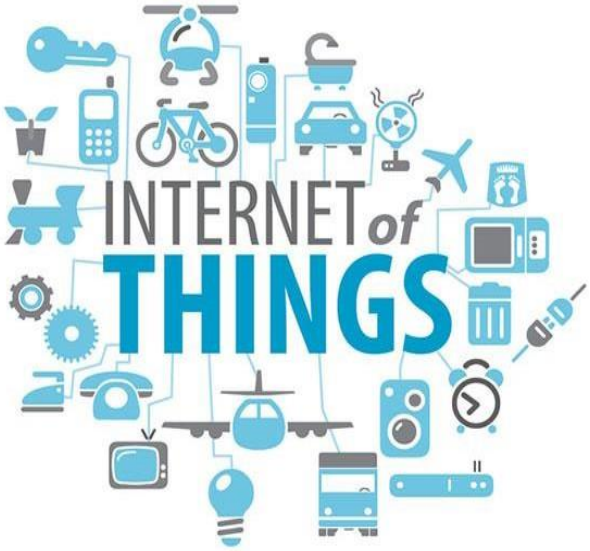
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

Τεχνοοικονομική Διοίκηση Τηλεπικοινωνιακών Συστημάτων

«Διαδίκτυο Των Πραγμάτων»



Κλαδίσιος Λάμπρος

Μεταπτυχιακή Διπλωματική Εργασία

Αθήνα, Ιανουάριος 2019

Α.Μ. ΜΤΔ 1707

ΠΕΡΙΛΗΨΗ

Είναι πλέον βέβαιο ότι διανύουμε μία νέα εποχή, την οποία πολλοί αποκαλούν Διαδίκτυο των Πραγμάτων - Internet Of Things (IoT). Αρκεί κάνεις να παρατηρήσει σε τι βαθμό αξιοποιείται το εν λόγω διαδίκτυο και πόσο απαραίτητο για την καθημερινότητά μας τείνει να γίνει, εάν δεν έχει γίνει ήδη αυτό. Το IoT αποτελείται από «έξυπνες συσκευές» οι οποίες επιδρούν και επικοινωνούν με άλλες συσκευές, περιβάλλοντα και υποδομές με αποτέλεσμα την παραγωγή τεράστιου όγκου δεδομένων, τα οποία παρέχουν χρήσιμες λειτουργίες για μια ζωή ευκολότερη και ασφαλέστερη. Οι δυνατότητες αυτής της νέας εποχής δείχνουν να είναι απεριόριστες, με πολύ μεγάλες προσδοκίες για τα οφέλη που μπορεί να μας παράσχει.

Στην παρούσα πτυχιακή εργασία επιχειρείται να γίνει μία εκτενής αναφορά στις δυνατότητες, τις εφαρμογές, την εξελιξιμότητα και την επίδραση γύρω από το IoT, καθώς και τις απειλές, αλλά και τις ευκαιρίες που εμφανίζονται από την απρόσκοπτη πορεία του. Στο πρώτο κεφάλαιο δίνεται ο ορισμός της τεχνολογίας IoT καθώς και η ιστορική αναδρομή της. Στο δεύτερο κεφάλαιο επεξηγείται η λειτουργία της τεχνολογίας, ενώ στο τρίτο κεφάλαιο αναλύονται ορισμένες βασικές τεχνολογίες που στηρίζεται και εφαρμόζεται το IoT. Στο τέταρτο κεφάλαιο παρουσιάζονται οι εφαρμογές της τεχνολογίας. Στο πέμπτο κεφάλαιο καταγράφονται οι απειλές, τα αδύναμα σημεία και οι προκλήσεις που δημιουργούνται. Στο επόμενο κεφάλαιο περιγράφεται η επίδραση της IoT στον επιχειρησιακό τομέα και τέλος μελετάται η στιγμιαία απεικόνιση της εφαρμογής της τεχνολογίας (στατιστικά και έρευνες) καθώς και οι προβλέψεις για τη μελλοντική της χρήση.

ABSTRACT

It is now certain that we are going through a new era, which many call the Internet of Things (IoT). It is enough to observe to what extent internet is exploited and how much it is necessary for our everyday life to become. The IoT consists of exciting devices that interact with other devices, environments and infrastructures. This has the effect of generating a huge amount of data that provides useful functions making our lives easier and safer. The possibilities of this new era seem to be unlimited, with great expectations for the benefits it can provide us.

This thesis attempts to make an extensive reference to the possibilities, applications, evolution, impact on IoT as well as the threats and opportunities presented by its uninterrupted development. The first chapter describes the definition of IoT technology and its historical background. The second chapter explains the operation of technology, while the third chapter discusses some of the key technologies that IoT supports and applies. The fourth chapter presents the applications of technology. The fifth chapter lists the threats, weaknesses and challenges that arise. The next chapter describes the impact of IoT on the business sector, and finally examines the instant impression of technology application (statistics and surveys) as well as forecasts for its future use.

Περιεχόμενα

Κεφάλαιο 1ο

1.1 Ορισμός του IoT

Ο όρος Internet of Things ιστορικά, επινοήθηκε στα τέλη της δεκαετίας του 1990 και πιο συγκεκριμένα το έτος 1999 από τον επιχειρηματία Kevin Ashton, έναν από τους ιδρυτές του auto-id center στο MIT (Massachusetts Institute of Technology). Ο Kevin Ashton αποτελεί ένα από τα μέλη της ομάδας, η οποία ανακάλυψε τον τρόπο με τον οποία επιτυγχάνεται η σύνδεση των συσκευών με το διαδίκτυο. Κατά την γνωστοποίηση και παρουσίαση του επιτεύγματός αυτού, έγινε για πρώτη φορά αναφορά στον όρο «Internet of Things» και έκτοτε καθιερώθηκε η χρήση του.

Παρά το μεγάλο διεθνές ενδιαφέρον γύρω από το Διαδίκτυο των πραγμάτων, δεν υπάρχει ένας παγκοσμίως κοινά αποδεκτός ορισμός. Διαφορετικοί ορισμοί χρησιμοποιούνται από διαφορετικές πλευρές για να περιγράψουν ή να προωθήσουν μια συγκεκριμένη άποψη και ενδεχομένως να εξυπηρετήσουν ιδιωτικά συμφέροντα.

Μερικοί από τους πιο διαδεδομένους ορισμούς είναι οι εξής:

- **Internet Architecture Board (IaB):**

Ο όρος Διαδίκτυο των πραγμάτων αφορά μία τάση όπου ένας μεγάλος αριθμός ενσωματωμένων συσκευών χρησιμοποιούν τις υπηρεσίες επικοινωνίας που προσφέρονται από τα διαθέσιμα πρωτόκολλα του Διαδικτύου. Πολλές από αυτές τις συσκευές, που συχνά αποκαλούνται «έξυπνα αντικείμενα», δεν λειτουργούν άμεσα από τον άνθρωπο, αλλά υπάρχουν ως ενδιάμεσοι σε κτίρια ή οχήματα, ή είναι διασκορπισμένα στο περιβάλλον.

- **International Telecommunication Union (ITU):**

Μία παγκόσμια υποδομή για την κοινωνία της πληροφορίας, που επιτρέπει προηγμένες υπηρεσίες μέσω της διασύνδεσης πραγμάτων με την υφιστάμενη αλλά και την υπό εξέλιξη λειτουργικότητα της τεχνολογίας και επικοινωνίας.

- **IEE Communications Magazine:**

Το IoT αποτελεί ένα πλαίσιο στο οποίο όλα τα πράγματα έχουν μια αντιπροσώπευση και μια παρουσία στο Διαδίκτυο. Το IoT έχει σαν στόχο να προσφέρει νέες εφαρμογές και υπηρεσίες γεφυρώνοντας τον πραγματικό με τον εικονικό κόσμο.

- **Wikipedia:**

Το Διαδίκτυο των πραγμάτων ή Ίντερνετ των πραγμάτων, αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό).

1.2 Ιστορική Αναδρομή

- Το IoT ξεκίνησε την ύπαρξη του ως ιδέα, ήδη από το 1950. Οι μηχανικοί της IBM (*International Business Machines* Corporation) αναγκάστηκαν να δώσουν μοναδικό χαρακτηριστικό γνώρισμα (ταυτότητα) σε κάθε αντικείμενο και μηχάνημα που χρησιμοποιούσαν στην επιχείρηση. Μετά από αρκετούς πειραματισμούς αλλά και τη διαρκή ενασχόληση με γραμμικά σχήματα, οδηγήθηκαν στην ανακάλυψη των Barcodes.
- Η πρώτη και αξιοσημείωτη συσκευή ήταν αυτή του Edward O. Throrp το 1955, ο οποίος κατασκεύασε ένα ρολόι. Η συσκευή αυτή πρόβλεπε τους κύκλους που έκαναν οι ρουλέτες στα καζίνα του Las Vegas, μέσα από περίπλοκους αλγορίθμους.
- Το 1967 από τον Hubet Upton δημιουργήθηκε η πρώτη συσκευή σε σχήμα γυαλιών μυωπίας, η οποία βοηθούσε τα άτομα με ειδικές ανάγκες να διαβάζουν τα χείλη των ανθρώπων. Το 2011 η εταιρία Google βασιζόμενη στην ιδέα του Hubert, δημιούργησε το project Google Glass.

- Το 1982 ήταν η «επαναστατική» γενιά του Internet και πιο συγκεκριμένα του πρωτόκολλου TCP/IP. Με το πρωτόκολλο αυτό γεννήθηκε μια νέα εποχή, ενός παγκόσμιου ιστού, και δίκτυα που ενώνονται μεταξύ τους, για να δημιουργηθεί το διαδίκτυο όπως το ξέρουμε σήμερα.
- Το 1973 ο Mario Cardullo δημιούργησε την τεχνολογία RFID (Radio Frequency Identification), η οποία επιτρέπει την ασύρματη ανάγνωση και εγγραφή δεδομένων σε συσκευές. Η χρήση του RFID έγινε ευρέως κυρίως στον επιχειρησιακό κλάδο, και ξεκίνησε το 2013 από την πολυεθνική Inditex. Η εταιρεία ενσωμάτωσε την λόγω τεχνολογία RFID μαζικά σε όλα τα καταστήματά της και έπειτα χρησιμοποιήθηκε στο έπακρο κατά την εποχή του Internet Of Things.
- Μια δεκαετία μετά, αναπτύχθηκε η σκέψη επικοινωνίας «machine to machine» από φοιτητές του Πανεπιστημίου Carnegie Mellon της Pennsylvania. Οι συγκεκριμένοι φοιτητές εγκατέστησαν μηχανισμούς στα μηχανήματα αυτόματων πωλητών που υπήρχαν εντός του Πανεπιστημίου, προκειμένου να παρακολουθείται η θερμοκρασία μέσω τερματικών υπολογιστών.
- Το 1990 ένας υπάλληλος της Xerox Parc ονόματι Mark Weiser, δημοσίευσε στον αμερικάνικο τύπο άρθρο για την εξέλιξη των υπολογιστών του 21ου αιώνα και στο άρθρο του αυτό έκανα αναφορά στους όρους «καθολικά συστήματα» και «ενσωματωμένα συστήματα επαυξημένης πραγματικότητας».
- Το 1995 η Siemens ανακοίνωσε το πρώτο chip, το οποίο μέσω δικτύου GSM δίνει τη δυνατότητα σε βιομηχανικά συστήματα να επικοινωνούν μεταξύ τους ασύρματα και να εκτελούν εντολές. Επίσης η εταιρεία IEEE (Institute of Electrical and Electronics Engineers) ξεκίνησε το πρώτο διεθνές φόρουμ για τα wearable computers.
- Το 1999 το MIT δημιούργησε το πρώτο κέντρο ερευνών με σύγχρονα συστήματα για έρευνες και μέσα σε 2 χρόνια ο David Brock ανακοίνωσε την εξέλιξη των Barcodes σε ένα νέο σύστημα βελτιωμένων τρόπων ανάγνωσης πληροφοριών. Αυτός ο τρόπος θα επέτρεπε τις τεχνολογίες RFID, Bluetooth και άλλες ασύρματες τεχνολογίες να τροποποιήσουν, διαβάσουν και να γράψουν δεδομένα σε

αντικείμενα, μέσω ενός RFID tag. Αυτό το νέο σύστημα ονομάστηκε EPC (Electronic Product Code).

- Ένα χρόνο μετά το Auto ID Center μετονομάστηκε σε Auto ID Labs και πραγματοποιήθηκε το πρώτο υπερσύγχρονο δίκτυο ανάπτυξης του Internet of Things, όνομα το οποίο ανακοινώθηκε από τον Kevin Ashton μέσα στο Auto ID Center.
- Δύο υπάλληλοι διαφορετικών εταιρειών, ο Andy Stanforf της IBM και ο υπάλληλος Arlen Nipper της εταιρίας Eurotech, κατασκεύασαν το πρώτο πρωτόκολλο επικοινωνίας Machine to Machine, για συσκευές οι οποίες είναι διασυνδεδεμένες με τον ιστό. Οι εφευρέτες ονόμασαν το πρωτόκολλο αυτό, MQ Telemetry Transport (MQTT) και ήταν ένα θεμελιώδες βήμα προς την ενίσχυση της ιδέας για το IoT .
- Το 2005 κατασκευάστηκε η πλατφόρμα Arduino, από ορισμένα μέλη του προγράμματος Interaction Design Institute Ivrea, ως μια φτηνή λύση μικρο-ελεγκτή με κύριους αποδέκτες τους φοιτητές.
- Το 2008 δημιουργήθηκε η ομάδα IPSO με σκοπό τη διάδοση του πρωτοκόλλου IP σε όλα τα μελλοντικά σχέδια και προτάσεις του Internet of Things. Η εν λόγω ομάδα κατέχει πάνω από 50 εταιρικά μέλη για την διάδοση του πρωτοκόλλου προς το μέλλον.
- Το 2010, η τεχνολογία του Bluetooth υπέστη αναβάθμιση και επανήλθε στην αγορά ένα νέο standard και ονομασία Smart Bluetooth ή αλλιώς Bluetooth Low Energy (BLE). Η τεχνολογία αυτή επιτρέπει σε νέες εφαρμογές και συνδεδεμένες συσκευές στους τομείς της υγείας, άθλησης, και home entertainment να μπορούν να ενταχθούν στον κόσμο του IOT .
- Την ίδια χρονική περίοδο διέρρευσαν πληροφορίες, οι οποίες έκαναν λόγω πως η υπηρεσία της Google, Street View είχε διαθέσιμες 360 μοιρών φωτογραφίες και αποτύπωνε γειτονιές και δρόμους σε ηλεκτρονική μορφή. Επίσης είχε αποθηκευμένο τεράστιο όγκο δεδομένων των δικτύων WiFi των ανθρώπων-χρηστών σε αυτές τις περιοχές. Οι πληροφορίες αυτές στάθηκαν αφορμή για τη συζήτηση μιας νέας στρατηγικής της Google η οποία προκάλεσε διχογνωμία στις απόψεις μεταξύ των χρηστών του διαδικτύου, αλλά και του φυσικού κόσμου. Την

ίδια χρονιά, η κυβέρνηση της Κίνας ανακοίνωσε ότι θα καταστήσει το IoT, έτσι ώστε να αυτό να αποτελεί στρατηγική προτεραιότητα στο πενταετές σχέδιό τους.

- Το 2011 συμπεριλήφθηκε ένα νέο όνομα στη λίστα της Gartner, το «Internet Of Things». Η Gartner είναι εκείνη η εταιρεία έρευνας της αγοράς που εφηύρε την περίφημη «διαφημιστική εκστρατεία του κύκλου για τις αναδυόμενες τεχνολογίες».
- Ένα χρόνο μετά, στη μεγαλύτερη διαδικτυακή διάσκεψη πανευρωπαϊκά (LeWeb), κύριο θέμα ήταν το «Internet Of Things». Παράλληλα, αρκετά δημοφιλή προς το ευρύ κοινό περιοδικά που περιλαμβάνουν μεταξύ άλλων τεχνολογική θεματολογία, ξεκίνησαν να κάνουν χρήση στο λεξιλόγιό τους, του όρου IoT. Ορισμένα εξ αυτών που επιχείρησαν αν περιγράψουν τη νέα αυτή τεχνολογική τάση είναι το Forbes, το Fast Company και το Wired. Επίσης πραγματοποιήθηκε η αλλαγή του πρωτόκολλου IP σε versioning (έκδοση). Η νέα αυτή έκδοση (IP version 6), δύναται να υποστηρίξει περισσότερες συσκευές, γρηγορότερες και αποδοτικότερες, πάντα με γνώμονα την ραγδαία ζήτηση νέων διευθύνσεων IP, έως το 2128.
- Η εταιρεία IDC (International Data Corporation) δημοσίευσε το 2013 μία έκθεση, στην οποία γινόταν αναφορά πως το IoT θα κόστιζε στην αγορά περίπου 8.900 $ εώς το έτος 2020.
- Ο όρος IoT ήρθε ακόμα πιο κοντά στην αγορά, όταν η Goggle εξαγόρασε την εταιρεία Nest, εταιρεία η οποία δημιουργούσε συσκευές/προϊόντα IoT
  Το 2014 δημιουργήθηκαν δύο νέες πλατφόρμες, το HealKit και το HomeKit από την Apple. Στόχος ήταν η ανάπτυξη υλοποιήσεων και η υποστήριξη της πλατφόρμας, με απώτερο σκοπό οι «έξυπνες συσκευές» και πιο συγκεκριμένα το «έξυπνο σπίτι» (smart home), αλλά και γενικότερα ο συγκεκριμένος τρόπος ζωής, να κάνει βήματα προσέγγισης προς το αγοραστικό κοινό.

Τα βασικότερα συστατικά για την ανάπτυξη του IoT όπως είδαμε στις παραπάνω ιστορικές αναδρομές, Internet of Things αποτελούν η **τεχνολογία του RFID** και οι σχετικές τεχνολογίες διευθυνσιοδότησης καθώς και οι **δυνατότητες του IPv6,** οι

οποίες θα επιτρέψουν κάθε αντικείμενο να έχει την δική του ξεχωριστή IP διεύθυνση, και εν τέλει τα αντικείμενα να έχουν πρόσβαση στον κόσμο του Internet Of Things.

Κεφάλαιο 2ο

2.1 Λειτουργία IoT

Έχει επιβεβαιωθεί πως οι τεχνολογίες analytics συνδράμουν στη συγκρότηση της πληθώρας δεδομένων συνεχούς ροής (streaming data) σε γνωστική πληροφορία. Προκύπτουν ωστόσο αρκετές ενστάσεις αναφορικά με τη συλλογή και επεξεργασία των δεδομένων αυτών μέσα από τη συνεχή ροή τους.

Στην παραδοσιακή ανάλυση, τα δεδομένα αρχικά αποθηκεύονται και μετά αναλύονται. Ωστόσο, στην περίπτωση των streaming data, όπως αυτά του IoT, τα μοντέλα και οι αλγόριθμοι είναι αυτά που αποκρυπτογραφούνται και τα δεδομένα περνούν μέσα από αυτά για ανάλυση. Αυτό το είδος της ανάλυσης συνιστά το μοχλό εντοπισμού και εξέτασης μοτίβων, καθώς τα δεδομένα δημιουργούνται αυτοστιγμιαίως. Έτσι πριν αποθηκευτούν τα δεδομένα στο cloud ή σε οποιοδήποτε άλλον χώρο αποθήκευσης, ελέγχονται.

Έπειτα χρησιμοποιούνται analytics ώστε να αποκρυπτογραφηθούν τα δεδομένα, ενώ όλες οι συσκευές συνεχίζουν να προωθούν και να συλλέγουν δεδομένα. Με τις τεχνικές advanced analytics, τα αποτελέσματα των παραπάνω αξιοποιούνται, πέρα από τη θέαση των υπαρχουσών συνθηκών και την αξιολόγηση των κατώτατων ορίων, για το σχεδιασμό μελλοντικών σεναρίων αλλά και τη διερεύνηση δυσεπίλυτων ερωτημάτων.

Για να πραγματοποιηθεί μία τέτοια αποτίμηση με τη χρήση αυτών των ροών δεδομένων, θα πρέπει να υπάρχουν τεχνολογίες μέγιστης απόδοσης, οι οποίες θα μπορούν να προσδιορίζουν μοτίβα στα δεδομένα, τη στιγμή της δημιουργίας τους. Μόλις ένα μοτίβο επικυρώνεται, μετρήσεις ενσωματωμένες στη ροή δεδομένων που

άπτονται της διαδικασίας, δίνουν τα κατάλληλα μηνύματα όπου είναι εφικτό και αναγκαίο για άμεσες δράσεις και λήψη ορθότερων αποφάσεων.

Αυτό ουσιαστικά βοηθά, πέρα από την άντληση πληροφοριών που προαναφέραμε, στην εκτίμηση υστερόχρονων γεγονότων και την εφαρμογή τους για αμέτρητα σενάρια.

Χαρακτηριστικά IoT «Smart Object»

Καθήκον της «έξυπνης συσκευής» είναι η επεξεργασία δεδομένων μέσω ενός μικροεπεξεργαστή και πολυάριθμων θυρών επικοινωνίας. Η έννοια του «έξυπνου» έγκειται στην ενσύρματη ή ασύρματη “επαφή” της συσκευής με τον χρήστη. Όλοι αυτοί οι αγωγοί ασύρματης επικοινωνίας και χρήσης της συσκευής αλλά και ο συγχρονισμός της για αυτοματοποιημένη λειτουργία είναι και ο κύριος λόγος χρήσης μιας «έξυπνης συσκευής».

Σφάλλουμε θεωρώντας ένα μηχάνημα έξυπνο επειδή προσφέρει κατασκευαστικά μεγάλες δυνατότητες στην ταχύτητα διαχείρισης πληροφοριών. Η εφαρμογή μιας έξυπνης συσκευής μπορεί να επιτευχθεί με την επεξεργασία των δεδομένων, όχι μονομιάς στην συσκευή αλλά στο Cloud. Μια συσκευή δεν κάνει η ίδια υπολογισμούς, αλλά αποστέλλει τα δεδομένα, μαζί με τις όποιες ρυθμίσεις και επιλογές του χρήστη στο cloud, με τρόπο ώστε η διαχείριση τους να λαμβάνει χώρα με απόντα το χρήστη.

Μια ακόμη σημαίνουσα πτυχή του IoT είναι η εξέλιξη των δικτύων και του cloud networking, καθώς τα δίκτυα θα πρέπει να αναβαθμίζονται εδραιώνοντας τόσο την αξιοπιστία τους όσο και τη μείωση του κόστους και της κατανάλωσης ενέργειας.

Οι περιοχές συνδεσιμότητας του IoT συμπεριλαμβάνουν σπίτια, πόλεις, αμάξια και δρόμους, με συσκευές να παρακολουθούν και να ταυτοποιούν δεδομένα και συμπεριφορές με σκοπό αυτών τη διαδραστικότητα έργων και υπηρεσιών. Για παράδειγμα, το Cisco Internet of Things Group (IOT G) προβλέπει ότι θα υπάρχουν πάνω από 50 δισεκατομμύρια συνδεδεμένες συσκευές μέχρι το 2020, ενώ οι μικροσυσκευές που θα συνδέονται στο διαδίκτυο και θα είναι μέρος του IOT, θα

φτάσουν σε αριθμό το ένα (1) τετράκις έως το 2025 και θα έχουν την δυνατότατά να συνδέονται με τα έξυπνα κινητά τηλέφωνα για να κωδικοποιήσουν περισσότερες πληροφορίες και καθημερινότητές μας.

Ένα παράδειγμα τις διείσδυσης της τεχνολογίας του IoT είναι η ποσότητα των έξυπνων συσκευών που θα διαθέτει ο κάθε άνθρωπος, καθώς αν ένας απλός χρήστης έχει μια συσκευή smartphone, με το Internet of Things, ο αριθμός των έξυπνων συσκευών θα συμπεριλαμβάνει οικιακές συσκευές, πόρτες και παράθυρα ως φορείς επικοινωνίας. Υπ' αυτό το πρίσμα, η αγορά των έξυπνων κινητών τηλεφώνων καθίσταται απλοϊκή και ασύμφορη. Συνεπώς, το Internet of Things καθορίζεται τεχνολογικά από την αλληλεπίδραση συσκευών με άλλα αντικείμενα, με το περιβάλλον, με υποδομές και με την ικανότητα τους να δρουν αυτοματοποιημένα με σκοπό την γεφύρωση πραγματικού και του εικονικού κόσμου. Τα κυριότερα από αυτά τα χαρακτηριστικά του είναι:

Διασύνδεση

Τα αντικείμενα έχουν τη δυνατότητα να δικτυώνονται με το Διαδίκτυο ή μεταξύ τους, να κάνουν χρήση δεδομένων και να αυτο-ενημερώνονται.

Ταυτοποίηση

Τεχνολογίες όπως η NFC (Near Field Communication), η RGID (Radio Frequency Identification) και άλλες καταφέρνουν τη μοναδική ταυτοποίηση των αντικειμένων. Με την ταυτοποίηση αυτή τα αντικείμενα συνδέονται με σχετικά μ' αυτά μηνύματα που μπορούν να προσληφθούν από έναν διακομιστή.

Συλλογή

Τα αντικείμενα καταγράφουν μέσω αισθητήρων πληροφορίες σχετικά με το περιβάλλον αλληλεπίδρασής τους.

Επεξεργασία

Τα αντικείμενα διαθέτουν επεξεργαστή και αποθηκεύουν δεδομένα χρηστικά και πλήρως αξιοποιήσιμα.

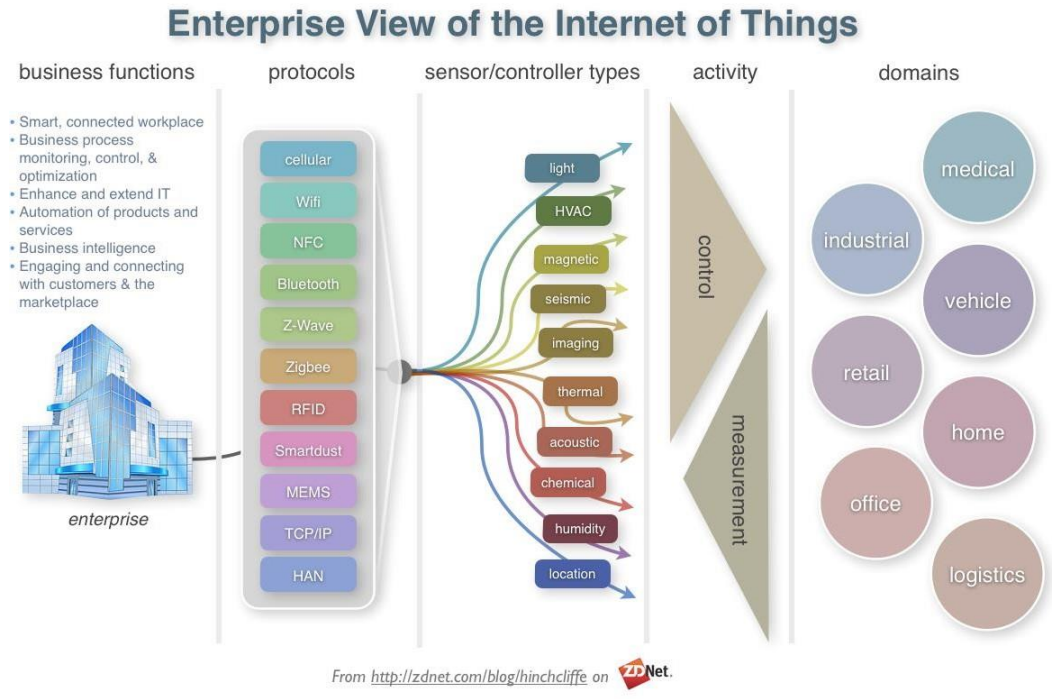
Διευθυνσιοδότηση

Μέσω της διευθυνσιοδότησης των αντικειμένων (χορήγησης IP διεύθυνσης) εξασφαλίζεται ο απομακρυσμένος έλεγχος τους.

Εντοπισμός

Τα αντικείμενα "γνωρίζουν" τον προσανατολισμό τους χάρη στο GPS ή στο δίκτυο κινητής τηλεφωνίας.

Δυστυχώς, η πλειοψηφία των παραπάνω applications χρειάζονται μόνο κάποια από τα παραπάνω χαρακτηριστικά, καθώς η πλήρης εφαρμογή όλων είναι επισφαλής και εξαιρετικά κοστοβόρα.



***Εικόνα 1**: Λειτουργικότητα IoT (Most Commonly Used Sensors for Developing Industrial IoT Solutions)* **[3]**

Κεφάλαιο 3ο

Οι επιλογές που υπάρχουν σχετικά με τα πρότυπα-τεχνολογίες για τα προϊόντα IoT και την ασύρματη επικοινωνία τους είναι πολλές. Κάθε πρότυπο έχει τα δικά του ισχυρά σημεία, τα οποία κατόπιν έντονης διεργασίας μπορούν να καταλήξουν σε μία εφαρμογή (application) για τους υποψήφιους χρήστες. Ορισμένα πρότυπα υπάρχουν ήδη στη εμβέλεια του IoT εδώ και χρόνια και οι σχεδιαστές τα έχουν αξιοποιήσει με δημιουργικό τρόπο. Τα πρότυπα IoT συνεχίζουν να εξελίσσονται, προσφέροντας τρόπους για να επεκτείνουν τη χρήση τους πέρα από την έννοια του παραδοσιακού ασύρματου πρωτοκόλλου, που αφορούσε συνήθως μία συσκευή σε έναν υπολογιστή ή ένα smartphone.

3.1 Μικρής Εμβέλειας Πρωτόκολλα

Στην κατηγορία των ασύρματων μικρής εμβέλειας πρωτόκολλων επικοινωνίας (Short range Wirelless), συγκαταλέγονται μεταξύ άλλων το Bluetooth, το WiFi και το Zigbee τα οποία λειτουργούν σε μη αδειοδοτημένες ζώνες συχνοτήτων (unlicensed frequency bands). Αυτές οι ζώνες αποκαλούνται ISM bands και ενώ δεν απαιτούν ειδική άδεια στις περισσότερες χώρες, υπάρχουν πρότυπα λειτουργίας για τα οποία πρέπει να ελέγχονται οι συσκευές. Το μειονέκτημά τους είναι ότι υπάρχουν πολλές από αυτές τις συσκευές σε ορισμένες τοποθεσίες που χρησιμοποιούν τις ίδιες ζώνες RF με διαφορετικά πρωτόκολλα on-the-air και οι παρεμβολές αποτελούν πρόβλημα, ειδικά στην «συνωστισμένη» ζώνη ραδιοσυχνότητας 2,4 GHz.

Η συχνότερα χρησιμοποιούμενη ζώνη ISM είναι η περιοχή 2.4 GHz που χρησιμοποιείται παγκοσμίως για WiFi και άλλα πρωτόκολλα. Αυτά τα ασύρματα πρότυπα (Bluetooth, ZigBee, WiFi και πολλά άλλα) υφίστανται εδώ και πολλά χρόνια και έχουν ευρεία υποστήριξη. Ο σχεδιασμός σε επίπεδο τσιπ προσφέρει μεγάλη ευελιξία στον σχεδιαστή IoT, ο οποίος μπορεί να επιλέξει τα πιο πρόσφατα ολοκληρωμένα συστήματα μόνο με τα χαρακτηριστικά και τις επιδόσεις που απαιτούνται για τη συσκευή IoT. Οι μονάδες RF είναι μικρές πλακέτες στις οποίες τα τσιπ, ο ελεγκτής, το λογισμικό και ακόμη και η κεραία έχουν ήδη δοκιμαστεί έτσι ώστε να εναρμονίζονται με τα ισχύοντα πρότυπα απόδοσης RF.

Τα περισσότερα ασύρματα πρότυπα μικρής εμβέλειας αποκαλούνται "Personal Area Networks" ή PANs και έχουν τυπικό εύρος από περίπου 10 έως 30 μέτρα (αν και υπό καλές συνθήκες μπορούν όλοι να παρέχουν μεγαλύτερη εμβέλεια). Επίσης αυτά τα πρότυπα, συχνά αποκαλούνται WLAN (Wireless Local Area Network).

Οι συσκευές PAN συχνά βελτιστοποιούνται για συγκεκριμένες εφαρμογές, χρησιμοποιώντας ορισμούς πρωτοκόλλου που ονομάζονται "προφίλ εφαρμογών" ή παρόμοιες ετικέτες. Αυτά προσαρμόζουν τη συσκευή για συγκεκριμένους τύπους λειτουργιών όπως η υγειονομική περίθαλψη, ο αθλητισμός, ο βιομηχανικός έλεγχος, ο αυτοματισμός κτιρίων και πολλά άλλα. Τα προφίλ επιτρέπουν σε συσκευές να εφαρμόζουν υποσύνολα των πλήρων προτύπων ασύρματου IoT, μειώνοντας την πολυπλοκότητα του υλικολογισμικού και της συσκευής, μειώνοντας το κόστος και εξοικονομώντας ενέργεια από την μπαταρία. Καθώς αυτά τα ασύρματα πρότυπα IoT συνεχίζουν να εξελίσσονται, παρόμοια ονόματα μπορούν να χρησιμοποιηθούν για νεότερες εκδόσεις προτύπων που μπορεί να μην είναι πλήρως συμβατά με προηγούμενους ορισμούς. Με την πάροδο του χρόνου, οι απλοί σύνδεσμοι RF από σημείο σε σημείο έχουν αναπτύξει ορισμούς υψηλότερων επιπέδων πρωτοκόλλου για δίκτυα δικτύου, μεταφορών και ακόμη και για εφαρμογές, επομένως η τελική επιλογή σας πιθανώς θα περιλαμβάνει τις εκτιμήσεις λογισμικού που προκύπτουν από το σκοπό και τη χρήση των δεδομένων από το IoT σας συσκευή.

ZigBee

Το ZigBee είναι ένα πρότυπο 802.15.4 και αποτελεί ένα αγαπημένο σε προτίμηση PAN για χαμηλή ισχύ, χαμηλή ταχύτητα μεταφοράς δεδομένων, ασφαλή ασύρματα δίκτυα. Χρησιμοποιεί τις ασύρματες ζώνες ISM , συμπεριλαμβανομένων των 2.4 GHz. Το ZigBee υποστηρίζει τα tree, start και mesh networks, έτσι ώστε οι συλλογές των συσκευών να μπορούν να μεταβιβάζουν από κοινού δεδομένα σε κόμβους ελέγχου. Αυτό μπορεί να αποτελεί έλξη για τα low data rate δίκτυα που κατανέμονται σε μια ευρύτερη περιοχή από ό, τι θα μπορούσε να φτάσει ένα απλό δίκτυο point-to-point υπό παρόμοιες συνθήκες. Το αντίτιμο για αυτό μπορεί να είναι η μικρότερη διάρκεια ζωής μπαταρίας για συσκευές που χρησιμεύουν ως repeaters για πιο απομακρυσμένες συσκευές ZigBee IoT, στέλνοντας δεδομένα και αναγνωρίσεις μεταξύ

κόμβων, όχι μόνο τα δικά τους δεδομένα. Ενώ το ZigBee Pro μπορεί να αλλάξει συχνότητα για την αποφυγή παρεμβολών, ολόκληρο το δίκτυο πρέπει να μετακινηθεί σε άλλο κανάλι σε περίπτωση παρεμβολής. Τα ποσοστά δεδομένων ποικίλλουν επίσης σε διάφορες περιοχές, από περίπου 10 έως 200 KBits / sec. Αυτές οι ταχύτητες μπορεί να είναι απολύτως επαρκείς για πολλές συσκευές IoT, οπότε αναμένεται χαμηλότερη απόδοση από ό, τι ίσως αναμένεται από τα πρωτόκολλα WiFi. Χαμηλότερες ταχύτητες συνήθως σημαίνουν πολύ χαμηλότερη κατανάλωση μπαταρίας (CPU ή λογικά τσιπ, ισχύ RF, κ.λπ.) για ένα δεδομένο εύρος λειτουργίας.

Το Zigbee έχει χρησιμοποιηθεί σε πολλές διαφορετικές εφαρμογές που απαιτούν σύνδεση χαμηλής ισχύος, συμπεριλαμβανομένων των αυτοματισμών οικιακής χρήσης και των βιομηχανικών δικτύων. Η κλειδαριά μπροστινής πόρτας και ο θερμοστάτης χωρίς κλειδί μπορεί να είναι συσκευές Zigbee.

3.2 Μεγάλης Εμβέλειας Πρωτόκολλα

Ενώ συνήθως το IoT χρησιμοποιεί τα PANs, υπάρχουν πολλές εφαρμογές IoT στις οποίες είναι ανάγκη να καλυφθούν μεγαλύτερες αποστάσεις (εύρη). Αυτά τα δίκτυα ευρείας περιοχής χαμηλής ισχύος αναφέρονται συχνά από το ακρωνύμιο LPWAN (Low Power Wide Area Networks). Οι εφαρμογές περιλαμβάνουν ιατρική παρακολούθηση ασθενών, πόρους (ποιότητα νερού, εξόρυξη πετρελαίου και ορυκτών), γεωργία (υγεία των ζώων και τοποθεσία, καιρικές συνθήκες, υγεία φυτών και χρήση νερού) κυκλοφορία, στάθμευση, ποιότητα του αέρα, μέτρηση χρησιμότητας και αποστράγγισης, παρακολούθηση κτιρίων και ούτω καθεξής. Αυτές οι εφαρμογές θα φέρουν επανάσταση στις λειτουργίες και θα επιτρέψουν την αναφορά και διαχείριση σε πραγματικό χρόνο.

LoRa

Το LoRa (Long Range) και έχει λίγο διαφορετικό χαρακτήρα από τα ασύρματα πρωτόκολλα μικρής εμβέλειας που περιγράψαμε προηγουμένως. Το LoRa χρησιμοποιεί ραδιοσυχνότητες υπο-1Gigahertz σε μη εξουσιοδοτημένο φάσμα σε VHF, UHF και 800-930 MHz ανάλογα με τις περιφερειακές κατανομές. Δεδομένου ότι

χρησιμοποιεί αυτές τις χαμηλότερες ραδιοσυχνότητες, έχει διαφορετικά χαρακτηριστικά RF από άλλα πρότυπα (2,4 ή 5 GHz) και τα σήματα LoRa μπορούν να διεισδύσουν βαθιά στα κτίρια και να φτάσουν σε τοποθεσίες που δεν είναι προσβάσιμες σε εξοπλισμό υψηλότερης συχνότητας.

Η διαμόρφωση LoRa αποτελεί σημαντική απόκλιση από άλλους τύπους διαμόρφωσης και είναι μία σημαντική πρόοδος στην τεχνολογία RF. Τα περισσότερα πρότυπα μικρής εμβέλειας χρησιμοποιούν κάποια μορφή φάσματος FSK, OFDM ή FHSS ή DSSS Spread. Το LoRa είναι ένα σύνολο τεχνικών διαμόρφωσης που κατοχυρώνονται με δίπλωμα ευρεσιτεχνίας από την Semtech χρησιμοποιώντας φορέα ραδιοσυχνοτήτων Chirped Spread Spectrum (CSS), το οποίο ποικίλει (chirps) στον ραδιοφωνικό φορέα κατά τη διάρκεια εκπομπής. Αυτό καθιστά το σήμα ανθεκτικό στο φαινόμενο Doppler (για χρήστες κινητών), και γενικότερα έχει σημαντικό επίπεδο αντίστασης στις παρεμβολές. Οι χαμηλοί ρυθμοί δυαδικών ψηφίων (έως 300 bits / sec) που κατανέμονται σε ένα εύρος συχνοτήτων συχνότητας μπορούν συχνά να αποφεύγουν παρεμβολείς όπως σήματα FSK και αποδιαμορφώνονται επιτυχώς. Αυτό μπορεί να δώσει μια αύξηση 15-dB σε σύγκριση με ένα σήμα FSK χρησιμοποιώντας παρόμοια ισχύ σήματος RF. Όσον αφορά τον θόρυβο, το LoRa μπορεί άνετα να λειτουργήσει κάτω από το επίπεδο θορύβου RF περιβάλλοντος και ακόμη και 20 dB ή περισσότερο κάτω από τις πηγές παρεμβολής, λόγω του κέρδους επεξεργασίας της διαφοροποιημένης διαμόρφωσης φάσματος. Το LoRa επιτρέπει επίσης διάφορους συνδυασμούς ρυθμού δεδομένων και διαμόρφωσης, τα οποία μπορούν να επιλεγούν για να αυξήσουν την ευαισθησία και να επιτύχουν μεγάλη απόσταση με χαμηλή ισχύ RF σε θορυβώδη περιβάλλοντα ή για να αυξήσουν τις ταχύτητες δεδομένων (έως περίπου 40 Kbits / sec) όταν απαιτείται. Είναι ενδιαφέρον ότι διαφορετικοί παράγοντες εκπομπής LoRa, μπορούν να είναι ενεργοί στο ίδιο κανάλι χωρίς να παρεμβάλλονται μεταξύ τους. Δεδομένου ότι το σήμα CSS είναι απλούστερο να αποκωδικοποιηθεί από άλλο φάσμα διάδοσης, μπορεί να επιτευχθεί με λιγότερη ισχύ επεξεργασίας. Αυτό μπορεί να σημαίνει μεγαλύτερη διάρκεια ζωής της μπαταρίας για τη συσκευή IoT, παρά την εξελιγμένη διαμόρφωση RF. Ο βασικός ορισμός του LoRa επικεντρώνεται κυρίως στα χαμηλότερα (PHY) στρώματα της ραδιοφωνικής λειτουργίας και αφήνει τη

δομή του δικτύου στη LoRa Alliance, μια κοινοπραξία που καθορίζει προδιαγραφές δικτύου υψηλότερου επιπέδου (οι οποίες ποικίλλουν σε διάφορες περιοχές του κόσμου). Τα δεδομένα ρέουν μέσω συνδέσεων RF της LoRa με Gateways (αποκαλούμενες επίσης συγκεντρωτές), οι οποίες συνδέονται με διακομιστές Internet και Cloud / Application. Η συμμαχία ορίζει επίσης τη δοκιμή και την πιστοποίηση για τη διασφάλιση της διαλειτουργικότητας διαφόρων συσκευών LoRa σε ένα δίκτυο. Το LoRa διαθέτει ασφαλή κλειδιά επικοινωνίας τόσο σε επίπεδο δικτύου όσο και σε επίπεδο εφαρμογών για ασφάλεια δικτύων και δεδομένων, τα οποία είναι πιο σημαντικά όταν τα ραδιοσήματα είναι ανιχνεύσιμα σε μια ευρύτερη περιοχή. Το LoRa αναπτύχθηκε για πρώτη φορά στην Ευρώπη, αλλά εξαπλώνεται σε πολλά μέρη του κόσμου.
Η δοκιμή συσκευών εξακολουθεί να απαιτείται ακόμη και αν χρησιμοποιείται φάσμα χωρίς άδεια χρήσης. Αν και αποτελεί ένα αρκετά νέο πρότυπο, τόσο τα chips όσο και τα modules είναι διαθέσιμα στους σχεδιαστές. Επίσης διάφορα όργανα δοκιμών και διάφορα εργαστήρια δοκιμών υποστηρίζουν ήδη την πιστοποίηση LoRa.

SigFox

Το SigFox είναι μια άλλη πρόσφατη ανάπτυξη τεχνολογίας LPWAN και μοιάζει κατά κάποιον τρόπο στην LoRa, ωστόσο ακολουθεί διαφορετικές μεθόδους για την επίτευξη παρόμοιων στόχων. Το SigFox είναι ιδιόκτητο ραδιοφωνικό πρωτόκολλο, το οποίο λειτουργεί στις ζώνες υπο-1 GHz και παρέχει ένα δίκτυο κυψελοειδών πύλων που συνδέονται με το Internet και το Cloud. Με αυτό τον τρόπο, είναι σαν τα εμπορικά δίκτυα της LoRa, αλλά δεν έχει ως στόχο ιδιωτικά δίκτυα (όπου μια εταιρεία εγκαθιστά και διατηρεί όλο το δικό της δίκτυο). Πρόκειται για ένα δίκτυο αστεριών (start network) με τις πύλες να εξυπηρετούν ως ελεγκτές του δικτύου. Όπως και το LoRa, έχει επίσης μεγάλπ εύρος και πολύ χαμηλή κατανάλωση μπαταρίας ως χαρακτηριστικά. Αλλά το SigFox το επιτυγχάνει με μια πολύ διαφορετική μετάδοση χρησιμοποιώντας ασύρματες εκπομπές πολύ χαμηλής ταχύτητας δεδομένων "Ultra Narrowband" (UNB). Το SigFox είναι πολύ «ελαφρύ» και μεταδίδει ένα ωφέλιμο φορτίο 12 bytes (επιπρόσθετα επιβαρύνσεις πακέτων) σε πολύ στενό εύρος ζώνης D-BPSK διαμόρφωσης σε 100 ή 600 bits ανά δευτερόλεπτο

Λόγω του πολύ στενού εύρους ζώνης, οι δέκτες μπορούν να έχουν πολύ χαμηλό θόρυβο περίπου -140 dBm και να συνδέουν γύρω στα -160 dB όταν χρησιμοποιούν gain antennas. Αυτό σημαίνει ότι χωρίς την κωδικοποίηση (λιγότερη CPU), με την χαμηλή ισχύς πομπού (14 dBm), τις χαμηλές ταχύτητες μεταφοράς δεδομένων, τον μικρό αριθμό μηνυμάτων (όχι περισσότερο από 140 μηνύματα την ημέρα), μπορεί να επιτευχθεί μεγάλη διάρκεια ζωής μπαταρίας σε SigFox IoT συσκευή. Το δίκτυο SigFox IoT, ξεκινώντας από τη Γαλλία, διαθέτει εγκαταστάσεις σε διάφορες ευρωπαϊκές χώρες, με σταθερή επέκταση του δικτύου τους (32 χώρες τη δεδομένη στιγμή).

3.3 5G

Υπάρχουν αναρίθμητες μελέτες που προσπαθούν να ποσοτικοποιήσουν και να προβλέψουν τις υλικές επιπτώσεις της Πέμπτης Γενιάς (5G) και του Διαδικτύου των πραγμάτων (IoT). Ορισμένες από αυτές επικεντρώνονται στην πτυχή του κόστους και άλλες στην αξία για την κοινωνία. Ωστόσο, παρόλο που αυτές οι μελέτες βρίσκονται σε εξέλιξη, είναι προφανές ότι η 5G θα προωθήσει την καινοτομία σε πολλές βιομηχανίες και θα παράσχει μια πλατφόρμα που θα επιτρέψει στις αναδυόμενες τεχνολογίες, όπως το IoT, να αποτελέσουν αναπόσπαστο κομμάτι της οικονομίας και του τρόπου ζωής μας.

Το 5G είναι το θεμέλιο για την αξιοποίηση του πλήρους δυναμικού του IoT. Ενώ η 5G έχει οριστεί για εμπορική διαθεσιμότητα κάποια στιγμή γύρω στο 2020, ο κλάδος εργάζεται ήδη για την ανάπτυξη νέων παγκόσμιων προτύπων και προ προϊόντων 5G για να ωφελήσει τις βιομηχανίες παντού. Η τελευταία έκθεση κινητικότητας της Ericsson AB επισημαίνει ότι θα υπάρξουν 550 εκατομμύρια συνδρομές 5G το 2022 και η Ασία-Ειρηνικός θα είναι η δεύτερη ταχύτερα αναπτυσσόμενη περιοχή με το 10% όλων των συνδρομών να είναι 5G το 2022.

Το πρώτο δίκτυο κινητής τηλεφωνίας (1G) αφορούσε τη φωνή, Το 2G αφορούσε τη φωνή και την αποστολή μηνυμάτων. Το 3G αφορούσε φωνή, γραπτά μηνύματα και δεδομένα. Το 4G ήταν όλα όσα έκανε το 3G αλλά με μεγαλύτερη ταχύτητα. Το 5G θα είναι ακόμα γρηγορότερο. Με το LTE / 4G, η βιομηχανία πλησιάζει τα θεωρητικά όρια

της χρήσης του χρόνου και της συχνότητας. Το 5G εκμεταλλεύεται τη χωρική διάσταση, χρησιμοποιώντας οποιαδήποτε δεδομένη συχνότητα ταυτόχρονα όσο το δυνατόν συχνότερα, εκπέμποντας αυστηρά εστιασμένα σήματα σε διαφορετικές κατευθύνσεις. Η βιομηχανία έχει προκλήσεις που δεν έχουν ακόμη ξεπεραστεί στην προσαρμογή και των δύο τεχνολογιών για το 5G. Σε αντίθεση με το LTE, το 5G λειτουργεί σε τρεις διαφορετικές ζώνες φάσματος. Ενώ αυτό μπορεί να μην φαίνεται σημαντικό, θα έχει δραματική επίδραση στην καθημερινή σας χρήση. Το φάσμα χαμηλής ζώνης μπορεί επίσης να περιγραφεί ως φάσμα υπό 1 GHz. Το φάσμα χαμηλής ζώνης προσφέρει μεγάλη περιοχή κάλυψης και διείσδυση τοίχων. Οι κορυφαίες ταχύτητες δεδομένων θα ξεπεράσουν τα 100Mbps. Η T-Mobile είναι ο «πρωταγωνιστής» όταν πρόκειται για φάσμα χαμηλών συχνοτήτων. Ο μεταφορέας συγκέντρωσε ένα τεράστιο φάσμα 600MHz σε μια δημοπρασία της Federal Communications Commission (FCC) το 2017 και το χρησιμοποιεί για να κατασκευάσει γρήγορα το εθνικό του δίκτυο 5G. Το μεσαίο εύρος ζώνης παρέχει γρηγορότερες ταχύτητες και χαμηλότερη καθυστέρηση από τη χαμηλή ζώνη. Εντούτοις, αποτυγχάνει να διεισδύσει στα κτίρια τόσο αποτελεσματικά όσο ένα φάσμα χαμηλής ζώνης. Αναμένονται μέγιστες ταχύτητες έως 1Gbps στο φάσμα των μέσων ζωνών. Το Sprint έχει την πλειοψηφία του αχρησιμοποίητου φάσματος μέσης ζώνης στις Η.Π.Α. Ο φορέας χρησιμοποιεί Massive MIMO για να βελτιώσει τη διείσδυση και την περιοχή κάλυψης στην μεσαία ζώνη. Οι μαζικές ομάδες MIMO ομαδοποιούν πολλαπλές κεραίες σε ένα ενιαίο κιβώτιο, και σε έναν ενιαίο πύργο κυψέλης. Αυτές οι κεραίες έχουν σκοπό τη δημιουργία πολλαπλών ταυτόχρονων δοκών σε διαφορετικούς χρήστες. Η Sprint θα χρησιμοποιήσει επίσης Beamforming για να ενισχύσει την υπηρεσία 5G στη μεσαία ζώνη. Αυτό στέλνει ένα μόνο εστιασμένο σήμα σε κάθε χρήστη. Τα συστήματα που το χρησιμοποιούν παρακολουθούν κάθε χρήστη για να βεβαιωθούν ότι έχουν ένα συνεπές σήμα.

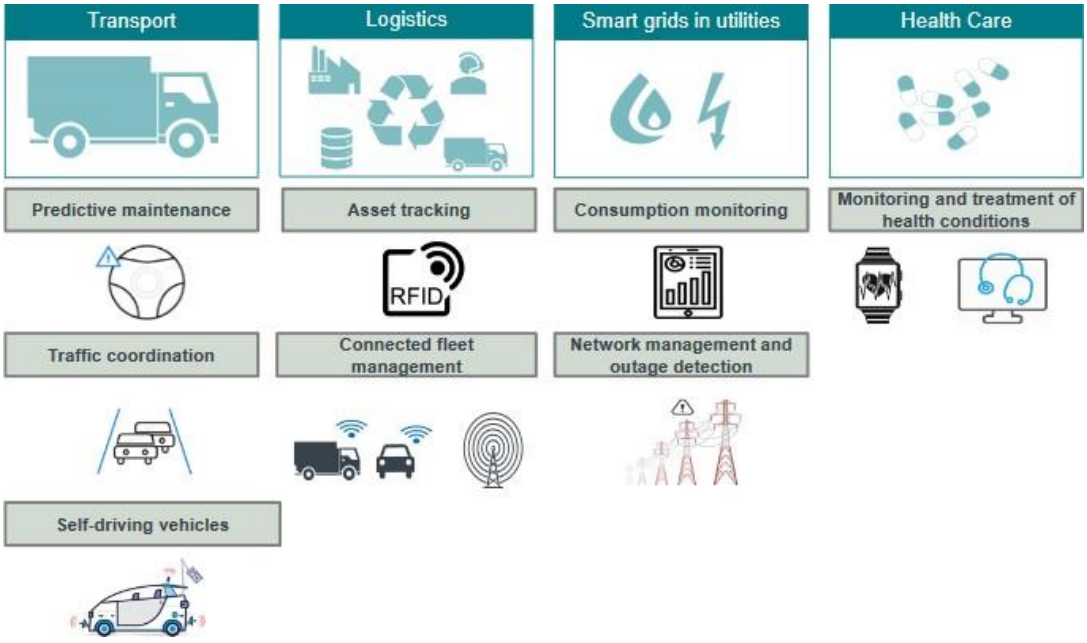
Το φάσμα υψηλών συχνοτήτων είναι αυτό που προσφέρει τις υψηλότερες επιδόσεις για 5G, αλλά με μεγάλες αδυναμίες. Συχνά αναφέρεται ως mmWave. Το φάσμα υψηλών συχνοτήτων μπορεί να προσφέρει μέγιστες ταχύτητες μέχρι 10Gbps και έχει εξαιρετικά χαμηλή λανθάνουσα κατάσταση. Το κύριο μειονέκτημα της υψηλής ζώνης είναι ότι έχει χαμηλή περιοχή κάλυψης και η διείσδυση του κτιρίου είναι κακή.

Η AT & T, η T-Mobile και η Verizon κυκλοφορούν όλο το φάσμα υψηλών συχνοτήτων. Η κάλυψη 5G για τους μεταφορείς θα αποσυρθεί από την LTE, ενώ εργάζονται για την κατασκευή

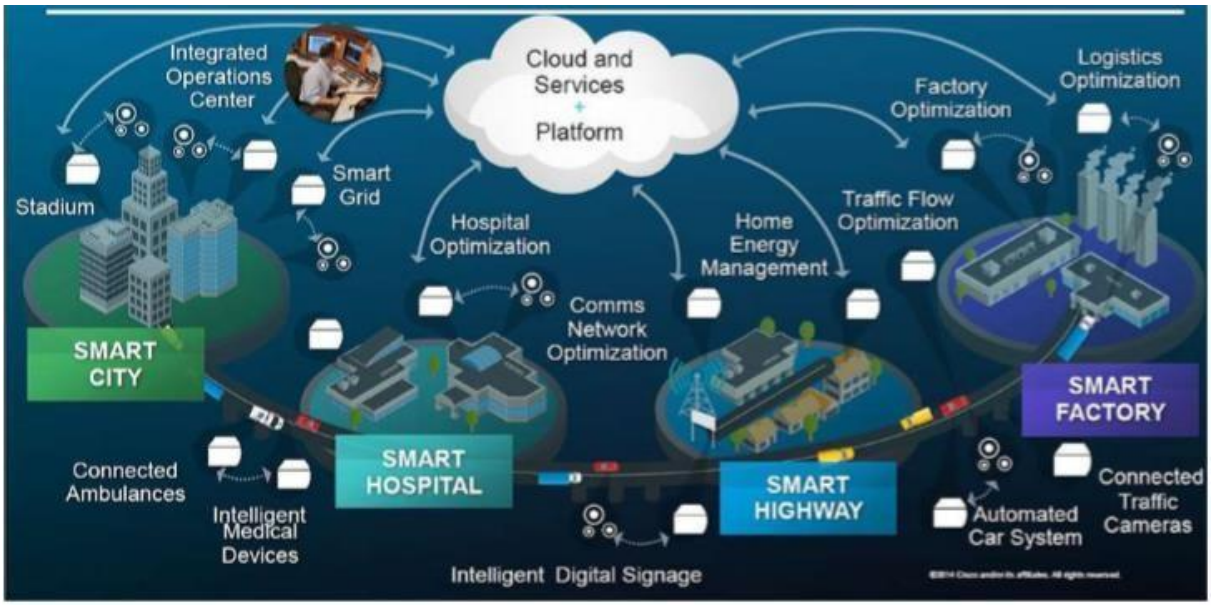
εθνικών δικτύων. Δεδομένου ότι οι θυσίες φάσματος υψηλών συχνοτήτων δημιουργούν διείσδυση και περιοχή κάλυψης για υψηλή ταχύτητα, θα βασίζονται σε πολλά μικρά «cells». Πρόκειται για σταθμούς βάσης χαμηλής κατανάλωσης που καλύπτουν μικρές γεωγραφικές περιοχές και μπορούν να συνδυαστούν με το Beamforming για την ενίσχυση της κάλυψης.

Κεφάλαιο 4ο

Το Διαδίκτυο των πραγμάτων βρίσκεται ακόμη στις απαρχές του, καθώς μερικές από τις έννοιές του και οι τεχνολογίες που θα επέτρεπαν την οριστική υλοποίησή του δεν έχουν αξιοποιηθεί πλήρως. Ένα ενδεχομένως μικρό χρονικό διάστημα θα χρειαστεί να παρέλθει, μέχρις ότου να γίνει αναπόσπαστο μέρος της καθημερινότητας των χρηστών του διαδικτύου, αλλά μέχρι τότε το IoT θα βρει πρώτα αποδοχή σε μίνι δίκτυα, στα βιομηχανικά , οικιακές συσκευές κλπ. Σε βάθος χρόνου όταν θα αποκτήσει αποδοχή και πλήρη εφαρμογή, θα υπάρξει πιθανότητα να σημειωθεί «έκρηξη» σε εκείνες τις αγορές που αφορούν ορισμένους βασικούς παράγοντες των βιομηχανιών.



***Εικόνα 2**: Βασικοί παράγοντες IoT (Frontier Economics March 2018 The Economic Impact of IoT PUTTING NUMBERS ON AREVOLUTIONARY TECHNOLOGY)* [**11**]



***Εικόνα 3**: Πεδίο εφαρμογής IoT (Internet of Things, Dr Rajiv Desai)* **[18]**

Εφαρμογές του Internet Of Things

Αφού φτάσαμε σε σημείο να συνδέσουμε περισσότερα αντικείμενα απ' ότι ανθρώπους στο Διαδίκτυο, ένα μεγάλο παράθυρο ανοιξε δίνοντάς μας την ευκαιρία να δημιουργήσουμε εφαρμογές σε πάρα πολλούς τομείς. Τέτοιοι τομείς αποτελούν η πολεοδομία, η διαχείριση αποβλήτων, το περιβάλλον και πολλοί άλλοι μεταξύ των οποίων περιγράφονται στα παραδείγματα που ακολουθούν.

4.1 Smart Cities

Οι έξυνες πόλεις είναι οι πόλεις εκείνες οι οποίες χρησιμοποιούν τις ψηφιακές τεχνολογίες προκειμένου να μπορούν να διαχειρίζονται τους δήμους με τέτοιο τρόπο ώστε να επιτυγχάνεται οικονομική ανάπτυξη, βελτίωση του βιοτικού επίπεδου των πολιτών, με ταυτόχρονη μείωση του κόστους και της χρησιμοποίησης πόρων.

Σύμφωνα με έρευνες (Pike research) σχετικά με τον τομέα των «Έξυπνων πόλεων», υπολογίζεται ότι έως το 2020 θα έχουν δαπανηθεί εκατοντάδες δισεκατομμυρίων ευρώ.

***Εικόνα 4**: Smart City («Smart Cities»: Οι ευφυείς πόλεις του μέλλοντος)* **[19]**

Υγεία κτιρίων

Η σωστή συντήρηση σε ιστορικά κτίρια μιας πόλης, απαιτούν τη συνεχή παρακολούθηση των πραγματικών συνθηκών κάθε κτιρίου και της ταυτότητας των περιοχών που επηρεάζονται περισσότερο από τις επιδράσεις των εξωτερικών παραγόντων.

Η αστική διαδικτυακή πύλη μπορεί να παρέχει μια κατανεμημένη βάση δεδομένων, η οποία θα περιλαμβάνει μετρήσεις δομικής ακεραιότητας, που συλλέγονται από κατάλληλους αισθητήρες που βρίσκονται στα κτίρια όπως οι κραδασμοί, αισθητήρες ατμοσφαιρικού παράγοντα στις γύρω περιοχές για την παρακολούθηση των επιπέδων ρύπανσης και αισθητήρες θερμοκρασίας και υγρασίας να υπάρχει ,μία πλήρης εικόνα αναφορικά με τις περιβαλλοντικές συνθήκες. Αυτή η βάση δεδομένων θα μπορεί να μειώσει το κόστος από του τακτικούς ελέγχους που αξιοποιούν ανθρώπινους πόρους.

Διαχείριση Αποβλήτων

Η διαχείριση των αποβλήτων αποτελεί πρωταρχικό ζήτημα για πολλές σύγχρονες πόλεις, λόγω του κόστους αλλά και της αποθήκευσης αυτών. Η διείσδυση

του IoT στον συγκεκριμένο τομέα μπορεί να επιφέρει οικονομικά και οικολογικά πλεονεκτήματα. Για παράδειγμα, η χρήση των ευφυών δοχείων απορριμμάτων, τα οποία ανιχνεύουν το επίπεδο φορτίου και επιτρέπουν τη βελτιστοποίηση των διαδρομών που επιχειρούν τα φορτηγά, μπορεί να μειώσει το κόστος συλλογής αποβλήτων και να βελτιωθεί η ποιότητα της ανακύκλωσης.

Ποιότητα Αέρα

Στο στόχο που έχει τεθεί για τη μείωση της ρύπανσης του ατμοσφαιρικού αέρα, μπορεί να συμβάλλει το IoT. Μπορεί να χρησιμοποιηθεί για την παρακολούθηση της ποιότητας του αέρα σε πολυσύχναστες περιοχές, πάρκα κ.α. Επίσης οι πολίτες θα μπορούν να εντοπίζουν τα σημεία τα οποία έχουν καλή ποιότητα αέρα, έτσι ώστε να υλοποιούν τις εξωτερικές τους δραστηριότητες όπως για παράδειγμα άθληση και περίπατο.

Παρακολούθηση Θορύβου

Ο θόρυβος θεωρείται ότι αποτελεί ηχητική ρύπανση, όπως ακριβώς προκαλεί το διοξείδιο του άνθρακα για τον αέρα. Σε αυτήν την κατεύθυνση μέσω του IoT μπορεί να επιτυγχάνεται παρακολούθηση της παραγωγής του θορύβου σε οποιοδήποτε χώρο τοποθετηθεί ο αντίστοιχος αισθητήρας. Επομένως αξιοποιώντας τη χρήση αυτή, μπορεί να διαπιστωθεί να τηρούνται οι ώρες κοινής ησυχίας τα όρια μέσα στα οποία μπορούν να λειτουργούν τα νυχτερινά μαγαζιά, ο εντοπισμός θορύβου συγκρούσεων, κ.α.

Κυκλοφορική συμφόρηση

Η κυκλοφοριακή συμφόρηση αποτελεί ένα από τα μεγαλύτερα προβλήματα που αντιμετωπίζουν οι μικρές και μεγάλες πόλεις σε ώρες αιχμής. Παρόλο που ήδη χρησιμοποιούνται οι κάμερες ρύθμισης της κυκλοφορίας, η πληροφορία δεν φτάνει άμεσα στον ενδιαφερόμενο. Η παρακολούθηση της κυκλοφορίας μπορεί να πραγματοποιηθεί μέσω των δυνατοτήτων ανίχνευσης και το GPS Που είναι ενσωματωμένα στα σύγχρονα οχήματα. Με αυτόν τον τρόπο η πληροφορία αναφορικά

με την κατάσταση που επικρατεί στους δρόμους είναι άμεση τόσο για του πολίτες όσο για τις αρχές. Έτσι μπορεί να επιλεχθεί η καταλληλότερη διαδρομή ή να γίνει εκ των προτέρων καλύτερος προγραμματισμός για επικείμενο ταξίδι.

'Έξυπνη Στάθμευση

Η έξυπνη υπηρεσία στάθμευσης βασίζεται σε αισθητήρες που είναι τοποθετημένοι στο δρόμο και βάσει των οποίων οι ιδιοκτήτες των οχημάτων ενημερώνονται για διαθέσιμη περιοχή στάθμευσης στην περιοχή ή στο δρόμο στον οποίο επιθυμούν να σταθμεύσουν. Αυτό έχει σαν αποτέλεσμα την εξοικονόμηση χρόνου του εκάστοτε οδηγού, την μείωση της κυκλοφοριακής συμφόρησης και της εκπομπής ρυπαντικών ουσιών των οχημάτων (CO, CO2 κ.α.).

Έξυπνος Φωτισμός

Η υπηρεσία αυτή μπορεί να βελτιστοποιήσει την χρήση του φωτισμού ανάλογα με την ώρα της ημέρα, την καιρική κατάσταση και τις συνθήκες που επικρατούν στο περιβάλλον. Αυτό προσφέρει εξοικονόμηση ενέργειας καθώς ο φωτισμός θα χρησιμοποιείται ακριβώς τη στιγμή και στην ένταση που αυτός είναι χρήσιμος. Επίσης θα δίνεται η δυνατότητα του άμεσου εντοπισμού βλαβών στο δίκτυο φωτισμού.

Περιβάλλον

Το «έξυπνο περιβάλλον» αποτελεί την ιδέα ενός φυσικού κόσμου που είναι συνυφασμένος με αισθητήρες, ενεργοποιητές οθόνες και υπολογιστικά αρχεία. Με τη σωστή χρήση των παραπάνω προκύπτουν οι παρακάτω εφαρμογές:

Πυρανίχνευση δασικών περιοχών

Έλεγχος των αερίων καύσης και των συνθηκών που ευνοούν την έναρξη πυρκαγιάς.

Πρόληψη κατολισθήσεων

Παρακολούθηση του εδάφους σχετικά με την υγρασία, τις δονήσεις και της πυκνότητα για την έγκαιρη πρόβλεψη επικίνδυνων φαινομένων.

Ανίχνευση σεισμών

Έλεγχος συγκεκριμένων περιοχών, γνωστών για την σεισμολογική τους δραστηριότητα για την καλύτερη παρακολούθηση του φαινομένου και την πρώιμη ανίχνευση σεισμών.

Δημόσια κτίρια

Παρακολούθηση της κατανάλωσης ενέργειας και υγιεινής δημόσιων κτιρίων (σχολεία, μουσεία, δημόσιες υπηρεσίες) μέσω αισθητήρων που ελέγχουν τα φώτα, τη θερμοκρασία και την υγρασία. Με τον έλεγχο αυτών των παραμέτρων, μειώνεται το κόστος (ηλεκτρικού ρεύματος και θέρμανσης-ψύξης) και ταυτόχρονα επιδρά θετικά στην παραγωγικότητα των εργαζομένων που στεγάζονται στο εκάστοτε κτίριο.

4.2 Έξυπνο σπίτι

Τα «Έξυπνα Σπίτια» έχουν ως στόχο την βελτιστοποίηση του επιπέδου άνεσης αλλά και της μείωσης των συνολικών δαπανών. Επίσης είναι σε θέση να αντιμετωπίσουν με ικανοποιητικό τρόπο διάφορα θέματα ασφαλείας όπως η ανίχνευση πυρκαγιάς, κλοπής ή παράνομης εισόδου. Σε συνεργασία με διάφορους τομείς (τηλεπικοινωνιακός πάροχος, εταιρείες προστασίας, εταιρείας παροχής ηλεκτρικής ενέργειας κ.α) προκύπτουν τα εξής:

- Η κατανάλωση ενέργειας και νερού παρακολουθούνται προκειμένου να ληφθούν αποφάσεις οι οποίες θα επιφέρουν μείωση των πόρων αλλά και του κόστους.
- Διαχείριση συσκευών εξ’ αποστάσεως για βελτιστοποίηση της άνεσης αλλά και της εξοικονόμησης ενέργειας.

- Ανίχνευση συγκεκριμένων σημείων μέσα στο χώρο (πόρτες, παράθυρα), ώστε να γίνονται αντιληπτές παραβιάσεις και να αντιμετωπίζονται άμεσα.

Εικόνα 5: *Smart Home (Aztech Introduces Kyla – Smart Home, Smart Life. (Press Release)* **[20]**

4.3 Έξυπνη Βιομηχανία

Οι εταιρείες είναι σε θέση να παρακολουθούν όλα τους τα προϊόντα μέσω ετικετών αναγνώρισης ραδιοσυχνοτήτων. Αυτό έχει σαν αποτέλεσμα τη μείωση των λειτουργικών τους εξόδων, αλλά και την βελτίωση της παραγωγικότητάς τους. Επιπρόσθετα διευκολύνεται η συντήρηση των μηχανημάτων μέσω συνδεδεμένων αισθητήρων οι οποίοι δίνουν τη δυνατότητα της παρακολούθησης σε πραγματικό χρόνο, έτσι ώστε έγκαιρα να εντοπίζεται τυχόν πρόβλημα που θα επηρεάσει την καλή λειτουργία και απόδοση.

Σε γενικές γραμμές το IoT παρέχει αυτοματοποιημένες διαδικασίες, οι οποίες μπορούν να μειώσουν δραστικά τον ανθρώπινο παράγοντα.

Άλλα οφέλη την ενσωμάτωσης του IoT στην βιομηχανία είναι:

- Παρακολούθηση του εσωτερικού αέρα αναφορικά με τα τοξικά επίπεδα φυσικού αερίου και οξυγόνου για την εξασφάλιση της ασφάλειας των εργαζομένων και των εμπορευμάτων
- Έλεγχος της θερμοκρασίας του εσωτερικού χώρου και ιδιαίτερα σε αυτούς που περιλαμβάνουν ευαίσθητα εμπορεύματα.
- Αξιολόγηση της παραγωγικής διαδικασίας ανά τομέα, με στόχο την βελτιστοποίηση.

4.4 Λιανική Πώληση

Το IoT λαμβάνει υπόψη τόσο τις ανάγκες των καταναλωτών όσο αυτές των επιχειρήσεων. Συγκρίνει την τιμή ενός προϊόντος σε σχέση με άλλα προϊόντα ίδια ποιότητας με χαμηλότερη τιμή και τροφοδοτεί με τις ανάλογες πληροφορίες και τις δύο πλευρές. Βάσει αυτής της πληροφόρησης οι επιχειρήσεις έχουν τη δυνατότητα να βελτιώνουν τις αγορές τους και να προσφέρουν ικανοποίηση στους καταναλωτές.

Επίσης με την ενσωμάτωση του IoT οι επιχειρήσεις μπορούν να εκμεταλλευτούν τα παρακάτω:

- **Έλεγχος Προμηθειών**

  Παρακολούθηση συνθηκών αποθήκευσης των προϊόντων.

- **Εφαρμογές Έξυπνης αγοράς**

  Παροχή πληροφοριών στο σημείο πώλησης αναφορικά με τις συνήθεις, τις ιδιαιτερότητες και τις προτιμήσεις των καταναλωτών.

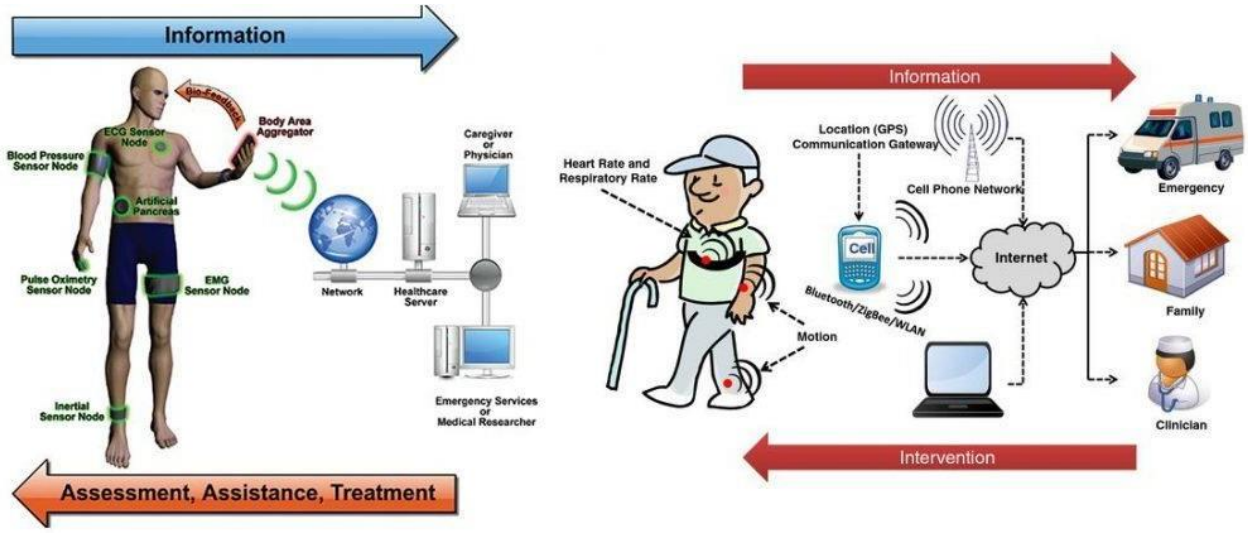
- **Έξυπνη διαχείριση προϊόντων**

  Έλεγχος των προϊόντων στις αποθήκες και στα ράφια για την αυτοματοποίηση των διαδικασιών άμεσης αντικατάστασης τους.

4.5 Ιατρική Παρακολούθηση

Σήμερα υπάρχει η δυνατότητα μέσω της ενσωμάτωσης του IoT, οι άνθρωποι να παρακολουθούνται και να ελέγχονται από τους ειδικούς ακόμα και αν βρίσκονται σε διαφορετικό μέρος. Η τεχνολογία αισθητήρων παρέχει πληροφορίες σε πραγματικό

χρόνο για ζωτικά σημεία και για άλλους δείκτες (σφυγμό, θερμοκρασία, πίεση) σχετικά με την υγεία και τη κατάσταση ενός ατόμου καθώς και την ταυτοποίηση και παρακολούθηση φαρμακευτικής αγωγής. Αυτά τα συστήματα βρίσκουν εφαρμογή στα νοσοκομεία, σε συστήματα παρακολούθησης της υγείας στο σπίτι, στα ιατρεία και στη φροντίδα ηλικιωμένων. Η εξ΄ αποστάσεως αλληλεπίδραση μεταξύ ασθενούς και ιατρού είναι εξαιρετικά σημαντική, καθώς μειώνει το κόστος και εξοικονομείται χρόνος.



Εικόνα 6: *Smart Health (Smart Health-Care :- Let the little gadgets save your life* **[13]**

4.6 Κτηνοτροφία

Χαρακτηριστικό παράδειγμα της αξιοποίησης του IoT στην κτηνοτροφία αποτελεί μία ολλανδική εταιρεία η οποία τοποθέτησε εμφυτεύματα-αισθητήρες στα αυτιά των βοοειδών. Με αυτόν τον τρόπο παρακολουθούνται κατά κύριο λόγο η υγεία των συγκεκριμένων ζώων καθώς και οι κινήσεις τους.

Άλλες εφαρμογές της «έξυπνης κτηνοτροφίας» είναι:

Φροντίδα

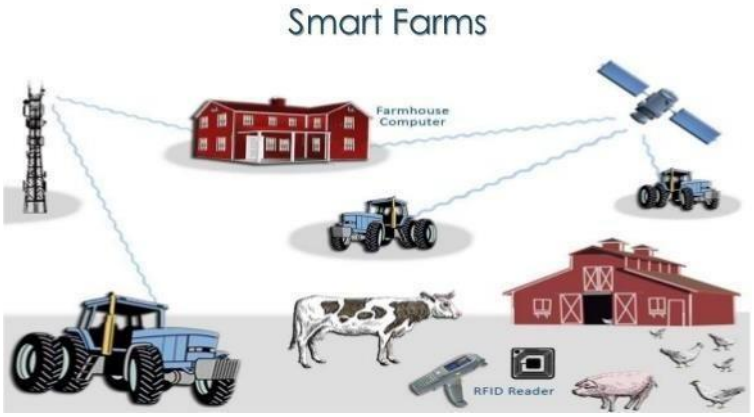
Έλεγχος των συνθηκών στις οποίες βρίσκονται οι απόγονοι των ζώων, ώστε να εξασφαλιστεί η υγεία τους και η ευζωία τους.

Παρακολούθηση

Εντοπισμός και αναγνώριση των ζώων.

Ποιότητα αέρα

Έλεγχος του περιβάλλοντος των ζώων σχετικά με την ποιότητα του αέρα και την ανίχνευση επιβλαβών για αυτά ουσιών.



Εικόνα 7: Smart Farm (Pervasive technologies Internet of Things(IOT) **[22]**

4.7 Γεωργία

Η εφαρμογή του IoT στην γεωργία, έχει αποδώσει ένα ευρύ φάσμα εφαρμογών που βελτιστοποιούν τις διαδικασίες που σχετίζονται με αυτή.

Θερμοκήπια

Έλεγχος συνθηκών κλίματος για τη μεγιστοποίηση της παραγωγής αλλά και της ποιότητας των προϊόντων που καλλιεργούνται.

Καιρικές συνθήκες

Μελέτη των καιρικών συνθηκών προκειμένου να προβλεφθούν οι επιβλαβείς αλλαγές που επηρεάζουν τις καλλιέργειες, όπως πάγος, χαλάζι, άνεμος, βροχή, και ξηρασία.

Έδαφος

Έλεγχος της υγρασίας και της θερμοκρασίας του εδάφους, προκειμένου να διασφαλισθεί ότι είναι πρόσφορο, αλλά και για την πρόληψη ανάπτυξης μικροβιακών ρύπων.

Εικόνα 8: *Utilizing the IoT for Smart Agriculture* **[12]**

4.8 Διαφήμιση

Η διαφήμιση έχει διαφορετική διάσταση με την επίδραση του. Ο συμβατικός τρόπος διαφήμισης αφορά πάντα ένα σενάριο όπου ένας διαφημιζόμενος δημιουργεί μια πλατφόρμα για τη διαφήμιση προϊόντων και υπηρεσιών που διοχετεύονται στους κατάλληλους δέκτες τους. Το προφανές ερώτημα στη διαφήμιση σε έναν κόσμο των IoT είναι με ποιόν τρόπο θα μπορέσει να επιτευχθεί η διείσδυση σε μία φαινομενικά κλειστή αγορά

Ο Plowman το 2014, περιγράφει μια κατάσταση όπου οι διαθέσεις των καταναλωτών μπορούν να διαβαστούν από αυτόνομες συσκευές και τα δεδομένα που προκύπτουν να συλλέγονται προς επεξεργασία. Αυτό επιτρέπει στους διαφημιστές να διοχετεύσουν καλύτερα το προϊόν τους, στους τομείς που το χρειάζονται. Σε γενικές γραμμές, με το

Διαδίκτυο των πραγμάτων είναι δυνατόν να συγκεντρωθούν πληροφορίες και να συνδεθούν διαφημίσεις στην καθημερινή ζωή των καταναλωτών και έτσι είναι σίγουρο ότι θα υπάρξει αύξηση των πωλήσεων λόγω της συνειδητοποίησης της τάσης της αγοράς.

Κεφάλαιο 5ο

5.1 Internet of Threats

Αναμφισβήτητα η νέα μεγάλη τάση στο τομέα της τεχνολογίας για την οποία όλοι συζητάνε παγκοσμίως είναι το Internet of Things. Στις παραμέτρους που συνοδεύουν το IoT σημαίνοντα ρόλο διαδραματίζει και η ασφάλεια. Μιλώντας για τη νέα αυτή παγκόσμια τεχνολογική αλλαγή, αναφερόμαστε σε ένα μεγάλο και πολυποίκιλο πεδίο δραστηριοποίησης. Σε αυτό λοιπόν το πεδίο χρησιμοποιούνται συσκευές καθημερινής χρήσης αλλά και επαγγελματικές εφαρμογές, που συλλέγουν πληροφορίες από το περιβάλλον ή άλλες διασυνδεδεμένες συσκευές, μεταδίδοντας δεδομένα σε άλλα συστήματα ή σε συσκευές του χρήστη, προσφέροντας ευκολίες και αυτοματισμούς σε πραγματικό χρόνο. Οι διασυνδεμένες συσκευές στα πλαίσια του IoT μπορούν να καλύπτουν τομείς καθημερινής δραστηριότητας στο σπίτι και το επαγγελματικό περιβάλλον, αλλά και διαδικασιών αγορών, εφαρμογών υγείας και ασφάλειας, επικοινωνίας, μεταφορών και άλλων λειτουργιών.

Από πλευράς κατασκευαστών τεχνολογικών λύσεων, η νέα τάση του IoT προσφέρει σίγουρα μια νέα μεγάλη ευκαιρία για να αναπτύξουν πρωτοποριακά προϊόντα που θα υποστηρίζουν τη συγκεκριμένη τάση. Παρόλα αυτά, όπως σε όλες τις νέες τάσεις, έτσι και σε αυτή τη περίπτωση, εγείρονται ορισμένοι προβληματισμοί, αφενός για τη διαχείριση των συλλεγόμενων πληροφοριών από τρίτους αλλά και για τον τρόπο που αυτές θα χρησιμοποιηθούν σε πραγματικό ή σε μελλοντικό χρόνο και αφετέρου και με δεδομένο ότι ο πυρήνας της συγκεκριμένης τάσης είναι η διασύνδεση στο διαδίκτυο, ανακύπτουν οι προβληματισμοί για τις κακόβουλες ενέργειες που πάντα

ελλοχεύουν και απασχολούν τους υπεύθυνους ψηφιακής ασφάλειας.

Το κοινό καταφεύγει στο Διαδίκτυο των πραγμάτων για την ευκολία του ελέγχου και της παρακολούθησης των έξυπνων συσκευών. Μια τέτοια εξάρτηση από το διαδίκτυο έχει ως αποτέλεσμα μια σημαντική ποσότητα δεδομένων που πρέπει να παραχθούν, να συλλεχθούν, να υποβληθούν σε επεξεργασία και να αναλυθούν. Οι μεγάλες αναλύσεις δεδομένων είναι εξαιρετικά ωφέλιμες για την ανάπτυξη των επιχειρήσεων. Ωστόσο, ταυτόχρονα με τις αναλύσεις αυτές, συνυπάρχουν πολλές απειλές για τη διαθεσιμότητα και προστασία της ιδιωτικής ζωής των δεδομένων των χρηστών, την ακεραιότητα των μηνυμάτων και των συσκευών, την ευπάθεια των συσκευών του διαδικτύου σε επιθέσεις κακόβουλου λογισμικού και τον κίνδυνο φυσικής καταστροφής των συσκευών. Όλα τα προαναφερθέντα σηματοδοτούν τους κινδύνους/απειλές που προκύπτουν έμμεσα, από την εξέλιξη και καθιέρωση του IoT.

Παρουσιάζουμε μια λεπτομερή μεθοδολογία επίθεσης που υιοθετήθηκε από μερικές από τις πιο επιτυχημένες επιθέσεις κακόβουλου λογισμικού σε IoT, συμπεριλαμβανομένων των ICS και CPS. Επίσης, συνάγουμε μια στρατηγική επίθεσης του botnet attackedroughDoService (DDoS) που ακολουθείται από απαιτούμενα μέτρα ασφαλείας. Στο τέλος, προτείνουμε μια σύνθετη κατευθυντήρια γραμμή για την ανάπτυξη ενός πλαισίου για την προστασία του περιβάλλοντος από τις καλύτερες πρακτικές στον τομέα της βιομηχανίας και επίσης να αναδείξουμε τα διδάγματα, τις παγίδες και τις ανοικτές ερευνητικές προκλήσεις.

IoT vs Παράδοση

Πριν συζητήσουμε τις απειλές του Διαδικτύου, είναι σημαντικό να κατανοήσουμε τις διαφορές μεταξύ των διαφόρων παραμέτρων και των παραδοσιακών δικτύων, καθώς αυτές οι διαφορές επηρεάζουν την ανάπτυξη των απαιτούμενων λύσεων ασφάλειας και προστασίας της ιδιωτικής ζωής για τα συστήματα IoT. Σημαντική διαφορά μεταξύ συμβατικών δικτύων και του IoT, είναι το επίπεδο της επινοητικότητας των τελικών συσκευών.

5.2 Γενικές απειλές

Εκτιμάται ότι με την αύξηση του αριθμού των πραγμάτων που συνδέονται με τα συστήματα IoT ταυτόχρονα τα πιθανά τρωτά σημεία θα αυξηθούν επίσης. Η αύξηση των σημείων αυτών που οφείλονται στην μη τυποποίηση των τεχνολογιών διαδικτύου, μπορεί να προκαλέσει προβλήματα ασφαλείας στα συστήματα διατήρησης των πληροφοριών. Ορισμένα από αυτά τα σημεία είναι:

1) Ασφάλεια και Προστασία Προσωπικών Δεδομένων:

Κατά τη διενέργεια ελέγχου ασφαλείας, ελέγχθηκαν πολυάριθμες έξυπνες συσκευές για παραβιάσεις ασφαλείας. Αποτέλεσμα του ελέγχου ήταν, ότι σχεδόν το 90% αυτών των συσκευών συλλέγει προσωπικές πληροφορίες σχετικά με τους χρήστες υπό κάποια μορφή. Αυτή η μη εξουσιοδοτημένη αποθήκευση πληροφοριών είναι ευάλωτη σε επιθέσεις ασφάλειας δεδομένων, ιδιωτικότητας και ακεραιότητας. Είναι επομένως ορατός ο κίνδυνος που αφορά τα θέματα ασφάλειας και ιδιωτικής ζωής και την εμπιστευτικότητα των δεδομένων αλλά και την ιδιωτική ζωή των χρηστών. Η έλλειψη αξιόπιστου μηχανισμού επαλήθευσης ταυτότητας σε συσκευές IoT είναι επίσης ένας παράγοντας που συμβάλλει στην ανασφαλή ασφάλεια του Διαδικτύου. Επιπλέον, η έλλειψη κρυπτογράφησης δεδομένων και μέτρων ελέγχου πρόσβασης στο δίκτυο επιτρέπουν σε έναν εισβολέα να αποτελέσει πραγματική απειλή για την ιδιωτική ζωή των χρηστών ως αποτέλεσμα της υποκλοπής και της ανάλυσης της κίνησης δεδομένων.

2) IoT στην Υγεία

Το δίκτυο βιοϊατρικών αισθητήρων (BSN) είναι μια εξειδικευμένη περίπτωση, στην οποία οι αισθητήρες χρησιμοποιούνται για την παρακολούθηση της υγείας των ασθενών και επίσης για τη διευκόλυνση της μακροχρόνιας ασφάλειάς τους. Το BSN έχει δυναμική τοπολογία δικτύου λόγω κινητών κόμβων, περιορισμών ισχύος και

πρωτοκόλλων επικοινωνίας IoT χαμηλού εύρους ζώνης. Ως εκ τούτου, η BSN είναι ευάλωτη σε πολλές επιθέσεις, συμπεριλαμβανομένου του DoS, υποκλοπής, μετακόμισης και μη εξουσιοδοτημένης αποκάλυψης προσωπικών πληροφοριών υγείας. Μια επιτυχημένη επίθεση μπορεί να είναι απειλητική για τη ζωή και μπορεί επίσης να προκαλέσει απώλεια δεδομένων, κατάχρηση πρόσβασης, απώλεια προσωπικών πληροφοριών, χειραγώγηση δεδομένων και ακόμη και σε ορισμένες περιπτώσεις μη διαθεσιμότητα κρίσιμων υπηρεσιών υγείας.

3) Ακεραιότητα

Η ανάπτυξη και η επιτυχής λειτουργία του Διαδικτύου σε κρίσιμες υποδομές όπως τα έξυπνα δίκτυα, η υγειονομική περίθαλψη, τα έξυπνα συστήματα κυκλοφορίας, τα έξυπνα οχήματα και τα έξυπνα σπίτια εξαρτώνται σε μεγάλο βαθμό από την αξιοπιστία των συσκευών και των δεδομένων που μεταδίδονται μεταξύ αυτών των συσκευών. Ωστόσο, οι τερματικές συσκευές IoT λειτουργούν ως επί το πλείστον σε ένα περιβάλλον χωρίς εμπιστοσύνη και χωρίς φυσική ασφάλεια. Ως εκ τούτου, αυτές οι συσκευές υπόκεινται σε φυσικές επιθέσεις, συμπεριλαμβανομένων επιθέσεων υλικού και επίγειων επιθέσεων.

4) Λογισμικό/Κωδικοποίηση

Η ακεραιότητα του λογισμικού, συμπεριλαμβανομένης της ακεραιότητας του λειτουργικού συστήματος, των εφαρμογών και των ρυθμίσεων των συσκευών IoT, αποτελεί βασικό στοιχείο για την εγγύηση της ασφάλειας και της ιδιωτικότητας των "Πραγμάτων". Πρόσφατα μια πρακτική εκδήλωση μιας τέτοιας επίθεσης την οποία βίωσε ο κόσμος, ονομάστηκε "Mirai". Αυτή η επίθεση δημιούργησε ένα botnet, το οποίο απέκτησε παράνομη πρόσβαση σε χιλιάδες συσκευές IoT, συμπεριλαμβανομένων των καμερών CCTV και των DVR, αξιοποιώντας την αδυναμία του λογισμικού και κατευθύνοντας τις συσκευές αυτές να ξεκινήσουν μια επίθεση DDoS σε έναν πάροχο υπηρεσιών DNS (Domain Name System) που ονομάζεται DYN. Πιστεύεται ότι η έλλειψη μηχανισμού ανίχνευσης anti-virus/malware σε IoT οδηγεί σε

επιθέσεις στην ακεραιότητα του κώδικα/λογισμικού μιας τελικής συσκευής.

Οι εφαρμογές για κινητά είναι μια άλλη πηγή κακόβουλου λογισμικού σε έξυπνες συσκευές που καταστρέφουν περαιτέρω τα δίκτυα υπολογιστών μέσω «μολυσμένων» μηνυμάτων ηλεκτρονικού ταχυδρομείου, εγγράφων και άμεσης σύνδεσης. Το 2016, περίπου ένας εκατομμύριο λογαριασμοί Google χάθηκαν λόγω ενός κακόβουλου λογισμικού Android που ονομάζεται "Gooligan". Ως εκ τούτου, οι συσκευές IoT πρέπει να προστατεύονται από επιθέσεις κακόβουλου λογισμικού, όπως τα trojans, οι ιοί και άλλα.

5) Πρωτόκολλα Επικοινωνίας

Οι περαιτέρω προκλήσεις στον σχεδιασμό της ασφάλειας του IoT / CPS προκύπτουν από το γεγονός ότι τα περισσότερα από τα τρέχοντα πρωτόκολλα ασύρματης επικοινωνίας τηρούν την αρχιτεκτονική πρωτοκόλλου OSI και η κρυπτογράφηση φυσικής στρώσης δεν συμπληρώνεται με πρόσθετους μηχανισμούς ασφαλείας στα ανώτερα στρώματα της επικοινωνίας. Μία επίθεση MITM (Manin-the-Middle) που ξεκίνησε με την καταγραφή του πρωτοκόλλου ανάλυσης διευθύνσεων (ARP) στο επίπεδο MAC, είναι ένα παράδειγμα μιας τέτοιας παραβίασης της ασφάλειας.

Επιπρόσθετα, ερευνητές έχουν εντοπίσει ότι τα ζητήματα διασυνοριακής ασφάλειας πληθαίνουν από την έλλειψη επικοινωνίας. Αυτά τα ζητήματα μπορούν εύκολα να επεκταθούν σε IoT και CPS. Το ίδιο έχει αποδειχθεί μέσω διαφόρων παραβιάσεων της ασφάλειας, όπως η κακόβουλη απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα όχημα Mitsubishi μέσω απόσπασης του κλειδιού WiFi, η εξαγωγή ιδιωτικών/ευαίσθητων δεδομένων από έναν υπολογιστή μέσω ενός κρυφού καναλιού FM, και η πειρατεία της ασύρματης ελεγχόμενης εμφυτεύσιμης ιατρικής συσκευής. Ομοίως, οι κυτταρικές τεχνολογίες όπως το UMTS, το GSM και το LTE επίσης υποφέρουν από συγκεκριμένα θέματα ασφαλείας. Λόγω της ανοιχτής εφαρμογής των stack ραδιοφωνικών ζωνών, τα δίκτυα κινητής τηλεφωνίας έχουν μια πρόσθετη απειλή hacking και επιθέσεις στον κυβερνοχώρο.

Έπειτα, τα δίκτυα GSM και UMTS είναι ευάλωτα στο "IMSI Catching" από έναν ενεργό εισβολέα. Επίσης υπάρχει καθυστέρηση στη ρύθμιση των πλαισίων ασφαλείας ενώ ένας εξοπλισμός χρήστη είναι είναι συνδεδεμένος με το σταθμό βάσης. Μια τέτοια καθυστέρηση μπορεί να αποβεί μοιραία για εφαρμογές ευαίσθητες σε καθυστέρηση, π.χ. αυτόνομα αυτοκίνητα, έξυπνα ιατρικά εργαλεία κλπ. Τα δίκτυα κινητής τηλεφωνίας είναι επίσης ευάλωτα σε επιθέσεις DoS που ξεκίνησαν από κινητά bots. Τα κινητά bots ενδέχεται να προσβάλλουν το MME (Mobile Management Entity) και το HSS (Home Subscriber Server). Αντίστοιχα, η παρεμβολή ραδιοσυχνοτήτων είναι η επίθεση DoS που προδιαγράφεται στην ασύρματη επικοινωνία. Μπορεί να ξεκινήσει μια έξυπνη επίθεση εναντίον του 3GPP (3η γενιά της συνεργασίας) σε κινητά δίκτυα χρησιμοποιώντας κινητά botnets, στα οποία μπορούν να αποκλειστούν επιλεκτικά τα κανάλια ελέγχου που είναι απαραίτητα για τη συνολική λειτουργία της ραδιοεπικοινωνίας. Οι επιθέσεις DoS αποτελούν ακόμη απειλή για τα δίκτυα 5G.

Επιπλέον, οι ασύρματες τεχνολογίες μικρής εμβέλειας, όπως η BluetoothandZigbeeare, δεν είναι κατάλληλες για εφαρμογές που απαιτούν μεγάλη εμβέλεια επικοινωνίας με χαμηλό εύρος ζώνης. Παρόλο που η κυψελοειδής τεχνολογία παρέχει μακρά κάλυψη για την επικοινωνία M2M, απαιτεί περισσότερη ισχύ. Ως εκ τούτου, από το 2015, η τεχνολογία LPWAN (Low Power Wide Area Network) θεωρείται κατάλληλη τεχνολογία για εφαρμογές που απαιτούν ευρεία κάλυψη, χαμηλή κατανάλωση ενέργειας, ποιότητα QoS, χαμηλό ρυθμό μετάδοσης δεδομένων, χαμηλή λανθάνουσα κατάσταση και χαμηλό κόστος. Οι Koushanfar και άλλοι αναφέροουν ότι τα πρωτόκολλα επικοινωνίας υπόκεινται σε επιθέσεις πρωτοκόλλου, συμπεριλαμβανομένων των επιθέσεων MITM και DoS. Εμφανίζεται μια εκδήλωση μιας από τις επιθέσεις DoS στο πρωτόκολλο ασύρματης επικοινωνίας 802.11b. Ο έλεγχος της ευπάθειας στην ανταλλαγή μηνυμάτων αποσύνδεσης μεταξύ του πελάτη και του σταθμού. Διαπιστώνεται ότι το μήνυμα αποστέλλεται χωρίς έλεγχο ταυτότητας. Ως εκ τούτου, επιτρέπει σε έναν εισβολέα να ξεκινήσει ένα μήνυμα αποσύνδεσης για λογαριασμό άλλων χρηστών για να σταματήσει τη σύνδεσή του στο δίκτυο. Αντίστοιχα, αυτό το DoS μπορεί να οδηγήσει σε σοβαρό πρόβλημα διαθεσιμότητας σε περίπτωση συστήματος CPS / IoT. Μπορεί περαιτέρω να συναχθεί ότι σχεδόν όλα τα

πρωτόκολλα επικοινωνίας όπως το 802.15.4, το Zigbee και το LoRaWAN παρέχουν συμβατικές κρυπτογραφικές εγγυήσεις ασφαλείας όπως η ακεραιότητα, η ακεραιότητα των δεδομένων, η αυθεντικότητα των δεδομένων, η προστασία επανάκλησης και η μη αποκήρυξη. Ωστόσο, η κρυπτογραφική ασφάλεια που είναι ενσωματωμένη στα πρωτόκολλα επικοινωνίας δεν προορίζεται να προστατεύσει από σοβαρές επιθέσεις και κακόβουλα προγράμματα.

Υπάρχει και μια άλλη επερχόμενη τεχνολογία επικοινωνίας, η οποία αναπτύσσεται από την ομάδα IEEEE802.1TSN (TimeSensitiveNetworks) TG (Task Group) για εφαρμογές που απαιτούν UltraLow Latency (ULL). Το TSN υπόσχεται μια ασφαλή διασύνδεση δικτύου μεταξύ ενός αποστολέα και ενός κόμβου δέκτη μέσω δικτύου ευαίσθητου στο χρόνο. Παρομοίως, η IETF (Task Force Internet Engineering) εργάζεται επίσης στο DetNet (Deterministic Networks) για τη διασύνδεση της απομονωμένης OT (επιχειρησιακής τεχνολογίας), δηλ. CPS με δίκτυα πληροφορικής. Ωστόσο, μια τέτοια διασύνδεση θα εκθέσει το CPS σε διάφορες εσωτερικές και εξωτερικές επιθέσεις. Επιπλέον, δεδομένου ότι πρόκειται για έργο που βρίσκεται σε εξέλιξη, οι κανόνες ασφαλείας απαιτούν τη δέουσα προσοχή για τον μετριασμό των εσωτερικών και εξωτερικών απειλών που κυμαίνονται από τη μεταβολή της ροής detNet σε χειρισμούς διαδρομής και επιθέσεων σε συγχρονισμένους μηχανισμούς χρόνου. Πηγαίνοντας στα μέσα επικοινωνίας του κεντρικού δικτύου, κυρίως το OFC διασυνδέει πολλά κέντρα εταιρικών δεδομένων ή έναν ISP με την πύλη διαδικτύου.

Ένα οπτικό κανάλι οπτικών ινών μπορεί να επηρεάσει άμεσα ένα σύστημα IoT, π.χ. μια συσκευή έξυπνης οικιακής πύλης είναι συνδεδεμένη με έναν ISP μέσω σύνδεσης FTTH (Fibre-To-The-Home), προκειμένου να παρέχει εξ αποστάσεως πρόσβαση σε διάφορες υπηρεσίες ο ιδιοκτήτης του σπιτιού και η ίδια σύνδεση μπορούν να χρησιμοποιηθούν από τον προμηθευτή για τη συντήρηση / απομακρυσμένη παρακολούθηση του συστήματος. Τα οπτικά κανάλια είναι ανθεκτικά σε υποκλοπές, παρεμβολές και επιθέσεις στη διαθεσιμότητα. Ένας επιτιθέμενος μπορεί να παρακολουθήσει τα ταξινομημένα / ιδιωτικά δεδομένα πατώντας σε ένα οπτικό πεδίο για μη κρυπτογραφημένα κανάλια ή παραβιάζοντας τα κλειδιά κρυπτογράφησης που είναι απομονωμένα από το ωφέλιμο φορτίο και μεταφέρονται μέσω του

συστήματος διαχείρισης δικτύου (NMS).

Ενώ οι επιθέσεις από παρεμβολές μπορούν να ξεκινήσουν με την εισαγωγή διασταυρούμενης ομιλίας εντός και εκτός ζώνης και με την εκμετάλλευση των τρωτών σημείων των εξωγενών μηκών κύματος. Μερικοί άλλοι παράγοντες που ενδέχεται να υποβαθμίσουν ένα οπτικό κανάλι με την εμφάνιση επιθέσεων εισαγωγής σήματος περιλαμβάνουν τα δίκτυα ανάμεικτης γραμμής (MLR), τη διαμόρφωση πλάτους On-Off-Keying (OOK) και τη διαμόρφωση CrossPolarization (XpolM).

6) Ευπάθεια υλικού

Οι συσκευές IoT αναπτύσσονται εμπορικά με μεγαλύτερη έμφαση στη λειτουργικότητα της συσκευής και όχι στην ασφάλεια. Ως εκ τούτου, τα χαρακτηριστικά ασφαλείας προστίθενται συχνά κατά τρόπο ad-hoc. Επομένως, οι εμπορικές συσκευές IoT έχουν υπολείμματα τρωτότητας υλικού όπως ανοικτές φυσικές διεπαφές και ευπάθειες διαδικασιών εκκίνησης που μπορούν να αξιοποιηθούν εξ αποστάσεως. Ότι η αξιόπιστη και ασφαλής λειτουργία των συστημάτων διανυσματικών πληροφοριών εξαρτάται από την ακεραιότητα των υποκείμενων συσκευών, ιδίως από την ακεραιότητα του κώδικα και των δεδομένων τους από τις κακόβουλες τροποποιήσεις.

7) Dos Επιθέσεις

Λόγω περιορισμένων πόρων, όπως η χαμηλή μνήμη, η χαμηλή υπολογιστική ισχύς και η χαμηλή κατανάλωση ενέργειας, οι συσκευές IoT είναι ευάλωτες σε επιθέσεις εξάντλησης πόρων. Αυτές οι επιθέσεις περιλαμβάνουν παρεμβολές καναλιών επικοινωνίας, εκτεταμένη μη εξουσιοδοτημένη ή κακόβουλη χρήση σημαντικών πόρων IoT, όπως εύρος ζώνης, μνήμη, χρόνος CPU, χώρος στο δίσκο και αλλαγή της ρύθμισης κόμβου. Όλες αυτές οι επιθέσεις θα επηρεάσουν κατά πάσα πιθανότητα τη λειτουργική λειτουργία των Υπηρεσιών και τη διαθεσιμότητα των υπηρεσιών τους στον αντίστοιχο χρήστη.

Το IoT περιλαμβάνει συνήθως ενσωματωμένες συσκευές περιορισμών πόρων,

όπως RFID και κόμβους αισθητήρων. Αυτές οι συσκευές έχουν χαμηλή μνήμη, χαμηλή υπολογιστική ισχύ, μικρό χώρο στο δίσκο και απαιτούν χαμηλή κατανάλωση ενέργειας. Αν λοιπόν τα παραδοσιακά δίκτυα μπορούν να υποστηριχθούν από πολύπλοκα πρωτόκολλα ασφάλειας, τα συστήματα IoT απαιτούν ελαφρούς αλγόριθμους ασφάλειας που διατηρούν μια ισορροπία μεταξύ της ασφάλειας και της κατανάλωσης πόρων, όπως η διάρκεια ζωής της μπαταρίας. Οι συσκευές IoT συνήθως συνδέονται με συσκευές Internet ή πύλης μέσω βραδύτερων και λιγότερο ασφαλών μέσων ασύρματης επικοινωνίας, όπως 802.15.4, 802.11a / b / g / n / p, LoRa, ZigBee, NB-IoT και SigFox. Κατά συνέπεια, τα συστήματα IoT είναι επιρρεπή σε διαρροή δεδομένων και σε άλλα ζητήματα προστασίας της ιδιωτικής ζωής. Ενώ στο παραδοσιακό διαδίκτυο, οι συσκευές τελικής επικοινωνίας επικοινωνούν μέσω ασφαλέστερων και ταχύτερων ενσύρματων/ασύρματων τηλεπικοινωνιακών συσκευών, DSL / ADSL, WiFi, 4GandLTE. Μια άλλη διαφορά είναι ότι τα τρισδιάστατα δίκτυα έχουν σχεδόν το ίδιο λειτουργικό σύστημα και μορφή δεδομένων, αλλά στην περίπτωση του IoT λόγω της λειτουργικότητας της εφαρμογής και της έλλειψης OS, υπάρχουν διαφορετικά περιεχόμενα και μορφές δεδομένων. Έτσι, εξαιτίας αυτής της ποικιλομορφίας, είναι δύσκολο να αναπτυχθεί ένα πρότυπο πρωτόκολλο ασφαλείας που να καλύπτει όλους τους τύπους συσκευών και συστημάτων IoT.

Αναπόφευκτα, ένα ευρύ φάσμα απειλών του Διαδικτύου είναι ακόμα χαλαρό και απειλεί την ασφάλεια και το απόρρητο των χρηστών. Αν εξετάσουμε το σχεδιασμό ασφάλειας, τα παραδοσιακά δίκτυα εξασφαλίζονται από ένα συνδυασμό στατικής προστασίας της περιμέτρου του δικτύου που βασίζεται σε αναβαθμίσεις, το IDS / IPS και οι τελικές συσκευές είναι ασφαλισμένες από προσεγγίσεις βασισμένες στον κεντρικό υπολογιστή, όπως οι αντι-ιούς και τα μπαλώματα ασφαλείας / λογισμικού. Ενώ η προσέγγιση ασφαλείας που βασίζεται στον κεντρικό υπολογιστή δεν μπορεί να εφαρμοστεί στις συσκευές IoT με περιορισμένες πηγές. Ομοίως, ο παραδοσιακός αμυντικός μηχανισμός περιμέτρου δεν μπορεί να εξασφαλίσει συσκευές IoT, καθώς αυτές οι συσκευές αναπτύσσονται βαθιά στο δίκτυο.

8) DDos Επιθέσεις

Η ανάλυση των παρελθόντων κυβερνητικών συμβάντων συμπεραίνει ότι τα τρωτά σημεία των συσκευών IoT την καθιστούν ιδανική πλατφόρμα για την εκτόξευση DDoS. Έχει επίσης αποκαλυφθεί ότι το 96% των συσκευών που εμπλέκονται σε επιθέσεις DDoS ήταν συσκευές IoT, το 3 τοις εκατό ήταν δρομολογητές στο σπίτι και το 1 τοις εκατό διακομιστές Linux.

9) Συσκευές RFID και Bluetooth

Λόγω της έλλειψης φυσικής προστασίας και της ασύρματης επικοινωνίας RFID, τα δεδομένα ετικετών RFID είναι ευάλωτα σε επιθέσεις αξιοπιστίας και ακεραιότητας. Ορισμένα ακόμη ζητήματα ασφάλειας περιλαμβάνουν την έλλειψη ενιαίας κωδικοποίησης, την προστασία της ιδιωτικής ζωής και εμπιστοσύνη της ετικέτας RFID, του σταθμού βάσης και του αναγνώστη. Ομοίως, η χρήση παλαιών συσκευών Bluetooth μπορεί να προκαλέσει συνδεσιμότητα σε μη εξουσιοδοτημένες / κακόβουλες συσκευές, εκθέτοντας έτσι ιδιωτικά δεδομένα ή δεδομένα ασφάλειας.

10) Χρήστες

Οι χρήστες είναι ένας από τους πιο συνηθισμένους φορείς επίθεσης. Λόγω έλλειψης κατάρτισης και ευαισθητοποίησης σχετικά με την ασφάλεια, οι εργαζόμενοι είναι ευάλωτοι στην κυβερνο-αλίευση (phishing) και τις τυχαίες παραβιάσεις ασφαλείας. Ως εκ τούτου, ένα εν αγνοία κατέβασμα κακόβουλων κωδικών, εισερχόμενος σε μολυσμένους συνδέσμους μηνυμάτων π.χ. ηλεκτρονικού ταχυδρομείου, μπορεί να αποβεί μοιραίο. Επιπλέον, η ανταλλαγή ευαίσθητων δεδομένων μέσω δημόσιων δικτύων από κινητές συσκευές αποτελεί μια άλλη αιτία της πρόληψης της ασφάλειας. Δεν είναι, λοιπόν, τυχαία η εκτίμηση, ότι η αύξηση των χρηστών smartphone μεγιστοποιεί τον κίνδυνο διάτρησης δεδομένων προσωπικού χαρακτήρα.

5.3 Προκλήσεις IoT

Το όραμα της μελλοντικής Διασύνδεσης Διαδικτύου είναι μια ευρεία ενσωμάτωση διάφορων τεχνολογιών, δηλαδή αισθητήρων, προσωπικών συσκευών όπως smartphones, υπηρεσιών τοποθεσίας, εφαρμογών, εξυπηρετητών κλπ. Τα δεδομένα που προέρχονται από πολλές συσκευές θα είναι διαθέσιμα για ανοικτή κοινή χρήση σε μια σειρά εφαρμογών, διακομιστών και χρηστών. Αυτή η δημόσια κοινή χρήση επιτυγχάνεται επί του παρόντος με τις τεχνολογίες cloud. Κατά τη διάρκεια της περιόδου, το cloud εξελίχθηκε για να επεξεργαστεί, να αναλύσει και να αποθηκεύσει μεγάλα δεδομένα. Ωστόσο, όταν τα δεδομένα εγκαταλείψουν την υπο-ομάδα και εισέλθουν στο cloud για ευρεία / ανοιχτή κοινή χρήση, τότε προκύπτουν πολλά θέματα ασφάλειας και προστασίας προσωπικών δεδομένων. Εκτός από την εμπιστευτικότητα των δεδομένων, υπάρχουν και άλλα ζητήματα στον τομέα του cloud computing σχετικά με το μηχανισμό εμπιστοσύνης μεταξύ του παρόχου υπηρεσιών και του παρόχου υποδομής cloud σε διάφορα επίπεδα της αρχιτεκτονικής cloud.

Η ασφάλεια των δεδομένων

Το cloud παρέχει συνήθως ασφαλή επικοινωνία χρησιμοποιώντας το TLS / DTLS (Datagram Transport Layer Security). Το TLS παρέχει μυστικότητα επικοινωνίας (χρησιμοποιώντας συμμετρική κρυπτογράφηση κλειδιού), έλεγχο ταυτότητας διακομιστή (με τη χρήση δημόσιου κλειδιού και ελεγκτές τομέα) και ακεραιότητα μηνυμάτων με χρήση του MAC. Αν τα δεδομένα κρυπτογραφούνται πριν από την αποστολή τους στο cloud, τότε ακολουθούν επιπτώσεις όπως:

- Ο πάροχος Cloud δεν θα έχει πρόσβαση σε ευανάγνωστα δεδομένα.
- Τα δεδομένα δεν μπορούν να μοιραστούν δημόσια.
- Επηρεάζεται η επεκτασιμότητα και περιορίζεται η συνάθροιση δεδομένων και η ανάλυση που θα εκτελεστεί από τον πάροχο cloud.

- Ο πάροχος του Cloud περιορίζεται να παρέχει μόνο αποθήκευση / IaaS (Υποδομή ως υπηρεσία).

Χειρισμός ετερογενών δεδομένων

Οι εφαρμογές IoT ασχολούνται με μεγάλα ποσά που έχουν διανεμηθεί από υποσυστήματα που βασίζονται σε πολλές συσκευές όπως WSN, RFID, smartphones, GPS κλπ. Αυτά τα διαφοροποιημένα δεδομένα μπορεί να υπάρχουν σε διαφορετικές μορφές και συνεπώς, η ενσωμάτωση και συγχώνευση τέτοιων ετερογενών δεδομένων μπορεί να δημιουργήσει ζητήματα που σχετίζονται με την προστασία της ιδιωτικής ζωής.

Διαχείριση Ανωνυμοτήτων Χρήστη Vis-a-Vis ID

Σε ένα IoT που υποστηρίζεται από cloud, η εξισορρόπηση μεταξύ ανωνυμίας χρήστη και διαχείρισης ελέγχου ταυτότητας και εξουσιοδότησης είναι μια μεγάλη πρόκληση. Για παράδειγμα, στις εφαρμογές ηλεκτρονικών δεδομένων υγείας, αυτά παρέχονται σε διάφορους οργανισμούς για την ανάλυση δεδομένων και την ανάπτυξη μελλοντικών πολιτικών σε θέματα υγείας. Η σημασία μιας τέτοιας χρήσης των δεδομένων των ασθενών για τη βελτίωση της υγειονομικής περίθαλψης δεν μπορεί να αμφισβητηθεί. Ωστόσο, δημιουργεί πάντα ανησυχίες για την ασφάλεια και την προστασία της ιδιωτικής ζωής των ασθενών. Συμπερασματικά, διάφορες τεχνικές ανωνυμίας των χρηστών ασκούνται για να αποσυνδέσουν την ταυτότητα των ασθενών από τα δεδομένα υγείας. Ταυτόχρονα, για να διασφαλιστεί η ασφάλεια των υπηρεσιών υγείας που βασίζονται σε cloud, ο έλεγχος ταυτότητας χρήστη είναι εξίσου απαραίτητος για τον περιορισμό της πρόσβασης στο δίκτυο μόνο στους νόμιμους χρήστες.

Μεγάλης κλίμακας διαχείριση

Η IOT θα μπορούσε να έχει τεράστιο αριθμό ετερογενών διαγνωστικών

συσκευών, smartphones, smartcontrollers κλπ. Επομένως, η καταγραφή και ο έλεγχος του δικτύου καθίσταται δύσκολος. Τι πρέπει να καταγράψει ο πάροχος του cloud; Με αποκεντρωμένο έλεγχο θα υπάρχουν διακυμάνσεις και κατά συνέπεια διαφορετικές ερμηνείες των καταγεγραμμένων δεδομένων. Επιπλέον, η ανεπαρκής καταγραφή και παρακολούθηση, σε συνδυασμό με την έλλειψη ή την αναποτελεσματική αντίδραση με την εμφάνιση δυσοίωνων περιστατικών, μπορεί να οδηγήσει σε αθέμιτο έλεγχο και λογοδοσία, επιτρέποντας έτσι στους επιτιθέμενους να ξεκινήσουν περαιτέρω κακοβουλίες στα συστήματα. Βάση μελετών, ο χρόνος ανίχνευσης μιας παραβίασης καλύπτει πάνω από 200 ημέρες κκαι ανιχνεύεται από εξωτερικές παρά εσωτερικές διαδικασίες.

Ευπάθεια σε επιθέσεις DoS

Οι πάροχοι cloud συνήθως εφαρμόζουν τους απαιτούμενους ελέγχους για να προστατεύσουν από διάφορες επιθέσεις στον κυβερνοχώρο. Οι έλεγχοι αυτοί περιλαμβάνουν τον μετριασμό των τρωτών σημείων με την ενημέρωση του λειτουργικού συστήματος καιι την ασφαλή χρήση υπολογιστών με χρήση του TPM για την προστασία από επιθέσεις κακόβουλου λογισμικού / κώδικα κλπ.

Η απειλή των κακόβουλων πράξεων

Το cloud μπορεί να εντοπίσει ένα κακόβουλο πράγμα / κόμβο κατά τη διάρκεια της διαδικασίας επικύρωσης. Επίσης, μπορεί να προσφέρει ένα προστατευτικό μέτρο ασφάλειας ενεργοποιώντας ενημερώσεις λογισμικού όπου αυτό κρίνεται απαραίτητο και με αποτέλεσμα την αποστολή μηνυμάτων ελέγχου σε ό,τι πρέπει να ανακληθεί από το δίκτυο. Ωστόσο, υπάρχουν ορισμένες προκλήσεις που σχετίζονται με τον προσδιορισμό / ανίχνευση των κακόβουλων κόμβων σε ένα σύστημα:

1. Ποια μέθοδος χρησιμοποιείται για τον εντοπισμό ή την ανίχνευση ενός κακόβουλου κόμβου;
2. Πότε πρέπει να ξεκινήσει η διαδικασία βεβαίωσης κόμβου;

3. Εάν η βεβαίωση βασίζεται σε έλεγχο λογισμικού / κώδικα, τότε θα είναι ένα πρωτόκολλο πρόκλησης-απόκρισης ή ένα μονόδρομο σύστημα βεβαίωσης;
4. Είναι αποτελεσματικό το πρόγραμμα πιστοποίησης βάσει λογισμικού ή υπάρχει ανάγκη για πρωτόκολλο βεβαίωσης υλικού;

Κεφάλαιο 6ο

6.1 Επιχειρησιακή Επίδραση

Το IoT, επιδρώντας σε κάθε δράση της ανθρώπινης καθημερινότητας, επηρεάζει με αίσιο τρόπο και το μέλλον των επιχειρήσεων. Θα εξυπηρετήσει στη βελτιστοποίηση του κέρδους των επιχειρήσεων, την άντληση και αξιολόγηση στοιχείων από ένα ευρύ φάσμα τεχνολογικών ανακαλύψεων και την άνοδο της πελατειακής ζήτησης. Έπειτα, το IoT θα προκαλέσει ριζική αλλαγή στις ζωές των υπαλλήλων. Τα έξυπνα κινητά τηλέφωνα και οι συσκευές του IoT θα μεταλλάξουν ως προς τον αριθμό και την ποιότητα τις συσκευές που συνδέονται στα συστήματα της εταιρείας και συνεπώς θα δημιουργήσουν παραγωγικότερους υπαλλήλους. Επιπρόσθετα, με το IoT οι νέοι δείκτες ταχυτήτων στην επικοινωνία της πληροφορίας θα μεγιστοποιήσουν τη δημόσια ασφάλεια, τις μεταφορές και την υγειονομική περίθαλψη, με την καλύτερη πληροφόρηση και την ταχύτερη επικοινωνία των πληροφοριών. Συμπερασματικά, τουλάχιστον τρία σημαντικά οφέλη του IoT που θα επηρεάσουν όλες τις επιχειρήσεις περιλαμβάνουν την επικοινωνία, τον έλεγχο και την εξοικονόμηση του κόστους.

Επικοινωνία (Communication)

Το IoT μεταδίδει πληροφορίες σε ανθρώπους και συστήματα για την ορθή λειτουργία του εξοπλισμού και τα δεδομένα που προκύπτουν από το αισθητηριακό

σύστημα παρακολούθησης σημαίνουν την κατάλληλη χρονική στιγμή για την όποια αναγκαιότητα συντήρησης και επισκευής της μηχανής. Πριν το IoT, οι επιχειρήσεις λάμβαναν τα μηνύματα των δράσεών τους χειροκίνητα μέσω του ανθρώπινου δυναμικού. Πλέον, όμως, ένα σύστημα IoT-enabled HVAC ενημερώνει εγκαίρως αν π.χ. το φίλτρο αέρα είναι χρήζει αλλαγής ή λειτουργεί σωστά. Επίσης, Mobile εξοπλισμός της επιχείρησης με σύστημα GPS σημειώνει τα κατάλληλα στοιχεία τοποθεσίας εξοπλισμού και εργατικού δυναμικού αλλά και συστοιχίας αντικειμένων από άλλο τεχνικό εξοπλισμό. Στον τομέα της υγείας, το IoT μπορεί να βοηθήσει ένα νοσοκομείο να εντοπίζει τον εξοπλισμό του, από αναπηρικά αμαξίδια μέχρι καρδιακούς απινιδωτές. Στον κλάδο των μεταφορών, μια επιχείρηση με το IoT μπορεί να γνωρίζει τη θέση ενός οχήματος ή και το ποσοστό καυσίμου που του απομένει.

Ελέγχος και Αυτοματισμός (Control and Automation)

Στον κόσμο του IOT, μια επιχείρηση θα παρακολουθεί στην κατάσταση μιας συσκευής. Σε πολλές περιπτώσεις, μια επιχείρηση ή ένας καταναλωτής θα είναι επίσης σε θέση να ελέγχει απομακρυσμένα μια συσκευή, όπως π.χ. τον κλιματισμό μια αίθουσας ή την αναστολή λειτουργίας μιας σειράς υπολογιστών.

Εξοικονόμηση κόστους (Cost Savings)

Πολλές εταιρείες θα χρησιμοποιήσουν το IoT για την ελαχιστοποίηση κόστους και προκλήσεων ζημίας. Με τα νέα δεδομένα των αισθητήρων, το IoT μπορεί να βοηθήσει μια επιχείρηση να εξοικονομήσει χρήματα και να αποτιμήσει ελέγχους, όπως την ελαχιστοποίηση των εξόδων καυσίμων και της φθοράς ελαστικών. Ουσιαστικά, το IoT οφελεί μια επιχείρηση στην εξοικονόμηση χρημάτων, στον αυτοματισμό των πράξεων και την υγιή εικόνα της επιχείρησης. Για να υπάρχουν τα οφέλη που μπορεί να προσφέρει το IoT, μια επιχείρηση θα πρέπει να καλύπτει τουλάχιστον τα ακόλουθα τέσσερα στοιχεία:

***Αισθητήρες*:** Κατά τη διάρκεια των επόμενων τριών ετών, οι συσκευές θα διαθέτουν αισθητήρες. Αυτό θα σημάνει νέες πηγές δεδομένων για τους ανθρώπους και εξέλιξη στις υπάρχουσες επιχειρηματικές διαδικασίες. Έτσι, ο καθορισμός των πληροφοριών που θα προέρχονται από αυτούς τους αισθητήρες θα αποτελέσουν τον οδηγό για την πρόοδο της επιχείρησης.

***Δίκτυο IOT και πιστοποίηση ασφάλειας*:** Πολλές επιχειρήσεις, πλέον, για την ορθή λειτουργία τους θα επιβάλλεται να συνδεθούν με συσκευές IoT και σε πρότυπα δίκτυα IP. Αυτό θα βοηθήσει τις επιχειρήσεις να εξασφαλίσουν την αξιοπιστία και λειτουργικότητα υποστήριξης ενός παγκόσμιου IoT δικτύου και της αλληλεπίδρασής του με άλλα οικοσυστήματα. Βέβαια, ο άμεσος αυξητικός αριθμός των συνδεδεμένων αισθητήρων και εξοπλισμού επιφέρει κνδύνους για την ασφάλεια των επιχειρήσεων. Γι' αυτό, δικλείδες ασφαλείας, όπως κρυπτογράφηση, ασφάλεια κτιρίων και προστασία δεδομένων κατά την αποστολή τους ειναι υποχρεωτική.

***Περισσότερα δεδομένα*:** Επιχειρήσεις απροετοίμαστες στη διαχείριση του IoT θα αντεπεξέλθουν με δυσκολία στη σωρεία δεδομένων που θα φέρει στην επιφάνεια. Συνεπώς, οι επιχειρήσεις χρειάζονται να φτιάξουν ένα πλάνο υποστήριξης και διαχείρισης των δεχόμενων πληροφοριών. Μια εταιρεία, εν συνεχεία, είναι υποχρεωτικό να λαμβάνει όλα τα δεδομένα που έχει ανάγκη για τη λειτουργία της. Ακόμα, η συγκέντρωση πρόσθετων πληροφοριών θα επιτρέψουν στην επιχείρηση να δώσει λύσεις σε μελλοντικά ερωτήματα που θα ανακύψουν.

***Μέγεθος και κλίμακα των παρόχων IoT*:** Το IoT χαρακτηρίζεται από μια έντονη πολυπλοκότητα, αφού καλύπτει πολλαπλές κατηγορίες και πλείστους προμηθευτές σε κάθε μια από αυτές. Οι τέσσερις κύριες κατηγορίες του IOT είναι: Ο αισθητήρας (-ες) και η κεραία (-ες) που συχνά βρίσκεται στο μηχάνημα, η M2M συσκευή διαχείρισης, η πλατφόρμα διανομής και εφαρμογές που επιτρέπουν σε συσκευές IoT να προωθούν ή να ενεργούν για δεδομένα. Αναπόφευκτα, η σύσφιξη επιχειρηματικών συνεργασιών θα

αποτελέσει τροχοπέδη στην ομαλή διαχείριση του ποικιλοτρόπου χαρακτήρα εφαρμογής του IoT.

Κεφάλαιο 7ο

7.1 Αποτύπωση στιγμής και προβλέψεις

Η εμφάνιση του IoT αποτελεί μια σύγχρονη πρόκληση όσον αφορά το ρυθμό ανάπτυξης του, τα εφόδια που προσφέρει, αλλά και το ρίσκο της διασφάλισης της ιδιωτικής ζωής και της επεξεργασίας πολύπλοκων συστημάτων. Η σύνδεση των έξυπνων συσκευών στο διαδίκτυο πραγματοποιείται αργά αργά, αλλά θεωρείται εφικτή η επιρροή του IoT στην καθημερινότητά μας νωρίτερα απ' ότι υπολογίζαμε. Έρευνες που έχουν πραγματοποιηθεί δείχνουν αύξηση της εφαρμογής του IoT. Σύμφωνα με το Gartner, εώς το 2020 θα υπάρχουν σχεδόν 26 δισεκατομμύρια συσκευές στο IoT. Η Schneider Electric, ο παγκόσμιος ειδικός στη διαχείριση ενέργειας και τον αυτοματισμό, ανέδειξε στην έκθεση του Business Report τη χρήση του IoT ως ένα από τα βασικά επιχειρηματικά εργαλεία των μεγάλων εταιρειών μέχρι το 2020.

Από επιχειρηματικής σκοπιάς, το IoT θεωρείται πως θα μεταλλάξει σε θετικό βαθμό τον τρόπο με τον οποίο ο κόσμος συναναστρέφεται στην καθημερινή του ζωή με το Διαδίκτυο. Παρόλα αυτά, η πορεία προς την πλήρη αποδοχή και υιοθέτησή του προκαταβάλλεται από σκεπτικισμό, δεδομένου ότι υπάρχουν αρκετοί περιορισμοί:

Τεχνολογικοί περιορισμοί

Για να γίνει πραγματικότητα το IoT, θα πρέπει να επιλυθούν προβλήματα ακεραιότητας, ιδιωτικότητας και ασφάλειας για τα οποία έγινε εκτενής αναφορά παραπάνω. Η συμπλοκή μεγάλου αριθμού συσκευών στα σενάρια IoT δεν αποκλείουν την πιθανότητα κακόβουλης επεξεργασίας δεδομένων. Αυτό θα επηρεάσει τα συμπεράσματα που προκύπτουν από τις έξυπνες μηχανές και συνεπώς θα οδηγήσουν

σε λανθασμένες αποφάσεις π.χ. μιας εγκατάστασης, με κατάληξη την απώλεια εισοδήματος.

Ωστόσο, η επικοινωνία μεταξύ των συσκευών στο Διαδίκτυο δεν είναι αδιάφορη. Τα οφέλη από τα πλεονεκτήματα του Διαδικτύου θα μπορούν να καρπωθούν μόνο μέσα από την ορθόδοξη επικοινωνία μεταξύ των συσκευών στο Διαδίκτυο. Ήδη, υπάρχει μια μετατόπιση από IPV4 σε IPV6 για να λυθεί το ζήτημα της διευθυνσιοδότησης συσκευών σε IoT, αλλά ένα υποσύνολο συσκευών IoT θα περιλαμβάνει συσκευές με χαμηλή ενέργεια, μνήμη και επεξεργαστική ισχύ δύσκολη να υπόκεινται σε πρωτόκολλα δικτύου σε αυτές τις συσκευές. Για παράδειγμα, οι ετικέτες RFID χρησιμοποιούν αναγνωριστικά 64-96 bits με βάση τα πρότυπα EPC global για διευθυνσιοδότηση, σε αντίθεση με το αναγνωριστικό 128 bits που απαιτείται από ένα δίκτυο IPV6. Εν τέλει, αν οι συσκευές IoT πρόκειται να συμμετάσχουν στο υπάρχον Διαδίκτυο τότε θα πρέπει να υπάρχει ένας τρόπος για την επίλυση ονομάτων και διευθύνσεων IP μεταξύ των συσκευών που συμμετέχουν. Πολλές έρευνες γίνονται και νέες θα προκύψουν για την επικοινωνία μέσω δικτύου μεταξύ συσκευών διαδικτύου προκειμένου να επιτευχθεί οικονομική άνοδος.

Ανθρώπινος παράγοντας

Επιθυμεί ο κάθε εμπλεκόμενος την τεχνολογία που του προσφέρεται; Το IoT αποτελεί τον προπομπό ενός πρωτοποριακού βίου, όπου οι μηχανές ή οι συσκευές βοηθούν την ανθρώπινη δράση παρακολουθώντας την και δίνοντας λύσεις στα όσα επιδρούν πάνω της. Σε ποιο βαθμό θα ήταν πρόθυμος ο άνθρωπος να έχουν ενσωματωμένες συσκευές στον καθημερινή του βίο;

Ο καθοριστικός παράγοντας για την αποδοχή μιας τέτοιας τεχνολογίας είναι η εξασφάλιση της ιδιωτικότητας και της ασφάλειας. Στην περίπτωση π.χ. των κινητών τηλεφώνων, οι πληροφορίες δύνανται να παραμείνουν προσωπικές μέσα στο κινητό τηλέφωνο, ακόμη και αν το τηλέφωνο είναι ένας κόμβος στο "Internet of things". Ωστόσο, τεχνολογίες όπως η RFID, οι κάμερες CCTV είναι η άμεση αντίθεση, όταν αφορούν για την προστασία της ιδιωτικής ζωής και την ασφάλεια των δεδομένων. Συνεπώς, τα πλεονεκτήματα αυτών των τεχνολογιών, αν και περισσότερα των

μειονεκτημάτων, εξακολουθούν να προκαλούν το δισταγμό των χρηστών.

Το Διαδίκτυο των Πραγμάτων είναι μια επαναστατική ιδέα με πολλές θετικές επιπτώσεις στην κοινωνία και τα οφέλη της εξετάζοντας την οικονομική οπτική, είναι ορατά και ιδιαίτερα σημαντικά. Ήδη υπάρχουν τεχνολογίες που επιτρέπουν την επιτυχία της έννοιας του Διαδικτύου των πραγμάτων, αλλά μέχρι η ανθρώπινη αποδοχή να καθιερωθεί, τα οφέλη που θα αποφέρει θα μειώνονται ή θα απολαμβάνονται καθυστερημένα.

Πάντως, θα πρέπει να σημειωθεί πως το 48% των εταιρειών, ήδη χρησιμοποιεί την εν λόγω τεχνολογία για να υποστηρίξει επιχειρησιακές αναδιοργανώσεις μεγάλης κλίμακας, ενώ το 33% των επιχειρήσεων στηρίζει ολοσχερώς την λειτουργία της στο IoT. Οι επιχειρήσεις τοποθετούν το IoT στο κέντρο της στρατηγικής τους και αυτό πρακτικά αποδίδει. Το 63% των χρηστών δηλώνουν αύξηση της επένδυσης η οποία κατά μέσον όρο μετράται κατά 20% σε βασικούς δείκτες απόδοσης, όπως έσοδα και κόστος ως αποτέλεσμα της χρήσης του IoT. Με το πέρας του χρόνου, ακόμα μια έρευνα αριθμεί το 89% των εταιρειών που επένδυσαν στο IoT και που τελικά αύξησαν την επένδυσή τους κατά τον τελευταίο χρόνο.

Όπως γίνεται σαφές από όλα τα παραπάνω, το Internet of Things είναι η επόμενη επανάσταση μετά την εποχή του Internet, και παρακάτω παρουσιάζονται κάποια στατιστικά στοιχεία αλλά και προβλέψεις για την αναδιάρθρωση που επίκειται. Η μελέτη της ΣΕΠΕ είχε υπολογίσει πως οι IOT συσκευές θα ξεπερνούσαν σε αριθμό τα έξυπνα κινητά τηλέφωνα το 2018 και αυτό θα προκαλούσε θόρυβο στην παγκόσμια αγορά συσκευών. Αυτή η αλλαγή αναμένεται να φέρει σημαντικές αλλαγές στον κόσμο του Internet of Things (IoT), δεδομένου ότι οι συσκευές που σχετίζονται με το Διαδίκτυο των Πραγμάτων ενδέχεται να ξεπεράσουν σε αριθμό τα κινητά τηλέφωνα και ως εκ τούτου θα αποτελεί την πληθυσμιακά μεγαλύτερη κατηγορία συνδεδεμένων συσκευών. Το IoT βρίσκεται στο επίκεντρο μια πορείας ψηφιοποίησης της οικονομίας και της κοινωνίας, με το οικοσύστημα, που δημιουργεί γύρω του, να διογκώνεται συνεχώς. Σύμφωνα πρόσφατη αναφορά του Ericsson Mobility, που δόθηκε στη δημοσιότητα, ο αριθμός των IoT συσκευών θα αυξάνεται μεταξύ 2016 και 2021 με

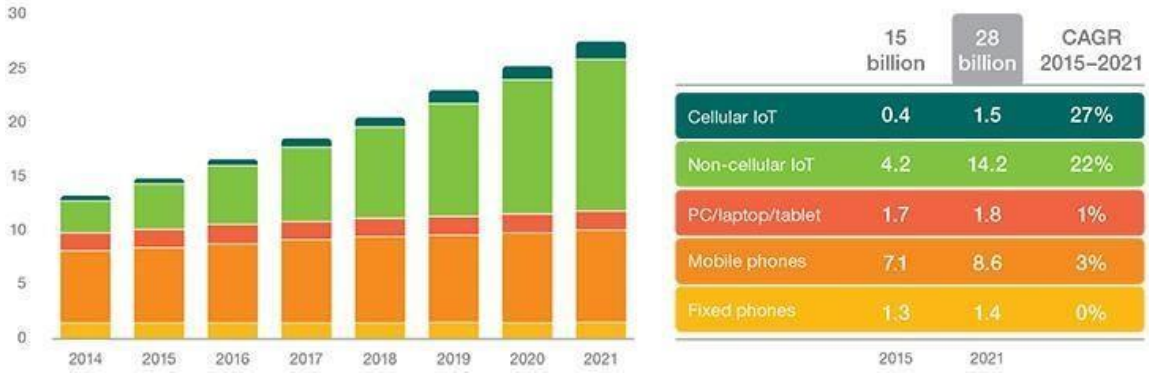
μέσο ετήσιο ρυθμό 23%. Με βάση αυτές τις εκτιμήσεις, η παγκόσμια αγορά θα μετρά, έως το 2021, 28 δις συνδεδεμένες συσκευές, εκ των οποίων τα 16 δις θα σχετίζονται με το IoT.

Σύμφωνα με έκθεση της ΣΕΠΕ, γίνεται πρόβλεψη πως κύριος τομέας ανάπτυξης του IoT θα είναι η Δυτική Ευρώπη. Εκτιμάται πως ο αριθμός συσκευών θα αυξηθεί 5 φορές σε αυτήν την περιοχή έως το 2021. Ωστόσο η ανάπτυξη αυτή δε θα επιτευχθεί μέσω της ζήτησης των απλών καταναλωτών. Προβλέπεται πως εξειδικευμένες ανάγκες-προϊόντα όπως «έξυπνοι μετρητές», εφαρμογές γύρω από το «έξυπνο σπίτι» και ούτω καθεξής, θα αποτελέσουν τη βάση για την αύξηση της ζήτησης για IoT συσκευές στη γηραιά ήπειρο.

Η αναμενόμενη πτώση του κόστους των συσκευών, θα είναι ένας ακόμα παράγοντας ο οποίος θα συμβάλει στην ανάπτυξη του IoT ευρωπαϊκά, αλλά και σε παγκόσμιο επίπεδο, καθώς και στην δημιουργία νέων πρωτότυπων εφαρμογών. Επιπρόσθετα η έλευση της τεχνολογίας 5G το 2020, θα παρέχει πολύ περισσότερες δυνατότητες, οι οποίες είναι άμεσα συ σχετιζόμενες με το IoT. Τούτο διότι θα δοθεί η δυνατότητα ένταξης περσότερων συσκευών στο διαδίκτυο αλλά και επικοινωνίας μεταξύ τους.

Σύμφωνα με την έρευνα της Ericsson Mobility, διαπιστώνεται πως το 2016 και πιο συγκεκριμένα το δεύτερο εξάμηνο, ο αριθμός των έξυπνων συσκευών ξεπέρασε αυτόν των απλών συμβατικών για πρώτη φορά. Το ίδιο έτος τα 4/5 (ήτοι 80 %) της αγοράς κινητών τηλεφώνων, αφορούσαν την κατηγορία smartphone. Όσον αφορά τους αριθμούς, η αγορά για την κατηγορία το 2016 ήταν 3,4 δις, ενώ αναμένεται να αγγίξει τα 6,3 δις το 2021. Επιπρόσθετα με την εφαρμογή της τεχνολογίας 5G, προβλέπεται και η ραγδαία αύξηση χρηστών. Εκτός από την Ericson, η κολοσσιαία Dell, δημιουργεί νέο επιχειρησιακό πρόγραμμα, το Dell Internet of Things Solutions Partner Program, με σκοπό να βοηθήσει τους ενδιαφερόμενους εταιρικούς πελάτες να αναγνωρίσουν τις ανάγκες τους, να επιλέξουν και να χτίσουν το κατάλληλο σύστημα IoT για αυτούς. Η συνεργασία της Dell γίνεται με περισσότερες από 25 εταιρείες στις οποίες περιλαμβάνονται οι GE, η Microsoft, η Software AG, η SAP, η OSIsoft. Πολλές

από αυτές τις εταιρείες χρησιμοποιούν τη σειρά Dell Edge Gateway 5000 στις δικές τους λύσεις IoT Ericsson.



Εικόνα 9: *Στατιστικά Συνδεδεμένων Συσκευών (Δισεκατομμύρια) www.Sepe.gr Οι συσκευές IoT θα ξεπεράσουν σε αριθμό τα κινητά τηλέφωνα το 2018* [**15**]

Εκτός από την Dell ένας πανευρωπαϊκός φορέας ο AIOTI (Alliance for Internet of Things Innovation) αποτελεί τον θεσμό της Ευρωπαϊκής Ένωσης, ο οποίος συντονίζει την έρευνα και τη χρηματοδότηση για την παρουσίαση καινοτόμων προτάσεων στον τομέα του Internet of Things στο πλαίσιο της πρωτοβουλίας Horizon 2020 της Ε.Ε.

Ιδιαίτερη βαρύτητα θα δοθεί στα οικοσυστήματα καινοτομίας, στα οποία οι εφαρμογές του Internet Of Things, θα διαδραματίσουν ενεργό ρόλο, ενώ ιδιαίτερης σημασίας είναι η διαδικασία ταυτοποίησης του πλαισίου, εντός του οποίου θα δύνανται να λειτουργούν οι διάφορες εφαρμογές του IoT. Τα ζητήματα που εγείρονται αναφορικά με την ιδιωτικότητα, ασφάλεια και αξιοπιστία μέσα από την εφαρμογή και χρήση του IoT, αποτελούν ένα μεμονωμένο «φλέγον ζήτημα», πάνω στο οποίο θα πραγματοποιηθούν έρευνες, με στόχο την υιοθέτηση ενός πλάνου, μίας στρατηγικής στις εν λόγω εφαρμογές. Επίσης το ζήτημα της βελτίωσης του τρόπου ζωής και των συνθηκών αυτής, της καλλιέργειας, της γεωργίας, των wearables, των πόλεων κ.ο.κ,

παράλληλα με τη χρήση του IoT, βρίσκονται ψηλά στου στόχους των φορέων της Ευρωπαϊκής Ένωσης για το Horizon 2020.

Βάσει στοιχείων της IDC, οι δαπάνες για το Internet Of Things εντός του έτους 2015, άγγιξαν το ποσό των 700 των δισεκατομμυρίων δολαρίων. Εκτιμάται πως οι δαπάνες αυτές εκτοξεύτηκαν στο 1,3 τρισεκατομμύρια δολάρια μέχρι το τέλος του 2019. Κύριοι «παίκτες» οι οποίοι κινούν τα «τεχνολογικά νήματα» για την εδραίωση του Internet of Things σε διάφορες πτυχές της καθημερινότητά μας, αποτελούν οι περιοχές της Ασίας και του Ειρηνικού. Οι τομείς που επηρεάζουν περισσότερο τις εξελίξεις του Internet of Things, είναι ο κατασκευαστικός καθώς και αυτός των μεταφορών. Είναι πιθανό, πως κατά το διάστημα της επόμενης πενταετίας η Λατινική Αμερική είναι μία γεωγραφική περιοχή στην οποία θα ανθίσει και θα αναπτυχθεί το Internet of Things. Τα πεδία στα οποία θα παρουσιάζεται ολοένα και μεγαλύτερη ανάπτυξη, αποτελούν η υγεία, οι ασφάλεια και οι καταναλωτικές συνήθειες. Την δεδομένη στιγμή οι περιοχές που προαναφέραμε, αξιοποιούν το 40 % των επενδύσεων στον τομέα του Internet of Things. Ακολουθούν η Βόρεια Αμερική και η Δυτική Ευρώπη. Δεν αναμένεται κάποια αλλαγή σε αυτήν την κατάσταση, ωστόσο εκτιμάται ότι ολοένα και περισσότερες περιοχές θα δίνουν έμφαση στο Internet of Things.

Ελληνικές ομάδες οι οποίες συμμετέχουν στο Horizon 2020 με θέμα το Internet Of Things, κατάφεραν και εξασφάλισαν χρηματοδότηση σε τέσσερα έργα έρευνας και ανάπτυξης. Το πόσο που άντλησαν είναι 3,36 εκατομμύρια ευρώ από τη συνολική κοινοτική συγχρηματοδότηση 51,5 εκατομμύρια ευρώ. Μάλιστα την υψηλότερη βαθμολογία σε συγκριτική αξιολόγηση, έλαβε το project SymbloTe, το οποίο έχει αναλάβει και συντονίζει η Intracom A.E. Τα αποτελέσματα αυτά παρουσιάστηκαν στην ενημερωτική ημερίδα με θέμα «Χρηματοδότηση και καινοτομία μέσω του Internet of Things (IoT) στην Ελλάδα» την οποία διοργάνωσε το Εθνικό Κέντρο Τεκμηρίωσης (ΕΚΤ) και η Ευρωπαϊκή Συμμαχία για το Διαδίκτυο των Πραγμάτων (Alliance for the Internet of Things Innovation) με την υποστήριξη της Ευρωπαϊκής Επιτροπής.

Τα υπόλοιπα που επελέγησαν είναι το AGILE Project με επικεφαλής τον Χάρη Δούκα της Create-net, το VICINITY Project με επικεφαλής τον Θανάση Τρυφερίδη,

ΕΚΕΤΑ, και το BIG IT, ECONAIS (Λέττα Καλαμαρά, 2016). Αντίθετα, στο εξωτερικό και συγκεκριμένα στην Ολλανδία η οποία είναι η πρώτη χώρα, η οποία επιτρέπει στο δίκτυο κινητής τηλεφωνίας της χώρας, επιτρέπει την μεταφορά δεδομένων των IOT αντικειμένων και αισθητήρων, όπως οι αισθητήρες στο λιμάνι του Άμστερνταμ και οι βαλίτσες επιβατών του διεθνή αεροδρομίου της πόλης. Το δίκτυο LoRa επιτρέπει στις συσκευές να συνδέονται στο Διαδίκτυο ακόμα και χωρίς Wi-Fi, χρησιμοποιώντας ένα σύστημα που λειτουργεί συμπληρωματικά στο δίκτυο κινητής τηλεφωνίας. Μια επιπλέον μικρή κεραία που προστίθεται στους σταθμούς βάσης των δικτύων κινητής επιτρέπει τη μετάδοση και λήψη ραδιοσημάτων χαμηλής ισχύος αλλά μεγάλης εμβέλειας. Το δίκτυο ενεργοποιήθηκε σε πιλοτική βάση το Νοέμβριο στη Χάγη και το Ρότερνταμ, επεκτάθηκε όμως γρήγορα σε όλη την Ολλανδία λόγω «σημαντικού ενδιαφέροντος», λέει η KPN. Η εταιρεία έχει εξασφαλίσει συμφωνίες για τη σύνδεση 1,5 εκατομμυρίων συσκευών, αριθμός που αναμένεται να αυξηθεί μετά τη διάθεση της υπηρεσίας σε όλη την Ολλανδία.

Δοκιμές πραγματοποιούνται στο αεροδρόμιο Σίπολ του Άμστερνταμ για την παρακολούθηση των αποσκευών, ενώ ο σιδηροδρομικός σταθμός της Ουτρέχτης πειραματίζεται με το IoT για την παρακολούθηση των μηχανισμών που επιτρέπουν στα τρένα να αλλάζουν ράγες. (Βαγγέλης Πρατικάκης, 2016).

Η έρευνα διεξήχθη από τη Samsung Electronics Europe σε περισσότερους από 10.000 Ευρωπαίους σε 18 χώρες, συμπεριλαμβανομένης της Ελλάδας, για να διερευνήσει πώς η σχέση με την τεχνολογία αλλάζει, καθώς αυτή εξελίσσεται, σύμφωνα με σχετική ανακοίνωση, η μελέτη «αποκαλύπτει πως, παρόλο που ο ρυθμός της καινοτομίας επιταχύνει, οι Ευρωπαίοι δίνουν αγώνα για να συμβαδίσουν με τη γλώσσα της τεχνολογίας, που αλλάζει διαρκώς. Η μελέτη αυτή δείχνει ότι, ενώ ο ενθουσιασμός σχετικά με την τεχνολογία αυξάνεται, η βιομηχανία αντιμετωπίζει τον αυξανόμενο κίνδυνο του να αφήσει πίσω τους καταναλωτές με μια συγκεχυμένη τεχνολογική ορολογία».

Τα νούμερα για τους Έλληνες αποτυπώνουν πως το 17% του πληθυσμού ότι δεν θα μπορούσαν να ζήσουν χωρίς τις ευκολίες της τεχνολογίας, και 58% ότι

χρησιμοποιεί περισσότερο την τεχνολογία συγκριτικά με 2 χρόνια πριν, ενώ ένα ποσοστό περίπου 80% προσποιείται ότι κατανοεί τους όρους Cloud Computing & IOT. Πανευρωπαϊκά "για να εξασφαλίσει ότι οι μελλοντικές γενιές θα είναι εξοικειωμένες με την τελευταία λέξη της τεχνολογίας, η Samsung συνεργάζεται με σχολεία και πανεπιστήμια, προκειμένου να διευκολύνει την προηγμένη εκμάθηση ψηφιακών δεξιοτήτων μέσα από δύο βασικά προγράμματα: τις Ψηφιακές Τάξεις και τα Ινστιτούτα Τεχνολογίας.

Βιβλιογραφία

- **[1] «Overview of the Internet of Things ITU, June 15, 2012»** http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=Y.2060
- **[2] «Internet Of Things (IoT) Τεχνολογίες και Εφαρμογές»** https://www.synergic.gr/web/synergic-software/-/internet-of-things-IoT-
- **[3] 7 Most Commonly Used Sensors for Developing Industrial IoT Solutions** https://www.embitel.com/blog/embedded-blog/7-most-commonly-used-sensors-for-developing-industrial-iot-solutions
- **[4] «RFC 7452, —Architectural Considerations in Smart Object Networking|| (March 2015)»** https://tools.ietf.org/html/rfc7452
- **[5] «Wikipedia-Διαδίκτυο πραγμάτων»** https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CF%84%CF%89%CE%BD_%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%AC%CF%84%CF%89%CE%BD
- **[6] «Internet of Things: Τι είναι με απλά λόγια το Διαδίκτυο των Πραγμάτων»** https://www.mobilenews.gr/internet-of-thingsti-einai-me-apla-logia-to-diadiktyo/
- **[7] «Internet of Things – From Research and Innovation to Market Deployment»** http://internet-of-thingsresearch.eu/pdf/IoTFrom%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf
- **[8] «Cross-Layer Design of Coded Multicast for Wireless Random Access Networks»** https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6740844
- **[9] «Internet of Things. Προκλήσεις & Στρατηγική Ασφάλειας»** https://www.itsecuritypro.gr/internet-things-proklisis-stratigiki-asfalias/
- **[10] 5G and IoT: Ushering in a new era** https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-iot-ushering-in-a-new-era
- **[11] «The Economic Impact of IoT»** https://www.frontier-economics.com/media/1167/201803_the-economic-impact-of-IoT_frontier.pdf
- **[12] Utilizing the IoT for Smart Agriculture** https://www.iotevolutionworld.com/iot/articles/443325-utilizing-iot-smart-agriculture.htm
- **[13] Smart Health-Care :- Let the little gadgets save your life** http://magicoakiotsolutions.com/2018/06/27/smart-health-care-let-the-little-gadgets-save-your-life/
- **[14] «Σύνδεσμος Επιχειρήσεων Πληροφορικής & Επικοινωνιών Ελλάδας: Οι συσκευές IoT θα ξεπεράσουν σε αριθμό τα κινητά τηλέφωνα το 2018»** http://www.sepe.gr/gr/research-studies/article/6338364/oi-suskeues-iot-tha-xeperasoun-se-arithmo-ta-kinita-tilefona-to-2018/
- **[15] Keysight Technologies The Menu at the IoT Café: A Guide to IoT Wireless Technologies** https://www.keysight.com/zz/en/assets/7018-05810/application-notes/5992-2412.pdf
- **[16] The top 5 5G wireless technologies** https://www.edn.com/the-top-5-5g-wireless-technologies/
- **[17] 5G: Τι είναι και ποια τα χαρακτηριστικά του** https://www.in.gr/2019/12/05/tech/5g-ti-einai-kai-poia-ta-xaraktiristika-tou/
- **[18] INTERNET OF THINGS (IoT)** http://drrajivdesaimd.com/2016/07/19/internet-of-things-iot/comment-page-7**/**
- **[19] «Smart Cities»: Οι ευφυείς πόλεις του μέλλοντος**

https://greenagenda.gr/smart-cities-%CE%BF%CE%B9-%CE%B5%CF%85%CF%86%CF%85%CE%B5%CE%AF%CF%82-%CF%80%CF%8C%CE%BB%CE%B5%CE%B9%CF%82-%CF%84%CE%BF%CF%85-%CE%BC%CE%AD%CE%BB%CE%BB%CE%BF%CE%BD%CF%84%CE%BF%CF%82vid/

- **[20] Aztech Introduces Kyla – Smart Home, Smart Life. (Press Release)** https://www.aztech.com/insights/kicking-off-the-new-year-with-ces2019-in-consumer-electronics-show-2-2-3/
- **[21] «Internet Of Threats»** https://public.dhe.ibm.com/common/ssi/ecm/62/en/62013962usen/internet_of_threats_benchmarkinsightsibv_62013962USEN.pdf
- **[22] PERVASIVE TECHNOLOGIES INTERNET OF THINGS (IOT) By Panopoulos D., Biliri E., Askounis D** https://www.google.com/url?sa=i&url=http%3A%2F%2Facademics.epu.ntua.gr%2FLinkClick.aspx%3Ffileticket%3DOTJUeR2p_Zo%253D%26tabid%3D385%26mid%3D2360%26forcedownload%3Dtrue&psig=AOvVaw0xtfPlF9zMA-1Gbh5Neo1m&ust=1581535492339000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKjO2PycyucCFQAAAAAdAAAAABAD
- **[23] «IMPACT OF THE INTERNET OF THINGS ON THE ECONOMY AND SOCIETY»** http://www.woiz.polsl.pl/znwoiz/z93/Szewczyk%20P_.pdf
- **[24] «Internet of Things: Impact on Economy»** Plowman L. Advertising on the internet of things; 2014. Available: http://wallblog.co.uk/2014/05/01/advertising-on-the-internet-of-things/
- **[25] Λέττα Καλαμαρά, (2016) 'Ελληνικά τα τέσσερα από τα επτά έργα IOT στην Ναυτεμπορική Αθήνα** https://m.naftemporiki.gr/story/1064355
- **[26] Βαγγέλης Πρατικάκης (2016) Η Ολλανδία λανσάρει το πρώτο εθνικό δίκτυο για το Internet of Things Αθήνα** https://www.in.gr/2016/07/01/tech/h-ollandia-lansarei-to-prwto-ethniko-diktyo-gia-to-internet-of-things/