα smartphone, τότε αυτό το λογισμικό μπορεί να πάρει την μορφή μιας εφαρμογής που αποτελεί ζεύγος με την συσκευή Internet of Thing και επικοινωνεί με μια cloud υπηρεσία. Αυτό μπορεί να είναι μια συσκευή φυσικής κατάστασης που συνδέεται με το cloud μέσω μιας εφαρμογής smartphone, όπως η Nike+, ή εφαρμογές οικιακού αυτοματιμού που περιλαμβάνουν συσκευές που συνδέονται σε ένα κέντρο, όπως το σύστημα SmartThings της Samsung. Επίσης, οι gateway συσκευές μπορούν να γεφυρώσουν το χάσμα διαλειτουργικότητας μεταξύ συσκευών που επικοινωνούν με διαφορετικά πρότυπα-[7].



Σχήμα 5: Επικοινωνία Device – to – Gateway -[8]

Το μοντέλο Back – End Data – Sharing (Σχήμα 6) ουσιαστικά επεκτείνει το μοντέλο Device – to – Cloud, έτσι ώστε οι συσκευές Internet of Things και τα δεδομένα αισθητήρων να μπορούν να έχουν πρόσβαση σε εξουσιοδοτημένα τρίτα μέρη. Σύμφωνα με το μοντέλο αυτό, οι χρήστες μπορούν να εξάγουν και να αναλύουν δεδομένα έξυπνων αντικείμενων από μια cloud υπηρεσία σε συνδυασμό με δεδομένα από άλλες πηγές και να τα στέλνουν σε άλλες υπηρεσίες για ανάλυση-[7].



Σχήμα 6: Μοντέλο Back – End Data – Sharing -[8]

Τα μοντέλα αναφοράς (Σχήμα 7) χωρίζονται σε εφτά επίπεδα, τα οποία είναι επίπεδο 1 – φυσικές συσκευές και ελεγκτές, επίπεδο 2 – συνδεσιμότητα, επίπεδο 3 – υπολογιστική τύπου Fog, επίπεδο 4 – συσσώρευση δεδομένων, επίπεδο 5 – αφαίρεση δεδομένων, επίπεδο 6 – εφαρμογής και επίπεδο 7 – διαδικασίες συνεργασίας.

Σχήμα 7: Μοντέλο Αναφοράς -[9]

Το επίπεδο 1 (Σχήμα 8) αφορά φυσικές συσκευές και ελεγκτές που μπορεί να ελέγχουν πολλές συσκεύες. Αυτά είναι τα «πράγματα» στο Internet of Things και περιλαμβάνουν ένα ευρύ φάσμα συσκευών που στέλνουν και λαμβάνουν πληροφορίες. Οι συσκευές είναι διαφορετικές και δεν υπάρχουν κανόνες σχετικά με το μέγεθος, την τοποθεσία, την μορφή ή την προέλευση-[10].

Σχήμα 8: Επίπεδο 1 -[10]

Στο επίπεδο 2 (Σχήμα 9) είναι συγκεντρωμένες οι επικοινωνίες και η συνδεσιμότητα. Η πιο σημαντική λειτουργία του επιπέδου αυτού είναι η αξιόπιση και έγκαιρη μετάδοση πληροφοριών. Περιλαμβάνει εκπομπές μεταξύ συσκυεών (Επίπεδο 1) και του δικτύου, στα δίκτυα και μεταξύ του δικτύου (Επίπεδο 2) και χαμηλού επιπέδου επεξεργασία πληροφορίων που πραγματοποιείται στο επίπεδο 3-[10].

Σχήμα 9: Επίπεδο 2 -[10]

Οι λειτουργίες του επιπέδου 3 καθοδηγούνται από την ανάγκη μετατροπής των ροών δεδομένων δικτύου σε πληροφορίες που είναι κατάλληλες για αποθήκευση και υψηλότερου επιπέδου επεξεργασία στο επίπεδο 4 (συσσώρευση δεδομένων). Αυτό σημαίνει ότι οι δραστηριότητές του επικεντρώνονται σε ανάλυση και μετασχηματισμό υψηλής έντασης δεδομένων. Η επεξεργασία επιπέδου 3 εκτελείται σε βάση packet – by – packet-[10].

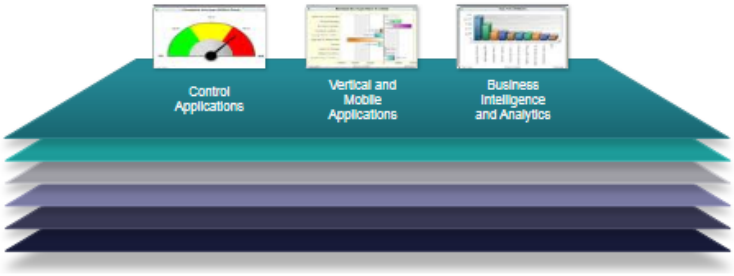
Στο επίπεδο 4 (Σχήμα 10), συσσώρευση δεδομένων, τα δεδομένα σε κίνηση μετατρέπονται σε δεδομένα σε ηρεμία. Το επίπεδο 4 καθορίζει αν τα δεδομένα ενδιαφέρουν υψηλότερα επίπεδα και αν ναι, η επεξεργασία επιπέδου 4 είναι το πρώτο επίπδεο που έχει διαμορφωθεί για να εξυπηρετήσει τις συγκεκριμένες ανάγκες ενός υψηλότερου επιπέδου. Επίσης, καθορίζει αν τα δεδομένα πρέπει να διατηρηθούν και ποιός είναι ο απαιτούμενος τύπος αποθήκευσης. Τέλος, καθορίζει αν τα δεδομένα είναι σωστά οργανωμένα και ελέγχει αν πρέπει να ανασυνταχθούν ή να αναπληρωθούν-[10].

Σχήμα 10: Επίπεδο 4 -[10]

Οι λειτουργίες αφαίρεσης δεδομένων του επιπέδου 5 (Σχήμα 11) επικεντρώνονται στην απόδοση δεδομένων και την αποθήκευσή τους με τρόπους που επιτρέπουν την ανάπτυξη επλούστερων εφαρμογών με βελτιωμένη απόδοση. Κάποιες από τις εργασίες του επιπέδου είναι ο συνδυασμός πολλαπλών μορφών δεδομένων από διαφορετικές πηγές, η διασφάλισης συνεκτικής σημασιολογίας δεδομένων σε πηγές, η επιβεβαίωση ότι τα δεδομένα είναι πλήρη, η ενοποίηση δεδομένων σε ένα μέρος, η προστασία δεδομένων με κατάλληλη πιστοποίηση ταυτότητας και εξουσιοδότηση και η κανονικοποιήση δεδομένων για γρήγορη πρόσβαση-[10].

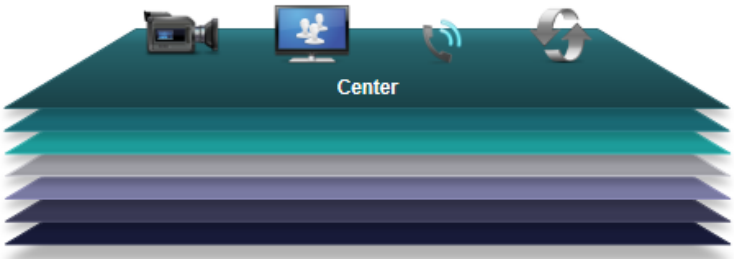
Σχήμα 11: Επίπεδο 5 -[10]

Το επίπεδο 6 (Σχήμα 12) είναι το επίπεδο εφαρμογή όπου λαμβάνει χώρα η ερμηνεία των πληροφοριών. Το λογισμικό σε αυτό το επίπεδο αλληλεπιδρά με το επίπεδο 5 και τα δεδομένα που είναι σε κατάσταση ηρεμίας, οπότε δεν χρειάζεται να λειτουργεί με ταχύτητες δικτύου-[10].



Σχήμα 12: Επίπεδο 6 -[10]

Στο επίπεδο 7 (Σχήμα 13), διαδικασίες συνεργασίας, τα δεδομένα εφαρμογών απαιτούν την ανθρώπινη παρέμβαση και νέες διεργασίες. Ουσιαστικά αυτό το επίπεδο αφορά τη συνεργασία και τον διαμοιρασμό δεδομένων με άλλου ανθρώπους ή διεργασίες-[10].



Σχήμα 13: Επίπεδο 7 -[10]

2.4 ΠΑΡΑΔΕΙΓΜΑΤΑ ΧΡΗΣΗΣ

Οι εφαρμογές του Internet of Things στις μέρες μας είναι πολυάριθμες. Το «έξυπνο» σπίτι (Σχήμα 14) είναι η πιο δημοφιλής εφαρμογή γιατί είναι πιο προσιτή και άμεσα διαθέσιμη στους καταναλωτές. Υπάρχουν εκατοντάδες προϊόντα στην αγορά που μπορούν να ελέγξουν οι χρήστες με τη φωνή τους για να κάνουν τη ζωή τους πιο εύκολη από ποτέ. Παράδειγμα αυτής της εφαρμογής αποτελεί το Amazon Echo που λειτουργεί μέσω της φωνής της βοηθού, Alexa, με την οποία μπορούν να μιλήσουν οι χρήστες προκειμένου να εκτελέσουν διάφορες λειτουργίες όπως να ακούσουν μουσική, να μάθουν τον καιρό, να ενημερωθούν για αθλητικά αποτελέσματα, να καλέσουν ένα Uber και πολλά άλλα.

Σχήμα 14: «Έξυπνο» σπίτι

Επιπλέον, τα ρολόγια δεν χρησιμοποιούνται πλέον μόνο για την ώρα. Το Apple Watch καθώς και άλλα smartwatches (Σχήμα 15) στην αγορά έχουν μετατρέψει τα ρολόγια σε smartphone επιτρέποντας μηνύματα κειμένου, τηλεφωνήματα και άλλα. Συσκευές όπως οι Fitbit και Jawbone έχουν βοηθήσει όσους ασχολούνται με την γυμναστική, δίνοντάς τους περισσότερα δεδομένα σχετικά με τις προπονήσεις τους. Συγκεκριμένα το Fitbit One παρακολουθεί τα βήματα, τις θερμίδες που καίγονται και την ποιότητα του ύπνου. Η συσκευή συγχρονίζεται ασύρματα με υπολογιστές και smartphones, προκειμένου να παρουσιάσει τα δεδομένα της γυμναστικής σε διαγράμματα για την καλύτερη παρακολούθηση της προόδου.

Σχήμα 15: Smartwatch

Το Internet of Things έχει τη δυνατότητα να μετασχηματίσει ολόκληρες πόλεις με την επίλυση προβλημάτων που αντιμετωπίζουν οι πολίτες κάθε μέρα. Με τις σωστές συνδέσεις και δεδομένα, το Internet of Things μπορεί να λύσει προβλήματα κυκλοφοριακής συμφόρησης και να μειώσει τον θόρυβο, την εγκληματικότητα και την ρύπανση. Η Ισπανική πόλη, Βαρκελώνη, είναι μία από τις πιο «έξυπνες» πόλεις (Σχήμα 16) του κόσμου μετά την εφαρμογή πολλών πρωτοβουλιών του Internet of Things, οι οποίες βοήθησαν την ενίσχυση της έξυπνης στάθμευσης και του περιβάλλοντος.

Σχήμα 16: «Έξυπνη» πόλη

Τα Connected Cars (Σχήμα 17) είναι οχήματα τα οποία είναι εξοπλησμένα με πρόσβαση στο Διαδίκτυο και μπορούν να μοιράζονται πρόσβαη και με άλλους ακριβώς όπως γίνεται και με τη σύνδεση με ασύρματο δίκτυο σε ένα σπίτι ή γραφείο. Όλο και περισσότερα οχήματα αρχίζουν να είναι εξοπλισμένα με αυτή τη λειτουργία,

έτσι ώστε να προετοιμαστούν για περισσότερες εφαρμογές που θα περιλαμβάνονται στα μελλοντικά αυτοκίνητα. Για παράδειγμα, η AT & T πρόσθεσε 1.3 εκατομμύρια αυτοκίνητα στο δίκτυό της το δεύτερο τρίμηνο του 2016, ανεβάζοντας τον συνολικό αριθμό των αυτοκινήτων που αυτή συνδέει σε 9.5 εκατομμύρια. Οι οδηγοί δεν χρειάζεται να εγγραφούν ή να καταβάλλουν κάποια μηνιαία αμοιβή για τα δεδομένα ώστε η AT & T να τους θεωρήσει συνδρομητές-[11].

Σχήμα 17: Connected cars

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ ΣΤΟ INTERNET OF THINGS

3.1 ΒΑΣΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Η ασφάλεια των Internet of Things αποτελεί ένα δύσκολο έργο, λόγω της αυξανόμενης πολυπλοκότητας του συστήματος. Όλες οι υπηρεσίες τους Internet of Things πρέπει να ικανοποιούν κάποιες βασικές ιδιότητες ασφάλειας, όμως ενδέχεται να απαιτούνται πρόσθετες απαιτήσεις ασφάλειας για μια συγκεκριμένη υπηρεσία.

Οι υπηρεσίες του Internet of Things ενδέχεται να περιέχουν ευαίσθητα δεδομένα. Έτσι, τα συνδεδεμένα με το Internet of Things αντικείμενα πρέπει να διατηρούνται με σιγουριά. Η **εμπιστευτικότητα** μπορεί να επιτευχθεί μέσω κρυπτογράφησης, αξιοποιώντας διαφορετικά υπάρχοντα συμμετρικά και ασύμμετρα συστήματα κρυπτογράφησης. Όμως, η επιλογή του κατάλληλου τύπου κρυπτογράφησης εξαρτάται σε μεγάλο βαθμό από την εφαρμογή και τις δυνατότητες της συσκευής-[12].

Οι υπηρεσίες του Internet of Things ανταλλάσουν κρίσιμα δεδομένα με άλλες υπηρεσίες και με τρίτους, οι οποίοι προωθούν την αυστηρή απαίτηση ότι τα δεδομένα που ανιχνεύονται, αποθηκεύονται και διαβιβάζονται δεν πρέπει να αλλοιώνονται ούτε κακόβουλα ούτε τυχαία. Η προστασία **ακεραιότητας** των δεδομένων των αισθητήρων είναι ζωτικής σημασίας για το σχεδιασμό αξιόπιστων Internet of Things εφαρμογών. Αυτό εξασφαλίζεται με κωδικούς αναγνώρισης μηνυμάτων (MAC) χρησιμοποιώντας λειτουργίες κατακερματισμού. Η επιλογή της τεχνικής MAC εξαρτάται από την εφαρμογή και τις δυνατότητες της συσκευής-[12].

Το προβλεπόμενο περιβάλλον του Internet of Things περιλαμβάνει υπηρεσίας φιλοξενίας κόμβων αισθητήρων. Συνεπώς, είναι εξαιρετικά σημαντικό οι υπηρεσίες Internet of Things να είναι διαθέσιμες από οπουδήποτε και ανά πάσα στιγμή προκειμένου να παρέχονται συνεχώς πληροφορίες. Δεν υπάρχει κάποιο πρωτόκολλο

ασφάλειας που μπορεί να ικανοποιήσει αυτή την ιδιότητα. Ωστόσο, μπορούν να ληφθούν διαφορετικά μέτρα για να διασφαλιστεί η **διαθεσιμότητα**-[12].

Η **αυθεντικότητα** σχετίζεται με την επαλήθευση της ταυτότητας κάποιου. Στο πλαίσιο του Internet of Things, απαιτείται αμοιβαία επαλήθευση ταυτότητας επειδή τα δεδομένα χρησιμοποιούνται σε διαφορετικές διαδικασίες λήψης αποφάσεων και ενεργοποίησης. Έτσι, τόσο ο πάροχος υπηρεσιών όσο και ο καταναλωτής υπηρεσιών πρέπει να βεβαιωθούν ότι η υπηρεσία είναι προσβάσιμη από αυθεντικό χρήστη και ότι η υπηρεσία παρέχεται από μια αυθεντική πηγή. Επιπλέον, πρέπει να αναπτυχθεί ισχυρός μηχανισμός επαλήθευσης ταυτότητας, προκειμένο να αποφευχθεί η πλαστοπροσωπία. Η επιβολή οποιουδήποτε μηχανισμού ελέγχου ταυτότητας απαιτεί την καταχώριση ταυτοτήτων χρήστη και ο περιορισμός των πόρων των αντικειμένων Internet of Things θέτει αυστηρούς περιορισμούς ώστε να καθίσταται δυνατή οποιαδήποτε τεχνική επαλήθευσης ταυτότητας-[12].

Η **εξουσιοδότηση** αναφέρεται στα μέσα έκφρασης των πολιτικών πρόσβασης που εκχωρούν συγκεκριμένα δικαιώματα. Το περιβάλλον του Internet of Things πρέπει να παρέχει λεπτομερείς, επαναχρησιμοποιούμενες, δυναμικές και εύχρηστες πολιτικές που ορίζουν και αναπροσαρμόζουν τον μηχανισμό. Έτσι, είναι επιτακτική η εξωτερική ανάθεση του ορισμού πολιτικής και του μηχανισμού επιβολής των υπηρεσιών Internet of Things. Επίσης, ο περιορισμός των πόρων του κόμβου αισθητήρα Internet of Things περιορίζει την εφαρμογή αυτού τους μηχανισμού-[12].

Ο **έλεγχος πρόσβασης** αφορά ένα μηχανισμό επιβολής που επιτρέπει μόνο της πρόσβαση των εξουσιοδοτημένων χρηστών στους πόρους. Η επιβολή βασίζεται συνήθως στις αποφάσεις του ελέγχου πρόσβασης-[12].

Πολλές εφαρμογές που έχουν ευαίσθητο χαρακτήρα πρέπει να αξιολογούν την **αξιοπιστία** πολλών εμπλεκόμενων φορέων. Όσον αφορά το Internet of Things, η αξιολόγηση της αξιοπιστίας των αισθητήρων και των δεδομένων των αισθητήρων είναι σημαντική. Οι κακοί κόμβοι αισθητήρων και τα λανθασμένα ή μη αξιόπιστα δεδομένα αισθητήρων μπορούν να οδηγήσουν σε καταστροφή. Τα δεδομένα μη αξιόπιστων αισθητήρων ενδέχεται να προέρχονται από αξιόπιστο κόμβο αισθητήρα. Η μη αξιόπιστη συμπεριφορά μπορεί να οφείλεται στη σκόπιμη κακή συμπεριφορά ή στα ακούσια λάθη-[12].

Ο **έλεγχος** παρακολουθεί την αλληλεπίδραση του χρήστη με το σύστημα. Τα περιβάλλοντα του Internet of Things πρέπει να γνωρίζουν πότε οι υπηρεσίες τους είναι προσβάσιμες, ποιος κάνει το αίτημα παροχής υπηρεσίων, πότε γίνεται το αίτημα. Οι πληροφορίες αυτές όχι μόνο θα βοηθήσουν στη διαχείριση της ασφάλειας, αλλά και στην αξιολόγηση του κινδύνου ασφάλειας. Σε περίπτωση παραβίασης της ασφάλειας, αυτές οι πληροφορίες μπορεί να βοηθήσουν στην αναγνώριση της οπής της ασφάλειας που υπάρχει στο σύστημα. Η διατήρηση ενός ίχνου ελέγχου στις υπηρεσίες του Internet of Things αποτελεί ένα δύσκολο έργο-[12].

3.2 ΑΣΦΑΛΕΙΑ ΣΤΗΝ ΑΡΧΙΤΕΚΤΟΝΙΚΗ

3.2.1 ΕΠΙΠΕΔΟ ΑΝΤΙΛΗΨΗΣ

Το επίπεδο αντίληψης αφορά κυριώς τη συλλογή πληροφοριών, την αντίληψη αντικειμένων και τον έλεγχο αντικειμένων. Μπορεί να χωριστεί σε δύο μέρη: κόμβος αντίληψης (αισθητήρες, ελεγκτές κ.λπ.) και δίκτυο αντίληψης που επικοινωνεί με το δίκτυο μεταφοράς. Ο κόμβος αντίληψης χρησιμοποιείται για την απόκτηση δεδομένων και τον έλεγχο δεδομένων, το δίκτυο αντίληψης στέλνει συλλεγμένα δεδομένα στην πύλη ή αποστέλλει οδηγίες ελέγχου στον ελεγκτή. Οι τεχνολογίες στρώματος αντίληψης περιλαμβάνουν τα RFID, WSNs, RSN, GPS, κλπ-[13].

3.2.1.1 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΗΣ RFID ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΛΥΣΕΙΣ

Η αναγνώριση ραδιοσυχνοτήτων (RFID) είναι μια τεχνολογία αυτόματης αναγνώρισης χωρίς επαφή, η οποία μπορεί να εντοπίσει αυτόματα το σήμα της ετικέτας προορισμού για να αποκτήσει σχετικά δεδομένα προσδιορίζοντας ότι η διαδικασία δεν απαιτεί χειροκίνητη παρέμβαση και μπορεί να λειτουργήσει σε σκληρά περιβάλλοντα. Ενώ η RFID χρησιμοποιείται ευρέως, δημιουργεί πολλά προβλήματα όπως αναφέρεται παρακάτω.

Ομοιόμορφη κωδικοποίηση Αυτή τη στιγμή δεν υπάρχει ενιαίο διεθνές πρότυπο κωδικοποίησης για την ετικέτα RFID. Τα σημαντικότερα πρότυπα είναι τα πρότυπα UID (Universal Identification) που υποστηρίζονται από την Ιαπωνία και το πρότυπο EPC (Electronic Product Code) που υποστηρίζεται από την Ευρωπαϊκή Ένωση. Δεδομένου ότι το ενιαίο πρότυπο δεν έχει ακόμη διαμορφωθεί, μπορεί να προκαλέσει προβλήματα που ο αναγνώστης δεν μπορεί να αποκτήσει πρόσβαση στις πληροφορίες της ετικέτας ή ενδέχεται να προκύψουν σφάλματα στη διαδικασία ανάγνωσης.

Conflict collision Πολλαπλές ετικέτες RFID μπορούν να μεταδίδουν πληροφορίες ταυτότητας στον αναγνώστη ταυτόχρονα, γεγονός που μπορεί να

προκαλέσει την αδυναμία λήψης των δεδομένων από τον αναγνώστη. Η χρήση της τεχνικής κατά της σύγκρουσης μπορεί να αποτρέψει την ταυτόχρονη μετάδοση πληροφοριών από τον αναγνώστη σε πολλαπλές ετικέτες. Το Conflict collision RFID μπορεί να χωριστεί σε δύο κατηγορίες, οι οποίες είναι συγκρούσιες ετικετών και σύγκρουση αναγνωστών. Όταν ένας μεγάλος αριθμός ετικετών βρίσκεται στο πεδίο εργασίας του αναγνώστη και ο αναγνώστης δεν μπορεί να έχει πρόσβαση στα δεδομένα σωστά, αυτό ονομάζεται σύγκρουση ετικετών. Το Internet of Things απαιτεί ευρύ φάσμα κάλυψης αισθητήρων RFID και το έργο συνεργασίας πολλών αναγνωστών είναι ιδιαίτερα σημαντικό, αλλά το πεδίο εργασίας του αναγνώστη επικαλύπτεται. Έτσι, οι πληροφορίες μπορεί να καταστούν περιττές, πράγμα που αυξάνει την επιβάρυνση για τη μετάδοση του δικτύου. Αυτό ονομάζεται σύγκρουση αναγνωστών.

Προστασία απορρήτου RFID Οι ετικέτες χαμηλού κόστους οδήγησαν σε περιορισμένους πόρους RFID, όπως η χαμηλή χωρητικότητα αποθήκευσης και οι αδύναμες υπολογιστικές δυνατότητες, απαιτεί έτσι ελαφρές λύσεις για την προστασία της ιδιωτικής ζωής, η οποία περιλαμβάνει την ιδιωτικότητα δεδομένων και την ιδιωτικότητα της τοποθεσίας. Όσον αφορά την ιδιωτικότητα δεδομένων, οι τεχνολογίες ασφάλειας και ιδιωτικού απορρήτου RFID μπορούν να χωριστούν σε δύο κατηγορίες: σχήματα βασισμένα σε φυσική μορφή και συστήματα με βάση τον κωδικό πρόσβασης, η προηγούμενη εντολή kill kill, ετικέτες μπλοκ, ετικέτες κλιπ, ετικέτες ψευδώνυμων, Faraday δίχτυα, παρεμβολές σήματος, ανάλυση ενέργειας κεραίας κλπ. Τα τελευταία περιλαμβάνουν σχέδια όπως κλειδαριές κατακερματισμού, τυχαία κλειδαριά, αλυσίδα κατακερματισμού, ανώνυμη ταυτότητα, επανακρυπτογράφηση. Οι διαφορετικές μορφές οργάνωσης για το διαδίκτυο απαιτούν διαφορετικούς τρόπους συμφωνίας προστασίας της ιδιωτικής ζωής. Μια συμβιβαστική λύση για τα ζητήματα απορρήτου δεδομένων είναι η αποθήκευση λιγότερο σημαντικών πληροφοριών στην ετικέτα RFID και η αποθήκευση σημαντικών πληροφοριών στην υπηρεσία επάνω επιπέδου. Όσον αφορά το απόρρητο της τοποθεσίας, αν και οι ετικέτες RFID δεν αποθηκεύουν σημαντικές πληροφορίες, οι hackers μπορούν ακόμα να λάβουν τις πληροφορίες ταυτότητας ετικέτας για τον εντοπισμό της θέσης της ετικέτας.

Διαχείριση της εμπιστοσύνης Στο Internet of Things, πρέπει να λάβουμε πιο σοβαρά υπόψη την ιδιωτική ζωή των κόμβων. Επομένως, πρέπει να εισαγάγουμε τη

διαχείριση εμπιστοσύνης στο σύστημα RFID του Internet of Things. Η διαχείριση της εμπιστοσύνης υπάρχει όχι μόνο ανάμεσα στους αναγνώστες και τις ετικέτες RFID, αλλά και μεταξύ των συσκευών ανάγνωσης και των σταθμών βάσης. Στον τομέα διαχείρισης εμπιστοσύνης, η τεχνολογία ψηφιακής υπογραφής έχει μεγάλη χρησιμότητα. Έχει χρησιμοποιηθεί για τον έλεγχο ταυτότητας δεδομένων, τον έλεγχο ταυτότητας συσκευών και την ανταλλαγή δεδομένων μεταξύ διαφορετικών εφαρμογών για μεγάλο χρονικό διάστημα. Οι κρυπτογραφικοί αλγόριθμοι και πρωτόκολλα διαδραματίζουν σημαντικό ρόλο για την τεχνολογία ψηφιακής υπογραφής. Ενώ οι τυπικοί κρυπτογραφικοί αλγόριθμοι και πρωτόκολλα απαιτούν χώρο αποθήκευσης και υπολογιστικούς πόρους περισσότερο από τους διαθέσιμους πόρους των ετικετών RFID, ο αλγόριθμος ελέγχου ταυτότητας RFID πρέπει όχι μόνο να λαμβάνει υπόψη τα θέματα ασφάλειας και προστασίας της ιδιωτικής ζωής, αλλά και την αποθήκευση ετικετών και την υπολογιστική ισχύ.-[13]

3.2.1.2 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΤΕΧΝΙΚΕΣ ΛΥΣΕΙΣ ΣΕ WSNs

Τα WSNs είναι δίκτυα αυτο-οργάνωσης με δυναμική τοπολογία δικτύου και ευρέως διανεμημένα ασύρματα δίκτυα πολλαπλών λόγων. Λαμβάνοντας υπόψην το κόστος, τα WSNs έχουν περιορισμένους πόρους, συμπεριλαμβανομένης της μικρής ποσότητας αποθήκευσης, κακής ικανότητας υπολογισμού, στενού εύρους ανίχνευσης, ο οποίος οδηγεί σε μια σειρά κινδύνων ασφάλειας δικτύου. Ένας στόχος του στρώματος αντίληψης είναι η πλήρης εφαρμογή του περιβάλλοντος. Περιορισμένη εμβέλεια ενός μοναδικού κόμβου καθιστά τη δικτυακή δομή πολύπλοκη με μεγάλο αριθμό κόμβων ανίχνευσης. Το επίπεδο αντίληψης, που είναι για τη συλλογή πληροφοριών, είναι προσανατολισμένο στα δεδομένα. Έτσι για την έρευνα WSNs θα επικεντρωθούμε στην ανάλυση δεδομένων. Στη διαδικασία συλλογής δεδομένων, το μήνυμα ενδέχεται να υποβληθεί σε υποκλοπή, κακόβουλη δρομολόγηση, παραβίαση μηνυμάτων και άλλα ζητήματα ασφάλειας, τα οποία επηρεάζουν την ασφάλεια ολόκληρου του Internet of Things. Τα θέματα ασφάλειας δεδομένων μπορούν να συνοψιστούν σε εμπιστευτικότητα δεδομένων, αυθεντικότητα δεδομένων και ακεραιότητα δεδομένων. Αυτοί οι τέσσερις τύποι ζητημάτων ασφαλείας μπορούν να

επιλυθούν σε τέσσερις πτυχές: κρυπτογραφικούς αλγόριθμους, διαχείριση κλειδιών, ασφαλή δρομολόγηση, εμπιστοσύνη κόμβων.

Κρυπτογραφικοί αλγόριθμοι σε WSNs Οι κύριοι τομείς εφαρμογής του ασύρματου δικτύου αισθητήρων είναι ευρείς, αυτό απαιτεί υψηλή ασφάλεια δεδομένων, συμπεριλαμβανομένης της εμπιστευτικότητας των δεδομένων και της ακεραιότητας των δεδομένων, τα οποία μπορούν να επιλυθούν με κρυπτογράφηση δεδομένων. Ο κρυπτογραφικός αλγόριθμος είναι μια πολύ σημαντική μέθοδος για να διασφαλιστεί η ασφάλεια του δικτύου του φυσικού επιπέδου και είναι βασική για την εξασφάλιση της ασφάλειας ολόκληρης της υπηρεσίας δικτύου.

Διαχείριση κλειδιών σε WSNs Η διαχείριση κλειδιών είναι ένα βασικό ζήτημα που αναμένει να λυθεί για την ασφάλεια του ασύρματου δικτύου αισθητήρων. Επίσης, είναι ένας από τους βασικούς χώρους για την αντιμετώπιση άλλων ζητημάτων ασφάλειας. Η διαχείριση κλειδιού περιλαμβάνει τη διαδικασία δημιουργίας μυστικών κλειδιών, διανομής, αποθήκευσης, ενημέρωσης και καταστροφής, όπου η βασική διανομή είναι το πιο σημαντικό θέμα στη διαχείριση κλειδιών. Η διανομή των κλειδιών, συμπεριλαμβανομένης της διανομής του δημόσιου κλειδιού και του μυστικού κλειδιού, αφορά τη διασφάλιση ότι το κλειδί θα μεταφερθεί και θα αποσταλεί ασφαλώς στους νόμιμους χρήστες. Το κύριο πρόβλημα είναι το πώς θα σχεδιαστεί ένα ελαφρύ σύστημα διανομής μυστικού κλειδιού με βάση τους κόμβους αισθητήρων με περιορισμένους πόρους, υποστηρίζοντας όλα τα επίπεδα των πρωτοκόλλων, των εφαρμογών και της ασφάλειας των υπηρεσιών.

Ασφαλή πρωτόκολλα δρομολόγησης για WSNs Η τεχνολογία δρομολόγησης στρώματος δικτύου παίζει βασικό ρόλο στο ασύρματο δίκτυο αισθητήρων. Οι επιθέσεις κατά του δρομολογίου θα οδηγήσουν άμεσα στην κατάρρευση του δικτύου. Επομένως, η εγκατάσταση ασφαλούς και αποτελεσματικού πρωτοκόλλου δρομολόγησης αποτελούσε πάντα το επίκεντρο της έρευνας στο ασύρματο δίκτυο αισθητήρων. Δεδομένου ότι ο περιορισμός της ισχύος, της ικανότητας υπολογισμού και της χωρητικότητας αποθήκευσης δεν είναι δυνατό να εφαρμοστούν σε ασύρματα δίκτυα αισθητήρων, ακόμη και τα πρωτόκολλα δρομολόγησης που μελετώνται συχνά στο δίκτυο Ad hoc αντιμετωπίζουν νέο πρόβλημα στα WSNs.

Έλεγχος εμπιστοσύνης των κόμβων σε WSNs Το WSN έχει πολλά ειδικά χαρακτηριστικά, όπως οι περιορισμένοι πόροι των κόμβων αισθητήρων, η εύκολη σύλληψη των κόμβων και ο μοναδικός τρόπος επικοινωνίας (οι κόμβοι των αισθητήρων συλλέγουν πληροφορίες και αναφέρουν στον σταθμό βάσης) κλπ. Αυτά τα χαρακτηριστικά καθιστούν το δίκτυο των αισθητήρων πιο ευάλωτο σε διάφορες επιθέσεις. Ωστόσο, το WSN δεν μπορεί να εγγυηθεί την ασφάλεια ασύρματων δικτύων αισθητήρων βασιζόμενη αποκλειστικά σε μηχανισμούς κωδικού πρόσβασης και κρυπτογραφικούς αλγόριθμους. Πρέπει να εισαγάγουμε μηχανισμό διαχείρισης εμπιστοσύνης για να εξασφαλίσουμε την ασφάλεια των ασύρματων δικτύων αισθητήρων.-[13]

3.2.2 ΕΠΙΠΕΔΟ ΜΕΤΑΦΟΡΑΣ

Το επίπεδο μεταφοράς παρέχει κατά κύριο λόγο περιβάλλον πρόσβασης για το επίπεδο αντίληψης, αντίληψη της μετάδοσης και αποθήκευσης πληροφοριών και φόρτωση του επιπέδου εφαρμογής σε άλλες συναφείς επιχειρήσεις. Το επίπεδο μεταφοράς μπορεί να χωριστεί σε τρία επίπεδα ανάλογα με τη λειτουργία: το δίκτυο πρόσβασης, το κεντρικό δίκτυο και την τοπική περιοχή. Είναι ένας συνδυασμός ποικιλίας ετερογενών δικτύων.-[13]

3.2.2.1 ΛΕΙΤΟΥΡΓΙΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΕΠΙΠΕΔΟΥ ΜΕΤΑΦΟΡΑΣ ΤΩΝ ΘΕΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Δίκτυο πρόσβασης Το δίκτυο πρόσβασης παρέχει περιβάλλον πρόσβασης για το επίπεδο αντίληψης. Το επίπεδο αντίληψης και το κεντρικό δίκτυο θα έχουν προβλήματα ασφαλείας όταν το επίπεδο αντίληψης αποκτά πρόσβαση στο κεντρικό δίκτυο. Το δίκτυο πρόσβασης περιλαμβάνει ασύρματα δίκτυα, δίκτυο Ad hoc κ.λπ.

Κύριο δίκτυο Το κύριο δίκτυο των διαφόρων παραμέτρων είναι κυρίως υπεύθυνο για τη μετάδοση δεδομένων. Το κύριο δίκτυο είναι βασικά Διαδίκτυο. Δεδομένου ότι ένας μεγάλος αριθμός κόμβων χρειάζεται πρόσβαση στο Internet, το οποίο απαιτεί πολλές διευθύνσεις IP, το παραδοσιακό Internet με βάση το

πρωτόκολλο IPv4 δεν είναι σε θέση να ανταποκριθεί σε τόσους κόμβους αισθητήρων, οπότε η επόμενη γενιά του Διαδικτύου που βασίζεται στο IPv6 μπορεί να λύσει αυτό το πρόβλημα. Προκειμένου να χρησιμοποιηθούν δίκτυα αισθητήρων IPv6 με χαμηλή κατανάλωση ενέργειας για ετερογενή ολοκλήρωση, μπορούμε να χρησιμοποιήσουμε την τεχνολογία 6Lowpan για να λύσουμε το πρόβλημα των διευθύνσεων IPv6.

Τοπικό δίκτυο Στο Internet of Things, το τοπικό δίκτυο πρέπει να λαμβάνει σοβαρά υπόψη τη διαρροή δεδομένων και τα ανεξάρτητα θέματα ασφαλείας του διακομιστή. Για να υιοθετήσουμε τα ακόλουθα μέτρα, μπορούμε να ενισχύσουμε τη διαχείριση της ασφάλειας στο τοπικό δίκτυο. Ο έλεγχος πρόσβασης στο δίκτυο είναι για να διασφαλιστεί η νόμιμη χρήση των πόρων του δικτύου, η οποία αποτελεί την κύρια στρατηγική προστασίας της ασφάλειας δικτύων. Άλλοι, όπως η άρνηση του κακόβουλου κώδικα, το κλείσιμο ή η διαγραφή περιττών υπηρεσιών συστήματος και η συνεχής ενημέρωση των ενημερωτικών εκδόσεων του λειτουργικού συστήματος, χρησιμοποιώντας έναν ασφαλή κωδικό πρόσβασης και τον κωδικό πρόσβασης, μπορούν να χρησιμοποιηθούν για την προστασία του τοπικού δικτύου Internet of Things.-[13]

3.2.2.2 ΚΟΙΝΑ ΘΕΜΑΤΑ ΤΗΣ ΑΝΑΛΥΣΗΣ ΤΟΥ ΕΠΙΠΕΔΟΥ ΜΕΤΑΦΟΡΑΣ

Συγκριτικά θέματα ετερογενών δικτύων σύγκλισης της ανάλυσης επιπέδου μεταφοράς Το επίπεδο μεταφοράς του Internet of Things αποτελείται από μια ποικιλία ετερογενών δικτύων (όπως το Ad hoc δίκτυο, το Διαδίκτυο, τα δίκτυα 3G, κ.λπ.), έτσι υπάρχουν ζητήματα ασφάλειας ετερογενούς σύντηξης. Προκειμένου να επιλυθούν τα ζητήματα ασφάλειας της ετερογενούς ενσωμάτωσης, η δικτύωση έλαβε τους ακόλουθους τέσσερις τρόπους: σφιχτή σύζευξη, χαλαρή σύζευξη, ACENET, AN net, κ.λπ.

Επίπεδα επίθεσης της ανάλυσης του επιπέδου μεταφοράς Η επίθεση DDoS είναι η πιο συνηθισμένη επίθεση δικτύου, ειδικά στο Internet of Things. Λόγω της ετερογένειας και της πολυπλοκότητας του δικτύου Internet of Things, το επίπεδο μεταφοράς είναι ευάλωτο σε επίθεση. Συνήθως η λύση είναι να αναβαθμιστεί το σύστημα και να χρησιμοποιηθεί DDoS επίθεση ανίχνευσης και πρόληψης. Επί του παρόντος, δεν υπάρχει καλή λύση για την επίλυση της επίθεσης DDoS δικτύου.-[13]

3.2.3 ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΩΝ

3.2.3.1 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΕΠΙΠΕΔΟΥ ΥΠΟΣΤΗΡΙΞΗΣ ΕΦΑΡΜΟΓΗΣ

Το επίπεδο υποστήριξης εφαρμογής, ένα επίπεδο πάνω από το επίπεδο μεταφοράς, υποστηρίζει κάθε είδους επιχειρηματικές υπηρεσίες και πραγματοποιεί έξυπνο υπολογισμό και κατανομή πόρων κατά την επιλογή, την παραγωγή και την επεξεργασία δεδομένων. Κατά τη διάρκεια ολόκληρης της διαδικασίας, το επίπεδο υποστήριξης εφαρμογών μπορεί να αναγνωρίσει έγκυρα δεδομένα, δεδομένα ανεπιθύμητης αλληλογραφίας, ακόμη και κακόβουλα δεδομένα και να τα φιλτράρει εγκαίρως. Το επίπεδο υποστήριξης εφαρμογών μπορεί να οργανωθεί με διάφορους τρόπους σύμφωνα με διαφορετικές υπηρεσίες. Συνήθως περιλαμβάνει ενδιάμεσο λογισμικό, M2 M, πλατφόρμα υπολογιστικού νέφους και πλατφόρμα υποστήριξης υπηρεσιών.

Απειλές ασφαλείας Σύμφωνα με έρευνα της IDC, το ζήτημα της ασφάλειας είναι η πιο ενδιαφέρουσα πτυχή του υπολογιστικού νέφους. Όλοι οι συμμετέχοντες έχουν ανησυχίες για τη τεχνική ασφάλειας. Στην πραγματικότητα, η πλατφόρμα υπολογιστικού νέφους κρυπτογραφεί τα δεδομένα και δημιουργεί αντίγραφα ασφαλείας των δεδομένων των χρηστών, τα οποία δεν θα διαγραφούν μέχρι ένα συγκεκριμένο χρονικό διάστημα. Επομένως, πρέπει κάποιος να πραγματοποιήσει εκτίμηση κινδύνου και να καταλήξει σε σχέδια έκτακτης ανάγκης πριν τοποθετήσει τα δεδομένα του στο νέφος.

Διακοπή υπηρεσίας και ζήτημα επίθεσης Σύμφωνα με την εμπειρία του παρελθόντος της υπηρεσίας υπολογιστικού νέφους, συμβαίνουν πάντα κάποιες συχνές διακοπές υπηρεσίας, συμπεριλαμβανομένης της δημιουργίας αντιγράφων ασφαλείας δεδομένων, τερματισμού συστήματος και εκτός σύνδεσης δεδομένων. Ευτυχώς αυτές οι αποτυχίες μπορούν να προβλεφθούν.

Διερεύνηση ζητημάτων ελέγχου Στο υπολογιστικό νέφος, ο υπολογισμός, η αποθήκευση, οι υπηρεσίες εύρους ζώνης δικτύου μπορούν να προσπελαστούν σε

παγκόσμιο επίπεδο, αλλά οι πληροφορίες λογαριασμού που παρέχονται από τους χρήστες μπορεί να είναι πλαστές. Επιπλέον, διαφορετικές χώρες και περιφέρειες έχουν διαφορετικές απαιτήσεις για την απόκτηση αποδεικτικών στοιχείων για παράνομες συμπεριφορές, επομένως τα εγκλήματα δικτύου που βασίζονται στην πλατφόρμα υπολογιστικού νέφους είναι δύσκολο να εντοπιστούν. Η ανίχνευση εγκλημάτων μπορεί να είναι πιο δύσκολη όταν οι πόροι της πλατφόρμας προέρχονται από ποικίλους προμηθευτές τρίτων μερών πολλαπλών επιπέδων.-[13]

3.2.3.2 ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ IoT ΕΦΑΡΜΟΓΩΝ

Το επίπεδο εφαρμογής περιλαμβάνει ολοκληρωμένες ή μεμονωμένες ειδικές εφαρμογές εφαρμογών. Τα ζητήματα ασφάλειας που αντιμετωπίζει δεν μπορούν να λυθούν σε άλλα επίπεδα, όπως η προστασία της ιδιωτικής ζωής, η οποία δεν εμφανίζεται στο επίπεδο αντίληψης και στο επίπεδο μεταφοράς, αλλά μπορεί να γίνει η πραγματική ζήτηση σε ορισμένα ειδικά περιβάλλοντα του επιπέδου εφαρμογής ή μπορεί επίσης να ονομαστεί ειδική ζήτηση ασφάλειας του στρώματος εφαρμογής.

Ευφυής μεταφορά Το Internet of Things χρησιμοποιείται ευρέως στη βιομηχανία εφοδιαστικής. Η τεχνολογία της πληροφορικής, η ολοκληρωμένη διαχείριση της εφοδιαστικής και η παρακολούθηση της διαδικασίας μπορούν όχι μόνο να βελτιώσουν την αποδοτικότητα των επιχειρήσεων εφοδιαστικής και να βοηθήσουν στον έλεγχο του κόστους εφοδιαστικής, αλλά και να βελτιώσουν το επίπεδο ενημέρωσης της επιχείρησης. Η εφαρμογή του ευφυούς συστήματος εφοδιαστικής περιλαμβάνει τη λήψη, τη μεταφορά, τη διαλογή, την αποστολή, τη μεταφορά και άλλα συναφή υποσυστήματα. Κάθε υποσύστημα επιτυγχάνει διαχείριση αποθεμάτων, παράδοση αγαθών, αυτοματοποιημένη χρέωση και άλλες επιχειρηματικές λειτουργίες.-[13]

ΚΕΦΑΛΑΙΟ 4:
ΣΥΜΠΕΡΑΣΜΑΤΑ

4.1 ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Το Internet of Things έχει πληθώρα πλεονεκτημάτων. Μερικά από αυτά παρουσιάζονται στη συνέχεια:

1. Δεδομένα: Όσο περισσότερες είναι οι πληροφορίες, τόσο πιο εύκολο είναι να ληφθεί σωστή απόφαση για κάποιο ζήτημα τις καθημερινότητας και κατ' επέκταση να εξοικονομήσει χρόνο-[4].
2. Παρακολούθηση: Οι υπολογιστές ελέγχουν τόσο την ποιότητα όσο και τη βιωσιμότητα των πραγμάτων στο σπίτι. Η γνώση της ημερομηνίας λήξης των προϊόντων που υπάρχου στο σπίτι προτού να τα καταναλώσει βελτιώνει την ασφάλεια και την ποιότητα ζωής-[4].
3. Χρόνος: Ο χρόνος που εξοικονομείται από την παρακολούθηση των αντικειμένων στο σπίτι είναι πολύ μεγάλος-[4].
4. Χρήματα: Αυτό αποτελεί το μεγαλύτερο πλεονέκτημα, καθώς αυτή η τεχνολογία μπορεί να αντικαταστήσει τους ανθρώπου που εργάζονται στην παρακολούθηση και στην συντήρηση των προϊόντων-[4].

4.2 ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Όπως είναι λογικό υπάρχουν και αρκετά μειονεκτήματα, η διαπίστωση των οποίων συντελεί στην βελτίωση του Internet of Things. Μερικά από τα μειονεκτήματα περιγράφονται παρακάτω:

1. Συμβατότητα: Μέχρι σήμερα, δεν υπάρχει πρότυπο για την τοποθέτηση ετικετών και την παρακολούθηση με αισθητήρες. Απαιτείται μια ενιαία ιδέα όπως το Universal Serial Bus (USB) ή το Bluetooth, που δεν είναι τόσο δύσκολο να υλοποιηθούν-[4].
2. Πολυπλοκότητα: Υπάρχει μεγάλη πιθανότητα για την αποτυχία των πολύπλοκων συστημάτων-[4].
3. Προστασία προσωπικών δεδομένων: Η προστασία των προσωπικών δεδομένων αποτελεί ένα μεγάλο πρόβλημα στο Διαδίκτυο. Όλα τα δεδομένα πρέπει να είναι κρυπτογραφημένα, έτσι ώστε να γίνονται γνωστά μόνο σε όσους χρειάζεται-[4].
4. Ασφάλεια: Υπάρχει πιθανότητα να παραβιαστεί το λογισμικό και κατά συνέπεια να καταχραστούν τα προσωπικά δεδομένα. Αυτή η πιθανότητα είναι μεγάλη-[4].

4.3 ΣΥΜΠΕΡΑΣΜΑΤΑ

Το Internet of Things είναι η έννοια στην οποία ο εικονικός κόσμος της τεχνολογίας πληροφοριών συνδέεται με τον πραγματικό κόσμο των πραγμάτων. Οι τεχνολογίες του Internet of Things, όπως RFID και Sensor, κάνουν τη ζωή μας καλύτερη και πιο άνετη. Η υλοποίηση του είναι πολύ κοντά καθώς οι περισσότερες αναγκαίες τεχνολογικές εξελίξεις που απαιτούνται έχουν ήδη πραγματοποιηθεί. Οι κύριοι λόγοι για τους οποίους δεν έχει εφαρμοστεί πραγματικά είναι ο αντίκτυπος που θα έχει αυτό στον νόμο, στη δεοντολογία, στην ασφάλεια και στον κοινωνικό τομέα. Οι εργαζόμενοι θα μπορούσαν πιθανώς να το καταχραστούν, οι χάκερ να έχουν πρόσβαση, οι εταιρείας να μην θέλουν να μοιραστούν τα δεδομένα τους και οι άνθρωποι να είναι δυσαρεστημένοι από την απουσία του ιδιωτικού απορρήτου.

Αξιοσημείωτο είναι ότι χρησιμοποιώντας αυτό το είδος προϊόντων το κέρδος είναι μεγάλος καθώς και η εξοικονόμηση χρόνου. Έτσι, όλο και περισσότεροι άνθρωποι ακολουθούν την τάση να προμηθευτούν αυτά τα προϊόντα, αλλά και όλο και περισσότερες εταιρείες οδηγούνται στην δημιουργία τέτοιων προϊόντων. Δυστυχώς το κόστος προμήθειας είναι υψηλό, αλλά η επένδυση αυτή αποδεικνύεται καλή.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]http://www.samsung.com/gr/discover/new/the-internet-of-things-smart-home/

[2]https://www.intelligentmedia.gr/item/internet-of-things-%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-%CE%BA%CE%B1%CE%B9-%CF%80%CF%89%CF%82-%CE%BC%CF%80%CE%BF%CF%81%CE%B5%CE%AF-%CE%BD%CE%B1-%CE%B1%CE%BB%CE%BB%CE%AC%CE%BE%CE%B5%CE%B9-%CF%84%CE%B7-%CE%B6%CF%89%CE%AE-%CE%BC%CE%B1%CF%82

[3]http://osarena.net/internet-things-diadiktyo-ton-pragmaton-ti-einai-ayto

[4]https://e27.co/advantages-disadvantages-internet-things-20160615/

[5]https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

[6] https://www.hindawi.com/journals/jece/2017/9324035/

[7]http://www.channelfutures.com/best-practices/four-internet-things-connectivity-models-explained

[8]https://www.kernelsphere.com/four-internet-things-communications-models/

[9]https://www.slideshare.net/Cisco/building-the-internet-of-things-an-iot-reference-model

[10]http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

[11]http://www.businessinsider.com/internet-of-things-devices-applications-examples-2016-8

[12]https://pdfs.semanticscholar.org/ec90/b77e4734f22782b14776918c228e5b707297.pdf

[13]http://csi.dgist.ac.kr/uploads/Seminar/1407_IoT_SSH.pdf