

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ



Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

Διπλωματική Εργασία

"Το διαδίκτυο των πραγμάτων- Internet of Things"

Σπουδαστής : Μπόικος Ανδρέας-Σταμάτιος

Επιβλέπων Καθηγητής: Βλάμος Παναγιώτης

Κέρκυρα, 2019

Περιεχόμενα

Ευρετήριο Εικόνων.....	5
ΠΕΡΙΛΗΨΗ	7
Λέξεις Κλειδιά.....	7
ABSTRACT	8
Keywords	8
Κεφάλαιο 1:Εισαγωγή στο Internet of Things.....	10
1.1:Εισαγωγή	10
1.2: Radio frequency identification (RFID)	12
1.3: Ασύρματα Δίκτυα Αισθητήρων	15
1.4: Επικοινωνία Συσκευών.....	18
1.5 Cloud Computing	21
Κεφάλαιο 2: Ασφάλεια & Ιδιωτικότητα στο IoT.....	24
2.1:Εισαγωγή στην Ασφάλεια & Ιδιωτικότητα.....	24
2.2: Ευπάθειες στο IoT	25
2.3: Βασικές Απειλές στο IoT	26
2.3.1: Προστασία Ενάντια στις Απειλές	29
2.4: Τεχνολογίες Ασφάλειας & Ιδιωτικότητας	30
2.4.1: Πρότυπα ασφαλείας RFID	31
2.4.2: Πρωτόκολλα Ασφαλείας στο IoT.....	31
2.4.3: Τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET).....	32
2.5: Συμπεράσματα	34
Κεφάλαιο 3:Εφαρμογές του Internet of Things	35
3.1: Έξυπνη Πόλη.....	35
3.2: Έξυπνο Περιβάλλον.....	38
3.3: IoT στην Υγεία.....	39
3.4: Έξυπνο Σπίτι.....	41
3.5: Smart Farming	44
3.5.1: Εφαρμογές στη Γεωργία.....	44
3.5.2: Εφαρμογές στην Κτηνοτροφία.....	45
3.6: Smart Water	46
3.7: Smart Metering	47
3.8: Smart Retail	48
3.9: Εφαρμογές στη Βιομηχανία (Industrial IoT).....	50

3.10: Εφαρμογές για καταστάσεις εκτάκτου ανάγκης και ασφάλεια περιοχών	51
3.11: Συμπεράσματα	52
Κεφάλαιο 4: Υλοποίηση σε Arduino.....	53
4.1: Arduino	53
4.2: Διαδικασία Υλοποίησης	54
4.2.1: Κώδικας για Arduino	55
4.3: Αποτελέσματα	58
4.4: Συμπεράσματα	59
Κεφάλαιο 5: Internet of Bio-Nano Things	60
5.1: Νανοτεχνολογία	60
5.2: Νανοϊατρική	61
5.3: Internet of Bio-Nano Things	64
5.4: Συμπεράσματα	67
Κεφάλαιο 6: Έρευνα σχετικά με το Internet of Things.....	69
6.1: Εισαγωγή	69
6.2: Ερευνητικά ερωτήματα	69
6.3: Αποτελέσματα Έρευνας	70
6.4: Στατιστική Ανάλυση	76
6.5: Συμπεράσματα	79
Βιβλιογραφία	80

Ευρετήριο Εικόνων

Εικόνα 1.1: <i>Passive RFID tag & RFID reader</i>	12
Εικόνα 1.2: Παράδειγμα RFID ετικετών σε ρούχα και σε φάρμακα.....	14
Εικόνα 1.3: Αισθητήρες συλλέγουν δεδομένα και τα αποστέλλουν στην πόλη	15
Εικόνα 1.4: Οι αισθητήρες κάνουν μετρήσεις περιβαλλοντολογικών συνθηκών σε δάσος.....	16
Εικόνα 1.5: Τα δεδομένα των αισθητήρων του ανθρώπινου σώματος στέλνονται μέσω του διαδικτύου προς εξέταση.....	17
Εικόνα 1.6: Απεικόνιση επικοινωνίας H2H, H2M & M2M	18
Εικόνα 1.7: Παράδειγμα επικοινωνίας device-device.....	19
Εικόνα 1.8: Παράδειγμα επικοινωνίας device-cloud.....	19
Εικόνα 1.9: Παράδειγμα επικοινωνίας device-gateway.....	20
Εικόνα 1.10: Παράδειγμα επικοινωνίας back-end-data.....	21
Εικόνα 1.11: Οι υπηρεσίες συνδέονται στο Cloud και ανταλλάσσουν δεδομένα μεταξύ τους.....	22
Εικόνα 2.1: Ο κακόβουλος χρήστης κρύβει τον σαρωτή & τον τοποθετεί κοντά στο θύμα έτσι ώστε να κλέβει ασύρματα τις πληροφορίες της κάρτας πληρωμών του θύματος.....	27
Εικόνα 2.2: Τι θα συνέβαινε αν το ransomware κλείδωνε όλες τις έξυπνες συσκευές ενός σπιτιού?.....	29
Εικόνα 3.1: Αισθητήρας τοποθετημένος σε κάδο για την παρακολούθηση των απορριμμάτων.....	36
Εικόνα 3.2: Έξυπνο φανάρι στη Βαρκελώνη.....	37
Εικόνα 3.3: Η πλατφόρμα Intel Galileo Generation 2.....	40
Εικόνα 3.4: Ο έξυπνος θερμοστάτης Tado.....	42
Εικόνα 3.5: Η έξυπνη κάμερα Nest Hello	43
Εικόνα 3.6: Η τοποθεσία του πληθυσμού του κοπαδιού των αγελάδων αποτυπώνεται στην εφαρμογή Cow Tracking.....	45
Εικόνα 3.7: Το ποσοστό του νερού της δεξαμενής στέλνεται μέσω internet σε Smartphone.....	47
Εικόνα 3.8: Το σύστημα Reji-Robo.....	49
Εικόνα 3.9: Το σύστημα ανίχνευσης ραδιενέργειας “RadWall”	51

Εικόνα 4.1: Η πλακέτα <i>Arduino Mega</i>	53
Εικόνα 4.2: Το κύκλωμα της υλοποίησης, συνδεδεμένο με το <i>Arduino Uno</i>	54
Εικόνα 4.3: Οι θερμοκρασίες του περιβάλλοντος αποτυπώνονται στην εφαρμογή του <i>Arduino</i>	58
Εικόνα 4.4: Με την προσθήκη πάγου στο <i>Thermistor</i> η θερμοκρασία πέφτει άμεσα.....	58
Εικόνα 4.5: Εμφάνιση των θερμοκρασιών σε Κελσίου, Φάρεναιτ και Κέλβιν.....	59
Εικόνα 5.1: Σύγκριση μεγεθών της νανοκλίμακας σε σχέση με μεγαλύτερα μεγέθη.....	60
Εικόνα 5.2 Το ηλεκτρονικό μικροσκόπιο <i>SPM</i> , το οποίο ανακαλύφθηκε το 1981.....	61
Εικόνα 5.3: Η βασική αρχιτεκτονική του <i>IoNT</i> στον τομέα της ιατρικής.....	65

ΠΕΡΙΛΗΨΗ

Η εργασία αυτή έχει ως στόχο να μελετήσει την τεχνολογία του Internet of Things, τις λύσεις που μπορεί να προσφέρει στους τελικούς χρήστες αλλά και τους πιθανούς κινδύνους που εμπεριέχονται σε αυτό. Πιο συγκεκριμένα στο πρώτο κεφάλαιο γίνεται εισαγωγή στα Δίκτυα Αισθητήρων καθώς και στα RFID chips αλλά και στο Cloud Computing. Στη συνέχεια στο δεύτερο κεφάλαιο δίνεται έμφαση σε θέματα ασφάλειας και ιδιωτικότητας όσον αφορά το IoT. Εκεί αναλύονται οι σημαντικότερες ευπάθειες, απειλές αλλά και λύσεις ασφαλείας σχετικά με την προστασία των χρηστών. Στο τρίτο κεφάλαιο γίνεται προσπάθεια προσέγγισης όλου του φάσματος των σημερινών εφαρμογών του Internet of Things. Ύστερα, στο τέταρτο κεφάλαιο παρουσιάζεται μια εφαρμογή μετάδοσης θερμοκρασιών του περιβάλλοντος στον Η/Υ με το Arduino Uno. Η αποστολή των θερμοκρασιών μέσω του Cloud μπορεί να εφαρμοστεί σε αρκετές εφαρμογές του IoT. Στο πέμπτο κεφάλαιο γίνεται αναφορά σε βασικές αρχές της νανοτεχνολογίας και στο Internet of Bio-Nano Things. Το τελευταίο μπορεί να συνεισφέρει στον τομέα της ιατρικής και στην προσπάθεια θεραπείας και μελέτης αρκετών ασθενειών. Τέλος, στο έκτο κεφάλαιο γίνεται έρευνα έτσι ώστε αποσαφηνιστούν οι αντιλήψεις των χρηστών σχετικά με το IoT, την ασφάλεια και την ιδιωτικότητα σε αυτό αλλά και τις λύσεις που μπορεί να προσφέρει στον τομέα της υγείας.

Λέξεις Κλειδιά

Δίκτυα Αισθητήρων, RFID, IoT, Cloud, Ασφάλεια, Ιδιωτικότητα, Arduino, Thermistor, Νανοτεχνολογία, Internet of Bio-Nano Things.

ABSTRACT

This work aims to study the Internet of Things technology, the solutions it can offer end users, and the potential risks involved in it. More specifically, the first chapter introduces in Sensor Networks as well as RFID chips and Cloud Computing. Then, the second chapter highlights security and privacy issues with regard to IoT. There are analyzed the major vulnerabilities, threats and security solutions related to user protection. The third chapter attempts to approach the whole range of current Internet of Things applications. Then, in the fourth chapter there is presented an application of ambient temperature transmission to the PC with the Arduino Uno. Temperatures from Cloud can be applied to several IoT applications. In the fifth chapter, reference is made to basic principles of nanotechnology and the Internet of Bio-Nano Things. The latter may contribute to the field of medicine and the treatment and study of several diseases. Finally, research is being done in the sixth chapter to clarify users' perceptions of IoT, security and privacy, as well as the solutions it can offer to the health sector.

Keywords

Sensor Networks, RFID, IoT, Cloud, Security, Privacy, Arduino, Thermistor, Nanotechnology, Internet of Bio-Nano Things.

Κεφάλαιο 1:Εισαγωγή στο Internet of Things

1.1:Εισαγωγή

Σε έναν κόσμο που συνεχώς εξελίσσεται το Διαδίκτυο των πραγμάτων (IoT) αποτελεί κατά κάποιον τρόπο ένα μονοπάτι σε έναν έξυπνο κόσμο στον οποίο όλα τα αντικείμενα της καθημερινότητας μας μπορούν να συνδεθούν και να αλληλεπιδράσουν μέσω του διαδικτύου. Επιδιώκει να διευκολύνει τους χρήστες κάνοντας όλες ή μεγάλο μέρος των διεργασιών τους αυτόματα. Αναλυτικότερα, γίνεται κατανοητό ότι με την διάχυτη υπολογιστική (ubiquitous computing), ο υπολογιστής θα μπορεί να ενσωματωθεί παντού και θα προγραμματιστεί να δράσει αυτόματα χωρίς χειροκίνητη ενεργοποίηση. (Chaouchi,2010) Ο όρος "Ιντερνετ των πραγμάτων" επινοήθηκε από τον Kevin Ashton το 1999, ο οποίος για την περιγραφή του προτιμούσε τη φράση "Internet for things". Ο Ashton θεωρούσε την αναγνώριση ραδιοσυχνοτήτων (RFID) ως απαραίτητη για το Διαδίκτυο των πραγμάτων, που θα επέτρεπε στους υπολογιστές να διαχειρίζονται όλα τα μεμονωμένα πράγματα. Σήμερα οι υπολογιστές και το Διαδίκτυο κατακλύζονται από τεράστιο πλήθος δεδομένων και πληροφοριών. Σχεδόν όλα τα περίπου 50 petabytes των δεδομένων που είναι διαθέσιμα στο Διαδίκτυο συλλέχθηκαν και δημιουργήθηκαν αρχικά από ανθρώπους, πληκτρολογώντας ή πιέζοντας ένα πλήκτρο, τραβώντας μια ψηφιακή εικόνα ή σαρώνοντας ένα bar code. Η τεχνολογία των RFID και των αισθητήρων επιτρέπει στους υπολογιστές να παρατηρούν, να αναγνωρίζουν και να κατανοούν τον κόσμο - χωρίς τους περιορισμούς των δεδομένων που έχουν εισαχθεί από τον άνθρωπο. (Ashton,2009) Στο IoT, τα περιβαλλοντικά και καθημερινά αντικείμενα ή "μηχανές" ενισχύονται με την τεχνολογία πληροφορικής και επικοινωνίας . Σε αυτό το πλαίσιο, οι ασύρματες και οι ενσύρματες τεχνολογίες παρέχουν ήδη τις δυνατότητες επικοινωνίας και τις αλληλεπιδράσεις, καλύπτοντας ποικίλες υπηρεσίες βασισμένες σε προσωπικές συναλλαγές, που αφορούν αλληλεπιδράσεις προσώπου με μηχανή, μηχανή με πρόσωπο ή αλληλεπίδραση μηχανής με μηχανή. Οι υπηρεσίες με βάση το IoT θα παρέχουν περισσότερη αυτοματοποίηση διαφόρων εργασιών γύρω από ανθρώπους και συναφή αντικείμενα, προκειμένου να οικοδομηθεί ένας έξυπνος κόσμος που αφορά ακόμα και το γραφείο ή το σπίτι και θα είναι διάχυτο γύρω από τους ανθρώπους . Οι περισσότερες από αυτές τις υπηρεσίες θα βασίζονται στην παρακολούθηση των συνδεδεμένων αντικειμένων. Το γεγονός αυτό μπορεί να βρει εφαρμογή στο πλαίσιο της αποφυγής της κλιματικής αλλαγής όπου νέες εφαρμογές θα εγκατασταθούν σε αντικείμενα προκειμένου να δράσουν προς ατή την κατεύθυνση . Σε αυτές τις περιπτώσεις, συγκεκριμένες εφαρμογές θα παρακολουθούν το περιβάλλον θα συλλέγουν

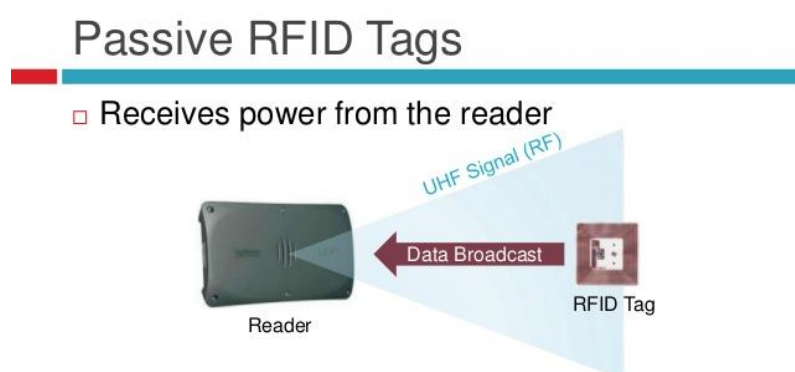
πληροφορίες ακόμα και θα αντιδρούν αυτόματα, για παράδειγμα, για την ελαχιστοποίηση της σπατάλης ενέργειας ή την αποφυγή φυσικών καταστροφών. Επομένως κύριες λειτουργίες του IoT, όπως αναλύθηκε και παραπάνω, θα είναι η αναγνώριση, η ανίχνευση και η αυτόματη λήψη αποφάσεων. Για την υλοποίηση των παραπάνω η χρήση ετικετών RFID και αισθητήρων θα είναι απαραίτητη. Τα παραπάνω αναμένεται να συνδέουν δισεκατομμύρια αντικείμενα ή πράγματα στο δίκτυο τα επόμενα χρόνια. Άλλες τεχνολογίες που επιτρέπουν αυτή τη δικτυακή υπηρεσία πραγματικού κόσμου περιλαμβάνουν τη νανοτεχνολογία και τη ρομποτική ή ακόμα και νεοεμφανιζόμενες τεχνολογίες που καθιστούν πραγματική τη λειτουργία του οραματισμένου έξυπνου κόσμου. Το IoT θα συνδέσει ετερογενείς συσκευές και θα είναι πολύ πυκνό, συνδέοντας δισεκατομμύρια αντικείμενα. Ένα πρωτόκολλο Internet-, IP- (πρωτόκολλο Internet) ή πρωτόκολλο TCP / IP θα αφορά και τις υπηρεσίες του IoT. Στην σημερινή εποχή λοιπόν κλασικές συσκευές όπως οι υπολογιστές και τα κινητά τηλέφωνα είναι ήδη συνδεδεμένα αντικείμενα χρησιμοποιώντας ενσύρματη ή ασύρματη επικοινωνία. Το IoT θα επεκτείνει τη διασύνδεση των αντικειμένων που ήδη υπάρχουν με νέα αντικείμενα που συνδέονται μέσω τεχνολογιών αναγνώρισης ραδιοσυχνοτήτων, όπως δίκτυα αισθητήρων ή RFID, επιτρέποντας την ανάπτυξη νέων υπηρεσιών που περιλαμβάνουν πληροφορίες από το περιβάλλον. Όσον αφορά τη σημερινή εποχή οι διευθύνσεις IP εντοπίζουν κόμβους στο Internet και χρησιμεύουν για τη δρομολόγηση τους. Το IPv6 επιτρέπει μεγαλύτερο χώρο διευθύνσεων από το IPv4. Στο IoT λοιπόν είναι εμφανές ότι θα χρειαστεί ένας μεγάλος χώρος για να καλύψει την αναγνώριση του τεράστιου αριθμού των συνδεδεμένων αντικειμένων. Στην περίπτωση που αυτό βασίζεται στην IP, το πρόβλημα θα αφορά περισσότερο τη σημασιολογία του αναγνωριστικού, την επεκτασιμότητα του χώρου διευθυνσιοδότησης και τον περιορισμό του μεγέθους μνήμης των συσκευών. Ο όρος "αναγνωριστικό" είναι παρόμοιος με τον όρο "όνομα". Ένα όνομα λοιπόν δεν αλλάζει με την αλλαγή τοποθεσίας, σε αντίθεση με μια "διεύθυνση", η οποία προορίζεται να χρησιμοποιηθεί για να αναφερθεί η τοποθεσία ενός αντικειμένου. Παραδείγματος χάριν, σε ένα μουσείο, ένα αναγνωριστικό σε μια ετικέτα που επισυνάπτεται σε έναν πίνακα ζωγραφικής θα μπορούσε να χρησιμοποιηθεί για να βρει περισσότερες πληροφορίες σχετικά με τον καλλιτέχνη. Σε ένα παντοπωλείο, ένα αναγνωριστικό σε μια συσκευασία τροφίμων θα μπορούσε να χρησιμοποιηθεί για να ελέγξει ότι το φαγητό είναι ασφαλές και ότι δεν πρόκειται για κάποιο δείγμα που έχει βρεθεί ότι έχει μολυνθεί με κάποιο τρόπο. Άλλοι τομείς στους οποίους η πρόσβαση στις πληροφορίες που προκαλείται από τα αναγνωριστικά μπορεί να είναι πολύτιμες αποτελούν: τα φάρμακα, η γεωργία, οι βιβλιοθήκες, το

εμπόριο αλλά και η τουριστική βιομηχανία. Τελικά οι υπηρεσίες IoT οι οποίες βασίζονται σε ασύρματα δίκτυα έχουν γίνει πιο διαδεδομένες, αυτές δηλαδή που μεταφέρουν πληροφορίες μέσω ραδιοσυχνοτήτων. (Chaouchi,2010) Τέτοιες υπηρεσίες σχετίζονται με τα RFIDs και τα ασύρματα δίκτυα αισθητήρων (WSNs) και γι αυτό το λόγω θα ασχοληθούμε με αυτές τις τεχνολογίες παρακάτω.

1.2: Radio frequency identification (RFID)

Με τον όρο RFID αναφερόμαστε στην τεχνολογία η οποία λειτουργεί κάνοντας αναγνώριση ραδιοσυχνοτήτων, μέσω των οποίων, δίνεται η δυνατότητα να γίνει αυτόματη αναγνώριση και παρακολούθηση των ετικετών (tags) που υπάρχουν σε μικροτσιπ τα οποία συνδέονται με αντικείμενα. Το υλικό RFID περιλαμβάνει ετικέτες και συσκευές ανάγνωσης (reader). Αναλυτικότερα η ετικέτα περιέχει ένα ολοκληρωμένο κύκλωμα και μια κεραία. Από την άλλη πλευρά η άλλη σημαντική παράμετρος στο σύστημα είναι ο αναγνώστης. Ο αναγνώστης λοιπόν αναζητά το περιεχόμενο της ετικέτας χρησιμοποιώντας κύματα ραδιοσυχνοτήτων (RF) και αποκτά τις πληροφορίες της ετικέτας μέσω των κυμάτων ραδιοσυχνοτήτων. Για την επικοινωνία των συσκευών RFID reader με RFID tags χρησιμοποιείται ένα τυποποιημένο μοντέλο επικοινωνίας ISO που ονομάζεται ISO 18000.

Εικόνα 1.1: Passive RFID tag & RFID reader.



Οι ετικέτες περιέχουν ηλεκτρονικά αποθηκευμένες πληροφορίες, εκείνες οι οποίες λειτουργούν χωρίς μπαταρίες αναφέρονται ως παθητικές ετικέτες (Εικόνα 1.1) και συλλέγουν ενέργεια από το σήμα επικοινωνίας που αποστέλλεται από τον αναγνώστη RFID. Αντιθέτως, οι ενεργές ετικέτες

χρησιμοποιούν μια μπαταρία για να τροφοδοτηθούν με ενέργεια. Τα συστήματα RFID λειτουργούν σε διάφορες ζώνες συχνотήτων. Τα συστήματα RFID που λειτουργούν στη ζώνη Low Frequency αναπτύχθηκαν στα αρχικά στάδια της αγοράς και είχαν σχέση με βιομηχανικές εφαρμογές μικρής εμβέλειας και συσκευές immobilizer αυτοκινήτου (όπου αν χρησιμοποιηθεί κλειδί διαφορετικό από το αυθεντικό το αυτοκίνητο δεν ξεκινάει). Αυτά τα συστήματα ενδείκνυνται σε συστήματα όπου τα ποσοστά πληροφορίας δεν είναι πολύ υψηλά. Τα συστήματα RFID HF (high frequency) είναι προγραμματισμένα έτσι ώστε να χειρίζονται πολύ υψηλότερα ποσοστά δεδομένων σε σχέση με το σύστημα LF και η κεραία που περιέχεται στην ετικέτα είναι αρκετά μικρότερη. Τα συστήματα HF περιέχουν μεγαλύτερο εύρος ανάγνωσης σε σύγκριση με τα συστήματα LF. Το σύστημα UHF (ultra-high frequency) RFID έχει πολύ μεγαλύτερο εύρος ανάγνωσης και δέχεται υψηλότερο ρυθμό δεδομένων σε σύγκριση με τα συστήματα LF και HF. Παρόλα αυτά όμως το σύστημα UHF δεν λειτουργεί πολύ καλά όταν έχει να κάνει με μεταλλικά αντικείμενα, νερό ή και το ανθρώπινο σώμα - αν το συγκρίνουμε με το σύστημα LF. Ένα γεγονός που δεν θα πρέπει να παραβλεφθεί είναι ότι μπορεί να υπάρχουν αρκετές ετικέτες που προσπαθούν να μεταδώσουν πληροφορίες στον αναγνώστη και αρκετοί αναγνώστες προσπαθούν να διαβάσουν πολλές ετικέτες ταυτόχρονα. Αυτό έχει ως αποτέλεσμα τη δημιουργία μιας σύγκρουσης δεδομένων που μεταφέρονται μεταξύ των συσκευών ανάγνωσης και των ετικετών καθιστώντας τα μη λειτουργικά προς το χρήστη. Εξάλλου έχουν δημιουργηθεί αρκετοί αλγόριθμοι, οι περισσότεροι εξ αυτών λειτουργώντας με επιτυχία, που έχουν ως στόχο τον περιορισμό αυτών των συγκρούσεων. (Chaouchi, 2010) Σε αντίθεση με ένα bar code, η ετικέτα δεν χρειάζεται να βρίσκεται εντός της οπτικής επαφής του αναγνώστη, επομένως μπορεί να ενσωματωθεί στο αντικείμενο που παρακολουθείται. Η τεχνολογία RFID είναι μια μέθοδος για την αυτόματη αναγνώριση και καταγραφή δεδομένων. Παράδειγμα χρήσης τους αποτελούν ετικέτες RFID προσαρμοσμένες σε ένα αυτοκίνητο κατά τη διάρκεια παραγωγής του οι οποίες χρησιμοποιούνται για την παρακολούθηση της προόδου του. Επιπρόσθετα είναι εφικτό να γίνει χρήση των ετικετών RFID σε φαρμακευτικά προϊόντα με αποτέλεσμα τα τελευταία να μπορούν να εντοπιστούν. Τέλος η εμφύτευση μικροτσιπ RFID στα κατοικίδια ζώα επιτρέπει την ταυτοποίηση τους. Ένας παράγοντας που μπορεί να είναι δυνητικά επικίνδυνος είναι ότι οι ετικέτες RFID μπορούν να συνδεθούν με πιστωτικές κάρτες, ρούχα (Εικόνα 1.2) ή να εμφυτευτούν σε ανθρώπους. Το παραπάνω συνεπάγεται πως υπάρχει η δυνατότητα ανάγνωσης προσωπικών πληροφοριών χωρίς τη συγκατάθεση των χρηστών

και δημιουργεί σοβαρές ανησυχίες που έχουν σχέση με την ιδιωτικότητα. (Angell, Kietzmann, 2006)

Εικόνα 1.2: Παράδειγμα RFID ετικετών σε ρούχα και σε φάρμακα.



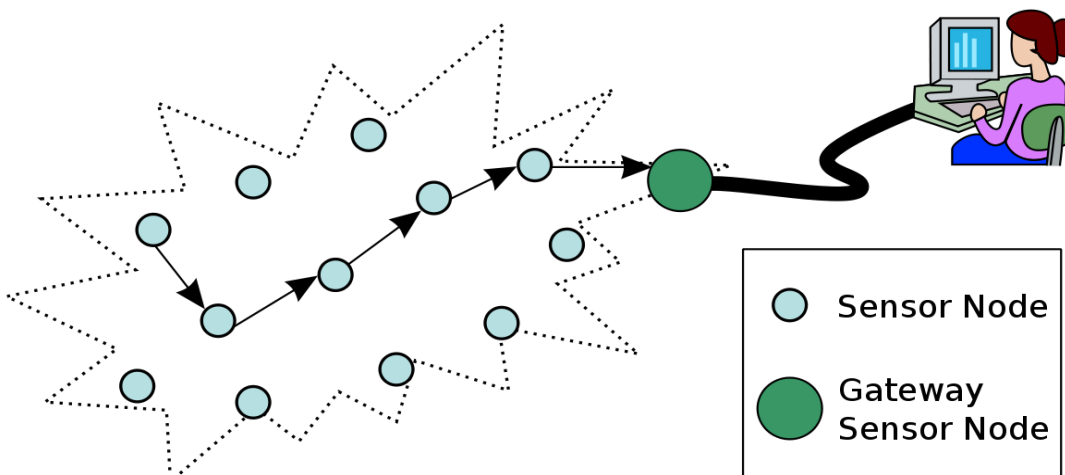
Όσον αφορά τις ετικέτες RFID, αυτές μπορούν να έχουν διαφορετικές δυνατότητες αποθήκευσης ξεκινώντας από μερικά bit και φτάνοντας σε αρκετά megabyte. Επιπλέον, οι τελευταίες μπορεί να είναι σε μορφή μόνο για ανάγνωση ή σε εκείνη των επανεγγράψιμων ετικετών, σύμφωνα με τις ιδιότητες τους. Ακόμη τα RFID περιέχουν middleware, το λογισμικό το οποίο είναι υπεύθυνο για την προώθηση των δεδομένων σε άλλο σύστημα, όπως βάση δεδομένων, προσωπικό υπολογιστή ή σύστημα σχετικό με ρομπότ, ανάλογα με την εφαρμογή. Αναλυτικότερα τα συστήματα που περιέχουν πληθώρα δεδομένων που δημιουργούνται στον RFID reader, είναι απαραίτητο να υποστούν κάποιο είδος προ-επεξεργασίας προτού μεταφερθούν οι πληροφορίες στην εφαρμογή. Εφαρμογές RFID μπορούν να εφαρμοστούν ακόμη και στη λιανική όπου τα μελλοντικά καταστήματα, για τη βελτίωση των υπηρεσιών τους, θα εφαρμόζουν τις ετικέτες στα προϊόντα με αποτέλεσμα μέσω των εφαρμογών οι λιανοπωλητές να μπορούν να κάνουν καλύτερη διαχείριση και βελτίωση των παραπάνω. Ακόμα οι εργασίες αποθήκευσης θα απλοποιηθούν σημαντικά και η εξυπηρέτηση πελατών θα βελτιωθεί. Σημαντική αλλαγή θα προέλθει και όσον αφορά τη διαχείριση αποθεμάτων αφού οι ετικέτες RFID σε προϊόντα θα μειώσουν τη χειρωνακτική εργασία που έχει σχέση με στην απογραφή τους. Για παράδειγμα, τα έξυπνα ράφια μπορούν να αναφέρουν αυτόματα των αριθμό των προϊόντων με συνέπεια τα περιεχόμενα και οι εργαζόμενοι να μπορούν γρήγορα να κάνουν απογραφή με τη βοήθεια των κινητών φορητών συσκευών ανάγνωσης, γεγονός που θα βοηθήσει στην ορθότερη λήψη αποφάσεων σχετικά με τις

παραγγελίες και την αποφυγή καταστάσεων όπου το κατάστημα θα είναι εκτός αποθέματος. (Evdokimov et al.,2011)

1.3: Ασύρματα Δίκτυα Αισθητήρων

Στη σημερινή εποχή τα ασύρματα δίκτυα αισθητήρων (WSNs) βρίσκονται παντού γύρω μας. Το πεδίο εφαρμογής λοιπόν των ασύρματων αισθητήρων διαχωρίζεται σε τρεις κύριες κατηγορίες οι οποίες αφορούν: παρακολούθηση του χώρου (περιβάλλον), παρακολούθηση των αντικειμένων (γέφυρες) και παρακολούθηση των αλληλεπιδράσεων μεταξύ των αντικειμένων και του χώρου, για την αποφυγή φυσικών καταστροφών (πλημμύρες, φωτιές, ηφαιστεια κτλ). (Christin et al.,2014) Οι αισθητήρες χρησιμοποιούνται κυρίως για παρατηρήσεις που αφορούν θερμοκρασία, φυσικά φαινόμενα/καταστροφές και γενικότερα συλλογή δεδομένων τα οποία συλλέγονται και αποστέλλονται προς ένα κεντρικό κόμβο προς ανάλυση. Ακόμα μπορεί να γίνει εφαρμογή τους στην υγεία και σε εφαρμογές ρύθμισης της κυκλοφορίας. Το ενδιαφέρον μάλιστα για τα WSNs αυξήθηκε σχεδόν παράλληλα με το ενδιαφέρον για το IoT (αρχές 21 αιώνα). Η ανάπτυξη τους λοιπόν εμφανίστηκε αρχικά από εφαρμογές που είχαν σχέση με το στρατό (επιτήρηση περιοχών). Ένα WSN μπορεί γενικά να περιγραφεί ως ένα δίκτυο κόμβων (αισθητήρων) που ελέγχουν το περιβάλλον, επιτρέποντας την αλληλεπίδραση των ανθρώπων ή των υπολογιστών με το περιβάλλον. Για τη λειτουργικότητα τους και την επικοινωνία των κόμβων μεταξύ τους μπορούν να χρησιμοποιηθούν τα πρότυπα: WirelessHART , IEEE 1451, ZigBee / 802.15.4, ZigBee IP αλλά και το 6LoWPAN. Τα δεδομένα που συλλέγονται από τους κόμβους φτάνουν στην πύλη και από εκεί μπορούν να συλλεχθούν από υπολογιστές και ανθρώπους.(Εικόνα 1.3)

Εικόνα 1.3: Αισθητήρες συλλέγουν δεδομένα και τα αποστέλλουν στην πύλη .



Λόγω του φθηνού τους κόστους μάλιστα εφαρμόζονται όλο και περισσότερο παγκοσμίως. Πηγή ενέργειας για τη λειτουργία τους αποτελεί το ρεύμα από τη ΔΕΗ ή ακόμα και ενέργεια που προέρχεται από φωτοβολταϊκά. (Yinbiao, 2014) Είναι η γέφυρα που συνδέει τον πραγματικό κόσμο με τον ψηφιακό κόσμο. Ουσιαστικά λοιπόν τα ασύρματα δίκτυα αισθητήρων (WSN) είναι σαν τα μάτια και τα αυτιά του διαδικτύου των πραγμάτων. (Egan, 2012) Επιπροσθέτως στη σημερινή εποχή, τέτοια δίκτυα εγκαθίστανται από εξειδικευμένο και έμπειρο προσωπικό, όμως η πλειοψηφία αυτών των συστημάτων τοποθετούνται από άτομα που δεν έχουν κάποια ιδιαίτερη τεχνική εμπειρία. Ένα γεγονός που δε θα πρέπει να παραβλεφθεί είναι ότι τα περισσότερα δίκτυα αισθητήρων δεν είναι συνδεδεμένα στο Internet, αλλά είναι συνδεδεμένα σε ένα σύστημα που χρησιμοποιεί τα δεδομένα τοπικά και οι πληροφορίες τους δεν εκτείνονται πέρα από το ίδιο το δίκτυο αισθητήρων. Τελικά υπάρχουν χιλιάδες διαφορετικά είδη αισθητήρων, όπου καθένα από αυτά έχει με τις δικές του προδιαγραφές και δυνατότητες. Ακόμη και σε περιπτώσεις που αφορούν ένα συγκεκριμένο αισθητήρα οι διαφορετικές εκδόσεις του θα λέγαμε ότι ποικίλουν σε σχέση με τις επιδόσεις, τις διεπαφές ακόμα και την συσκευασία του. Έτσι είναι γεγονός πως δεν υπάρχει μια ενιαία και γενική διεπαφή αισθητήρων. (Chaouchi, 2010)

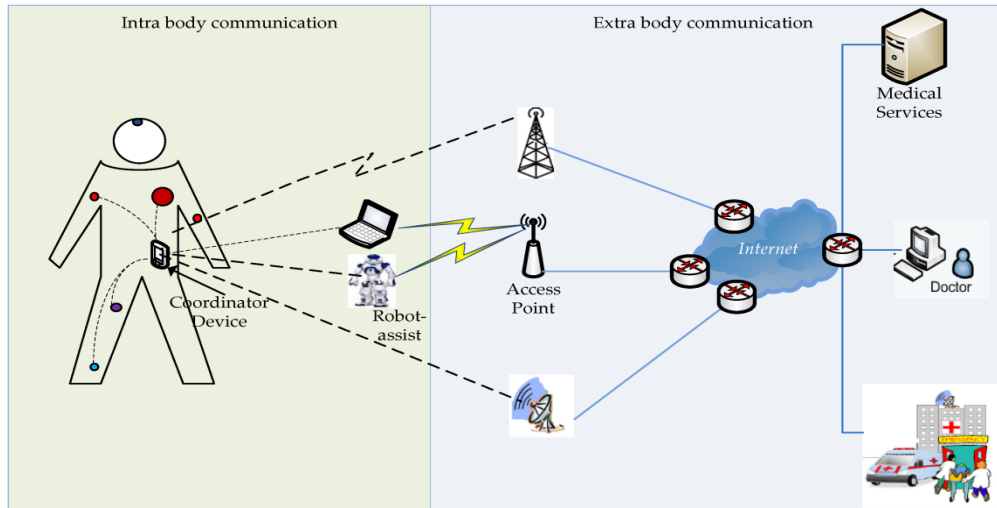
Εικόνα 1.4: Οι αισθητήρες κάνουν μετρήσεις περιβαλλοντολογικών συνθηκών σε δάσος.



Ένα παράδειγμα για τη χρήση ασύρματων δικτύων αισθητήρων θα αποτελούσε ένα δάσος στο οποίο θα γίνονταν μελέτες όσον αφορά την υγρασία των φύλλων, την υγρασία του περιβάλλοντος και τη θερμοκρασία του εδάφους (Εικόνα 1.4). Οι μετρήσεις θα αποκάλυπταν τις μικροκλιματικές συνθήκες που ευνοούν την ταχεία φυσική αναγέννηση ενός τροπικού δάσους που έχει καταστραφεί. Επιπρόσθετα αισθητήρες εφαρμόζονται σε δάση ως

μέτρο προστασίας ενάντια στις πυρκαγιές. Συγκεκριμένα μετρήσεις όπως η θερμοκρασία του αέρα, η ταχύτητα του ανέμου και η κατεύθυνση του , ο καπνός και η ατμοσφαιρική πίεση αποτελούν σημαντικά δεδομένα που μετά τη συλλογή τους αποστέλλονται στις αρμόδιες αρχές. (ZHANG et al.,2009) Τέλος η ασφάλεια που έχει σχέση με τα WSNs αποτελεί ένα παράγοντα που πρέπει να δοθεί μεγάλη προσοχή. Ιδιαίτερως μάλιστα όταν οι εφαρμογές αφορούν δεδομένα του στρατού ή της εθνικής ασφάλειας αλλά και δεδομένα από αισθητήρες που έχουν σχέση με εφαρμογές υγείας και περιέχουν ευαίσθητα προσωπικά δεδομένα χρηστών. Επιπρόσθετα θα πρέπει να αναπτυχθούν νέες μέθοδοι ασφαλείας αφού λόγω των μοναδικών χαρακτηριστικών των WSNs, οι παραδοσιακές μέθοδοι ασφαλείας δικτύων υπολογιστών θα ήταν άχρηστες ή λιγότερο αποτελεσματικές. (Butun et al., 2014) Σε μια εποχή που η τεχνολογία συνεχώς εξελίσσεται, αισθητήρες εφαρμόζονται και στο ανθρώπινο σώμα για την παρακολούθηση της υγείας του ασθενή (Εικόνα 1.5). Τέτοια συστήματα είναι γνωστά και ως “συστήματα ασύρματων δικτύων σώματος” (WBAN). Με αυτά γίνονται μετρήσεις σχετικά με ανθρώπινες ζωτικές λειτουργίες του οργανισμού όπως καρδιακός ρυθμός, πίεση αίματος, αναπνοή και οξυγόνο. (Yilmaz et al.,2013)

Εικόνα 1.5: Τα δεδομένα των αισθητήρων του ανθρώπινου σώματος στέλνονται μέσω του διαδικτύου προς εξέταση.



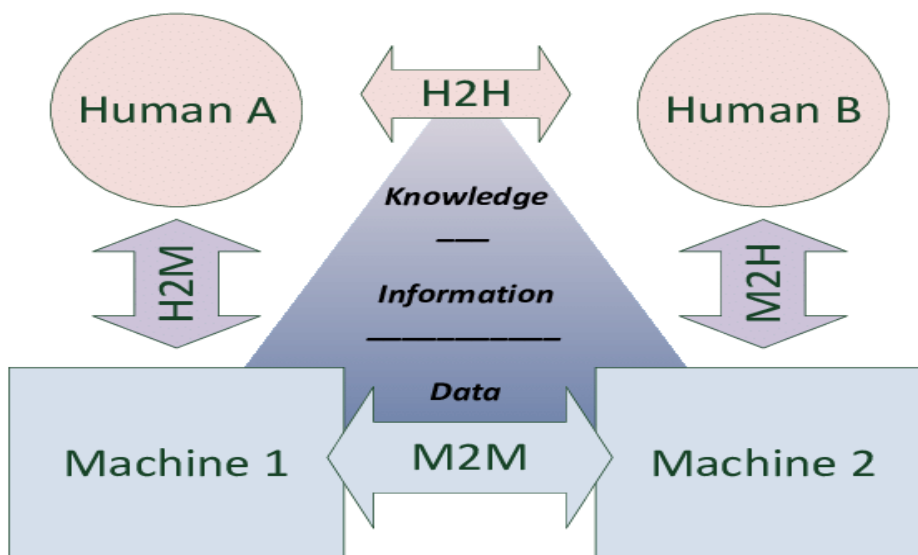
Στη συνέχεια τα δεδομένα των μετρήσεων που συλλέγονται από όλα τα WBANs του ασθενή στέλνονται τελικά σε ένα κέντρο υγείας έτσι ώστε να συλλεχτούν ως μόνιμα και να χρησιμοποιηθούν ως ιστορικό του ασθενή μελλοντικά. Οι θεράποντες ιατροί μπορούν να έχουν πρόσβαση εξ αποστάσεως σε αυτές τις αναλύσεις για να αξιολογήσουν την κατάσταση της υγείας του ασθενούς. Το δίκτυο των αισθητήρων που σχηματίζεται από το WBAN βρίσκεται συνήθως στο ανθρώπινο σώμα ή είναι πολύ κοντά σε αυτό. Επίσης οι αισθητήρες θα πρέπει να τοποθετηθούν στα κατάλληλα σημεία του σώματος έτσι ώστε το σήμα τους να είναι ισχυρό και να μην εξασθενίσει για

παράδειγμα λόγω κάποιων ιστών. Επιπλέον τα δεδομένα μπορεί να διαρρεύσουν ή να παραποιηθούν μέσω κακόβουλου λογισμικού. Επομένως η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των δεδομένων είναι επισφαλείς. Τα WBAN θεωρούνται ως μια υποκατηγορία των WSNs. Η αλήθεια όμως είναι ότι τα παραδοσιακά δίκτυα αισθητήρων δεν είναι ειδικά στο να κάνουν παρακολούθηση των ζωτικών λειτουργιών του ανθρώπου. Οι αισθητήρες που εμφυτεύονται σε έναν ιστό ή στο σώμα του ασθενή πρέπει να είναι πολύ μικρού μεγέθους και είναι αναγκαία η μεγάλη διάρκεια ζωής των αισθητήρων. (Baskaranb, 2011)

1.4: Επικοινωνία Συσκευών

Μία ακόμα παράμετρος σημαντική ως προς τη μελέτη της αποτελούν τα μοντέλα επικοινωνίας στων συσκευών IoT. Αρχικά λοιπόν από την επικοινωνία ανθρώπου με άνθρωπο (H2H) μέσω της τεχνολογίας φτάσαμε στην επικοινωνία ανθρώπου με μηχανή (H2M) ενσύρματα ή ασύρματα. Τέλος η σημερινή τάση οδηγεί στην επικοινωνία των μηχανών μεταξύ τους (M2M). Το IoT λοιπόν έχει σχέση με την επικοινωνία και την ανταλλαγή δεδομένων των συσκευών μεταξύ τους. (Εικόνα 1.6)

Εικόνα 1.6: Απεικόνιση επικοινωνίας H2H, H2M & M2M.



Τα βασικότερα μοντέλα που αφορά την επικοινωνία των συσκευών μεταξύ τους είναι τέσσερα και παρουσιάζονται παρακάτω.

1] Μοντέλο Device to Device

Το μοντέλο επικοινωνίας μεταξύ συσκευής προς συσκευή έχει σχέση με την απευθείας σύνδεση και την επικοινωνία δύο συσκευών μεταξύ τους και χωρίς

την ύπαρξη κάποιου διακομιστή. Αυτά τα μοντέλα χρησιμοποιούν πρωτόκολλα όπως το IP, το Bluetooth ή το δίκτυο ZigBee για να επιτύχουν την άμεση επικοινωνία. Ένα τέτοιο παράδειγμα αποτελεί η σύνδεση του διακόπτη φωτός με την αντίστοιχη λάμπα, η επικοινωνία τους γίνεται μέσω Bluetooth ή ZigBee. (Εικόνα 1.6)

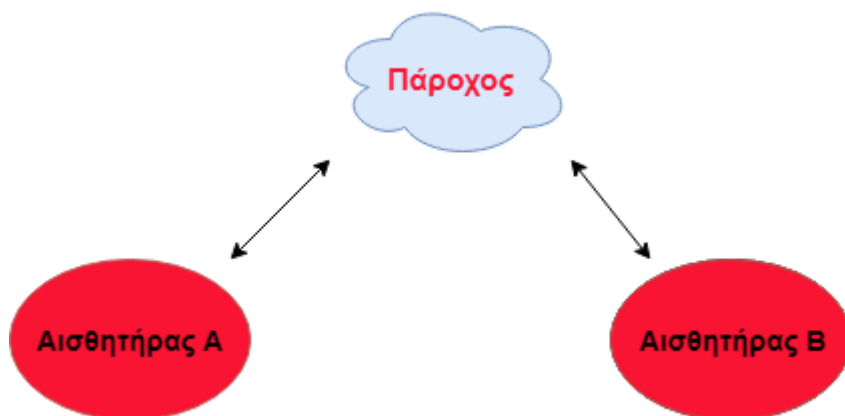
Εικόνα 1.7: Παράδειγμα επικοινωνίας device-device.



2] Μοντέλο Device to Cloud

Στο μοντέλο αυτό η συσκευή του IoT συνδέεται απευθείας με μια υπηρεσία cloud στο Internet, μέσω Ethernet ή Wi-Fi. Συνήθως η υπηρεσία Cloud και η συσκευή ανήκουν στον ίδιο προμηθευτή. Η σύνδεση αυτή έχει στόχο τη μεταφορά και ανταλλαγή δεδομένων αλλά και τη διαχείριση κίνησης μηνυμάτων. Για παράδειγμα δύο αισθητήρες διαφορετικού τύπου στέλνουν δεδομένα στο Cloud και μέσω αυτού ανταλλάσσουν χρήσιμα δεδομένα. (Εικόνα 1.7)

Εικόνα 1.8: Παράδειγμα επικοινωνίας device-cloud.

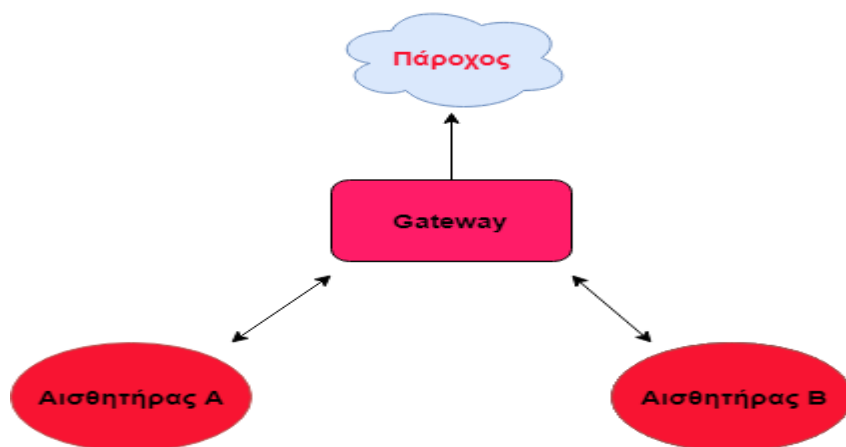


Η σύνδεση με cloud επίσης επιτρέπει στο χρήστη να αποκτήσει απομακρυσμένη πρόσβαση σε πληροφορίες, όπως πληροφορίες που έχουν σχέση με το θερμοστάτη του, μέσω ενός smartphone. Ακόμα χρησιμοποιείται σε έξυπνες τηλεοράσεις για την ανάλυση πληροφοριών του χρήστη.

3] Μοντέλο Device to Gateway

Στο μοντέλο αυτό , που είναι γνωστό και ως device-to-application-layer gateway (ALG) η συσκευή IoT χρησιμοποιεί την πύλη (Gateway) ως ένα πέρασμα για τη μεταφορά των δεδομένων στο cloud. Η λειτουργία της πύλης περιγράφεται παρακάτω. Σε αυτήν περιλαμβάνεται λειτουργικό πακέτο λογισμικού εφαρμογών , η οποία ενεργεί ως μεσολαβητής μεταξύ της συσκευής και επομένως της υπηρεσίας cloud , παρέχει ασφάλεια και μπορεί να κάνει μετάφραση δεδομένων ή πρωτοκόλλων (Εικόνα 1.8). Σε πολλές περιπτώσεις, τρόπος εισόδου μπορεί να είναι ένα smartphone που διαθέτει ένα λογισμικό το οποίο μπορεί να μεταβιβάσει πληροφορίες στο cloud, παράδειγμα αποτελεί μια συσκευή παρακολούθησης της φυσικής κατάστασης του χρήστη.

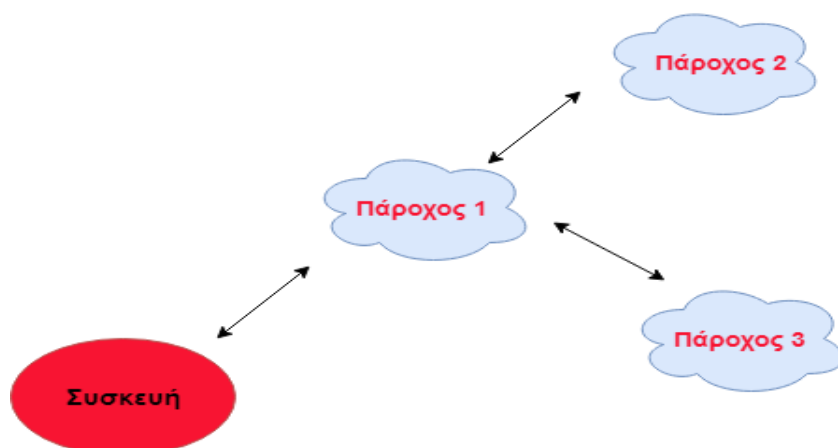
Εικόνα 1.9: Παράδειγμα επικοινωνίας device-gateway.



4] Back-End Data-Sharing Model

Το back and data sharing μοντέλο αναφέρεται σε μια μορφή επικοινωνίας που επιτρέπει στους χρήστες να εξάγουν και να αναλύουν πληροφορίες και δεδομένα ενός αντικειμένου (αισθητήρα). Επιπρόσθετα όμως μπορεί να γίνει μια τέτοια εξαγωγή γνώσης και από τρίτα συνδεδεμένα αντικείμενα (Εικόνα 1.9). Για παράδειγμα προκειμένου να γίνει καλύτερη διαχείριση ενέργειας σε μια εταιρία, συλλέγονται στο cloud δεδομένα που αφορούν όλους τους αισθητήρες IoT της εταιρίας, έτσι ώστε να γίνει αποδοτικότερη διαχείριση ενέργειας και οικονομία στους πόρους της. (Kulkarni, 2017)

Εικόνα 1.10: Παράδειγμα επικοινωνίας back-end-data.

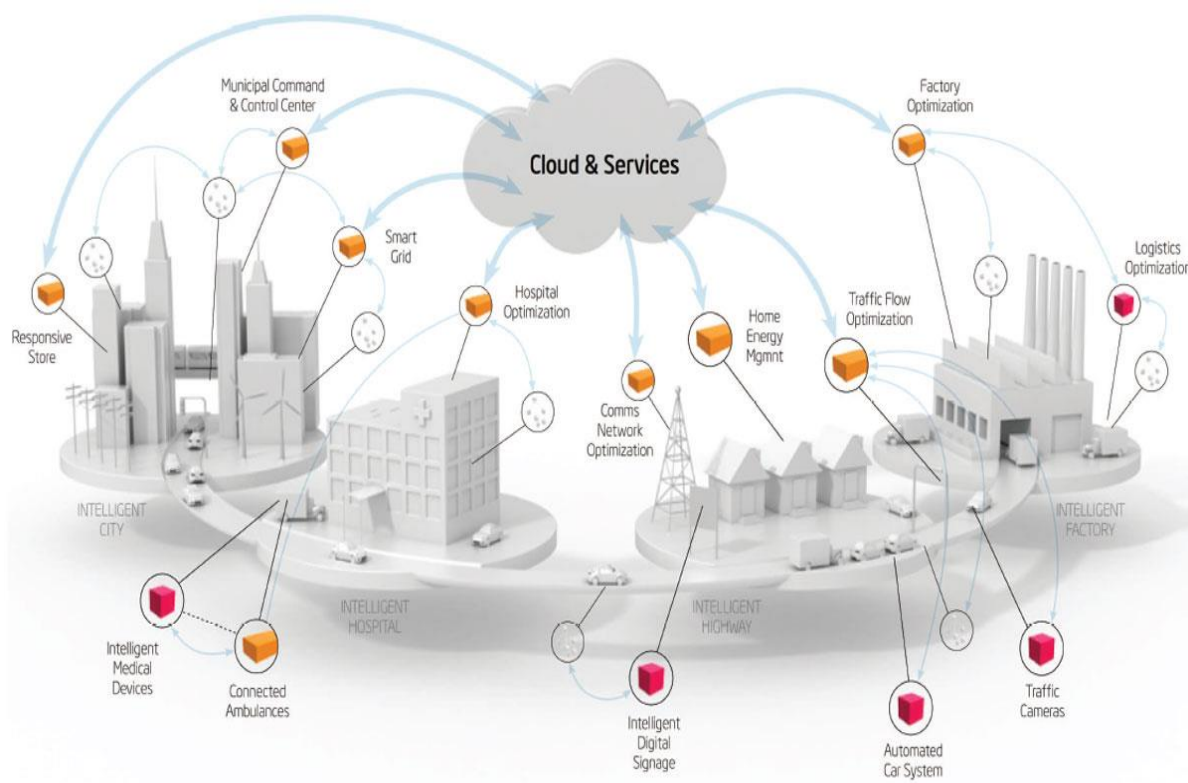


1.5 Cloud Computing

Με τον όρο cloud computing αναφερόμαστε στην τεχνολογία η οποία χρησιμοποιεί ένα δίκτυο απομακρυσμένων διακομιστών (servers) του διαδικτύου για την αποθήκευση, διαχείριση και επεξεργασία δεδομένων αντί για έναν τοπικό server ή έναν προσωπικό υπολογιστή. Η βασική ιδέα πίσω από το cloud computing δεν είναι νέα αφού ο John McCarthy στη δεκαετία του 1960 είχε ήδη οραματιστεί ότι οι εφαρμογές της πληροφορικής θα μπορούσαν να παρέχονται στο ευρύ κοινό, σαν μια υπηρεσία. Στα πλεονεκτήματα του περιλαμβάνεται ο μεγάλος διαθέσιμος αποθηκευτικός χώρος, το γεγονός ότι ο χρήστης μπορεί να έχει πρόσβαση από οποιονδήποτε υπολογιστή συνδεδεμένο στο διαδίκτυο αλλά και η οικονομία που προσφέρει αφού ο χρήστης μπορεί να χρησιμοποιεί διαδικτυακά ένα λογισμικό για συγκεκριμένο χρονικό διάστημα, πληρώνοντας αρκετά λιγότερα χρήματα από την περίπτωση που θα το εγκαθιστούσε τοπικά στον υπολογιστή του. Από την άλλη πλευρά όμως θα πρέπει να δημιουργηθούν νέα συστήματα ασφαλείας προκειμένου οι πληροφορίες και τα προσωπικά δεδομένα του χρήστη να μην διαρρεύσουν/καταστραφούν από άλλα κακόβουλα λογισμικά. Αρχικά, θα μπορούσαμε να πούμε ότι η τεχνολογία του Cloud Computing και του Internet of Things είναι δύο πολύ διαφορετικές τεχνολογίες. Στη σημερινή εποχή όμως υπάρχει η ανάγκη επικοινωνίας και συνεργασίας αυτών των δύο τεχνολογιών προκειμένου ο τεράστιος όγκος δεδομένων που προκύπτουν να είναι διαχειρίσιμος και πολλές εφαρμογές IoT να είναι λειτουργικές και αυτόνομες. (Rao et al., 2012) Υπάρχει λοιπόν το

όραμα όλες οι υπηρεσίες να συνδέονται στο Cloud και να ανταλλάσσουν δεδομένα μεταξύ τους μέσω αυτού (Εικόνα 1.11) .

Εικόνα 1.11: Οι υπηρεσίες συνδέονται στο Cloud και ανταλλάσσουν δεδομένα μεταξύ τους.



Όσον αφορά λοιπόν το cloud υπάρχουν αρκετά διαφορετικά είδη του τελευταίου και κατά συνέπεια το καθένα έχει τα δικά του οφέλη και μειονεκτήματα. Αρχικά στο δημόσιο cloud οι πάροχοι προσφέρουν τους πόρους τους ως υπηρεσίες προς το ευρύ κοινό. Στα οφέλη τους περιλαμβάνεται μεταξύ άλλων το γεγονός ότι δεν απαιτείται καμία αρχική επένδυση κεφαλαίου για τις υποδομές , ωστόσο τα δημόσια clouds δεν διαθέτουν λεπτομερή έλεγχο των δεδομένων, του δικτύου και έχουν αρκετές ελλείψεις ρυθμίσεων ασφαλείας, γεγονός που παρεμποδίζει την αποτελεσματικότητά τους. Το ιδιωτικό cloud (γνωστό και ως εσωτερικό cloud), είναι σχεδιασμένο για αποκλειστική χρήση από έναν μόνο οργανισμό. Τα πλεονεκτήματα που προσφέρει έχουν σχέση με υψηλότερο βαθμό ελέγχου της απόδοσης του, της αξιοπιστίας και της ασφάλειας του. Στη συνέχεια τα υβριδικά cloud είναι ένας συνδυασμός δημόσιου και ιδιωτικού μοντέλου cloud που προσπαθούν να αντιμετωπίσουν τους περιορισμούς κάθε προσέγγισης. Σε ένα υβριδικό cloud, μέρος της υποδομής των υπηρεσιών τρέχει σε ιδιωτικό μοντέλο ενώ το υπόλοιπο μέρος τρέχει σε δημόσιο. Αυτά

προσφέρουν μεγαλύτερη ευελιξία από δημόσια και ιδιωτικά cloud. Συγκεκριμένα, παρέχουν αυστηρότερο έλεγχο και ασφάλεια σε σύγκριση με τα δημόσια , διευκολύνοντας παράλληλα την επέκταση των υπηρεσιών. Χρειάζεται όμως μεγάλη προσοχή στο σχεδιασμό του και απαιτεί τον προσδιορισμό μεταξύ των λειτουργιών των δημόσιων και ιδιωτικών στοιχείων του cloud. Τέλος το εικονικό ιδιωτικό cloud (VPC) αποτελεί μια ακόμα εναλλακτική λύση για την αντιμετώπιση των περιορισμών τόσο των δημόσιων όσο και των ιδιωτικών. Ένα VPC είναι ουσιαστικά μια πλατφόρμα που τρέχει πάνω από τα δημόσια cloud. Η κύρια διαφορά είναι ότι ένα VPC αξιοποιεί την τεχνολογία εικονικού ιδιωτικού δικτύου (VPN) και επιτρέπει στους παρόχους υπηρεσιών να σχεδιάσουν τη δική τους τοπολογία και ρυθμίσεις ασφαλείας. (Zhang et al., 2010)

Κεφάλαιο 2: Ασφάλεια & Ιδιωτικότητα στο IoT

2.1:Εισαγωγή στην Ασφάλεια & Ιδιωτικότητα

Η τάση της σημερινής εποχής λοιπόν είναι όλο και περισσότερα αντικείμενα να συνδέονται μεταξύ και τους και να αλληλεπιδρούν με τα υπόλοιπα. Τα έξυπνα αντικείμενα θα είναι διάχυτα στην καθημερινότητα των ανθρώπων αλλά και στο περιβάλλον. Οι αισθητήρες θα ενσωματωθούν σε κτίρια, οχήματα και στο περιβάλλον προκειμένου να κάνουν μετρήσεις, θα συνδέονται με τα ζώα έτσι ώστε να εντοπίζεται η τοποθεσία τους. Για παράδειγμα, τα κινητά τηλέφωνα θα άλλαζαν αυτόματα την λειτουργία τους σε αθόρυβη ,όταν ο ιδιοκτήτης τους πρόκειται να έχει μια σημαντική συνάντηση ,μετά από εντολή του. Οι υπηρεσίες έκτακτης ανάγκης , οι οποίες είναι αναγκαίες , θα είναι σε θέση να ειδοποιούν από απόσταση και αυτόματα να εντοπιστεί πυρκαγιά σε ένα κτίριο ή στον τομέα της υγείας εάν οι ζωτικές λειτουργίες ενός ασθενούς πέσουν πέρα από ένα κρίσιμο όριο. Είναι προφανές λοιπόν ότι αν διαρρεύσουν πληροφορίες και προσωπικά δεδομένα από τις προαναφερθείσες εφαρμογές IoT θα πληγεί η ασφάλεια και η ιδιωτικότητα του χρήστη, βάζοντας τον σε κίνδυνο. Αρχικά με τον όρο ιδιωτικότητα αναφερόμαστε στην ικανότητα ενός ατόμου να κρατάει πληροφορίες για τον εαυτό του και έτσι να εκφράζεται επιλεκτικά. (Solove, 2008) Ο όρος «ασφάλεια» περιλαμβάνει τις έννοιες της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της πληροφορίας. Παρά το γεγονός ότι η ιδιωτικότητα έχει σχέση με την ασφάλεια, οι δύο έννοιες δεν ταυτίζονται. Έτσι , για παράδειγμα , δύο άνθρωποι που συζητούν ένα αστυνομικό τμήμα είναι ασφαλείς (λόγω των αστυνομικών και των καμερών) αλλά δεν υπάρχει ιδιωτικότητα μεταξύ των όσων κουβεντιάσουν. Από την άλλη πλευρά σε μία ιδιωτική συζήτηση σε μια καφετέρια υπάρχει ιδιωτικότητα όχι όμως ασφάλεια. (Krumm, 2010) Έτσι λοιπόν στον τομέα του διαδικτύου , που από τη θετική του πλευρά είναι ένας πολύτιμος πόρος , αλλά αντίθετη πλευρά υπάρχει επίσης εγκληματικότητα που επιδιώκει να κερδίσει από την παράνομη χρήση του διαδικτύου. Το πιο ανησυχητικό είναι ότι λόγω της φύσης του οι επιθέσεις μπορούν να γίνουν από οποιαδήποτε θέση στον κόσμο, γεγονός που καθιστά την ασφάλεια των χρηστών επισφαλή. Η εμπιστευτικότητα αφορά τη διατήρηση δεδομένων ιδιωτικά, έτσι ώστε μόνο οι εξουσιοδοτημένοι χρήστες να έχουν πρόσβαση στα δεδομένα αυτά. Η κρυπτογραφία είναι μια βασική τεχνολογία για την επίτευξη της εμπιστευτικότητας. Η ακεραιότητα των δεδομένων αφορά την επαλήθευση ότι τα δεδομένα δεν έχουν αλλοιωθεί και ότι μπορούν να εξακριβωθούν ότι έχουν αποσταλεί από τον ισχυρισμένο συγγραφέα. Τέλος η διαθεσιμότητα είναι η ικανότητα του χρήστη να έχει πρόσβαση στα δεδομένα του οποιαδήποτε

χρονική στιγμή. Όπως προαναφέρθηκε απειλές εμπιστευτικότητας είναι αυτές που οδηγούν στην ανεπιθύμητη απελευθέρωση ευαίσθητων πληροφοριών. Για παράδειγμα, οι παραβιάσεις της εμπιστευτικότητας σε ένα σύστημα που παρακολουθεί τις ιατρικές ενδείξεις του ασθενή μπορεί να οδηγήσει στην ακούσια απελευθέρωση ευαίσθητων ιατρικών του δεδομένων. Η απώλεια της εμπιστευτικότητας σε πράγματα όπως οι κωδικοί πρόσβασης θα οδηγήσει σε αθέμιτες απειλές πρόσβασης στο σύστημα. Έτσι λοιπόν η μη εξουσιοδοτημένη πρόσβαση, καθιστά ολόκληρο το σύστημα του χρήστη επισφαλές. Γενικότερα σήμερα υπάρχουν πολύ λίγες έξυπνες συσκευές που παρέχουν οποιαδήποτε κανονική υπηρεσία ενημέρωσης λογισμικού για να καλύψουν τις ευπάθειες ασφαλείας. Λόγω του χαμηλού κόστους τους, οι υπολογιστικές συσκευές IoT γενικά δεν είναι τόσο ισχυρές όσο οι υπολογιστές. Οι περισσότερες συσκευές IoT έχουν χαμηλές ενεργειακές απαιτήσεις και περιορισμένη μνήμη. Αυτοί οι ελεγκτές λοιπόν προσαρμόζονται στις απαιτήσεις καθημερινών συσκευών όπως ένα πλυντήριο ρούχων, ένα ψυγείο ή ένας φούρνος. Ωστόσο, τα υπάρχοντα πρωτόκολλα Διαδικτύου δεν σχεδιάζονται συνήθως για αυτούς τους δικτυωμένους ελεγκτές IoT, έτσι είναι λογικό να αναπτύσσονται ευπάθειες ασφαλείας των συστημάτων αυτών. Έχουν καταβληθεί πολλές προσπάθειες για την ανάπτυξη ασφαλών δικτύων που είναι συμβατά με το πρωτόκολλο IP, τα οποία είναι κατάλληλα για συσκευές IoT και χρησιμοποιούν τεχνικές ασφαλείας τελευταίας τεχνολογίας. Ωστόσο, πολλές από αυτές τις τεχνικές απαιτούν προσεκτική σχεδίαση από έμπειρους μηχανικούς δικτύου για τη συντήρηση ενός IoT συστήματος. (Lin, Bergmann, 2016) Γενικότερα στόχο επιθέσεων κατά της ασφάλειας και της ιδιωτικότητας μπορεί να αποτελέσουν κυβερνητικές ιστοσελίδες, χρηματοπιστωτικά συστήματα, websites ειδήσεων ή μέσων ενημέρωσης αλλά και στρατιωτικά δίκτυα. Τα κίνητρα της επίθεσης μπορεί να κυμαίνονται από την κλοπή ταυτότητας, δεδομένων πνευματικής ιδιοκτησίας ή και χρηματοοικονομική απάτη. Ο σκοπός των χάκερ διαφέρει από περίπτωση σε περίπτωση και ο προσδιορισμός του αποτελεί αντικείμενο μελέτης. Για παράδειγμα, η κλοπή πληροφοριών πιστωτικών καρτών έχει γίνει χόμπι για κάποιους χάκερ στις μέρες μας και οι ηλεκτρονικές τρομοκρατικές επιθέσεις που έχουν στόχο κυβερνητικά συστήματα υλοποιούνται για να εξυπηρετήσουν πολιτικά ή θρησκευτικά συμφέροντα. (Abomhara, Køien, 2015)

2.2: Ευπάθειες στο IoT

Με τον όρο ευπάθεια μπορούμε να περιγράψουμε ποια είναι τα τρωτά σημεία ενός συστήματος (λανθασμένος σχεδιασμός) που επιτρέπει στον εισβολέα πάρει τον έλεγχο του, να αποκτά πρόσβαση σε μη εξουσιοδοτημένα δεδομένα

(υποκλοπή δεδομένων) ή ακόμα και να πραγματοποιήσει επιθέσεις άρνησης εξυπηρέτησης (DoS). Συγκεκριμένα, τέτοιες ευπάθειες, μπορεί να είναι είτε αστοχίες στο υλικό ή το λογισμικό του συστήματος, είτε λανθασμένες πολιτικές και διαδικασίες που αφορούν τις συσκευές ή ακόμα και αδυναμία του χρήστη να χειριστεί μια τέτοια συσκευή με ορθό τρόπο. Οι ευπάθειες του υλικού (hardware) είναι πολύ δύσκολο να εντοπιστούν αλλά και να διορθωθούν ακόμη και αν αυτές εντοπιστούν κατά τη διάρκεια ελέγχου της συμβατότητας του υλικού. Όσον αφορά τα τρωτά σημεία του λογισμικού, αυτά μπορούν να εντοπιστούν στα λειτουργικά συστήματα, στο λογισμικό των συσκευών ή ακόμα και στα πρωτόκολλα επικοινωνίας των συσκευών. Επιπρόσθετα παράγοντες που μπορούν να φθείρουν το λογισμικό και να το κάνουν πιο ευάλωτο σε επιθέσεις αποτελούν η πολυπλοκότητα του ή ακόμα και λανθασμένες κινήσεις των χρηστών και κατασκευαστών. Για παράδειγμα η έλλειψη πόρων, δεξιοτήτων και γνώσεων και η αδυναμία διαχείρισης του συστήματος είναι σίγουρο ότι θα δημιουργήσουν προβλήματα. (Abomhara, Køien, 2015)

2.3: Βασικές Απειλές στο IoT

Μία απειλή εκμεταλλεύεται τις αδυναμίες ασφαλείας ενός συστήματος (ευπάθειες) και έχει αρνητικές επιπτώσεις σε αυτό. Οι απειλές μπορεί να είναι φυσικές ή να προέρχονται από ανθρώπους. Για παράδειγμα οι φυσικές απειλές (φωτιές, πλημμύρες, σεισμοί) μπορούν να καταστρέψουν συσκευές IoT και τα δεδομένα τους. Απειλές όμως που πραγματοποιούνται από κακόβουλους χρήστες μπορούν να πλήξουν την ασφάλεια και την ιδιωτικότητα των ατόμων, αυτές είναι αρκετές και συνεχώς αυξάνονται. (Abomhara, Køien, 2015)

Παρακάτω εξετάζονται κάποιες βασικές απειλές αλλά και οι επιπτώσεις τους.

I. Υποκλοπή Δεδομένων

Η πρώτη περίπτωση αφορά την υποκλοπή δεδομένων, για παράδειγμα, εν μέσω μιας συναλλαγής ένας χάκερ θα είχε την ευκαιρία να υποκλέψει πληροφορίες που θα μπορούσε να χρησιμοποιήσει προς δικό του όφελος. Ο τελευταίος θα μπορούσε να λάβει τα μηνύματα των RFID tags, αν αυτά πρώτα δεν έχουν κρυπτογραφηθεί. Τα δεδομένα που εκπέμπονται από την κάρτα καθώς και τα δεδομένα που εκπέμπονται από τον αναγνώστη μπορούν να παρακολουθούνται από τον χάκερ. Η απόσταση μέσα στην οποία θα μπορούσε να πραγματοποιηθεί η υποκλοπή εξαρτάται από την ευαισθησία του δέκτη και της κεραίας λήψης. Πιο συγκεκριμένα μετά από έρευνες

υποστηρίζεται ότι η επικοινωνία μεταξύ μιας κάρτας και ενός αναγνώστη μπορεί να υποκλαπεί από απόσταση 4 μέτρων.

II. Skimming

Το Skimming αποτελεί απειλή σχετική με απομακρυσμένη ενεργοποίηση του συστήματος. Επειδή μια ανέπαφη κάρτα δεν διαθέτει διακόπτη ON / OFF, δεν είναι απαραίτητο να ζητηθεί από τον κάτοχο της κάρτας η για να ενεργοποιηθεί αυτή. Σε αυτή την περίπτωση, ένας μη εξουσιοδοτημένος χρήστης μπορεί να προσπαθήσει να πάρει τον έλεγχο της κάρτας. Το ηλεκτρονικό διαβατήριό ,για παράδειγμα, θα μπορούσε να είναι ένας ιδανικός στόχος αυτού του είδους της επίθεσης. Έτσι είναι δυνατό, και μάλιστα από απόσταση , πληροφορίες ευαίσθητες για ένα άτομο να διαρρεύσουν. Φυσικά, ορισμένες λειτουργίες ασφάλειας που έχουν σχέση με τον έλεγχο πρόσβασης έχουν ενσωματωθεί για να αντιμετωπιστούν οι απειλές. Μάλιστα επειδή ένας άνθρωπος δεν είναι σε θέση να ανιχνεύσει ένα ηλεκτρομαγνητικό πεδίο, αυτή η επίθεση είναι πολύ ανησυχητική για την προστασία της ιδιωτικότητας του ατόμου. Ο τρόπος λειτουργίας του είναι απλός: συγκεκριμένα με έναν ενσωματωμένο -σε ένα κινητό- αναγνώστη NFC μπορούν να ανιχνευθούν παράνομα, δεδομένα ανέπαφων καρτών συναλλαγής. Ο κακόβουλος χρήστης μπορεί να κρύψει τον σαρωτή και να τον τοποθετήσει κοντά στο θύμα έτσι ώστε να κλέβει ασύρματα τις πληροφορίες της κάρτας πληρωμών του θύματος . (Εικόνα 2.1)

Εικόνα 2.1: Ο κακόβουλος χρήστης κρύβει τον σαρωτή & τον τοποθετεί κοντά στο θύμα έτσι ώστε να κλέβει ασύρματα τις πληροφορίες της κάρτας πληρωμών του θύματος.



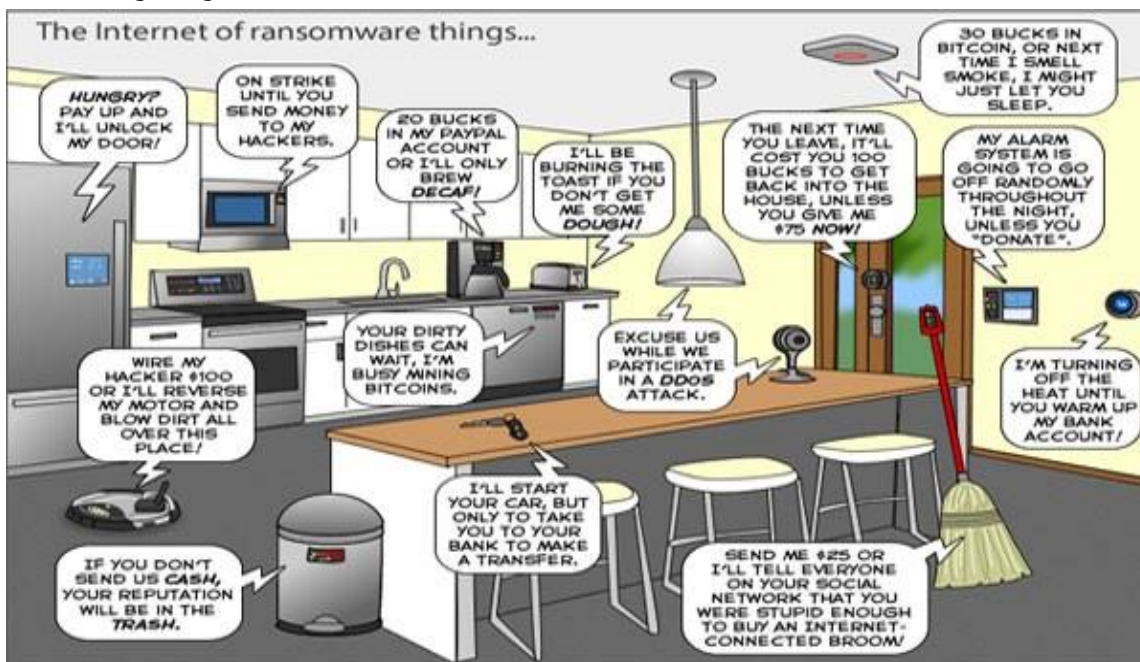
III. Blockers

Η χρήση μιας blocker tag έχει προταθεί ως λύση για την προστασία των δεδομένων. Συγκεκριμένα εμποδίζει τους κακόβουλους readers να εντοπίζουν τις ετικέτες και να λαμβάνουν πληροφορίες από το σύστημα. Αν και αυτή η λύση είναι απλή στην εφαρμογή και έχει χαμηλό κόστος, είναι δυνητικά επικίνδυνη και μπορεί να χαρακτηριστεί ως μια επιπρόσθετη απειλή για το σύστημα RFID αν χρησιμοποιηθεί ως κακόβουλο εργαλείο για να επιτεθεί στο σύστημα. Αυτή μπορεί να χαρακτηριστεί ως απειλή άρνησης πρόσβασης (DoS). Με τους blockers λοιπόν παρουσιάζεται μια νέα κατηγορία επιθέσεων: επιθέσεις που αποσκοπούν στην αποτροπή της σωστής λειτουργίας του συστήματος. Οι κακόβουλοι blockers χρησιμοποιούν το βασικό πρωτόκολλο με τέτοιο τρόπο ώστε η συναλλαγή να μην προχωρά και να πραγματοποιείται ασταμάτητα μια προκαταρκτική φάση ταυτοποίησης. (Savry,Vacherand, 2010)

IV. Ransomware

Το Ransomware αποτελεί μια κατηγορία κακόβουλου λογισμικού το οποίο κλειδώνει τα αρχεία του χρήστη η απειλεί να τα δημοσιοποιήσει μέχρις ότου αυτός δώσει λύτρα. Το λογισμικό αυτό είναι πάρα πολύ διαδεδομένο στους οικιακούς υπολογιστές και στα εταιρικά δίκτυα και χρησιμοποιεί κρυπτογράφηση ούτως ώστε να κλειδώσει τα αρχεία. Ακόμα, μπορεί να μεταδοθεί πολύ εύκολα από υπολογιστή σε υπολογιστή. Τελευταία όμως, οι ερευνητές τονίζουν ότι είναι απλώς θέμα χρόνου πριν οι κακόβουλοι χρήστες του ransomware ξεκινήσουν να κλειδώνουν και έξυπνες συσκευές. (Εικόνα 2.2) Μάλιστα έχει ήδη επιδειχθεί από ειδικούς ερευνητές που ασχολούνται με την ασφάλεια ο τρόπος με τον οποίο θα μπορεί να εγκατασταθεί ransomware σε έξυπνους θερμοστάτες. Με τον τρόπο αυτό λοιπόν θα μπορούσαν να αυξήσουν τη θερμοκρασία σε μία μέγιστη τιμή και να απειλήσουν τον ιδιοκτήτη ότι για να τη επαναφέρουν στο φυσιολογικό εκείνος θα πρέπει να πληρώσει λύτρα με Bitcoin. Παρόμοιες, μάλιστα επιθέσεις είναι βέβαιο ότι μπορούν να πραγματοποιηθούν και σε άλλα αντικείμενα όπως έξυπνες πόρτες γκαράζ, ψυγείο ή ακόμα και τηλεοράσεις. Έτσι λοιπόν η χρήση γνήσιου λογισμικού, η χρήση προγραμμάτων για προστασία από ιούς αλλά και η τακτική ενημέρωση του λογισμικού θεωρούνται απαραίτητα μέτρα προς αποφυγή τέτοιων καταστάσεων. (Liska,Gallo, 2017)

Εικόνα 2.2: Τι θα συνέβαινε αν το ransomware κλείδωνε όλες τις έξυπνες συσκευές ενός σπιτιού?



2.3.1: Προστασία Ενάντια στις Απειλές

Noisy Reader

Γενικά τα συστήματα RFIDs τροφοδοτούν τις ετικέτες (tags) με ένα σήμα σταθερού πλάτους που εκπέμπεται από τον αναγνώστη (reader) . Η ιδέα προκειμένου να αποτραπούν οι υποκλοπές είναι να σχεδιαστεί ένας reader ο οποίος κατά τη διάρκεια της ανάγνωσης της ετικέτας, εκπέμπει ένα κατάλληλα διαμορφωμένο "θορυβώδες" σήμα αντί ενός σταθερού εύρους. Αυτό το θορυβώδες σήμα με τη σειρά του διαμορφώνεται κατά απόκριση της ετικέτας. Δεδομένου ότι ο αναγνώστης είναι ο μόνος που γνωρίζει το συγκεκριμένο σχέδιο θορύβου, είναι επίσης ο μόνος που μπορεί να αφαιρέσει τον (διαμορφωμένο) θόρυβο έτσι ώστε να "αποκρυπτογραφήσει" τις πληροφορίες που μεταδίδονται από την ετικέτα. Οποιοσδήποτε άλλος αναγνώστης λοιπόν δεν θα μπορέσει να καταγράψει τον θόρυβο και συνεπώς να διαβάσει σωστά τα δεδομένα της ετικέτας. (Savry,Vacherand, 2010)

Βιομετρία

Οι παραδοσιακές μέθοδοι προστασίας όπως ο κωδικός πρόσβασης , για τον έλεγχο ταυτότητας σε έναν έξυπνο κόμβο, δεν ικανοποιούν στην πραγματικότητα την τεχνολογία του IoT, αφού έτσι κι αλλιώς η παραπάνω μέθοδος δεν εξασφαλίζει σε επαρκή βαθμό την ασφάλεια. Στην προκειμένη

περίπτωση ο σκοπός είναι η επίτευξη του μέγιστου βαθμού ασφαλείας για συστήματα IoT, όπου όπως αναφέρθηκε και παραπάνω οι παραδοσιακές μέθοδοι επαλήθευσης γνησιότητας καθίστανται εμπόδιο σε αυτό. Οι κωδικοί πρόσβασης μπορούν να ξεχαστούν, να ευρεθούν ή να διαρρεύσουν και να θέσουν σε κίνδυνο την ασφάλεια του χρήστη. Μπορεί επίσης να τεθεί σε κίνδυνο και η ασφάλεια άλλων συσκευών IoT εάν χρησιμοποιηθεί ο ίδιος κωδικός πρόσβασης. Ο συνδυασμός του κωδικού πρόσβασης με έναν πρόσθετο παράγοντα επαλήθευσης ταυτότητας ενισχύει την ασφάλεια, αλλά μειώνει την ευκολία χρήσης της εφαρμογής. Όλες αυτές οι αδυναμίες των παραδοσιακών μεθόδων επαλήθευσης ταυτότητας μπορούν να διορθωθούν με τη χρήση βιομετρικών στοιχείων για τον έλεγχο ταυτότητας όσον αφορά τη συσκευή του IoT. Η βιομετρία χρησιμοποιεί τα οργανικά χαρακτηριστικά ενός ατόμου, όπως τα δακτυλικά αποτυπώματα ή τα χαρακτηριστικά της ίριδας του ματιού, έτσι ώστε να ταυτοποιηθεί ο χρήστης. Δεδομένου ότι αυτά τα χαρακτηριστικά είναι μοναδικά για ένα άτομο, μπορούν να χρησιμοποιηθούν ως ασφαλής μέθοδος πιστοποίησης. Ένα άλλο στοιχείο που ενισχύει τη μέθοδο αυτή είναι ότι τα βιομετρικά χαρακτηριστικά δεν διαφοροποιούνται με το χρόνο ή την ηλικία, ούτε είναι εύκολο να αντιγραφούν. Όλες αυτές οι ιδιότητες προσδίδουν στην βιομετρία ένα πλεονέκτημα έναντι της παραδοσιακής μεθόδου ταυτοποίησης. Η βιομετρία εξαλείφει τις αδυναμίες των κωδικών πρόσβασης ενώ από την άλλη προσφέρει μια αναμφισβήτητα καλύτερη λύση ελέγχου ταυτότητας. (Subha , 2017)

2.4: Τεχνολογίες Ασφάλειας & Ιδιωτικότητας

Αποτελεί κοινό τόπο ότι στο IoT τα RFIDs διαδραματίζουν σημαντικό ρόλο. Τα τελευταία όπως αναφέρεται και στην αρχή της εργασίας όλο και περισσότερο αναπτύσσονται και εφαρμόζονται στην καθημερινότητα των ανθρώπων. Μάλιστα , αυτά αναμένεται να αντικαταστήσουν της διάρρευσης των οποίων λοιπόν η ανάπτυξη μηχανισμών ασφαλείας και ιδιωτικότητας είναι σίγουρα αναγκαία. Για παράδειγμα εάν δεν εφαρμοστεί μια καλή εφαρμογή ασφαλείας, οι ετικέτες μπορούν να αναγνωστούν από μη εξουσιοδοτημένους κακόβουλους χρήστες. Επιπλέον, τα περισσότερα από τα διεθνή ή βιομηχανικά πρότυπα χρησιμοποιούν είτε έναν απλό έλεγχο ασφαλείας (με βάση τον κωδικό πρόσβασης) είτε δεν κάνουν χρήση καμίας μεθόδου ασφαλείας έτσι ώστε να διατηρήσουν τις εφαρμογές μιας ετικέτας πολύ φτηνές. Αυτό μπορεί να προκαλέσει σοβαρούς κινδύνους, δεδομένου ότι ένας κωδικός πρόσβασης μπορεί να χρησιμοποιηθεί εύκολα για να παρακολουθηθεί μια ετικέτα. Τελευταία έχουν γίνει πολλές προσπάθειες για

σχεδίαση ασφαλών αλγορίθμων (αλγόριθμοι κρυπτογράφησης ιδιωτικού κλειδιού). Ωστόσο, λόγω των περιορισμών των λειτουργιών των αλγορίθμων ιδιωτικού κλειδιού, δεν μπορούν να ικανοποιηθούν όλες οι ανάγκες των συστημάτων RFID, οι οποίες αφορούν την επεκτασιμότητα του συστήματος και την ασφάλεια έναντι των επιθέσεων παρακολούθησης.

2.4.1: Πρότυπα ασφαλείας RFID

Στη σημερινή εποχή έχουν δημιουργηθεί νέα πρότυπα ασφαλείας για τα RFID όπως το ISO / IEC και το EPCglobal (εξαιτίας των αυξανόμενων εφαρμογών για τις βιομηχανίες). Το τελευταίο έχει στόχο να δημιουργηθεί ένα παγκόσμιο πρότυπο για τα RFID και επιπλέον για την ανταλλαγή δεδομένων μέσω του δικτύου EPCglobal. Μερικά από τα σημαντικότερα παραδείγματα προτύπων είναι το ISO / IEC 14443/15693 για τις ασύρματες έξυπνες κάρτες, το ISO 11784 5/14223 για την παρακολούθηση των ζώων και το ISO / IEC 18000 για τη διαχείριση των στοιχείων. Στα περισσότερα πρότυπα, τα χαρακτηριστικά ελέγχου ταυτότητας βασίζονται σε ένα απλό σύστημα κωδικού πρόσβασης. Ως εκ τούτου, η ασφάλεια μπορεί να διακυβευτεί εύκολα, δεδομένου ότι ένας κωδικός πρόσβασης μπορεί απλά να διαβαστεί. Για την προστασία της ιδιωτικότητας, μια ετικέτα διαγράφεται όταν ένα προϊόν αγοράζεται από έναν τελικό χρήστη. (Ki Lee et al., 2010)

2.4.2: Πρωτόκολλα Ασφαλείας στο IoT

1] Πρωτόκολλο ZigBee

Το πρωτόκολλο αυτό χρησιμοποιείται για τη δημιουργία προσωπικών δικτύων αισθητήρων, ψηφιακά ραδιόφωνα, έξυπνα σπίτια ή ακόμα και για μια ιατρική συσκευή και είναι σχεδιασμένο για να λειτουργεί με ασύρματη σύνδεση. Το ZigBee είναι απλούστερο και λιγότερο δαπανηρό από ό, τι άλλα ασύρματα προσωπικά δίκτυα περιοχής (WPANs), όπως το Bluetooth ή το Wi-Fi. Τέλος μπορεί να καλύψει αποστάσεις μεταξύ 10-20 μέτρων. Το ZigBee βασίζεται στο πρότυπο IEEE 802.15.4, αλλά σε αντίθεση με το 6LoWPAN, δεν μπορεί εύκολα να επικοινωνήσει με άλλα πρωτόκολλα. Ένα πλεονέκτημα του ZigBee, ωστόσο, είναι ότι οι κόμβοι μπορούν να παραμείνουν σε λειτουργία αναστολής τις περισσότερες φορές, αυξάνοντας δραστικά τη διάρκεια ζωής της μπαταρίας. (Egan, 2012)

2] Πρωτόκολλο 6LoWPAN

Το 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) είναι ένα πρωτόκολλο σχεδιασμένο από το IETF για να επιτρέψει τη μεταφορά πακέτων IPv6 μέσω ασύρματων δικτύων IEEE 802.15.4. Η βασική ιδέα για τη δημιουργία του ήταν ότι το πρωτόκολλο IP πρέπει να εφαρμοστεί και σε όλα τα συστήματα που λειτουργούσαν με barcodes παλαιότερα. Ενώ αυτό δημιουργήθηκε για να εξυπηρετεί μικρότερες συσκευές (χαμηλής κατανάλωσης) του IoT. Η σουίτα IPsec Security Protocol (IPsec) έχει καθορισμένες κεφαλίδες ελέγχου ταυτότητας (AH) για να επιτρέψει την ακεραιότητα, την εμπιστευτικότητα και την αυθεντικότητα των δεδομένων. (Mulligan, 2007)

3] Πρωτόκολλο CoAP (Constrained Application Protocol)

Το CoAP είναι ένα πρωτόκολλο εφαρμογής τύπου HTTP σχεδιασμένο για δίκτυα συσκευών περιορισμένων πόρων. Καθώς υπάρχουν κάποιες ειδικές απαιτήσεις όπως για παράδειγμα η ανάγκη για ομαδική επικοινωνία σε δίκτυα IoT, το CoAP παρέχει υποστήριξη πολλαπλής διανομής κάτι το οποίο δεν παρέχει το HTTP. Προκειμένου να ταιριάζει καλύτερα στις συνδέσεις χαμηλού εύρους ζώνης και περιβάλλοντα χαμηλής υπολογιστικής ισχύος, το πρωτόκολλο User Datagram Protocol (UDP) υιοθετείται από το CoAP. (Lin, Bergmann, 2016)

2.4.3: Τεχνολογίες ενίσχυσης της ιδιωτικότητας (PET)

Οι απαιτήσεις απορρήτου και εξασφάλισης της ιδιωτικότητας των πελατών είναι δεδομένα αρκετά υψηλές. Έχουν αναπτυχθεί πολλές τεχνολογίες στον τομέα και το στοιχείο είναι να επιτευχθούν οι στόχοι για την προστασία της ιδιωτικότητας. Οι τεχνολογίες PET λοιπόν μπορούν να χωριστούν σε ορισμένες κατηγορίες. Η πρώτη σχετίζεται με τα ιδιωτικά εικονικά δίκτυα (VPN) που δημιουργούνται από κλειστές ομάδες επιχειρηματικών εταίρων. Όπως γίνεται αντιληπτό, στα δίκτυα αυτά δεν επιτρέπει μια δυναμική και παγκόσμια ανταλλαγή πληροφοριών και αυτές είναι διαθέσιμες σε περιορισμένους συμμετέχοντες, οι οποίοι κινούνται σε ένα ασφαλές περιβάλλον που υπόσχεται εμπιστευτικότητα και ακεραιότητα. Για την προστασία των δεδομένων εφαρμόζεται κρυπτογράφηση προκειμένου να εμποδιστεί η διάδοση των δεδομένων. Μέσα στις λειτουργίες του VPN περιλαμβάνονται λειτουργίες όπως κοινή χρήση και πρόσβαση σε δεδομένα που δεν είναι ελεύθερα προς το ευρύ κοινό. Για παράδειγμα κατά τη διάρκεια

ηλεκτρονικών αγορών ένας χρήστης χρειάζεται να στείλει τους προσωπικούς του κωδικούς στον server του καταστήματος, με τη χρήση λοιπόν του VPN γίνεται κρυπτογράφηση των δεδομένων του και αυτά παραμένουν ασφαλή. Άλλη μια κατηγορία αποτελεί το Onion Routing, κατά τη διάρκεια εφαρμογής του οποίου τα δεδομένα κρυπτογραφούνται κατά τη μεταφορά τους κάθε φορά που φτάνουν σε κάποιο κόμβο και τελικά στον τελευταίο κόμβο γίνεται η αποκρυπτογράφηση τους. Ένα γεγονός που δε θα πρέπει να παραβλεφθεί είναι ότι μέσω της τεχνικής αυτής αυξάνονται οι χρόνοι αναμονής και ως εκ τούτου δημιουργούνται θέματα επιδόσεων του συστήματος. Όσον αφορά τη νομική υπόσταση του ζητήματος η Ευρωπαϊκή Επιτροπή βρίσκεται σε επαγρύπνηση στα θέματα που αφορούν την ασφάλεια και την ιδιωτικότητα και σχετίζονται με τα RFIDs και το Διαδίκτυο. Το 2009 μάλιστα η Ευρωπαϊκή Επιτροπή αποφάσισε (σχετικά με την εφαρμογή των αρχών προστασίας δεδομένων σε εφαρμογές των RFIDs) να παρέχει οδηγίες στα κράτη μέλη της ώστε το σύνολο τέτοιων εφαρμογών να λειτουργεί σε ένα νόμιμο και δεοντολογικό πλαίσιο το οποίο θα σέβεται τα δικαιώματα των ανθρώπων στην ιδιωτικότητα και την προστασία των προσωπικών τους δεδομένων. Συγκεκριμένα, η σύσταση περιγράφει τα μέτρα τα οποία περιλαμβάνουν ότι η βιομηχανία σε συνεργασία με τους ενδιαφερόμενους φορείς θα πρέπει να αναπτύξει ένα πλαίσιο κανόνων για την ιδιωτικότητα αλλά και για την εκτίμηση αντίκτυπου παραβίασης ιδιωτικότητας (Privacy Impact Assessment). (Weber, 2010) Η PIA είναι μια μεθοδολογία για την προστασία της ιδιωτικότητας των ανθρώπινων δραστηριοτήτων ή άλλων υπηρεσιών που περιλαμβάνουν την επεξεργασία προσωπικών πληροφοριών. Μία PIA είναι μια συστηματική διαδικασία που προσδιορίζει και αξιολογεί, από την οπτική γωνία όλων των ενδιαφερομένων, τις πιθανές επιπτώσεις στην προστασία της ιδιωτικότητας που αφορά μία δραστηριότητα και περιλαμβάνει αναζήτηση τρόπων αποφυγής ή μετριασμού των αρνητικών επιπτώσεων στην ιδιωτικότητα. Τέλος εξετάζεται αν ο φορέας έχει λάβει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εξασφάλιση της αντίστοιχης προστασίας. (Wright, 2012) Η Ευρωπαϊκή Επιτροπή επίσης εκφράζει την ανάγκη για τη συνεχή παρακολούθηση της προστασίας του χρήστη. Επιπρόσθετα η επιτροπή σκοπεύει να ξεκινήσει μια συζήτηση σχετικά με τις τεχνικές και τις νομικές πτυχές του δικαιώματος να υπάρχει η δυνατότητα αποσύνδεσης των RFIDs από το δικτυακό περιβάλλον των χρηστών οποτεδήποτε εκείνοι το θελήσουν ("Right to Silence of the Chips"). Γενικότερα η χρήση της τεχνολογίας των RFIDs τεχνικά γίνεται με τον ίδιο τρόπο σε όλο τον κόσμο. Συνεπώς, η λειτουργία των επιχειρήσεων θα περιπλεχτεί εάν υπάρχουν διαφορετικοί εθνικοί νόμοι. Επομένως είναι

προφανές ότι εάν τα προϊόντα με ετικέτες RFID είναι διαθέσιμα σε παγκόσμιο επίπεδο, οι νομικές διαδικασίες πρέπει να συγχρονιστούν. (Weber, 2010)

2.5: Συμπεράσματα

Τελικά και όπως φαίνεται από τα παραπάνω παραδείγματα, ήδη αναπτύσσονται ιδέες σχετικά με την ασφάλεια της χρήσης IoT. Πολλές καινοτομίες έχουν στόχο τη δημιουργία ασφαλών δικτύων επικοινωνιών που είναι συμβατά με το πρότυπο IP και όπως συνεπάγεται είναι κατάλληλα για συσκευές περιορισμένης πρόσβασης κάνοντας χρήση τεχνικών ασφαλείας τελευταίας τεχνολογίας. Ωστόσο, η σχεδίαση τέτοιων συστημάτων πρέπει να γίνεται πολύ προσεκτικά και έμπειρους μηχανικούς δικτύου έτσι ώστε να σχεδιαστεί και να διατηρηθεί ένα ασφαλές σύστημα IoT.

Κεφάλαιο 3:Εφαρμογές του Internet of Things

3.1: Έξυπνη Πόλη

Με την τεχνολογία να εξελίσσεται στο ανθρώπινο περιβάλλον ολόένα και περισσότερο, το διαδίκτυο των πραγμάτων (IoT) στο εγγύς μέλλον, υπόσχεται ότι τα αντικείμενα της καθημερινής ζωής θα διασυνδεθούν με αισθητήρες και RFIDs για ψηφιακή επικοινωνία αλλά και κατάλληλα πρωτόκολλα για την επικοινωνία των συσκευών μεταξύ τους αλλά και με των άνθρωπο. Στο πλαίσιο αυτό το όραμα της έξυπνης πόλης, το οποίο έχει αρχίσει να υλοποιείται σε αρκετές πόλεις του πλανήτη, θα προσθέσει μια καλύτερη ποιότητα ζωής στους κατοίκους της αλλά και θα εξοικονομήσει πόρους. Μια έξυπνη πόλη αναλυτικότερα , μπορεί να ωφελήσει τους κατοίκους της σε τομείς όπως : στην διαχείριση και τη βελτιστοποίηση των δημόσιων υπηρεσιών (μέσα μαζικής μεταφοράς και στάθμευση) , στο φωτισμό , στη συντήρηση των δημόσιων κτηρίων και τη διατήρηση της πολιτιστικής κληρονομιάς αλλά και στην αποκομιδή των σκουπιδιών, την υγιεινή των νοσοκομείων και το σχολείο.

Παρακολούθηση και συντήρηση κτιρίων

Για τη σωστή συντήρηση ιστορικών κτιρίων μιας πόλης απαιτείται μια συνεχής παρακολούθηση της πραγματικής κατάστασης του κάθε κτιρίου αλλά και των περιοχών που επηρεάζονται περισσότερο από εξωτερικούς παράγοντες. Στην προκειμένη περίπτωση λοιπόν , το IoT μπορεί να υποστηρίξει μια βάση δεδομένων του κτιρίου η οποία θα περιέχει μετρήσεις αισθητήρων που αφορούν: μετρήσεις της δομικής ακεραιότητας του κτηρίου (κραδασμοί και παραμορφώσεις) , παρακολούθηση των επιπέδων ρύπανσης και της θερμοκρασίας αλλά και της υγρασίας έτσι ώστε να υπάρχει μια πλήρης καταγραφή των περιβαλλοντικών συνθηκών. Έτσι λοιπόν η βάση δεδομένων αυτή , θα μειώσει την ανάγκη για τακτικές δοκιμές του κτιρίου από τους αρμόδιους φορείς (η οποία απαιτεί αρκετές δαπάνες) και θα επιτρέψει μια αρκετά στοχευμένη και προληπτική συντήρηση και αποκατάσταση όσον αφορά το κτίριο. Η βάση δεδομένων αυτή επιπρόσθετα, μπορεί να γίνει διαθέσιμη στο κοινό έτσι ώστε οι πολίτες να ενημερώνονται για τις ανάγκες και τη φροντίδα που απαιτείται για τη διατήρηση της πολιτιστικής κληρονομιάς. Στην πραγματικότητα για την υλοποίηση αυτής της υπηρεσίας, απαιτείται εγκατάσταση αισθητήρων στα κτίρια και τις γύρω περιοχές αλλά και η διασύνδεσή μεταξύ τους . Τέλος, θα είναι δυνατή η μελέτη των σεισμών και των δονήσεων έτσι ώστε να μελετηθεί ενδελεχώς η επίδραση των σεισμών στα κτίρια της πόλης. Η τεχνική αυτή μπορεί να εφαρμοστεί (εκτός από σημαντικά κτίρια της πόλης) και σε γέφυρες αλλά και

μνημεία προκειμένου να εξοικονομηθούν πόροι και να προληφθούν μελλοντικοί κίνδυνοι. (Zanella et al., 2014)

Διαχείριση αποβλήτων

Η διαχείριση των αποβλήτων αποτελεί πρωταρχικό ζήτημα στις περισσότερες πόλεις, εξαιτίας κυρίως του προβλήματος της μεταφοράς και αποθήκευσης σκουπιδιών στις χωματερές. Ωστόσο, οι λύσεις που μπορεί να προσφέρει το IoT στον τομέα αυτό είναι σημαντικές. Αναλυτικότερα μια τέτοια έξυπνη υπηρεσία διαχείρισης αποβλήτων, περιλαμβάνει τη διασύνδεση των κάδων απορριμμάτων με αισθητήρες (Εικόνα 3.1), με σκοπό την παρακολούθηση του ύψους των σκουπιδιών, σε πραγματικό χρόνο, στους κάδους όλης της πόλης. Το αποτέλεσμα θα είναι μεγάλη οικονομία στην ενέργεια, αφού θα ήταν γνωστό από τα απορριματοφόρα ποιοι κάδοι είναι γεμάτοι και ποιοι όχι, αποφεύγοντας τις άσκοπες διαδρομές. Επιπλέον καμία περιοχή δε θα είχε πρόβλημα με το ύψος των σκουπιδιών λόγω της δράσης αυτής και τα οικολογικά οφέλη θα ήταν μεγάλα. Τέλος από το 2015 στην πόλη Νίτρα της Σλοβακίας έχουν εγκατασταθεί αισθητήρες για την καλύτερη διαχείριση απορριμμάτων, με τη χρήση στατιστικών εργαλείων παρακολουθείται αναλυτικά το ύψος και το είδος των ανακυκλώσιμων προϊόντων. Μάλιστα υπολογίζεται ότι έχουν εξοικονομηθεί πόροι πάνω από το 30%, που αφορούν το κόστος αποκομιδής σκουπιδιών. (Zanella et al., 2014)

Εικόνα 3.1: Αισθητήρας τοποθετημένος σε κάδο για την παρακολούθηση των απορριμμάτων.



Έξυπνος φωτισμός

Η βελτιστοποίηση της αποτελεσματικότητας του φωτισμού του δρόμου είναι ένα σημαντικό χαρακτηριστικό για την εξοικονόμηση ενέργειας. Ειδικότερα, με τη χρήση ειδικών αισθητήρων στους λαμπτήρες μπορεί να προσαρμοστεί η ένταση του φωτός του ανάλογα με την ώρα και τη φωτεινότητα από τον ήλιο.

Ακόμα ανάλογα με τις καιρικές συνθήκες και την παρουσία ανθρώπων το φως θα προσαρμόζεται αυτόματα . Η ασφάλεια των πολιτών επίσης μπορεί να αυξηθεί , και συγκεκριμένα με την ένταση του φωτός να είναι μεγαλύτερη σε σημεία που υπάρχουν διαβάσεις. (Zanella et al., 2014)

Έξυπνα φανάρια- Αποσυμφόρηση κίνησης

Τα έξυπνα φανάρια είναι μια νέα τεχνολογία που εφαρμόζεται πιλοτικά σε αρκετές πόλεις . Αυτά δημιουργούν ένα σύστημα ελέγχου της κυκλοφορίας των οχημάτων κατά το οποίο στα φανάρια εφαρμόζεται μια σειρά αισθητήρων έτσι ώστε να δρομολογούν έξυπνα την κίνηση των οχημάτων και των πεζών. Τα σήματα των αισθητήρων επικοινωνούν μεταξύ τους και προσαρμόζονται στις μεταβαλλόμενες συνθήκες κυκλοφορίας . Μάλιστα η νέα αυτή τεχνολογία παρακολουθεί τον αριθμό των οχημάτων και πραγματοποιεί αλλαγές σε πραγματικό χρόνο για να αποφευχθεί η συμφόρηση στο μεγαλύτερο δυνατό βαθμό. Δηλαδή να αυξάνονται τα πράσινα φανάρια εκεί όπου η κίνηση είναι μεγαλύτερη. Ειδικότερα, τα αυτοκίνητα εκείνα που περιέχουν κατάλληλο λογισμικό θα λαμβάνουν μηνύματα για την ταχύτητα που πρέπει να οδηγήσουν, ώστε να φτάσουν στα φανάρια ακριβώς όταν εκείνα γίνουν πράσινα. Επιπλέον στο Ηνωμένο Βασίλειο στην πόλη Swindon, δοκιμάζονται συστήματα για την πρόληψη των ατυχημάτων. Συγκεκριμένα τα φανάρια όταν αισθάνονται ότι ένας αυτοκινητιστής που βρίσκεται σε κοντινή απόσταση από αυτά ταξιδεύει πολύ γρήγορα αλλάζουν το χρώμα τους σε κόκκινο. (Schaffers et al, 2011)Παραπλήσια τέτοια συστήματα αρχίζουν μάλιστα να εφαρμόζονται και στην Ελλάδα και συγκεκριμένα στα Τρίκαλα, όπου έχουν εφαρμοστεί LED που απεικονίζουν το χρόνο έως ότου τα φανάρια γίνουν πάλι πράσινα ή κόκκινα, αλλά και ηχητικούς τόνους για τους τυφλούς πεζούς οι οποίοι με μια ηχητική ειδοποίηση ενημερώνονται για τη στιγμή που θα πρέπει να περάσουν τη διάβαση. Ενώ η εφαρμογή τέτοιων συστημάτων σχεδιάζεται να γίνει και σε αρκετές περιοχές της Δυτικής Ελλάδας μέχρι το τέλος του 2018. Επίσης τέτοια συστήματα εφαρμόζονται ήδη σε χώρες όπως η Αγγλία, η Ιαπωνία, η Ινδία , η Αυστραλία και η Ισπανία.

Εικόνα 3.2: Έξυπνο φανάρι στη Βαρκελώνη.



Άλλες Εφαρμογές

- **Smart Parking**

Παρακολούθηση της διαθεσιμότητας των χώρων στάθμευσης στην πόλη και ενημέρωση των οδηγών.

- **Noise Urban Maps**

Παρακολούθηση ήχου σε περιοχές που βρίσκονται μπαρ και κεντρικά σημεία σε πραγματικό χρόνο μέσω χαρτών.

- **Ανίχνευση Smartphone**

Εντοπισμός έξυπνων συσκευών (iPhone,Android) και γενικά οποιαδήποτε συσκευή που λειτουργεί με διασυνδέσεις WiFi ή Bluetooth.

- **Ευφυείς αυτοκινητόδρομοι**

Προειδοποιητικά μηνύματα σε οδηγούς ανάλογα με τις κλιματικές συνθήκες ή έκτακτα γεγονότα όπως ατυχήματα ή κυκλοφοριακή συμφόρηση. (Schaffers et al., 2011)

3.2: Έξυπνο Περιβάλλον

Έλεγχος μόλυνσης του αέρα

Η ποιότητα του αέρα είναι παράγοντας ζωτικής σημασίας για το περιβάλλον αλλά και τους ανθρώπους. Μια κακή τέτοια ποιότητα που συναντάται στις μεγάλες πόλεις μπορεί να εκθέσει τους πολίτες σε ατμοσφαιρική ρύπανση και να οδηγήσει σε κρίσεις άσθματος, καρκίνο του πνεύμονα, καρδιακές παθήσεις ή χρόνια βρογχίτιδα. Η ανάπτυξη των δικτύων χαμηλής ισχύος ευρείας περιοχής (LPWA) οδήγησαν σε διαθεσιμότητα μικρών, φορητών αλλά και χαμηλού κόστους και πάντα συνδεδεμένων αισθητήρων. Με χαμηλές ταχύτητες μεταφοράς δεδομένων και μεγάλη απόσταση, οι αισθητήρες LPWA μπορούν να συνδεθούν με διάφορα αντικείμενα, για να μετρήσουν και να αναφέρουν την ποιότητα του αέρα με πολύ μεγάλη ακρίβεια. Με την εξέλιξη του IoT θα είναι εφικτό να γίνεται έλεγχος των εκπομπών διοξειδίου του άνθρακα που προέρχεται από τα εργοστάσια, έλεγχος της ρύπανσης που εκπέμπεται από αυτοκίνητα και των τοξικών αερίων που παράγονται σε αγροκτήματα , μέσω αισθητήρων. Για παράδειγμα, σε χώρες όπως η Κίνα , η Γαλλία, η Ισπανία, η Πορτογαλία και η Βραζιλία διερευνάται κατά πόσο οι

συνδεδεμένοι αισθητήρες θα μπορούσαν να βελτιώσουν την παρακολούθηση της ποιότητας του αέρα. (Xiaojun et al, 2015)

Ανίχνευση Πυρκαγιάς

Με τη χρήση ειδικών αισθητήρων ,γίνεται έλεγχος και πρόληψη ενάντια στις πυρκαγιές . Πιο αναλυτικά αν η θερμοκρασία ανέβει πάνω από το φυσιολογικό ή αν ο άνεμος είναι πολύ ισχυρός σημαίνει συναγερμός προληπτικά και ειδοποιούνται οι αρμόδιες αρχές. Επίσης οι αισθητήρες ανίχνευσης καπνού στέλνουν τα κατάλληλα σήματα προς τις αρχές.(ZHANG, 2009)

Άλλες Εφαρμογές

Παρακολούθηση στάθμης χιονιού

Αισθητήρες μετρούν την στάθμη του χιονιού έτσι ώστε να γίνεται έλεγχος και πρόληψη για την αποφυγή χιονοστιβάδων.

Πρόωρη ανίχνευση σεισμού

Πραγματοποιείται έλεγχος με αισθητήρες σε συγκεκριμένα σημεία για πρόωρη ανίχνευση σεισμών. (Xiaojun et al, 2015)

3.3: IoT στην Υγεία

Το IoT μπορεί να δώσει αρκετές λύσεις όσον αφορά το σύστημα της υγείας βοηθώντας εκατομμύρια ασθενείς. Η συλλογή, αποθήκευση και ανάλυση μεγάλης ποσότητας ιατρικών πληροφοριών στο Cloud σε πραγματικό χρόνο, καθιστά δυνατή την ενεργοποίηση συναγερμού αν οι ζωτικές λειτουργίες ενός ανθρώπινου οργανισμού δεν συμπεριφέρονται φυσιολογικά. Αυτό το πρότυπο απόκτησης πληροφοριών επιτρέπει τη συνεχή και πανταχού παρούσα πρόσβαση σε ιατρικές πληροφορίες από οποιαδήποτε συνδεδεμένη συσκευή μέσω Διαδικτύου. Το πρωτόκολλο ZigBee μάλιστα βοηθάει στην εξοικονόμηση ενέργειας και τη μεγάλη διάρκεια ζωής των συνδεδεμένων αισθητήρων. Ένα παράδειγμα για το πόσο σημαντικό είναι ένα τέτοιο σύστημα αποτελεί ότι σύμφωνα με την έρευνα που πραγματοποιήθηκε στην Ινδία, η πλειοψηφία των οδικών ατυχημάτων οφείλεται στην άσχημη κατάσταση της υγείας των οδηγών, όπως τα καρδιακά προβλήματα ή οποιαδήποτε άλλα σοβαρά προβλήματα υγείας. Ένα έξυπνο σύστημα παρακολούθησης της υγείας μπορεί να μετράει παραμέτρους όπως η θερμοκρασία του σώματος και ο σφυγμός του ασθενή . Στη συνέχεια τα δεδομένα μεταδίδονται μέσω smartphone στο Internet. Αν ληφθούν από τον

οδηγό τυχόν μη φυσιολογικές τιμές, οι γιατροί μπορούν να ειδοποιηθούν σχετικά με τη θέση του οδηγού και να σταλεί ασθενοφόρο στην περιοχή. Τα δεδομένα που συλλέγονται από ένα νοσοκομείο για παράδειγμα μπορούν να σταλούν στην πλακέτα Intel Galileo Generation 2 (Εικόνα 3.3) η οποία λειτουργεί ως πύλη για την αποστολή των ληφθέντων δεδομένων μέσω Internet στο Cloud. Η τελευταία περιέχει έναν μικροεπεξεργαστή Intel Quark 400MHz, με μονό πυρήνα ενώ διαθέτει μπαταρία 7-15 volt και αποτελείται από 256 MB μνήμης RAM.

Εικόνα 3.3: Η πλακέτα Intel Galileo Generation 2.



Σε ένα σύστημα παρακολούθησης ασθενών στο νοσοκομείο ένας γιατρός μπορεί να έχει πρόσβαση στα δεδομένα του ασθενούς από οποιοδήποτε σημείο με δυνατότητα σύνδεσης στο Internet , να το αναλύσει και να ακολουθηθεί η σωστή θεραπεία. (Priyadarshini, 2016) Έτσι, το IoT όχι μόνο ενισχύει την ποιότητα της παρακολούθησης του ασθενούς αλλά και μειώνει το κόστος της περίθαλψης, θέτοντας τέλος στην ανάγκη για προσωπικό που ασχολείται με τη συλλογή δεδομένων και ανάλυση τους. (Kodali et al., 2015) Επιπρόσθετα εκτιμάται ότι μέχρι το 2050, περίπου το 20% του παγκόσμιου πληθυσμού θα είναι τουλάχιστον 60 ετών , αντιμετωπίζοντας όπως είναι λογικό προβλήματα που έχουν σχέση με χρόνιες ασθένειες όπως διαβήτης, καρδιαγγειακά νοσήματα ή καρκίνο . Όπως γίνεται λοιπόν κατανοητό δεν είναι δυνατό ούτε λογικό όλοι αυτοί οι ασθενείς να παραμένουν σε ιατρικά κέντρα ή νοσοκομεία για απεριόριστο χρονικό διάστημα. Η λύση θα ήταν διευκόλυνση της υγειονομικής περίθαλψης τους μέσω των εφαρμογών του IoT των οποίων τα δεδομένα του ασθενή αποστέλλονται και μελετώνται από γιατρούς οι οποίοι απομακρυσμένα θα προτείνουν την κατάλληλη θεραπεία. Με τους ασθενείς να λαμβάνουν τις θεραπείες και να τις εφαρμόζουν από το σπίτι τους (Doukas, Maglogiannis, 2012) . Σημαντική είναι και η βοήθεια προς τους ηλικιωμένους : πιο αναλυτικά μινιατούρες πομποί μπορούν να φορεθούν γύρω από το λαιμό ή τον καρπό , επιτρέποντας σε ένα άτομο να ζητήσει βοήθεια απλά πιέζοντας ένα κουμπί. Η συσκευή λοιπόν είναι ένα

τηλέφωνο έκτακτης ανάγκης συνδεδεμένο με ένα κέντρο εξυπηρέτησης ή κάποιο μέλος της οικογένειας. (Alam et al., 2012)

Άλλες Εφαρμογές:

Στατιστικά στοιχεία αθλητών

Μέτρηση απόδοσης αθλητή κατά την προπόνηση μέσω αισθητήρων για τον έλεγχο της φυσικής κατάστασης του αθλητή (καρδιακός ρυθμός, θερμοκρασία κλπ).

Ιατρικά ψυγεία

Έλεγχος συνθηκών και διαθεσιμότητας μέσα σε καταψύκτες που περιέχουν εμβόλια και φάρμακα. (Kodali et al., 2015)

3.4: Έξυπνο Σπίτι

Ένα έξυπνο σπίτι έχει σχέση με εφαρμογές χάρη στις οποίες παρακολουθείται το περιβάλλον του σπιτιού και διευκολύνεται ο απομακρυσμένος έλεγχος σε αυτό. Τα έξυπνα σπίτια αποτελούν έναν κλάδο της διάχυτης υπολογιστικής και περιλαμβάνουν την ενσωμάτωση του «έξυπνου» στις κατοικίες σε τομείς που αφορούν την άνεση, την υγειονομική περίθαλψη, την ασφάλεια και την εξοικονόμηση της ενέργειας.(Alam et al., 2012) Όσον αφορά τα οικιακά συστήματα άνεσης (θέρμανση , κλιματισμός , εξαερισμός , φωτισμός , πόρτες και παράθυρα) μπορούν να αυτοματοποιηθούν και να χρησιμοποιηθούν με τηλεχειρισμό μέσω ενός smartphone. Διάφορες ηλεκτρικές συσκευές όπως τα πλυντήρια ρούχων, τα πλυντήρια πιάτων, τα ψυγεία και οι συσκευές μαγειρέματος μπορούν να προγραμματιστούν έτσι ώστε να εκτελούν τα καθήκοντά τους. Στη σημερινή εποχή όλο και περισσότερα σπίτια ανά τον κόσμο αποκτούν τέτοιες εφαρμογές που έχουν στόχο τη βοήθεια των ηλικιωμένων αλλά και νεότερων ατόμων με νοητικά ή σωματικά προβλήματα υγείας. Οι εφαρμογές αυτές όμως έχουν στην πραγματικότητα στόχο να βελτιστοποιήσουν γενικότερα και την ποιότητα ζωής όλων των ανθρώπων. Μάλιστα στο Κολοράντο έχει αναπτυχθεί μια τέτοια εφαρμογή σπιτιού που χρησιμοποιεί νευρωνικά δίκτυα για τον έλεγχο της θερμοκρασίας, της θέρμανσης, και τον φωτισμό χωρίς να απαιτείται προηγούμενος προγραμματισμός από τους κατοίκους. Αυτό το σύστημα, που ονομάζεται ACHE, επιχειρεί να εξοικονομήσει ενέργεια με σεβασμό στο περιβάλλον αλλά των επιθυμιών των χρηστών. Η ACHE παρακολουθεί συνεχώς το περιβάλλον

και παρατηρεί τις συνήθειες των κατοίκων (χρήση των φώτων, ρύθμιση του θερμοστάτη). Από αυτά τα δεδομένα, δημιουργείται ένα είδος μηχανικής μάθησης, μια στοχαστική μορφή, έτσι ώστε να προβλεφθεί η μελλοντική συμπεριφορά. (Chana et al., 2008) Παρακάτω θα αναλυθούν κάποια από τα σημαντικότερα έξυπνα αντικείμενα που μπορούν να τοποθετηθούν σε ένα σπίτι.

Έξυπνος Θερμοστάτης

Ο έξυπνος θερμοστάτης Tado συνδέεται μέσω καλωδίου Ethernet στο ρούτερ προκειμένου να υπάρξει διασύνδεση μέσω του internet με ένα smartphone όπου ο χρήστης μπορεί μέσω της εφαρμογής του Tado να ρυθμίσει από το κινητό του τη θερμοκρασία του σπιτιού του. Αφού διασυνδεθούν όλοι οι θερμοστάτες στο σπίτι, η τελευταία εμφανίζεται στο κινητό και απεικονίζει τις συνθήκες του κάθε δωματίου ξεχωριστά. Επιπρόσθετα είναι δυνατό να δημιουργηθεί ένα πρόγραμμα που αφορά τις ώρες που ο θερμοσίφωνας θα ζεσταίνει το νερό. Για παράδειγμα ο χρήστης τις ώρες όπου λείπει από το σπίτι έχει προγραμματίσει να είναι απενεργοποιημένο το σύστημα και τις ώρες που είναι πιθανότερο να θέλει να κάνει μπάνιο ο θερμοστάτης αυτόματα θα είναι ενεργοποιημένος. Τέλος είναι δυνατό να αναπαρασταθούν στο smartphone και στατιστικά στοιχεία που αφορούν τη θερμοκρασία του σπιτιού για ολόκληρη την εβδομάδα. (30)

Εικόνα 3.4: Ο έξυπνος θερμοστάτης Tado.



Έξυπνες Λάμπες - Philips Hue

Οι έξυπνες λάμπες αυτές λειτουργούν ως εξής: Η γέφυρα συνδέεται στο ρούτερ με καλώδιο Ethernet, έτσι όπως αναφέρεται και παραπάνω επιτυγχάνεται η διασύνδεση με ένα smartphone. Αφού όλες οι λάμπες τοποθετηθούν, υπάρχει πλήρης έλεγχος από το κινητό τηλέφωνο για το ποιες χρονικές στιγμές θα ανοίγουν ή θα σβήνουν, για την ένταση του φωτός αλλά και την απόχρωση του. Τέλος είναι δυνατό οι παραπάνω λειτουργίες που αφορούν τα φώτα να πραγματοποιηθούν και με φωνητικές λειτουργίες. (31)

Έξυπνη Κάμερα-Nest Hello

Η κάμερα αυτή προσθέτει ασφάλεια σε ένα έξυπνο σπίτι, τοποθετείται στις εξώπορτες και διαθέτει αισθητήρες κίνησης. (Εικόνα 3.5) Μέσω της εφαρμογής που διαθέτει συνδέεται στο smartphone του κατόχου και τον ειδοποιεί όταν ένας επισκέπτης έρχεται στο σπίτι. Στο χρήστη μάλιστα δίνεται η δυνατότητα να ξεκλειδώσει την πόρτα (ειδικές κλειδαριές τοποθετούνται στις πόρτες) μέσω του κινητού του. Η αναγνώριση και αποθήκευση προσώπων αποτελεί επίσης μια σημαντική λειτουργία της κάμερας, έτσι όταν ένα γνωστό πρόσωπο καταφθάσει, ο ιδιοκτήτης ειδοποιείται φωνητικά. Η κάμερα αυτή καταγράφει εικοσιτέσσερις ώρες το εικοσιτετράωρο και το βίντεο αποθηκεύεται και γίνεται διαθέσιμο από την εφαρμογή της, έτσι επιτυγχάνεται μεγαλύτερος βαθμός ασφάλειας. (32)

Εικόνα 3.5: Η έξυπνη κάμερα Nest Hello .



Έξυπνοι Ανιχνευτές Καπνού

Οι ανιχνευτές αυτοί συνδέονται με ένα smartphone και ειδοποιούν το χρήστη στο κινητό του σε περίπτωση φωτιάς. Επίσης μπορεί να υποστηρίζεται και φωνητική λειτουργία μέσω λειτουργικού συστήματος. (33)

Συμπέρασμα

Σε περίπτωση λοιπόν όπου όλες οι παραπάνω εφαρμογές είναι συμβατές μεταξύ τους (από τον ίδιο κατασκευαστή) μπορεί να υπάρξει συνδυασμός των λειτουργιών τους μέσω μιας κοινής εφαρμογής. Για παράδειγμα ο χρήστης μπορεί να προγραμματίσει ότι αν ανιχνευθεί καπνός στο σπίτι οι λάμπες να αρχίσουν να αναβοσβήνουν ή σε περίπτωση που ανιχνευθεί κίνηση από τις κάμερες, τα φώτα να ανάβουν αυτόματα προς αποφυγή κάποιου κλέφτη.

3.5: Smart Farming

Η όλο και μεγαλύτερη ανάγκη για εξοικονόμηση πόρων έχει καταστήσει τις εφαρμογές του IoT μονόδρομο όσον αφορά τη γεωργία αλλά και την εκτροφή ζώων.

3.5.1: Εφαρμογές στη Γεωργία

Η ανάπτυξη υψηλής ακρίβειας ενσωματωμένων αισθητήρων οι οποίοι κάνουν μετρήσεις των περιβαλλοντολογικών συνθηκών στις φάρμες , έχει οδηγήσει στην ενεργοποίηση μιας νέου είδους γεωργίας, αυτή που λειτουργεί με βάση την ακρίβεια. Τα παραπάνω μπορούν να οδηγήσουν στη βελτίωση της παραγωγικότητας , την αύξηση των αποδόσεων και μεγαλύτερη κερδοφορία, την αποτελεσματικότερη άρδευση, την ακριβέστερη χρήση των λιπασμάτων και φυτοφαρμάκων για καλλιέργειες , μειώνοντας παράλληλα το περιβαλλοντικό αποτύπωμα. Μέσω τέτοιων εφαρμογών λοιπόν, οι οποίες συνδέονται με το internet και το cloud είναι δυνατή η επεξεργασία και ανάλυση των δεδομένων σε πραγματικό χρόνο, βελτιώνοντας έτσι την λήψη αποφάσεων από τους αγρότες. Οι καιρικές και περιβαλλοντικές συνθήκες (βροχή, υγρασία, χαλάζι) καθιστούν την γεωργία εξαιρετικά απρόβλεπτη , με την ανάγκη να ληφθούν τα κατάλληλα μέτρα έτσι ώστε να προστατευθούν οι καλλιέργειες να είναι μεγάλη. Για παράδειγμα, συνδυάζοντας δεδομένα από τη γονιμότητα του εδάφους , μαζί με υπηρεσίες για την πρόβλεψη καιρού, θα μπορούσαν να παρθούν καλύτερες αποφάσεις σχετικά με την άρδευση αλλά

και την τοποθέτηση μέσω λιπασμάτων συστατικών ουσιών στις οποίες υπάρχει έλλειψη στο έδαφος. Επιπρόσθετα ,παράσιτα και ασθένειες καταστρέφουν μεγάλο μέρος καλλιεργειών κάθε χρόνο, μικροί αισθητήρες και κάμερες εγκαθίστανται προκειμένου να παρακολουθούν την καλλιέργεια. Όταν εντοπίζεται κάποιο πρόβλημα ή ασθένεια στέλνεται μήνυμα στο smartphone του ιδιοκτήτη, αντίστοιχα τέτοια μηνύματα στέλνονται όταν η καλλιέργεια είναι έτοιμη για συγκομιδή. Επίσης ρομπότ και drones μπορούν να αφαιρέσουν με ακρίβεια τα ζιζάνια ή να τα εξολοθρεύσουν χρησιμοποιώντας λιγότερα χημικά. Ακόμα τα πρώτα είναι δυνατόν να χρησιμοποιηθούν για τη συλλογή της καλλιέργειας η οποία πραγματοποιείται σε αρκετά σημαντικότερο χρονικό διάστημα από την ανθρώπινη διαδικασία συλλογής. Τα drone αυτά επίσης, μέσω μηχανικής μάθησης, μπορούν να εντοπίσουν ανεπιθύμητη βλάστηση ή ζιζάνια και να αποστείλουν τα δεδομένα σε πραγματικό χρόνο στον αγρότη. (Kamilaris et al., 2016)

3.5.2: Εφαρμογές στην Κτηνοτροφία

Ένα έξυπνο σύστημα στον τομέα της κτηνοτροφίας, λειτουργεί έτσι ώστε τα δεδομένα -σε πραγματικό χρόνο- να στέλνονται σε ένα smartphone, έτσι ώστε να επιτυγχάνεται παρακολούθηση της κατάστασης και της τοποθεσίας των ζώων από να λειτουργεί από απόσταση. Στον τομέα της κτηνοτροφίας λοιπόν αισθητήρες, RFIDs και ειδικές κάμερες τοποθετούνται σε ζώα στις φάρμες. Αυτά συλλέγουν χρήσιμα στατιστικά στοιχεία όπως η τοποθεσία αυτού (Εικόνα 3.6) , τα βήματα που έκανε σε μια μέρα, πόση ώρα κάθεται σε μία

Εικόνα 3.6: Η τοποθεσία του πληθυσμού του κοπαδιού των αγελάδων αποτυπώνεται στην εφαρμογή Cow Tracking.



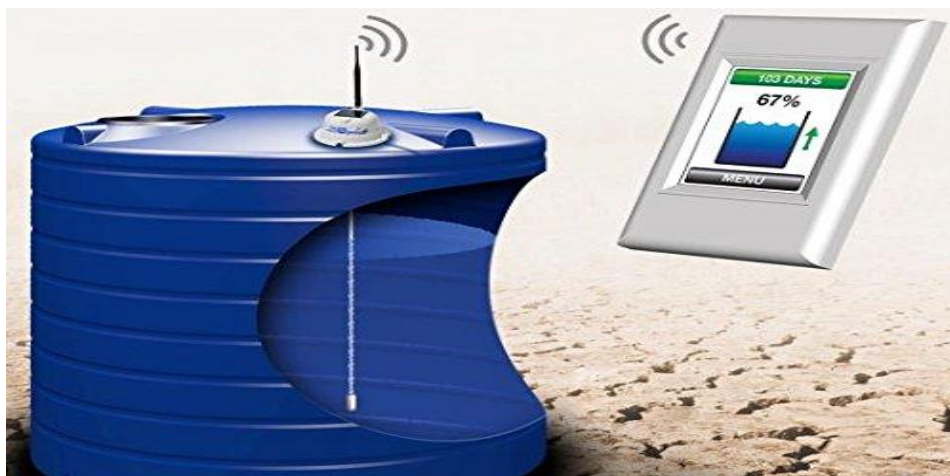
μέρα κλπ. Κάθε ζώο λοιπόν μέσω των RFIDs έχει τη δική του ταυτότητα. Τα συνολικά στατιστικά στοιχεία είναι διαθέσιμα σε μία εφαρμογή που μπορεί να περιέχει όλα τα ζώα της φάρμας μαζί με τα δεδομένα για το κάθε ένα. Η τεχνική αυτή βοηθάει σημαντικά στην αποδοτικότερη κατανάλωση τροφής τους. Στην Αυστραλία μάλιστα οι αγρότες υποχρεούνται από το νόμο να τοποθετήσουν παθητικά RFID στα αυτιά των βοοειδών τους έτσι ώστε οι μετακινήσεις των ζώων από φάρμα σε φάρμα να καταγράφονται σε μία ηλεκτρονική εθνική βάση δεδομένων. Θερμικές κάμερες επίσης, είναι ικανές να διαγνώσουν μια ασθένεια που δεν έχει εμφανιστεί ακόμα (π.χ μαστίτιδα). (Memon et al., 2016)

3.6: Smart Water

Στη σημερινή εποχή το νερό είναι ζωτικός παράγοντας για τη ζωή και για την οικονομία. Με το πρόβλημα της λειψυδρίας να είναι μεγάλο, μία από τις πιο σοβαρές προκλήσεις είναι η επίλυση του ζητήματος αυτού. Η διαχείριση των υδάτων ορίζεται ως η δραστηριότητα του σχεδιασμού, της ανάπτυξης, της διανομής και της διαχείρισης του για τη βέλτιστη χρήση των υδάτινων πόρων. Το νερό διαδραματίζει σημαντικό ρόλο σε πολλές ανθρώπινες δραστηριότητες, όπως στην παραγωγή τροφίμων, στην άρδευση, στον καθαρισμό αλλά και στην παραγωγή και αξιοποίηση ενέργειας. Το νερό είναι πολύτιμο και ο διαμοιρασμός του στους πολίτες είναι αναγκαίο να ρυθμίζεται σωστά. Η ζήτηση ύδατος αυξάνεται εκθετικά υψηλά με την αύξηση του πληθυσμού των αστικών περιοχών. Έτσι, όπως είναι λογικό, για να διατηρηθεί η σωστή αναλογία ζήτησης και εφοδιασμού, είναι σημαντικό να σχεδιαστεί ένα σύστημα όπου η χρήση του νερού θα ισορροπεί με τη διαθεσιμότητα, έτσι ώστε να αποτραπούν τυχόν απώλειες νερού. Το IoT όσον αφορά το smart water μπορεί να δώσει επίσης, λύσεις σε τομείς όπως η παρακολούθηση της ποσότητας του πόσιμου νερού, η παρακολούθηση μέσω μετρήσεων όσον αφορά την ποιότητα του νερού της βρύσης στις πόλεις, η ανίχνευση διαρροών ή αποβλήτων εργοστασίων σε ποτάμια, ο απομακρυσμένος έλεγχος των συνθηκών μιας πισίνας, τα επίπεδα ρύπανσης στη θάλασσα (έλεγχος διαρροών σε πραγματικό χρόνο), η ανίχνευση διαρροών νερού (παρουσία υγρών εκτός των δεξαμενών) και τέλος ανίχνευση υπερχείλισης ποταμών (παρακολούθηση των διακυμάνσεων της στάθμης των υδάτων σε ποτάμια, φράγματα και δεξαμενές). (Laxmi, 2017) Αναλυτικότερα ένα παράδειγμα χρήσης μιας τέτοιας εφαρμογής είναι το εξής: αισθητήρες μπορούν να τοποθετηθούν σε μία δεξαμενή και να ενημερώνουν συνεχώς για την στάθμη του νερού στην τρέχουσα ώρα (Εικόνα 3.7). Αυτές οι πληροφορίες ενημερώνονται και στέλνονται στο cloud. Στη συνέχεια ο

χρήστης χρησιμοποιώντας μια εφαρμογή (Android) , μπορεί να απεικονίσει την στάθμη νερού σε ένα Smartphone οπουδήποτε αυτό συνδέεται στο Internet. Όταν λοιπόν η στάθμη πέσει κάτω από ένα συγκεκριμένο όριο ο αισθητήρας στέλνει ειδοποίηση στο Smartphone του χρήστη, ενώ όταν το επίπεδο ξανά ανέβει στέλνεται το αντίστοιχο μήνυμα. (Wadekar et al.,2016)

Εικόνα 3.7: Το ποσοστό του νερού της δεξαμενής στέλνεται μέσω internet σε Smartphone.



3.7: Smart Metering

Οι έξυπνοι μετρητές (Smart Meters) επιτρέπουν μια αμφίδρομη επικοινωνία μεταξύ του μετρητή και του προμηθευτή. Οι επιλογές ασύρματης επικοινωνίας που χρησιμοποιούνται συχνά περιλαμβάνουν κυτταρικές επικοινωνίες (που μπορεί να είναι ακριβές), Wi-Fi , ασύρματα δίκτυα ad hoc , ασύρματα δίκτυα mesh και χαμηλής ισχύος ασύρματα δίκτυα μεγάλης εμβέλειας (LORA) . Ο όρος έξυπνος μετρητής συχνά αναφέρεται σε μετρητή ηλεκτρικής ενέργειας, αλλά μπορεί επίσης να υπάρχει η δυνατότητα μέτρησης κατανάλωσης φυσικού αερίου ή νερού. Η ανάπτυξη των έξυπνων μετρητών θεωρείται μια στρατηγική εξοικονόμησης ενέργειας. Οι μη έξυπνοι μετρητές ηλεκτρικής ενέργειας και αερίου μετρούν μόνο τη συνολική κατανάλωση, χωρίς να παρέχουν πληροφορίες για το πότε καταναλώθηκε η ενέργεια. Οι έξυπνοι μετρητές παρέχουν έναν τρόπο μέτρησης αυτών των πληροφοριών για συγκεκριμένες τοποθεσίες, επιτρέποντας στις εταιρείες να χρεώνουν διαφορετικές τιμές κατανάλωσης ανάλογα με την ώρα της ημέρας και την εποχή. Τα οφέλη που προκύπτουν από την τεχνολογία αυτή είναι αρκετά. Αρχικά αυτά έχουν να κάνουν με τους ιδιοκτήτες κατοικιών. Πιο συγκεκριμένα περιλαμβάνουν την κατάργηση των εκτιμώμενων

λογαριασμών (λογαριασμοί που εκδίδονται με βάση το κόστος της αντίστοιχης περσινής περιόδου), οι οποίοι αυξάνουν το τελικό κόστος για τους πελάτες και επιφέρουν τις διαμαρτυρίες τους. Επιπρόσθετα οι έξυπνοι μετρητές περιέχουν οθόνη εγκατεστημένη έξω από τα σπίτια των καταναλωτών οι οποίες παρέχουν ενημερωμένες πληροφορίες, σχετικά με την κατανάλωση φυσικού αερίου και ηλεκτρικής ενέργειας, βοηθώντας έτσι τους ανθρώπους να διαχειρίζονται καλύτερα τη χρήση ενέργειας και να μειώνουν το κόστος των λογαριασμών τους. Τέλος ο χειριστής του συστήματος της εταιρίας, μπορεί να τερματίσει ή να επανασυνδέσει την παροχή ρεύματος σε κάθε πελάτη με μηχανισμό εξ αποστάσεως.

Άλλες Εφαρμογές

Μέτρηση επιπέδου δεξαμενής

Παρακολούθηση των επιπέδων νερού, πετρελαίου και αερίου σε δεξαμενές αποθήκευσης.

Φωτοβολταϊκές εγκαταστάσεις

Παρακολούθηση και βελτιστοποίηση της απόδοσης σε σταθμούς ηλιακής ενέργειας. (Zheng et al., 2013)

3.8: Smart Retail

Οι τεχνολογίες του Internet of Things μπορούν να εφαρμοστούν και σε τομείς του λιανικού εμπορίου, με το στόχο του πρώτου να είναι: να μειωθεί το κόστος, να αυξηθεί η υπολογιστική ισχύς των συσκευών, τα δεδομένα να αποθηκεύονται σε υπηρεσίες cloud και φυσικά η διασφάλιση της ασφάλειας και της ιδιωτικότητας των χρηστών. Επίσης η δυνατότητα των αισθητήρων να παρέχουν διαδραστική επικοινωνία στους καταναλωτές που σκοπό έχει τη διευκόλυνση της κίνησης τους στο χώρο αναμένεται να αποτελέσει σημείο αναφοράς όσον αφορά τα οφέλη που μπορεί να προσφέρει το IoT. (Đurđević et al., 2016) Επιπλέον μία παράμετρος που προσφέρει πολλαπλά οφέλη αποτελεί η επισύναψη RFID στα προϊόντα, η οποία παρέχει την ευκαιρία να δοθεί στα καθημερινά αντικείμενα προς πώληση (όπως τρόφιμα, ρούχα, έπιπλα) μια ψηφιακή ταυτότητα (η ίδια διαδικασία μπορεί να πραγματοποιηθεί και με barcodes). Όπως είναι λογικό, μία από τις πλέον χρονοβόρες διαδικασίες στον τομέα της λιανικής πώλησης είναι η πληρωμή (σούπερ μάρκετ). Αφού οι πελάτες, αρκετές φορές είναι αναγκασμένοι να περιμένουν σε μία μεγάλη ουρά πριν μπορέσουν να προχωρήσουν στη

διαδικασία πληρωμής. Το Διαδίκτυο των πραγμάτων μπορεί να προσφέρει τη δυνατότητα να αντικατασταθεί εντελώς αυτή η διαδικασία πληρωμής όπως την ξέρουμε. Αναλυτικότερα, είναι σε θέση να ανιχνεύει αυτόματα όλα τα προϊόντα που εισάγονται στο καλάθι αγορών (όλες οι ηλεκτρονικές ετικέτες (RFID) ή τα barcodes θα διαβαστούν από το σύστημα, μετρώντας τις τιμές) . Τελικά οι πληροφορίες αυτές θα μεταφερθούν στο ασύρματο σύστημα πληρωμών και τα προϊόντα θα χρεώνονται αυτόματα στον πελάτη, ο οποίος αφού πληρώνει το ποσό θα λαμβάνει τα ψώνια. Αυτό θα επιτρέψει στον πελάτη να κάνει τη συναλλαγή και να εξέλθει από το κατάστημα χωρίς καμία καθυστέρηση. Επιπρόσθετα εκτός από την εξοικονόμηση χρόνου για τον πελάτη, θα εξοικονομούνται για την επιχείρηση αρκετά χρήματα αφού η τεχνολογία αυτή είναι σε θέση να αντικαταστήσει το προσωπικό του ταμείου. Μάλιστα ένα ανάλογο σύστημα, το οποίο ονομάζεται Reji-Robo, το οποίο κάνει τις παραπάνω αυτοματοποιημένες διαδικασίες πώλησης προϊόντων (λειτουργώντας με barcodes) δημιουργήθηκε από την Panasonic στην Ιαπωνία το 2017. (Εικόνα 3.8)

Εικόνα 3.8: Το σύστημα Reji-Robo



Ακόμα μία καινοτομία του IoT αποτελούν τα έξυπνα ράφια. Αυτά είναι εξοπλισμένα με ετικέτες και αναγνώστες RFID για τη σάρωση των προϊόντων στα ράφια. Έτσι υπάρχει η δυνατότητα να ενημερώνουν όταν τα προϊόντα τοποθετούνται λανθασμένα σε ένα ράφι, γεγονός που κάνει τη διαδικασία απογραφής αποδοτικότερη και ακριβέστερη. Τέλος ένα σύνηθες φαινόμενο αποτελεί οι πελάτες να ψάχνουν για ορισμένα προϊόντα, αλλά να μη μπορούν να τα βρουν χωρίς βοήθεια. Οι αρνητικές συνέπειες του γεγονότος αυτού περιλαμβάνουν πιθανές απώλειες πωλήσεων. Ως εκ τούτου, υπάρχει μια αυξανόμενη ανάγκη για εργαλεία και εφαρμογές που μπορούν να

λειτουργήσουν ως βοηθός αγορών (ρομπότ), τα οποία θα κατευθύνουν τους πελάτες προς τα αγαθά που αναζητούν. (B.G.J. ten Bok, 2016)

3.9: Εφαρμογές στη Βιομηχανία (Industrial IoT)

Το IoT στο χώρο των βιομηχανιών αρχικά αναφέρεται σε ένα πλαίσιο όπου ένας μεγάλος αριθμός συσκευών ή μηχανών συνδέονται και συγχρονίζονται με τη χρήση λογισμικού και αισθητήρων. Η χρήση και εφαρμογή των τεχνολογιών του διαδικτύου των πραγμάτων που αφορά την ενίσχυση της βιομηχανικής παραγωγής και των βιομηχανικών διαδικασιών αυξάνεται με ραγδαίους ρυθμούς. Με την παραδοχή λοιπόν πως οι έξυπνες μηχανές είναι καλύτερες από τον άνθρωπο για την ακριβή και σταθερή καταγραφή και επικοινωνία δεδομένων σε πραγματικό χρόνο, οι λύσεις που μπορούν να δοθούν είναι σημαντικές. Αφού με την επικοινωνία των μηχανών μεταξύ τους (M2M) δίνεται η δυνατότητα στις εταιρείες να εντοπίζουν νωρίτερα τις δυσλειτουργίες και τα προβλήματα σχετικά με την παραγωγή, εξοικονομώντας χρόνο και χρήματα. Η ιδέα λοιπόν της επικοινωνίας μηχανής προς μηχανή είναι να μειωθούν οι ανθρώπινες παρεμβάσεις όσο το δυνατόν περισσότερο, ώστε να επιτευχθεί το υψηλότερο επίπεδο αυτοματοποίησης. Ένα βιομηχανικό σύστημα IoT αποτελείται από: εφαρμογές, ελεγκτές, αισθητήρες και εξαρτήματα ασφαλείας - που μπορούν να ανιχνεύσουν, να επικοινωνήσουν και να αποθηκεύσουν πληροφορίες στο cloud. Μάλιστα η ABB, μια εταιρεία παροχής ενέργειας και ρομποτικής, χρησιμοποιεί συνδεδεμένους αισθητήρες για την παρακολούθηση και επιδιόρθωση των συσκευών της πριν από τη βλάβη των εξαρτημάτων. Επίσης η ποιότητα του αέρα μέσα στους χώρους των βιομηχανιών διαδραματίζει σημαντικό ρόλο στην καταλληλότητα των προϊόντων αλλά και την υγεία των εργαζομένων. Έτσι, η παρακολούθηση των τοξικών αερίων και των επιπέδων οξυγόνου μέσα στις εγκαταστάσεις είναι απαραίτητες για να εξασφαλιστεί η ασφάλεια των εργαζομένων και των εμπορευμάτων. Η έγκαιρη προειδοποίηση μη αναμενόμενων εκπομπών σε εύφλεκτα δοχεία αποθήκευσης ή σε άλλα που περιέχουν εκρηκτικό υλικό συμβάλλει επίσης στην ασφάλεια των υπαλλήλων. Ο έλεγχος θερμοκρασίας σε βιομηχανικά και ιατρικά ψυγεία με ευαίσθητα εμπορεύματα αποτελεί ακόμα έναν κρίσιμο τομέα όπου με τη χρήση τεχνολογιών του IoT αρκετές ζημιές είναι βέβαιο πως θα αποφευχθούν. Τέλος, η παρακολούθηση της τοποθεσίας των εμπορευμάτων αποτελεί σημαντικό παράγοντα για την προστασία τους. Ο έλεγχος και η παρακολούθηση των διαδρομών που ακολουθούνται για ευαίσθητα προϊόντα όπως φάρμακα, κοσμήματα ή εύθραυστα εμπορεύματα ενισχύει σε μεγάλο βαθμό την ασφάλεια. Η ικανότητα εύρεσης μεμονωμένων

αντικειμένων σε αχανής χώρους όπως αποθήκες ή λιμάνια απομακρύνει τον κίνδυνο για καταστροφή ή απώλεια τους. (Boyes et al., 2018)

3.10: Εφαρμογές για καταστάσεις εκτάκτου ανάγκης και ασφάλεια περιοχών

Σε καταστάσεις έκτακτης ανάγκης αλλά και παραβίασης της ασφάλειας η άμεση κινητοποίηση των αρχών διαδραματίζει τον σημαντικότερο ρόλο στην επίλυση του προβλήματος. Έτσι λοιπόν με την προσθήκη αισθητήρων σε περιοχές περιορισμένης πρόσβασης μπορεί να πραγματοποιηθεί έλεγχος που αφορά την ανίχνευση μη εξουσιοδοτημένων ατόμων σε απαγορευμένες περιοχές. Επιπλέον η ανίχνευση υγρών σε χώρους όπως αποθήκες και ευαίσθητες κτιριακές εγκαταστάσεις είναι αναγκαία προκειμένου να αποφευχθούν καταστροφές σε αυτά. Ακόμα, η μέτρηση των επιπέδων ραδιενέργειας σε χώρους πυρηνικών σταθμών -με ειδικούς αισθητήρες- θα σημαίνει άμεσο συναγερμό για την αντιμετώπιση των διαρροών. Μάλιστα το σύστημα RadWall (Εικόνα 3.9) παρακολουθεί τα επίπεδα ραδιενέργειας σε πραγματικό χρόνο. Ενώ υπάρχουν διάφοροι κατασκευαστές τέτοιου τύπου ανιχνευτών, το RadWall S300 είναι το πρώτο εμπορικό σύστημα που προσφέρει συνδεσιμότητα IoT. Το υλικό ανίχνευσης είναι ιδιαίτερα ευαίσθητο, πράγμα που σημαίνει ότι μια πολύ μικρή αλλαγή στα επίπεδα ραδιενέργειας μπορεί να εντοπιστεί σε πραγματικό χρόνο και να αναφερθεί σε στο σύστημα παρακολούθησης του δικτύου. Η εφεδρική μπαταρία εξασφαλίζει ότι σε περίπτωση διακοπής ρεύματος, το σύστημα θα συνεχίσει να παρακολουθεί τυχόν διαρροές.

Εικόνα 3.9: Το σύστημα ανίχνευσης ραδιενέργειας “RadWall”



Τέλος με την ανίχνευση επιπέδων αερίων πάνω από το όριο αλλά και διαρροών σε βιομηχανικά περιβάλλοντα, (όπως στα εσωτερικά των ορυχείων) διασφαλίζεται η καλύτερη ποιότητα εργασίας αλλά και η προστασία των εργαζομένων. (Kannappan, 2017)

3.11: Συμπεράσματα

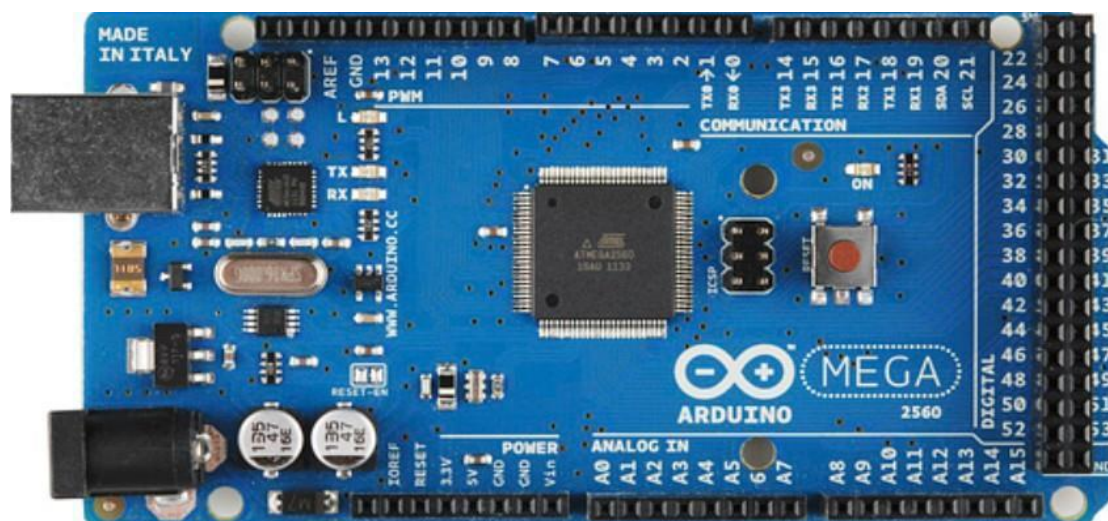
Οι εφαρμογές του IoT λοιπόν μπορούν να συμβάλουν στη ζωή του ανθρώπου κάνοντας τη πιο άνετη και να βελτιώσουν την ασφάλεια του. Εκείνες που αφορούν την υγεία του ασθενή μπορούν να του προσφέρουν μία διάγνωση από απόσταση ή να του παρέχουν άμεση βοήθεια σε περίπτωση που δε νιώθει καλά. Μετρήσεις σχετικές με το περιβάλλον θα συμβάλουν στην προστασία αυτού. Σημαντικά οφέλη θα έχουν και οι αγρότες και οι βιομηχανίες αφού το IoT θα βοηθήσει στην προστασία και ενίσχυση της παραγωγής τους. Επίσης με τη βοήθεια των έξυπνων μετρητών είναι δυνατή η εξοικονόμηση ενέργειας (ηλεκτρικό ρεύμα, νερό) σε σημαντικό βαθμό. Μάλιστα μέχρι το 2020 αναμένεται η αύξηση του αριθμού των συνδεδεμένων αντικειμένων σε 50,1 δις από 8,7 δις το 2012.

Κεφάλαιο 4: Υλοποίηση σε Arduino

4.1: Arduino

Όσον αφορά τις εφαρμογές του IoT που παρουσιάστηκαν στο προηγούμενο κεφάλαιο θα είχε ενδιαφέρον να παρουσιαστεί μια βασική εφαρμογή του στην πράξη. Συγκεκριμένα με την πλακέτα Arduino θα μπορούσε να γίνει μέτρηση της θερμοκρασίας του περιβάλλοντος και ψηφιακή απεικόνιση της στην οθόνη του υπολογιστή. Το Arduino είναι ένας μικροελεγκτής μονής πλακέτας, για την κατασκευή ψηφιακών συσκευών και διαδραστικών αντικειμένων που μπορούν να ανιχνεύσουν και να ελέγξουν αντικείμενα στον φυσικό και ψηφιακό κόσμο. Οι πλακέτες Arduino συνδέονται με τον υπολογιστή και μπορούν να προγραμματιστούν στη γλώσσα Wiring (παρόμοια με τη γλώσσα C++). Η αρχική ανάπτυξη τους ξεκίνησε το 2005, στο Τορίνο της Ιταλίας από τον Massimo Banzi και τον David Cueartielles, ενώ μέχρι σήμερα έχουν κυκλοφορήσει αρκετές εξελιγμένες εκδόσεις του. Τα Arduino συνδέονται σε Breadboards (στα οποία υλοποιούνται τα κυκλώματα) και λειτουργούν ως πύλη για τη μεταφορά των πληροφοριών του περιβάλλοντος (μετρήσεις αισθητήρων) στον υπολογιστή (μέσω της εφαρμογής Arduino) και στη συνέχεια στο cloud.

Εικόνα 4.1: Η πλακέτα Arduino Mega.



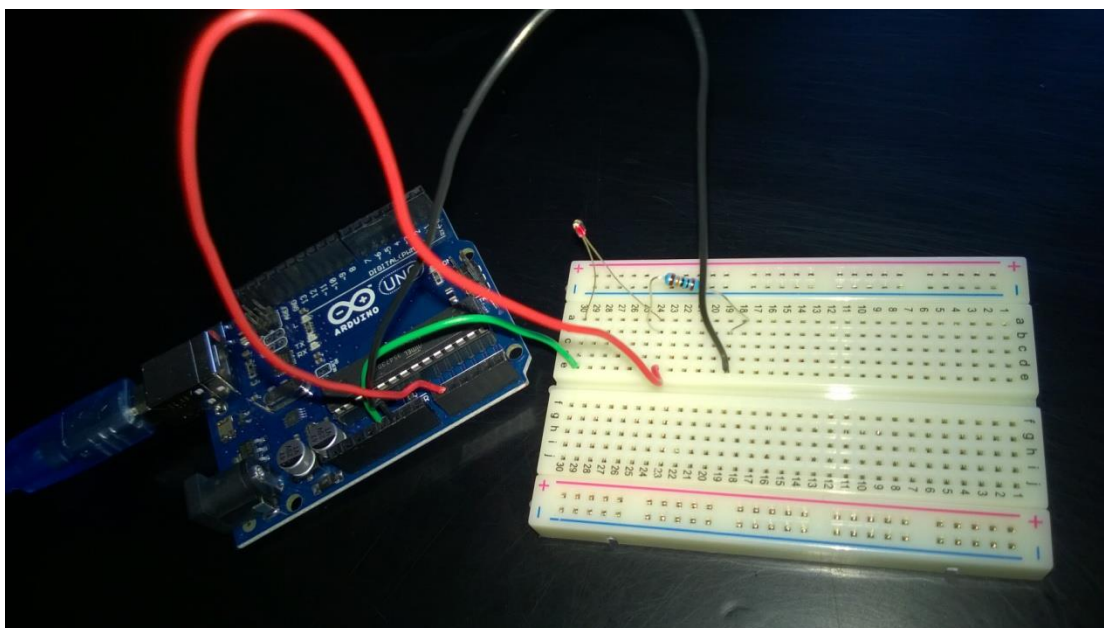
Ο σκοπός για τη δημιουργία ενός τέτοιου project ήταν να προσφέρει έναν χαμηλού κόστους και εύκολο τρόπο για τους αρχάριους και επαγγελματίες έτσι ώστε να δημιουργούν συσκευές που αλληλεπιδρούν με το περιβάλλον χρησιμοποιώντας αισθητήρες. Το αρχικό υλικό Arduino κατασκευάστηκε από την ιταλική εταιρεία Smart Projects. Ορισμένες πλακέτες Arduino έχουν σχεδιαστεί από τις αμερικανικές εταιρείες SparkFun Electronics και Adafruit

Industries . Μέχρι το 2016, δεκαεπτά εκδόσεις του Arduino έχουν παραχθεί και κυκλοφορήσει για εμπορικούς σκοπούς. (43)

4.2: Διαδικασία Υλοποίησης

Για την υλοποίηση του κυκλώματος θα γίνει χρήση breadboard. Σε αυτό θα διασυνδεθεί ένα Thermistor (αισθητήρας θερμοκρασίας) 100K, μία αντίσταση 100K Ohm καθώς και καλώδια διασύνδεσης jumper. Αναλυτικότερα στη μία πλευρά του Thermistor γίνεται σύνδεση ρεύματος που τροφοδοτεί το κύκλωμα (5V). Στην άλλη πλευρά του τελευταίου, τοποθετείται μία αντίσταση που στόχο έχει να προστατέψει από τυχόν βραχυκύκλωμα το σύστημα. Επίσης στο σημείο διασύνδεσης του Thermistor με την αντίσταση ένα καλώδιο jumper καταλήγει στη θέση Analog In του Arduino προκειμένου να γίνει η μεταφορά των μετρήσεων του αισθητήρα στον υπολογιστή. Τέλος για την προστασία του κυκλώματος απαιτείται και ένα καλώδιο γείωσης του ρεύματος. Στην Εικόνα 4.2 παρουσιάζεται το κύκλωμα , συνδεδεμένο με το Arduino Uno.

Εικόνα 4.2: Το κύκλωμα της υλοποίησης, συνδεδεμένο με το Arduino Uno.



Τα Thermistor λοιπόν είναι απλά, φθηνά και ακριβή εξαρτήματα που καθιστούν εύκολη την λήψη δεδομένων θερμοκρασίας. Οι απομακρυσμένοι μετεωρολογικοί σταθμοί, τα συστήματα αυτοματισμού στο σπίτι και τα κυκλώματα ελέγχου και προστασίας εξοπλισμού είναι μερικές εφαρμογές όπου τα πρώτα θα ήταν ιδανικά. Τα Thermistor είναι αντιστάσεις που αλλάζουν την αντίστασή τους με τη θερμοκρασία. Κατατάσσονται από τον τρόπο που η αντίστασή τους ανταποκρίνεται στις μεταβολές της

θερμοκρασίας. Σε Thermistor αρνητικού συντελεστή θερμοκρασίας (NTC), η αντίσταση μειώνεται με αύξηση της θερμοκρασίας, ενώ σε αυτά που ανήκουν στην κατηγορία θετικού συντελεστή θερμοκρασίας (PTC), η αντίσταση αυξάνεται με την αύξηση της θερμοκρασίας. Είναι λοιπόν δεδομένο πως είναι αναγκαίο να μετρηθεί η αντίσταση πριν υπολογιστεί η θερμοκρασία. Ωστόσο, το Arduino δεν μπορεί να μετρήσει άμεσα την αντίσταση, μπορεί να μετρήσει μόνο την τάση. Στο παραπάνω κύκλωμα χρησιμοποιήθηκε Thermistor τύπου NTC. (45) Έτσι λοιπόν με τον τύπο :

$$R2 = R1 * (V_{in}/V_{out} - 1)$$

είναι δυνατό να υπολογιστεί η αντίσταση R2 (αντίσταση Thermistor). Η τιμή V_{in} ισούται με 5V. Η αντίσταση που χρησιμοποιείται (R1) είναι 100K Ohm. Επομένως ο μόνος άγνωστος είναι η τιμή του V_{out} (η τάση που εξάγεται από το Thermistor και την αντίσταση). Το Arduino λοιπόν λαμβάνει τις τιμές V_{out} και στη συνέχεια υπολογίζεται το R2. Τέλος μέσω της εξίσωσης των Steinhart-Hart :

$$T = (1.0 / (c1 + c2 * \log R2 + c3 * \log R2 * \log R2 * \log R2))$$

φθάνουμε στην τιμή της θερμοκρασίας (σε Κέλβιν) μέσω της αντίστασης, όπου οι σταθερές $c1, c2, c3$ έχουν τιμές ανάλογα με τον τύπο του Thermistor όπου:

$$c1 = 1.009249522e-03$$

$$c2 = 2.378405444e-04$$

$$c3 = 2.019202697e-07 \text{ (44)}$$

4.2.1: Κώδικας για Arduino

Για τη δημιουργία βασικών προγραμμάτων δύο βασικές συναρτήσεις χρειάζεται να χρησιμοποιηθούν:

- ✓ `setup()`: μία συνάρτηση που τρέχει μία φορά στην αρχή του προγράμματος η οποία αρχικοποιεί τις ρυθμίσεις.
- ✓ `loop()`: μία συνάρτηση που καλείται συνέχεια μέχρι η πλακέτα να απενεργοποιηθεί.

Επιπλέον στον συγκεκριμένο κώδικα ορίζουμε την τιμή Vo (int) η οποία είναι αυτή που στέλνεται από το Arduino, την τιμή της αντίστασης αλλά και τις σταθερές C. Στη συνέχεια ορίζουμε τις προαναφερθείσες εξισώσεις. Η θερμοκρασία όπως αναφέρθηκε υπολογίζεται σε Κέλβιν. Για τη μετατροπή σε Κελσίου προσθέτουμε την εντολή $T = T - 273.15$, αφού 1 βαθμός Κελσίου ισούται με 273.15 Κέλβιν. Στη συνέχεια μπορούμε να μετρήσουμε τη θερμοκρασία και σε Φαρενάιτ. Για τη μετατροπή από Κελσίου σε Φαρενάιτ χρησιμοποιούμε τον τύπο $T = (T * 9.0) / 5.0 + 32.0$. Ακόμα με την τιμή delay ορίζουμε το πόσο συχνά επιθυμούμε να στέλνεται η μέτρηση της τάσης από το Arduino. Όσο αυξάνεται η τιμή, τόσο πιο αραιές μετρήσεις λαμβάνουμε, επομένως οι θερμοκρασίες εμφανίζονται ανά μεγαλύτερα χρονικά διαστήματα. Τέλος είναι δυνατό να ορίσουμε όρια θερμοκρασιών και να τις ξεχωρίσουμε σε χαμηλή, κανονική και υψηλή ανάλογα με την τιμή τους με τις παρακάτω βασικές εντολές:

```
if (T>25) {  
  
    Serial.print("Υψηλή Θερμοκρασία: ");  
  
    Serial.print(T);  
  
    Serial.println(" C"); }  
  
else if (T<=25 && T>10) {  
  
    Serial.print("Κανονική Θερμοκρασία: ");  
  
    Serial.print(T);  
  
    Serial.println(" C"); }  
  
else if (T<=10) {  
  
    Serial.print("Χαμηλή Θερμοκρασία: ");  
  
    Serial.print(T);  
  
    Serial.println(" C"); }
```

Παρακάτω παρουσιάζεται ο ολοκληρωμένος κώδικας της υλοποίησης:

```
int ThermistorPin = 0;  
  
int Vo;  
  
float R1 = 10000;
```

```

float logR2, R2, T;

float c1 = 1.009249522e-03, c2 = 2.378405444e-04, c3 = 2.019202697e-07;

void setup() {
  Serial.begin(9600); }

  void loop() {

    Vo = analogRead(ThermistorPin);

    R2 = R1 * (1023.0 / (float)Vo - 1.0);

    logR2 = log(R2);

    T = (1.0 / (c1 + c2*logR2 + c3*logR2*logR2*logR2));

    T = T - 273.15;

    //T = (T * 9.0)/ 5.0 + 32.0;

    if (T>25) {

      Serial.print("Υψηλή Θερμοκρασία: ");

      Serial.print(T);

      Serial.println(" C"); }

    else if (T<=25 && T>10) {

      Serial.print("Κανονική Θερμοκρασία: ");

      Serial.print(T);

      Serial.println(" C"); }

    else if (T<=10) {

      Serial.print("Χαμηλή Θερμοκρασία: ");

      Serial.print(T);

      Serial.println(" C"); }

    delay(500);

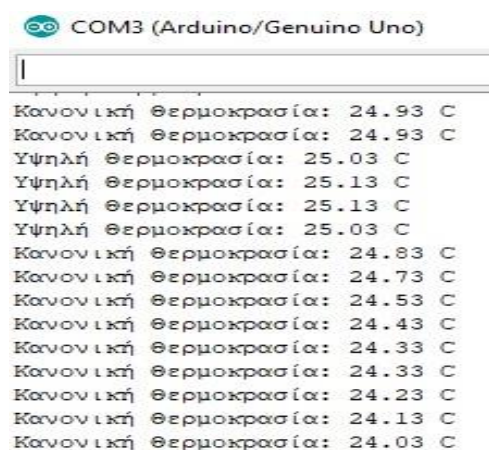
  }

```

4.3: Αποτελέσματα

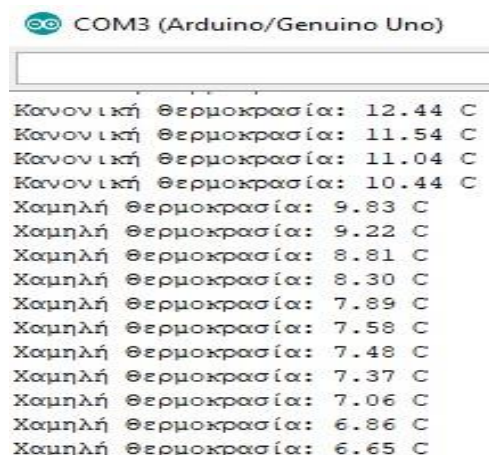
Αφού λοιπόν , το κύκλωμα έχει υλοποιηθεί και συνδεθεί στο Arduino , με την εισαγωγή του κώδικα στον υπολογιστή , λαμβάνονται οι θερμοκρασίες του περιβάλλοντος (Εικόνα 4.3).

Εικόνα 4.3: Οι θερμοκρασίες του περιβάλλοντος αποτυπώνονται στην εφαρμογή του Arduino.



Ενώ με την προσθήκη πάγου στο Thermistor η θερμοκρασία άμεσα κατεβαίνει αισθητά. (Εικόνα 4.4)

Εικόνα 4.4: Με την προσθήκη πάγου στο Thermistor η θερμοκρασία πέφτει άμεσα.



Επιπρόσθετα είναι δυνατή η εμφάνιση των θερμοκρασιών σε Κελσίου, Φάρεναιτ και Κέλβιν παράλληλα (Εικόνα 4.5), με την προσθήκη των κατάλληλων εντολών στον κώδικα. Δηλαδή με τη δήλωση των:

$$T = (1.0 / (c1 + c2*\log R2 + c3*\log R2*\log R2*\log R2))$$

$$T_c = T - 273.15 \text{ και } T_f = (T_c * 9.0) / 5.0 + 32.0$$

και φυσικά τις κατάλληλες εντολές για την εκτύπωση των παραπάνω στην οθόνη.

Εικόνα 4.5: Εμφάνιση των θερμοκρασιών σε Κελσίου, Φάρεναιτ και Κέλβιν.



4.4: Συμπεράσματα

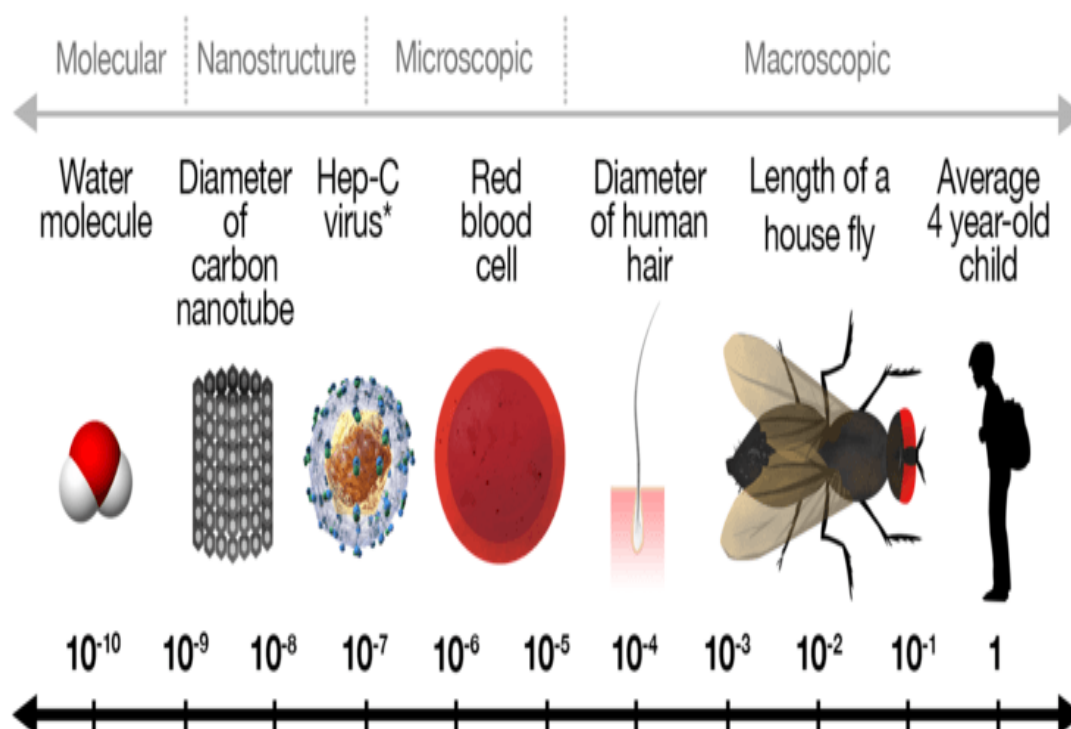
Μια τέτοια εφαρμογή λοιπόν θα μπορούσε να εφαρμοστεί στον τομέα της υγείας. Όπου αισθητήρες συνδεδεμένοι με ασθενείς μεταδίδουν τα δεδομένα στο Arduino και από εκεί μέσω του διαδικτύου και του cloud ο γιατρός από απόσταση και σε πραγματικό χρόνο θα μπορεί να ενημερώνεται σε περίπτωση όπου η θερμοκρασία των πρώτων ξεπεράσει τα κανονικά όρια και να επικοινωνήσει άμεσα με τον ασθενή. Επιπρόσθετα η συγκεκριμένη εφαρμογή θα μπορούσε να είναι ιδανική όσον αφορά την προστασία ενάντια στις πυρκαγιές των δασών. Συγκεκριμένα η πυροσβεστική λαμβάνοντας δεδομένα τέτοιου τύπου σε πραγματικό χρόνο, θα είναι ικανή να επέμβει άμεσα και να κατασβέσει τυχούσες πυρκαγιές. Τέλος τέτοιου είδους εφαρμογές θα μπορούσαν να εφαρμοστούν σε ορυχεία ή και εργοστάσια όπου υπάρχουν αέρια επικίνδυνα σε ανάφλεξη ή και ψυγεία με ευαίσθητα εμπορεύματα, όπου σκοπός θα είναι η προστασία των εργατών αλλά και των προϊόντων.

Κεφάλαιο 5: Internet of Bio-Nano Things

5.1: Νανοτεχνολογία

Η νανοτεχνολογία είναι η επιστήμη, η μηχανική και η τεχνολογία που διεξάγεται στη νανοκλίμακα, η οποία είναι περίπου 1 έως 100 νανόμετρα. Στην παρακάτω εικόνα παρουσιάζεται η σύγκριση μεγεθών της νανοκλίμακας σε σχέση με μεγαλύτερα μεγέθη (Εικόνα 5.1). Η νανοεπιστήμη

Εικόνα 5.1: Σύγκριση μεγεθών της νανοκλίμακας σε σχέση με μεγαλύτερα μεγέθη.



και η νανοτεχνολογία είναι η δημιουργία και χρήση λειτουργικών δομών και μπορούν να χρησιμοποιηθούν σε τομείς της επιστήμης, όπως η χημεία, η βιολογία, η φυσική, η επιστήμη των υλικών και η μηχανική. Οι ιδέες και οι έννοιες πίσω από τη νανοεπιστήμη και τη νανοτεχνολογία ξεκίνησαν από τον φυσικό Richard Feynman το 1959. Ο Feynman περιγράφει μια διαδικασία στην οποία οι επιστήμονες θα είναι σε θέση να χειραγωγήσουν και να ελέγξουν μεμονωμένα άτομα και μόρια. Πάνω από μια δεκαετία αργότερα, ο καθηγητής Norio Taniguchi εφάρμοσε τον όρο νανοτεχνολογία. Σύμφωνα με τον Taniguchi "η νανοτεχνολογία περιλαμβάνει κυρίως την επεξεργασία, τον διαχωρισμό, την ενοποίηση και την παραμόρφωση υλικών από ένα άτομο ή από ένα μόριο". (Taniguchi, 1974) Είναι δύσκολο να φανταστεί κανείς πόσο μικρές κλίμακες αφορά η τελευταία. Ένα νανόμετρο είναι ένα δισεκατομμύριο του μέτρου. Μόλις το 1981, με την ανάπτυξη του

ηλεκτρονικού μικροσκοπίου (Scanning Tunneling Microscope) (Εικόνα 5.2) που θα μπορούσε να «δει» μεμονωμένα άτομα, άρχισε η σύγχρονη νανοτεχνολογία. Όπως κανένα εργαλείο πριν από αυτό, η εφεύρεση του επέτρεψε στους επιστήμονες να απεικονίσουν τον κόσμο μέχρι τα μόρια και τα άτομα του. Το STM κέρδισε το Βραβείο Νόμπελ Φυσικής το 1986 και θεωρείται ευρέως ως το εργαλείο που άνοιξε την πόρτα για τη νανοτεχνολογία. Μέσω της τεχνολογίας αυτής, μπορούν να δημιουργηθούν πολλές νέες συσκευές με ευρύ φάσμα εφαρμογών, όπως η νανοϊατρική, η νανοηλεκτρονική, η παραγωγή βιομάζας αλλά και καταναλωτικά προϊόντα. (Drexler , 1986)

Εικόνα 5.2: Το ηλεκτρονικό μικροσκόπιο STM, το οποίο ανακαλύφθηκε το 1981.



5.2: Νανοϊατρική

Η νανοϊατρική μπορεί να οριστεί ως η χρήση νανosuσκευών και νανοδομών για την παρακολούθηση, την επιδιόρθωση ή τον έλεγχο ανθρώπινων βιολογικών συστημάτων σε μοριακό επίπεδο. Τα παραπάνω μπορούν να ταξινομηθούν σε 4 κατηγορίες: προϊόντα πρώτης γενιάς (2000) όπου περιλαμβάνονται νανοδομές (π.χ. κολλοειδή) καθώς και προϊόντα που ενσωματώνουν νανοδομές (π.χ., νανοδομημένα μέταλλα). Μετά, τα προϊόντα δεύτερης γενιάς (2000-2005) που έχουν σχέση με φυσικοχημικές ενεργές προσαρμόσιμες δομές (π.χ. ενεργοποιητές, ενισχυτές) και βιο-συσκευές ή φάρμακα με στοχευμένη δράση). Στη συνέχεια έρχονται τα νανosuστήματα 3ης γενιάς (2005-2010) τα οποία αφορούν τη ρομποτική και άλλα εξελιγμένα βιο-συστήματα. Τέλος η μοριακή νανοτεχνολογία και τα νανosuστήματα 4ης

γενιάς (2010-2020) όπου μοριακές συσκευές σχεδιασμένες και μοριακές δομές μπορούν να χρησιμεύσουν ως βάση για την αναγέννηση ή την αντικατάσταση χαμένων μερών του σώματος. Η ανάπτυξη συστημάτων χορήγησης φαρμάκων με βάση το νάνο περιλαμβάνει τη χρήση σωματιδίων ή μορίων νανοκλίμακας έτσι ώστε να ενθυλακωθεί το φάρμακο σε αυτά, να παραδοθεί στις θέσεις στόχους και να απελευθερωθεί με ελεγχόμενους τρόπους προκειμένου να επιδιορθωθεί οποιαδήποτε βλάβη κυττάρων. Επιπρόσθετα θα πρέπει να επισημανθεί ότι τα συστήματα χορήγησης φαρμάκων χρησιμοποιούνται κυρίως για τη θεραπεία νευρολογικών διαταραχών (π.χ. νόσων Alzheimer και Parkinson), HIV / AIDS (μόλυνση από ιό ανθρώπινης ανοσοανεπάρκειας / σύνδρομο επίκτητης ανοσολογικής ανεπάρκειας) και καρκίνου. Η νανοτεχνολογία επιτρέπει την ανάπτυξη νανοϋλικών που αυξάνουν την πρόσφυση, την ανθεκτικότητα και τη διάρκεια ζωής των εμφυτευμάτων σε εφαρμογές αντικατάστασης ιστών. Οι νανοδομές χρησιμοποιούνται επίσης για την προετοιμασία που αφορά τη βελτίωση και αναγέννηση των ιστών. Παράλληλα με τα εμφυτεύματα μαλακών μορίων, η νανοτεχνολογία παίζει κεντρικό ρόλο στην εξέλιξη των εμφυτευμάτων σκληρού ιστού, των υλικών υποκατάστασης των οστών και των οδοντικών αποκαταστάσεων. Επιπλέον ειδικά ασημένια νανοσωματίδια έχουν αποδειχθεί ότι αποτελούν κατάλληλη επιφανειακή επικάλυψη (π.χ για καρδιακές βαλβίδες) λόγω των αντιθρομβωτικών και αντιβακτηριδιακών ιδιοτήτων τους. Η νανοτεχνολογία επιτρέπει επίσης την ανάπτυξη χειρουργικών εργαλείων και ρομπότ που επιτρέπουν την εκτέλεση χειρουργείων με ακριβή τρόπο. Η οπτικοποίηση της χειρουργικής επέμβασης μπορεί να βελτιωθεί με τη χρήση νανοκαμερών, ενώ οι υπολογιστές μπορούν να χρησιμοποιηθούν για τον έλεγχο των χειρουργικών οργάνων νανοτεχνολογίας. Με αυτό τον τρόπο, η χειρουργική επέμβαση μπορεί να πραγματοποιηθεί σε ιστικά, γενετικά και κυτταρικά επίπεδα με σημαντικά μειωμένη πιθανότητα λάθους. Υπάρχουν πολυάριθμοι τύποι νανοσωματιδίων που επιτρέπουν την ανίχνευση προκαρκινικών κυττάρων, θραυσμάτων ιού, ειδικών πρωτεϊνών, αντισωμάτων και άλλων δεικτών και δεικτών νόσου. Η χρήση ιατρικών νανομηχανών για την καταστροφή της πέτρας των νεφρών, για τον καθαρισμό των πνευμόνων, των αρτηριών, των δοντιών και γενικότητα των οργάνων (π.χ. αποκατάσταση γαστρεντερικού και κοιλιακού ιστού) ή των οστών (αποκατάσταση οστικών καταγμάτων) . Ακόμη, τα νανοσωματίδια που ονομάζονται NanoFlares χρησιμοποιούνται για την ανίχνευση καρκινικών κυττάρων στην κυκλοφορία του αίματος. Έτσι λοιπόν, στο επίπεδο που έχει εξελιχθεί η επιστήμη βρισκόμαστε πιο κοντά από ποτέ στην ευρεία χρήση των τεχνολογιών αυτών σε πραγματικές συνθήκες και όχι μόνο σε πειραματικό επίπεδο. Άλλωστε λόγω της εξαιρετικά μεγάλης

ακρίβειας της μειώνει σε μηδαμινά επίπεδα την πιθανότητα λάθους. Τέλος, η τεχνολογία αυτή μοιάζει να είναι ίσως η μόνη που υπόσχεται ότι μπορεί να θεραπεύσει ανίατες ασθένειες. (Maksimonić, 2017) Από την άλλη πλευρά όμως και μετά τα τεράστια οφέλη που προσφέρει η τεχνολογία αυτή στην υγεία και αναφέρονται παραπάνω, υπάρχουν και αρκετοί κίνδυνοι που μπορούν να προκαλέσουν προβλήματα στον ασθενή και δε θα πρέπει να παραβλεφθούν. Τα νανοσωματίδια μπορούν να κατασκευαστούν από σχεδόν οποιοδήποτε υλικό μέσω διαφόρων τεχνικών επεξεργασίας και να έχουν οποιοδήποτε σχήμα και δομή. Η λειτουργία και το πλαίσιο των εφαρμογών των νανοσωματιδίων εξαρτώνται κυρίως από το μέγεθος τους . Τα μικρότερα νανοσωματίδια καθαρίζονται ευκολότερα από το αίμα μετά τη στοχευμένη θεραπεία. Αντίθετα όμως είναι σημαντικό το γεγονός ότι όσο μικρότερο είναι το σωματίδιο, τόσο πιο τοξικό είναι. Επιπλέον, ορισμένοι τύποι νανοϋλικών μπορεί να προκαλέσουν ανεπιθύμητες αντιδράσεις στους ασθενείς. Όπως γίνεται αντιληπτό λοιπόν η ανάπτυξη της επιστήμης της νανοτοξικολογίας-ως ερευνητικό πεδίο - αποτελεί έναν από τους σημαντικότερους παράγοντες για την κατανόηση των κινδύνων χρήσης νανοϋλικών και του αντίκτυπου των ζημιών που είναι πιθανό να προκαλέσει στον ανθρώπινο οργανισμό. Επιπροσθέτως, πολυάριθμες ερευνητικές μελέτες είναι αφιερωμένες στην ανάλυση της τοξικολογίας διαφόρων νανοσωματιδίων που χρησιμοποιούνται για σκοπούς υγειονομικής περίθαλψης όπως είναι ο χρυσός, ο άργυρος ή ο λευκόχρυσος. Ως εκ τούτου, όσον αφορά τη χρήση νανοσωματιδίων και νανοϋλικών για ιατρικούς σκοπούς, είναι σημαντικό να βρεθεί μια ισορροπία μεταξύ της ασφάλειας των νανοσωματιδίων και των νανοϋλικών που χρησιμοποιούνται και της αποτελεσματικότητας της θεραπείας. Η πολυπλοκότητα των νανοσωματιδίων, των νανοϋλικών και της νανοτεχνολογίας γενικά είναι ο κύριος λόγος για την έλλειψη ρυθμίσεων και προτύπων που καλύπτουν αυτόν τον επιστημονικό και ερευνητικό τομέα. (Takhar,P, Mahant, 2011) Προκειμένου να μειωθούν οι αρνητικές αυτές συνέπειες της νανοτεχνολογίας, οι πρόσφατες έρευνες επικεντρώνονται στη μετάβαση στη πράσινη νανοτεχνολογία. Η παραγωγή νανοσωματιδίων χρησιμοποιώντας την πράσινη χημεία είναι φιλική προς το περιβάλλον και μη τοξική καθώς και οικονομικά αποδοτική. Η σύνθεση νανοσωματιδίων μπορεί να πραγματοποιηθεί από φυτά, φύκια, βακτήρια ή ακόμα και μύκητες. Με τον τρόπο αυτό, η τελευταία αναμένεται να αποφέρει πολλά οφέλη σε διάφορους τομείς, συμπεριλαμβανομένης της ιατρικής και της υγειονομικής περίθαλψης, μειώνοντας κυρίως τις αρνητικές επιπτώσεις της νανοτεχνολογίας στην ανθρώπινη υγεία αλλά και το περιβάλλον. (Parveen et al., 2016) Ωστόσο τα βήματα που χρειάζεται να γίνουν έτσι ώστε η τεχνολογία αυτή να εφαρμόζεται σε ολόκληρο τον πλανήτη είναι αρκετά και δύσβατα. Ο

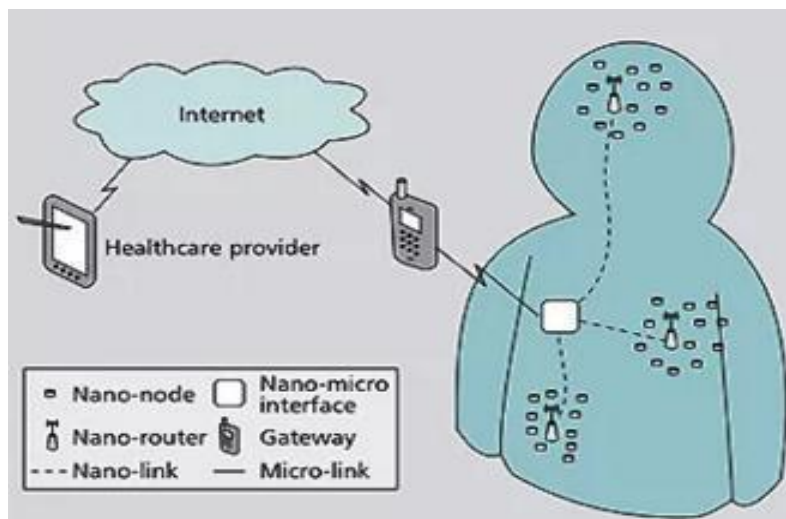
οικονομικός παράγοντας για τη δημιουργία, χρήση και αγορά συσκευών νανοτεχνολογίας διαδραματίζει αδιαμφισβήτητο ανασταλτικό σημείο. Στη σημερινή πραγματικότητα μόνο χώρες με ανεπτυγμένη οικονομία έχουν τη δυνατότητα αγοράς και χρήσης τέτοιου εξοπλισμού στα νοσοκομεία τους.

5.3: Internet of Bio-Nano Things

Οι ιδιότητες των νανοϋλικών, όπως το γραφένιο, που έχουν μελετηθεί, έχουν εμπνεύσει την έννοια του Internet of Nano Things (IoNT). Το Internet of Nano-Things (IoNT) αποτελείται από μικροσκοπικούς αισθητήρες που συνδέονται μεταξύ τους μέσω nano-networks για τη λήψη δεδομένων από αντικείμενα ή ανθρώπους. Η ενσωμάτωση της νανοτεχνολογίας στην ιατρική μέσω νανοϋλικών και νανοδεικτών, γνωστή ως νανοϊατρική, έχει φέρει πολλά οφέλη στην πρόληψη, τη διάγνωση και τη θεραπεία των ασθενειών, ενώ με τη σύνδεση των nanodevices στο Διαδίκτυο, δημιουργήθηκε το πρότυπο του IoNT. Μάλιστα η νανοτεχνολογία και το IoNT έχουν τη δυνατότητα να φέρουν μεγάλη επανάσταση την υγειονομική περίθαλψη στον 21ο αιώνα, δημιουργώντας ένα σύστημα που θα επιτρέπει έγκαιρη ανίχνευση και διάγνωση ασθενειών, ακολουθούμενη από ακριβή, έγκαιρη και αποτελεσματική θεραπεία με σημαντικά μειωμένο κόστος για την υγειονομική περίθαλψη. Με τη διερεύνηση ζητημάτων που αφορούν την ανάπτυξη και επέκταση νέων εφαρμογών σε σχέση με το Internet of Things δε θα πρέπει να παραβλεφθεί και η ανάγκη για νέους τομείς εφαρμογών όπου απαιτούνται να συμπεριληφθούν πολύ μικροσκοπικά, κρυφά και μη παρεμβατικά πράγματα. Παρά το γεγονός ότι είναι ένας παράγοντας που ανοίγει νέους ορίζοντες για πολλές εφαρμογές, η τεχνητή φύση των συσκευών IoNT μπορεί να αποβεί επιζήμια και συγκεκριμένα να οδηγήσει σε ανεπιθύμητες επιπτώσεις στην υγεία ενός ασθενούς. Με βάση τα βιολογικά κύτταρα και τις λειτουργίες τους, το Internet of Bio-NanoThings υπόσχεται να επιτρέψει σε εφαρμογές όπως δίκτυα αίσθησης και ενεργοποίησης, τη συλλογή -εντός του σώματος- πληροφοριών σχετικές με την υγεία και τη μετάδοση τους σε έναν εξωτερικό πάροχο υγειονομικής περίθαλψης μέσω του Διαδικτύου. Το Bio-Nano Things, προτείνεται ως βάση για πολυάριθμες μελλοντικές εφαρμογές, όπως στους τομείς της στρατιωτικής, της υγειονομικής περίθαλψης και της ασφάλειας, όπου τα νανοϋλικά χάρη στο περιορισμένο μέγεθος τους, μπορούν να αποκρύπτονται εύκολα, να εμφυτεύονται και να διασκορπίζονται στο περιβάλλον, όπου μπορούν να συνεργάζονται για την ανίχνευση, την ενεργοποίηση, την επεξεργασία και τη δικτύωση τους. (Akyildiz et al., 2015) Αναλυτικότερα λοιπόν, Το IoNT βασίζεται στη χρήση νανομηχανών, μικρών εξαρτημάτων ικανών να

εκτελούν απλές εργασίες επεξεργασίας, ανίχνευσης και ελέγχου που χρησιμοποιούνται για την ανάπτυξη νανοεπεξεργαστών. Τα nano-nodes που χρησιμοποιούνται στη νανοϊατρική είναι νανομηχανές που αποτελούνται από μονάδα ελέγχου και αποθήκευσης, μονάδα επικοινωνίας, μονάδα ισχύος και μια ποικιλία αισθητήρων και ενεργοποιητών. Λαμβάνοντας υπόψη τα δίκτυα αισθητήρων σώματος, οι βιολογικοί αισθητήρες τοποθετημένοι στο ανθρώπινο σώμα θεωρούνται nano-nodes. (Nayyar et al., 2017) Τα διασυνδεδεμένα nano-nodes (συσκευές που μπορούν να ανιχνεύσουν, να συλλέξουν, να επεξεργαστούν και να αποθηκεύσουν πληροφορίες) μέσα ή έξω από το ανθρώπινο σώμα επικοινωνούν απευθείας μέσω nano-routers και nano-micro συσκευές διασύνδεσης με εξωτερικές συσκευές, συνθέτοντας έτσι nanonetworks. Οι nano-micro συσκευές διασύνδεσης εκτελούν το έργο συγκέντρωσης πληροφοριών που προέρχονται από nano-routers και τις μεταδίδουν στην νάνο-κλίμακα. Επίσης χρησιμοποιούν τεχνικές επικοινωνίας νάνο και παραδοσιακά δίκτυα επικοινωνίας με κλασικά πρωτόκολλα δικτύου. Ο ρόλος της πύλης (Gateway) είναι το γεγονός ότι αυτή δίνει τη δυνατότητα τηλεχειρισμού ολόκληρου του δικτύου μέσω Internet. Τα nano-routers έχουν μεγάλη υπολογιστική ισχύ σε σύγκριση με τα nano-nodes και λειτουργούν ως συσσωρευτές πληροφοριών που προέρχονται από τα τελευταία. Τέλος τα nano-routers διαδραματίζουν επίσης καθοριστικό ρόλο στον έλεγχο των nano-nodes μέσω εντολών ελέγχου και ανταλλαγής (on/ off, sleep, read value). Η διαδικασία περιγράφεται στην Εικόνα 5.3.

Εικόνα 5.3: Η βασική αρχιτεκτονική του IoNT στον τομέα της ιατρικής.



Τελικά όπως γίνεται αντιληπτό με τη χρήση της πύλης όλα τα δεδομένα αισθητήρων από το ανθρώπινο σώμα μπορούν να είναι προσβάσιμα οπουδήποτε και παντού μέσω του ίντερνετ. Έτσι τα δεδομένα μέσω του τελευταίου μπορούν να μεταδοθούν σε κέντρα υγείας όπου γίνεται συλλογή

ιατρικών δεδομένων. Τα παραπάνω δικτυωμένα συστήματα παρακολουθούν συνεχώς τις συνθήκες των ασθενών και μεταδίδουν τα δεδομένα σε πραγματικό χρόνο είτε μέσω ενσύρματης είτε ασύρματης τεχνολογίας όπου αυτά μπορούν να παρακολουθούνται και να υποβάλλονται σε επεξεργασία από εκπαιδευμένο ιατρικό προσωπικό. Η χρήση των Nanonetworks στην ιατρική και την υγειονομική περίθαλψη συναντάται περισσότερο στις χειρουργικές επεμβάσεις σε νάνο-κλίμακα, στην έξυπνη χορήγηση φαρμάκων και στην ανίχνευση και διαχείριση της ταχείας εξάπλωσης λοιμωδών νοσημάτων. Για παράδειγμα, οι διαγνωστικοί νανοαισθητήρες θα επιτρέψουν την έγκαιρη ανίχνευση διαφόρων νόσων, όπως ο καρκίνος, στην αρχή της εμφάνισης των συμπτωμάτων, πριν η νόσος γίνει αντιληπτή από τον ασθενή. Η έγκαιρη ανίχνευση σημαίνει μεγαλύτερες πιθανότητες επιτυχούς θεραπείας της νόσου. (Mikličanin et al., 2015) Το πρότυπο IoNT επιτρέπει στους γιατρούς και τους παρόχους υγειονομικής περίθαλψης να αποκτήσουν γνώση σχετικά με την τρέχουσα κατάσταση υγείας του ασθενούς, καθώς επίσης και να παρακολουθούν εξ αποστάσεως και να ελέγχουν οποιαδήποτε ξαφνική αλλαγή στο σώμα μέσω των νανοαισθητήρων που είναι ενσωματωμένοι στο σώμα του ασθενούς. Μερικά παραδείγματα αποτελούν , η παρακολούθηση του επιπέδου της γλυκόζης στο αίμα, παρέχοντας ένα φάρμακο σε περίπτωση ανάγκης ή η παρακολούθηση των βιοδεικτών του καρκίνου. Η συμπερίληψη των νανουσυσκευών και του IoNT στην ιατρική και την υγειονομική περίθαλψη επιτρέπει την πρόσβαση σε περιοχές που προσεγγίζονται με μεγάλη δυσκολία και περιέχουν ζωτικής σημασίας πληροφορίες . Με αυτόν τον τρόπο, είναι δυνατό να ανιχνευθούν ασθένειες και να γίνει ακριβής διάγνωση αρκετά νωρίτερα , γεγονός που αυξάνει σημαντικά τις πιθανότητες επιτυχούς θεραπείας των ασθενειών. Έτσι λοιπόν δημιουργείται ένα εντελώς νέο πλαίσιο για την επανάσταση της υγειονομικής περίθαλψης και της ιατρικής στον 21ο αιώνα. Επιπλέον, δικαιολογημένα υπάρχουν αρκετές ανησυχίες σχετικά με θέματα ασφάλειας και προστασίας της ιδιωτικότητας. Τα ιατρικά δεδομένα φυσικά, είναι αρκετά ευαίσθητα και πρέπει να προστατεύονται σωστά. Για να μειωθεί ο κίνδυνος κακόβουλων επιθέσεων απαιτείται μια ισχυρή υποδομή ασφάλειας δικτύων για όλες τις περιοχές επικοινωνίας που περιλαμβάνει τις νανουσυσκευές, το δρομολογητή , την πύλη, και το Cloud. (Miraz et al., 2018) Το γεγονός ότι οι τρέχουσες λύσεις ασφάλειας δεν είναι κατάλληλες για την προστασία των IoNT δεδομένων υποδηλώνει την ανάγκη για ένα νέο πλαίσιο αλλά και μηχανισμούς ασφάλειας και προστασίας της ιδιωτικότητας. Τα ζητήματα ιδιωτικού απορρήτου πρέπει να αντιμετωπίζονται με τον κατάλληλο τρόπο για να εξασφαλιστεί η κατάλληλη χρήση των ευαίσθητων δεδομένων που συλλέγονται από τις προσωπικές συσκευές παρακολούθησης της υγείας.

Κάποιες λύσεις που θα μπορούσαν να δοθούν στον τομέα αυτό περιλαμβάνουν ελέγχους σχετικά με την ακεραιότητα των πληροφοριών με χρήση αλγορίθμων και χρήση αλγορίθμων κρυπτογράφησης σε πληροφορίες κώδικα πριν από τη μεταφορά τους μεταξύ των νανοσυσκευών έτσι ώστε να διασφαλιστεί ότι μόνο αναγνωρισμένοι και εξουσιοδοτημένοι χρήστες θα μπορούν να έχουν πρόσβαση σε nanonetworks. Έτσι λοιπόν το IoNT απαιτεί το συνδυασμό της νανοτεχνολογίας και πολλών άλλων τεχνολογιών όπως το Internet of Things, τα δίκτυα αισθητήρων, το Cloud Computing αλλά και το Big Data Analytics. (Maksimović, 2017)

5.4: Συμπεράσματα

Ενώ το διαδίκτυο των πραγμάτων (IoT) επιτρέπει τη διασύνδεση των αντικειμένων μεταξύ τους αλλά και στο διαδίκτυο, το Internet of Nano-Things προεκτείνει τα όρια και την έννοια του Internet of Things σε συσκευές νανοκλίμακας με δυνατότητα εφαρμογής της νανοτεχνολογίας, οι οποίες μπορούν εύκολα να κρύβονται, να εμφυτεύονται και να διασκορπίζονται στο περιβάλλον. Τελικά η εφαρμογή της νανοτεχνολογίας είναι εξαιρετικά σημαντική στον τομέα της βιοϊατρικής, όπου σημειώνονται πρόοδοι τόσο σε διαγνωστικούς όσο και σε θεραπευτικούς τομείς. Για το λόγο αυτό η νανοϊατρική κατατάσσεται ως μία από τις πέντε πρώτες τάσεις της νανοτεχνολογίας. Αυτή, έχει φαινομενικά απεριόριστες δυνατότητες να φέρει επανάσταση σε όλες τις πτυχές της ζωής μας. Από τα σημαντικότερα πλεονεκτήματα της αποτελούν αρχικά η έγκαιρη διάγνωση και θεραπεία ασθενειών μέσω της νανοτεχνολογίας και στη συνέχεια η αποτελεσματικότερη και ακριβέστερη παρακολούθηση των λειτουργιών του ανθρώπινου οργανισμού. Τα νανο- και μικρο-δίκτυα αισθητήρων επιτρέπουν τη συνεχή παρακολούθηση της υγείας και την καταγραφή ζωτικών παραμέτρων των ασθενών. Για την αποφυγή αρνητικών συνεπειών (όπως η νανοτοξικότητα) και τη διασφάλιση της ιδιωτικότητας και της ασφάλειας θα πρέπει να σημειωθούν ακόμα αρκετά βήματα προόδου. Με τη χρήση πρακτικών πράσινης νανοτεχνολογίας (έτσι ώστε να εκλείψουν ζητήματα νανοτοξικότητας) και δημιουργώντας μηχανισμούς ασφάλειας και προστασίας της ιδιωτικότητας υπάρχει η ελπίδα ότι η νανοτεχνολογία θα αντικαταστήσει σε μεγάλο βαθμό τις παραδοσιακές πρακτικές και τεχνικές ιατρικής περίθαλψης. Τέλος μια μεγάλη πρόκληση για την ανθρωπότητα αποτελεί η ίαση των ανίατων ασθενειών και κατά συνέπεια η αύξηση του μέσου όρου ζωής των ανθρώπων. Καθ' αυτό τον τρόπο λοιπόν η νανοτεχνολογία και το IoNT θα διαδραματίσουν σημαντικό ρόλο στην προσπάθεια επίτευξης των παραπάνω στόχων. Το Internet of Nano Things

(IoNT), θεωρείται ως το επόμενο βήμα εξέλιξης στον κόσμο της νανοτεχνολογίας.

Κεφάλαιο 6: Έρευνα σχετικά με το Internet of Things

6.1: Εισαγωγή

Το IoT είναι σίγουρο ότι θα αποτελέσει σημείο αναφοράς τα επόμενα χρόνια και όλο και περισσότερα αντικείμενα θα συνδέονται καθημερινά με το internet. Για το λόγο αυτό είναι απαραίτητο να πραγματοποιηθεί μια έρευνα που θα αποσαφηνίσει τις απόψεις φοιτητών/πτυχιούχων πληροφορικής όσον αφορά το Internet of Things στη σημερινή εποχή αλλά και θα διερευνήσει τις μελλοντικές προκλήσεις του.

6.2: Ερευνητικά ερωτήματα

Αρχικά θα πρέπει να διερευνηθούν οι αντιλήψεις των ατόμων σχετικά με το εάν το Internet of Things θα συμβάλει θετικά στη ζωή των ανθρώπων αλλά και την εξοικείωση τους με συσκευές IoT. Επιπρόσθετα θα πρέπει να διασαφηνιστούν οι απόψεις σχετικά με το σε ποιον τομέα θα βρουν μεγαλύτερη χρήση οι εφαρμογές IoT στο μέλλον. Ένα αμφιλεγόμενο σημείο όσον αφορά το IoT έχει σχέση με την ασφάλεια και την ιδιωτικότητα που προσφέρουν οι εφαρμογές του. Σύμφωνα με τους Kumar et.al 2016 η γνώμη που υπερισχύει είναι ότι οι απλές εφαρμογές της καθημερινότητας μας έχουν τα ίδια προβλήματα και ευπάθειες ασφαλείας με τις εφαρμογές του IoT. Ακόμη, σε αρκετές έρευνες εκφράζεται η ανησυχία όσον αφορά την ιδιωτικότητα των χρηστών μελλοντικά. Επίσης είναι αναγκαίο να ερευνηθούν οι αντιλήψεις σχετικά με το ποια θεωρείται η μεγαλύτερη απειλή για την ασφάλεια και την ιδιωτικότητα αλλά και η καλύτερη λύση προστασίας απέναντι στις απειλές. Τέλος σε πολλές έρευνες υπάρχουν αρκετές επιφυλάξεις σχετικά με τους κινδύνους διαρροής ευαίσθητων ιατρικών δεδομένων ασθενών μέσω του διαδικτύου σε τρίτους (Maksimović, 2017). Έτσι λοιπόν στην παρούσα έρευνα γίνεται προσπάθεια διαπίστωσης ή μη των παραπάνω. Ένα ακόμη σημαντικό θέμα προς διερεύνηση είναι το Internet of Bio-Nano Things και οι λύσεις που μπορεί να προσφέρει στην υγεία σε συνδυασμό με τη νανοτεχνολογία με το οποίο ασχολούνται αρκετές ακόμα έρευνες, όπως αυτή των Alansari et al., 2018. Σκοπός της έρευνας λοιπόν είναι να αποσαφηνιστούν οι αντιλήψεις σχετικά με την χρησιμότητα του IoT, σχετικά με την ασφάλεια και ιδιωτικότητα (απειλές και λύσεις) και τέλος σχετικά με το ρόλο που θα διαδραματίσουν οι εφαρμογές του στην υγεία και την ιατρική. Επίσης έχει σημασία να διερευνηθεί το εάν και κατά πόσο το φύλο, η ηλικία και η εκπαίδευση διαδραματίζει κάποιο ρόλο σχετικά με τις αντιλήψεις των ερωτηθέντων.

6.3: Αποτελέσματα Έρευνας

Η έρευνα απευθύνεται κατά βάση σε φοιτητές/τελειόφοιτους πληροφορικής. Πιο συγκεκριμένα έγινε λήψη ογδόντα απαντήσεων, μέσω των Google Forms. Το ερωτηματολόγιο μπορεί να χωριστεί σε τέσσερα τμήματα. Το πρώτο αναφέρεται στο προφίλ των ατόμων που συμμετείχαν, το δεύτερο έχει σχέση με τις αντιλήψεις και την εξοικείωση τους σχετικά με το Internet of Things. Το τρίτο σκέλος έχει σχέση με τις αντιλήψεις των ατόμων σχετικά με ζητήματα ασφάλειας και ιδιωτικότητας στο IoT. Τέλος με την τέταρτη ενότητα γίνεται προσπάθεια να απεικονιστεί το κατά πόσο το IoT και το Internet of Bio Nano Things θα συμβάλει στη βελτίωση της υγείας των ασθενών μελλοντικά. Τα χαρακτηριστικά των ατόμων που συμμετείχαν στην έρευνα παρουσιάζονται στους παρακάτω πίνακες.

Ηλικία	Ποσοστό
18-30	78,4%
31-43	15%
44-56	5%
57 και πάνω	1,6%

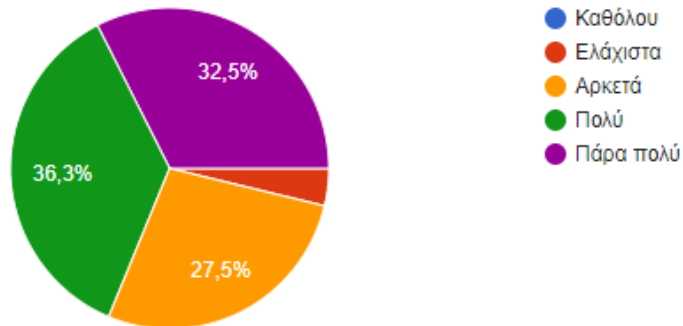
Φύλο	Ποσοστό
Αρσενικό	61,3%
Θηλυκό	38,7%

Εκπαίδευση	Ποσοστό
Απόφοιτος Γυμνασίου/Λυκείου	42,5%
Πτυχιούχος ΑΕΙ/ΤΕΙ	42,5%
Κάτοχος Μεταπτυχιακού Τίτλου	15%
Κάτοχος Διδακτορικού Τίτλου	0%

Αρχικά διερευνάται το κατά πόσο το Internet of Things θα συμβάλει θετικά στη βελτίωση της καθημερινότητας των ανθρώπων. Όπου το συντριπτικό ποσοστό 96,2% πιστεύει ότι θα διαδραματίσει σημαντικό ρόλο. Αναλυτικότερα το 27,5% πιστεύει ότι θα συμβάλει αρκετά, το 36,3% πολύ και το 32,5% πάρα πολύ. Το 3,8% πιστεύει ότι θα συμβάλει ελάχιστα, ενώ κανένας δεν είχε την άποψη ότι δε θα συμβάλει καθόλου. Τα αποτελέσματα αναπαρίστανται και στο παρακάτω γράφημα.

Πιστεύω ότι το Internet of Things θα συμβάλει θετικά στη βελτίωση της καθημερινότητας των ανθρώπων

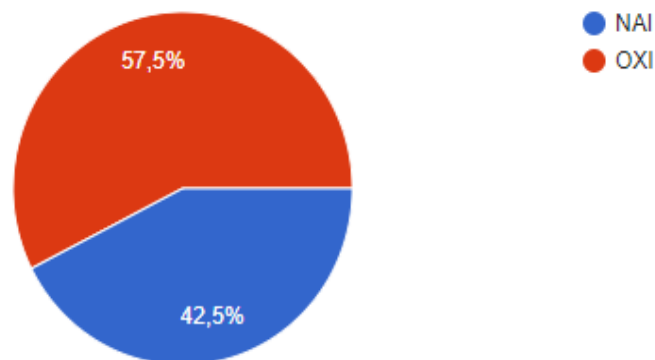
80 απαντήσεις



Στη συνέχεια φαίνεται ότι το 57,5% των ερωτηθέντων δεν έχει στην κατοχή του κάποιο IoT προϊόν, ενώ το 42,5% δήλωσε πως έχει τουλάχιστον ένα στην κατοχή του. Επομένως δεν υπάρχει μεγάλη απόκλιση στα ευρήματα.

Έχετε στην κατοχή σας κάποιο IoT προϊόν (smartwatch , έξυπνο ψυγείο, συσκευές έξυπνου σπιτιού) ?

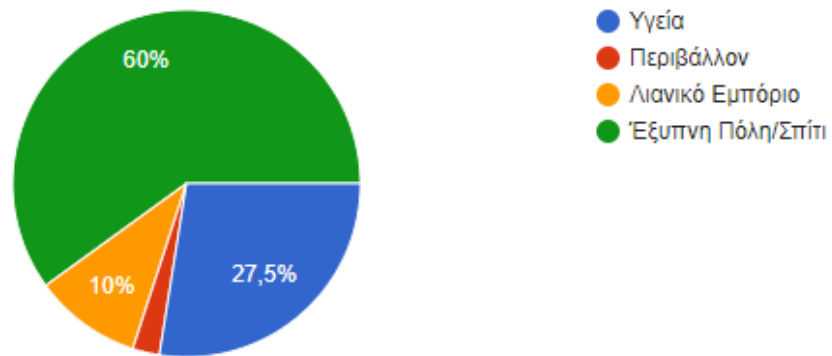
80 απαντήσεις



Επιπλέον υπάρχει η άποψη ότι μεγαλύτερη χρήση των εφαρμογών του IoT μελλοντικά θα υπάρξει στον τομέα της έξυπνης πόλης/σπιτιού (60%), το 27,5% πιστεύει ότι αυτό θα συμβεί στον τομέα της υγείας. Ενώ μικρότερα ποσοστά πιστεύουν ότι το λιανικό εμπόριο (10%) και εφαρμογές σχετικές με το περιβάλλον (2,5%) θα έχουν μεγαλύτερη χρήση. Ακολουθεί το γράφημα των αποτελεσμάτων.

Ποιος τομέας του IoT θα έχει μεγαλύτερη χρήση στο μέλλον?

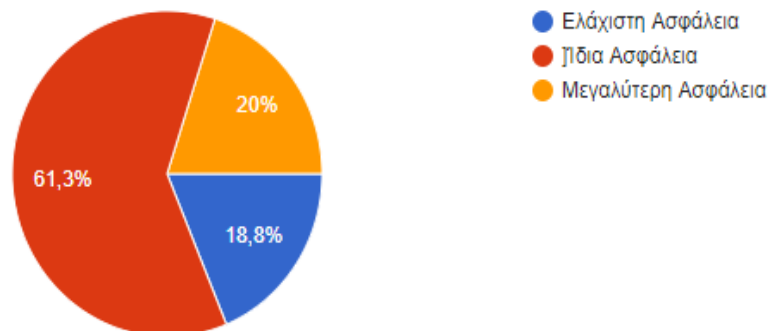
80 απαντήσεις



Επιπρόσθετα σχετικά με την ασφάλεια των εφαρμογών της καθημερινότητας σε σύγκριση με τις εφαρμογές του IoT υπάρχει η εντύπωση ότι οι τελευταίες θα προσφέρουν ίδια ασφάλεια (κατά 61,3%) όπως επιβεβαιώνει και η έρευνα του Kumar et.al 2016, 18,8% πιστεύει ότι οι εφαρμογές του IoT θα προσφέρουν ελάχιστη ασφάλεια σε σχέση με τις σημερινές ενώ το 20% πιστεύει ότι αυτές θα προσφέρουν μεγαλύτερη ασφάλεια, όπως φαίνεται και παρακάτω.

Συγκριτικά με την ασφάλεια στις εφαρμογές της καθημερινότητας και στις εφαρμογές του IoT θεωρείτε ότι οι τελευταίες προσφέρουν:

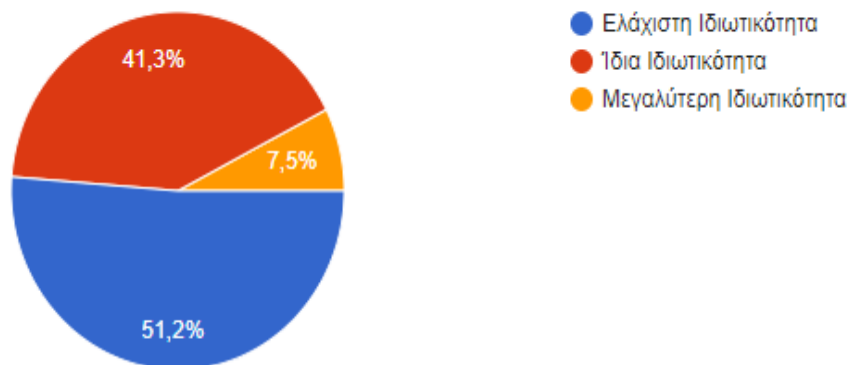
80 απαντήσεις



Σε σχέση με την ιδιωτικότητα που θα προσφέρουν οι εφαρμογές του IoT όμως τα αποτελέσματα διαφοροποιούνται. Έτσι λοιπόν η άποψη που υπερισχύει είναι ότι οι τελευταίες θα προσφέρουν ελάχιστη ιδιωτικότητα (51,2%), το 41,3% θεωρεί ότι δε θα υπάρξουν διαφοροποιήσεις (ίδια ασφάλεια), ενώ η μειοψηφία (7,5%) πιστεύει ότι αυτές θα προσφέρουν μεγαλύτερη ιδιωτικότητα. Ακολουθεί η γραφική αναπαράσταση των παραπάνω.

Συγκριτικά με την ιδιωτικότητα στις εφαρμογές της καθημερινότητας και στις εφαρμογές του IoT θεωρείτε ότι οι τελευταίες προσφέρουν:

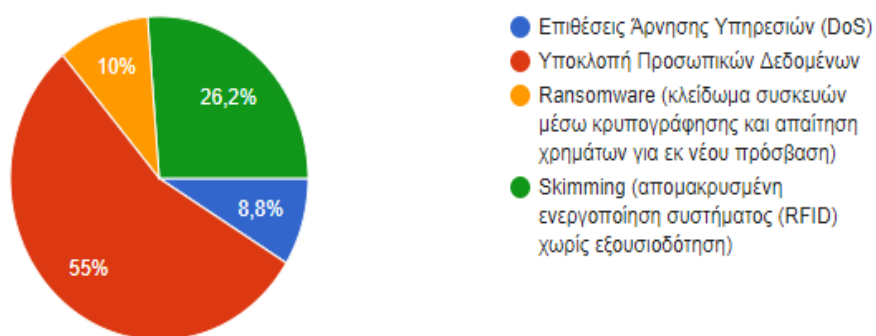
80 απαντήσεις



Ένα ακόμα σημαντικό θέμα προς διερεύνηση είναι το ποιο είναι το μεγαλύτερο πρόβλημα (απειλή) όσον αφορά την ασφάλεια και ιδιωτικότητα στο IoT. Εκεί η κυρίαρχη άποψη είναι ότι μεγαλύτερο πρόβλημα αποτελεί η υποκλοπή προσωπικών δεδομένων (55%), στη συνέχεια έρχεται το Skimming (26,2%) και μετά με μικρότερα ποσοστά ακολουθούν το Ransomware (10%) και οι επιθέσεις άρνησης υπηρεσιών (DoS) με 8,8%.

Ποιο θεωρείτε το μεγαλύτερο πρόβλημα όσον αφορά την ασφάλεια και ιδιωτικότητα στο IoT?

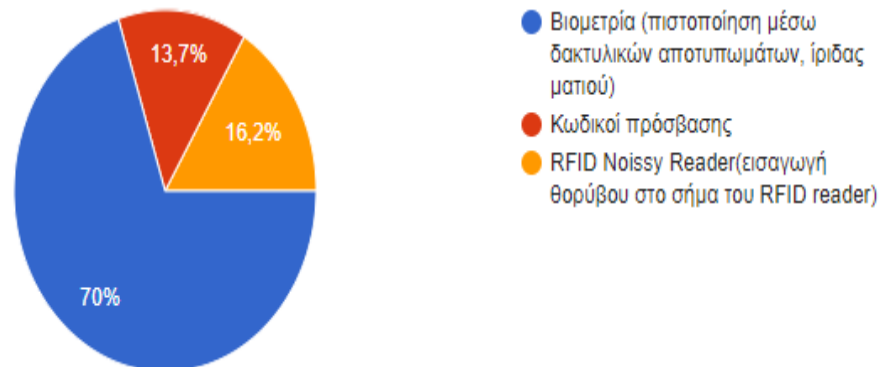
80 απαντήσεις



Αφού λοιπόν εξετάστηκαν οι μεγαλύτερες απειλές που έχουν σχέση με την ασφάλεια και την ιδιωτικότητα διερευνήθηκε το ποιες θα μπορούσαν να είναι οι λύσεις για την προστασία των χρηστών. Εκεί η βιομετρία έλαβε το μεγαλύτερο ποσοστό (70%) . Ενώ το RFID Noissy Reader έλαβε 16,2% και οι κωδικοί πρόσβασης με 13,7% θεωρήθηκαν ως η χειρότερη λύση ασφαλείας, όπως φαίνεται και παρακάτω.

Θεωρείτε ότι καλύτερη λύση ασφαλείας για το IoT μπορεί να είναι:

80 απαντήσεις



Όσον αφορά τη χρήση του IoT στην υγεία υπάρχει η άποψη ότι θα υπάρξει βελτίωση της αμεσότητας παροχής υπηρεσιών (95% των ερωτηθέντων). Ενώ μόλις το 5% πιστεύει ότι είτε δε θα υπάρξει διαφοροποίηση στην παροχή υπηρεσιών, είτε θα υπάρξει παροχή κατώτερης ποιότητας υπηρεσιών (λόγω πιθανών τηλεπικοινωνιακών προβλημάτων).

Με τη χρήση εφαρμογών του IoT στην υγεία θα υπάρξει:

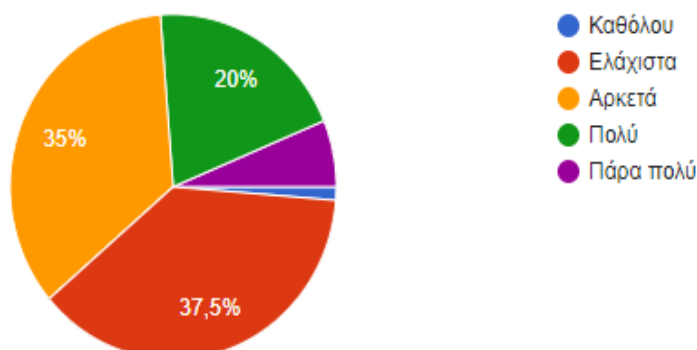
80 απαντήσεις



Επιπρόσθετα όσον αφορά τον τομέα της υγείας οι ερωτηθέντες θεωρούν κατά 1,2% ότι δε θα υπάρξουν προβλήματα ιδιωτικότητας (διαρροή προσωπικών πληροφοριών) και το 37,5% έχει την άποψη ότι θα υπάρξουν ελάχιστα. Από την άλλη πλευρά, το 61,3% θεωρεί ότι θα υπάρξουν προβλήματα, είτε σε μικρό είτε σε μεγαλύτερο βαθμό.

Στον τομέα της υγείας θεωρείτε πιθανό να υπάρξουν προβλήματα ιδιωτικότητας(διαρροή προσωπικών πληροφοριών)?

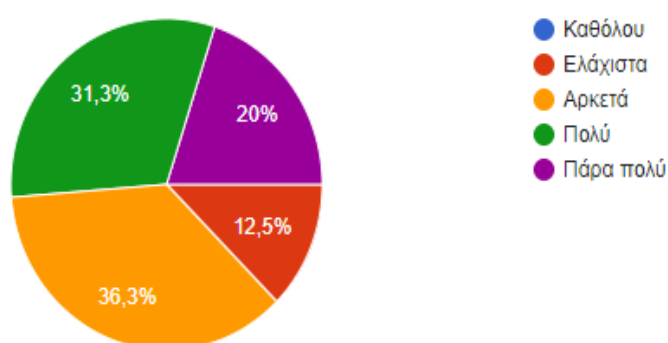
80 απαντήσεις



Σχετικά με το Internet of Bio-Nano Things και τη νανοτεχνολογία το 87,5% πιστεύει ότι θα συμβάλει στην ίαση ανίατων μέχρι σήμερα ασθενειών (είτε αρκετά είτε πάρα πολύ). Ενώ το 12,5% πιστεύει ότι οι εφαρμογές του θα συμβάλουν ελάχιστα σχετικά με τα παραπάνω. Στη συνέχεια αποτυπώνονται τα αποτελέσματα της έρευνας αναλυτικότερα.

Κατά πόσο το Internet of Bio-Nano Things (αποστολή και μελέτη πολύ λεπτομερών μετρήσεων βιοδεικτών του οργανισμού μέσω δικτύου σε πραγματικό χρόνο) και η νανοτεχνολογία θα συμβάλει στην ίαση ανίατων μέχρι σήμερα ασθενειών?

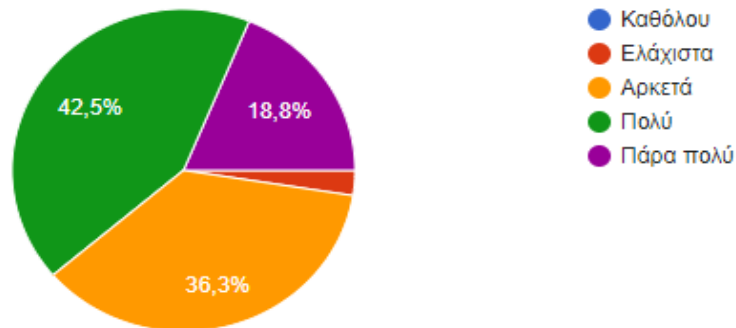
80 απαντήσεις



Τέλος η συντριπτική πλειοψηφία των ερωτηθέντων 97,5% πιστεύει ότι το μέλλον της ιατρικής βρίσκεται στη χρήση εφαρμογών νανοτεχνολογίας (από αρκετά έως πάρα πολύ). Αντίθετα μόλις το 2,5% εκτιμά ότι η νανοτεχνολογία θα συμβάλει ελάχιστα στην ιατρική. Τα αναλυτικά αποτελέσματα παρουσιάζονται στο παρακάτω γράφημα.

Το μέλλον της ιατρικής βρίσκεται στη χρήση εφαρμογών νανοτεχνολογίας

80 απαντήσεις



6.4: Στατιστική Ανάλυση

Για την περαιτέρω στατιστική επεξεργασία των δεδομένων έγινε χρήση του λογισμικού SPSS. Προτού πραγματοποιηθεί η στατιστική ανάλυση των δεδομένων έγινε έλεγχος αξιοπιστίας για την κατηγορία που αφορά τις αντιλήψεις σχετικά με τη βοήθεια που θα προσφέρει το Internet of Bio Nano Things και η νανοτεχνολογία στον τομέα της ιατρικής αλλά και το αν το IoT θα συμβάλει θετικά στη βελτίωση καθημερινότητας των ανθρώπων. Ο δείκτης Cronbach's alpha έχει σχέση με την αξιοπιστία ενός δείγματος. Όσο υψηλότερη τιμή έχει, τότε τόσο πιο αξιόπιστο είναι το δείγμα. Αν μάλιστα η τιμή του ξεπερνά το 0,7 τότε το δείγμα είναι αρκετά αξιόπιστο.

Case Processing Summary			
		N	%
Cases	Valid	80	100,0
	Excluded ^a	0	,0
	Total	80	100,0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics	
Cronbach's Alpha	N of Items
,727	3

Επομένως εφ' όσον ο δείκτης έχει την τιμή 0,72, το αποτέλεσμα δείχνει ότι στο δείγμα υπάρχει αρκετά μεγάλη αξιοπιστία. Για να φανεί εάν το φύλο των ατόμων έχει σχέση σε σχέση και επηρεάζει τις παραπάνω αντιλήψεις έγινε εφαρμογή του independent T-test. Επίσης έγινε ομαδοποίηση των

μεταβλητών των αντιλήψεων σε μία. Τα αποτελέσματα φαίνονται στον παρακάτω πίνακα:

T-Test

Group Statistics					
	Φύλο	N	Mean	Std. Deviation	Std. Error Mean
Αντιλήψεις	Αρσενικό	49	3,8503	,68062	,09723
	Θηλυκό	31	3,6667	,72521	,13025

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Αντιλήψεις	Equal variances assumed	,411	,523	1,146	78	,255	,18367	,16021	-,13528	,50263
	Equal variances not assumed			1,130	60,926	,263	,18367	,16254	-,14135	,50870

Επομένως, οι άνδρες έχουν ελαφρώς θετικότερες αντιλήψεις (3,85) από τις γυναίκες (3,66) όσον αφορά τη βελτίωση της καθημερινότητας των ανθρώπων αλλά και την συμβολή του IoBNT και της νανοτεχνολογίας στην ιατρική, χωρίς παρ' όλα αυτά να διαπιστώνεται σημαντικότητα. Αυτό εξηγείται από το γεγονός ότι το Levene's Test είναι πάνω από 0,05 το οποίο είναι το όριο , κάτω από το οποίο υπάρχει σημαντικότητα. Στην προκειμένη περίπτωση η τιμή του είναι 0,52. Έτσι αποδεικνύεται ότι το φύλο δεν επηρεάζει τις παραπάνω αντιλήψεις σχετικά με το IoT. Επίσης σχετικά με την ασφάλεια και ιδιωτικότητα παρατηρείται επίσης ότι το φύλο δεν επηρεάζει τις αντιλήψεις.

T-Test

Group Statistics

Φύλο	N	Mean	Std. Deviation	Std. Error Mean	
Ασφάλειωτ	Αρσενικό	49	1,7857	,52042	,07435
	Θηλυκό	31	1,7903	,52874	,09497

Independent Samples Test

Levene's Test for Equality of Variances				t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
Ασφάλειωτ	Equal variances assumed	,003	,958	-,038	78	,970	-,00461	,12017	-,24385	,23463
	Equal variances not assumed			-,038	63,204	,970	-,00461	,12061	-,24560	,23639

Αφού οι απαντήσεις των ανδρών (1,78) είναι πάρα πολύ κοντά στις απαντήσεις των γυναικών (1,79) και δεν υπάρχει όπως είναι λογικό

στατιστική σημαντικότητα ($0,95 > 0,05$). Επίσης έγινε χρήση του εργαλείου one-way anova έτσι ώστε να ελεγχθεί αν υπάρχει στατιστική σημαντικότητα σχετικά με την ηλικία των ατόμων και τις απόψεις τους σχετικά με το IoT.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Αντιλήψεις	Between Groups	1,169	3	,390	,790	,503
	Within Groups	37,486	76	,493		
	Total	38,654	79			
Ασφίδιωτ	Between Groups	,960	3	,320	1,191	,319
	Within Groups	20,427	76	,269		
	Total	21,388	79			

Όπως φαίνεται λοιπόν, δεν υπάρχει σημαντικότητα αφού αυτή ξεπερνά ($0,50$ και $0,31$) το $0,05$. Τελικά, σύμφωνα με τα παραπάνω η ηλικία δε διαδραματίζει σημαντικό ρόλο στις απόψεις των ερωτηθέντων. Τέλος ελέγχεται αν η εκπαίδευση παίζει κάποιο ρόλο στις αντιλήψεις τους.

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Αντιλήψεις	Between Groups	2,618	2	1,309	2,797	,067
	Within Groups	36,036	77	,468		
	Total	38,654	79			
Ασφίδιωτ	Between Groups	,824	2	,412	1,542	,220
	Within Groups	20,564	77	,267		
	Total	21,388	79			

Τα παραπάνω αποτελέσματα δείχνουν ότι δεν υπάρχει σημαντικότητα μεταξύ της εκπαίδευσης και των αντιλήψεων για την ασφάλεια και ιδιωτικότητα ($0,22$) όμως υπάρχει κάποια σημαντικότητα μεταξύ της πρώτης και των γενικότερων αντιλήψεων σχετικά με το IoT ($0,067$). Παρακάτω με τη χρήση του post hoc test είναι δυνατό να εντοπιστεί η σημαντικότητα αυτή.

Post Hoc Tests

Multiple Comparisons

		LSD					
Dependent Variable	(I) Εκπαίδευση	(J) Εκπαίδευση	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
Αντιλήψεις	Απόφοιτος Γυμνασίου/Λυκείου	Πτυχιούχος ΑΕΙ/ΤΕΙ	,21569	,16592	,198	-,1147	,5461
		Κάτοχος Μεταπτυχιακού Τίτλου	-,31536	,22971	,174	-,7728	,1420
	Πτυχιούχος ΑΕΙ/ΤΕΙ	Απόφοιτος Γυμνασίου/Λυκείου	-,21569	,16592	,198	-,5461	,1147
		Κάτοχος Μεταπτυχιακού Τίτλου	-,53105*	,22971	,023	-,9885	-,0736
	Κάτοχος Μεταπτυχιακού Τίτλου	Απόφοιτος Γυμνασίου/Λυκείου	,31536	,22971	,174	-,1420	,7728
		Πτυχιούχος ΑΕΙ/ΤΕΙ	,53105*	,22971	,023	,0736	,9885

Φαίνεται λοιπόν ότι η στατιστική σημαντικότητα υπάρχει ανάμεσα στους Πτυχιούχους ΑΕΙ/ΤΕΙ και στους κατόχους Μεταπτυχιακού Τίτλου η οποία είναι 0,023. Επομένως υπάρχει οριακά διαφοροποίηση των αντιλήψεων μεταξύ των δύο παραπάνω ομάδων.

6.5: Συμπεράσματα

Τελικά, φαίνεται ότι οι χρήστες έχουν θετικές αντιλήψεις (σε συντριπτικό ποσοστό) όσον αφορά τη βελτίωση της ζωής των ανθρώπων μέσω των IoT συσκευών. Επιπρόσθετα η πλειοψηφία των ερωτηθέντων δε διαθέτει κάποιο IoT προϊόν, κάτι που είναι πιθανό να αλλάξει στο μέλλον. Επίσης εφαρμογές έξυπνης πόλης/σπιτιού θα χρησιμοποιηθούν σε μεγαλύτερο βαθμό σύμφωνα με την έρευνα. Σχετικά με την ασφάλεια των εφαρμογών του IoT υπάρχει η πεποίθηση ότι αυτές θα προσφέρουν την ίδια ασφάλεια σε σχέση με τις σημερινές εφαρμογές, αλλά μικρότερη ιδιωτικότητα. Μεγαλύτερη απειλή θεωρείται η υποκλοπή προσωπικών δεδομένων, ενώ πιο αξιόπιστη λύση ασφαλείας αυτή της βιομετρίας. Ακόμα κυριαρχεί η άποψη ότι θα υπάρξει βελτίωση της αμεσότητας παροχής υπηρεσιών υγείας μέσω του IoT, αλλά και ότι είναι αρκετά πιθανό να υπάρξουν προβλήματα διαρροής προσωπικών πληροφοριών. Ύστερα, η νανοτεχνολογία θεωρείται ότι αποτελεί το μέλλον της ιατρικής και ότι η πρώτη αλλά και το Internet of Bio-Nano Things θα συμβάλει στην μελέτη και ίαση ανίατων μέχρι σήμερα ασθενειών. Τέλος το φύλο και η ηλικία των ατόμων που συμμετείχαν στην έρευνα δεν επηρεάζει τις απόψεις τους σχετικά με το IoT. Όμως υπάρχει στατιστική σημαντικότητα μεταξύ της εκπαίδευσης και των αντιλήψεων (Πτυχιούχοι ΑΕΙ/ΤΕΙ-Κάτοχοι Μεταπτυχιακού Τίτλου).

Βιβλιογραφία

- 1] Chaouchi, H, "The Internet of Things: Connecting Objects", 2010.
- 2] Ashton, K, "That 'Internet of Things' Thing", 2009.
- 3] Angell, I., Kietzmann, J.,. "RFID and the end of cash?", 2006.
- 4] Evdokimov,S, Fabian,B , Gunther,O, Ivantysynova,L, Ziekow,H ,,"RFID and the Internet of Things: Technology, Applications, and Security Challenges", 2011.
- 5] Yinbiao, S,"Internet of Things: Wireless Sensor Networks", 2014.
- 6] Egan,D, "ZigBee Propagation for Smart Metering Networks", 2012.
- 7] Christin,D, , Reinhardt,A, Mogre,P, Steinmetz,R,"Wireless Sensor Networks and the Internet of Things: Selected Challenges", 2014.
- 8] ZHANG,J, LI,W, YIN,Z, LIU,S, GUO,X," Forest Fire Detection System based on Wireless Sensor Network", 2009.
- 9] Butun, I, Morgera, S, Sankar, R, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", 2014.
- 10] Yilmaz,T, Munoz,M, Foster,R, Hao,Y, "Wearable Wireless Sensors for Healthcare Applications", 2013.
- 11]Baskaranb,K, "A Survey on Futuristic Health Care System: WBANs", 2011.
- 12]Kulkarni,S, "Communication Models in Internet of Things: A Survey", 2017.
- 13] Rao P, Saluja,P, Sharma,N, Mittal,A, Veer Sharma,S,"Cloud Computing for Internet of Things & Sensing Based Applications", 2012.
- 14] Solove, D,"Understanding Privacy", 2008.
- 15] Krumm, J, "Ubiquitous Computing Fundamentals", 2010.
- 16] Lin,H, Bergmann,N, "IoT Privacy and Security Challenges for Smart Home Environments", 2016.
- 17] Mulligan, G, "The 6LoWPAN architecture", 2007.
- 18] Ki Lee,Y,Batina,L,Verbauwhede,I," The Internet of Things :20th Tyrrhenian Workshop on Digital Communications", 2010.
- 19] Savry,O, Vacherand,F, ," The Internet of Things :20th Tyrrhenian Workshop on Digital Communications", 2010.
- 20] Weber,R," Internet of Things – New security and privacy challenges", 2010.

- 21] Wright,D,“The state of the art in privacy impact assessment”, 2012.
- 22] Liska,A,Gallo,T,“ Ransomware: Defending Against Digital Extortion”, 2017.
- 23] Abomhara,M, Køien,G,“ Cyber Security and the Internet of Things: Vulnerabilities,Threats,Intruders and Attacks”, 2015.
- 24] Zanella, A, Bui,N, Castellani,A, Vangelista,L , Zorzi,M, “Internet of Things for Smart Cities” , 2014.
- 25] Schaffers,H, Komninos,N, Pallot,M, Trousse,B, Nilsson,M, Oliveira ,A, “Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation”, 2011.
- 26] Xiaojun ,C, Xianpeng,L, Peng,X, “ IOT- Based Air Pollution Monitoring and Forecasting System”, 2015.
- 27] Kodali,R, Swamy ,G,Lakshmi,B, “An Implementation of IoT for Healthcare”, 2015.
- 28] Alam ,M, Reaz ,M ,Ali,M, “A Review of Smart Homes – Past, Present, and Future”, 2012.
- 29] Chana,M, Esteve,D, Escribaa,C, Campo ,E, “A review of smart homes –Present state and future challenges”, 2008.
- 30]https://www.tado.com/gr/?gclid=EAIaIQobChMI3ZbV9p-k3gIVRed3Ch1gAAFYEAAYASAAEgKaBfD_BwE/
- 31] <https://www.philips.co.in/c-m-li/hue-personal-wireless-lighting>
- 32] <https://nest.com/doorbell/nest-hello/overview/>
- 33] <https://nest.com/smoke-co-alarm/overview/>
- 34] Kamilaris,A,Gao,F ,Prenafeta-Boldu,F, Ali,M , “Agri-IoT: A Semantic Framework for Internet of Things-enabled Smart Farming Applications”, 2016.
- 35] Memon,M,Aamir,M,Kumar,P, Chowdhry,B, “Internet of Things (IoT) Enabled Smart Animal Farm”, 2016.
- 36] Laxmi ,P, Laxmi Deepthi,G, “SMART WATER MANAGEMENT PROCESS ARCHITECTURE WITH IOT BASED REFERENCE” , 2017.
- 37] Wadekar,S, Vakare,V, Prajapati,R, Yadav,S,Yadav,V,“Smart Water Management Using IOT”, 2016.
- 38] Zheng ,J, Lin ,L, Wenzhong Gao ,D, “Smart Meters in Smart Grid: An Overview”, 2013.

- 39] Đurđević,N,Labus,A, Bogdanović,Z,Despotović-Zrakić,M"Internet of things in marketing and retail" , 2016.
- 40] B.G.J. ten Bok , "Innovating the Retail Industry; an IoT approach" , 2016.
- 41] Boyes,H, Hallaq,B ,Cunningham,J ,Watson,T, " The industrial internet of things (IIoT): An analysis framework" , 2018.
- 42] Kannappan ,A, Prasad,H, "Toxic Gas and Radiation Detection Monitoring Using IOT", 2017.
- 43] <https://www.arduino.cc/>
- 44] https://en.wikipedia.org/wiki/Steinhart%E2%80%93Hart_equation
- 45] <http://www.circuitbasics.com/arduino-thermistor-temperature-sensor-tutorial/>
- 46] Akyildiz,I, Pierobon, M, Balasubramaniam,S, Koucheryavy,Y, " THE INTERNET OF BIO-NANOTHOINGS" , 2015.
- 47] Drexler, K, " Engines of Creation: The Coming Era of Nanotechnology", 1986.
- 48] Maksimović,M, "The roles of nanotechnology and internet of nano things in healthcare transformation", 2017.
- 49] Parveen,K, Banse,V, Ledwani,L, "Green synthesis of nanoparticles: Their advantages and disadvantages", 2016.
- 50] Takhar,P, Mahant, S, "In vitro methods for nanotoxicity assessment: advantages and applications", 2011.
- 51] Nayyar,A, Puri,V, Le,D, " Internet of Nano Things (IoNT): Next Evolutionary Step in Nanotechnology", 2017.
- 52] Taniguchi,N, "On the basic concept of nano-technology, in: Proceeding of the International Conference on Production Engineering", 1974.
- 53] Mikličanin,E , Maksimović,M,Vujović,V,"The Future of Healthcare: Nanomedicine and Internet of Nano Things", 2015.
- 54] Miraz,M, Ali, M, Excell,P, Picking,R, "Internet of Nano-Things, Things and Everything: Future Growth Trends", 2018.
- 55] Zhang,Q , Cheng ,L, Boutaba,R, "Cloud computing: state-of-the-art and research challenges", 2010.
- 56] Kumar,P, Kunwar,R, Sachan,A, " A Survey Report on Security & Challenges in Internet of Things" , 2016.
- 57] Subha,R, "Biometrics in Internet of Things (IoT) Security" , 2017.

- 58] Priyadarshini,S,Sahebzathi,S,Narmatha M, Delshi Howsalya Devi," The Internet of Things in Healthcare: A Survey ", 2016.
- 59]Alansari,Z, Soomro,S, M, Belgaum, Shamshirband,S "The Rise of Internet of Things (IoT) in Big Healthcare Data: Review and Open Research Issues", 2018.
- 60] Doukas,C, Maglogiannis,I, "Bringing IoT and Cloud Computing towards Pervasive Healthcare", 2012.