ΠΑΝΕΠΙΣΤΉΜΙΟ ΠΑΤΡΏΝ

ΠΟΛΥΤΕΧΝΙΚΉ ΣΧΟΛΉ

ΤΜΉΜΑ ΜΗΧΑΝΙΚΏΝ ΗΛΕΚΤΡΟΝΙΚΏΝ ΥΠΟΛΟΓΙΣΤΏΝ

& ΠΛΗΡΟΦΟΡΙΚΉΣ

ΕΡΓΑΣΙΑ ΕΞΑΜΗΝΟΥ

ΓΙΑ ΤΟ ΜΑΘΗΜΑ

ΤΗΛΕΜΑΤΙΚΗ ΚΑΙ ΝΕΕΣ ΥΠΗΡΕΣΙΕΣ

Internet of Things: Τεχνολογίες, Πρωτόκολλα και Εφαρμογές

ΜΠΑΜΠΑΤΣΙΚΟΥ ΡΟΔΟΥΛΑ

Α.Μ 1051325

ΔΙΔΆΣΚΩΝ: ΧΡΉΣΤΟΣ ΜΠΟΥΡΑΣ

ΠΆΤΡΑ 2020

ΑΚΡΩΝΥΜΙΑ

- IoT: Internet of Things
- IBM: International Business Machines Corporation
- ARPANET: Advanced Research Projects Agency Network
- TCP/IP: Transmission Control Protocol/Internet Protocol
- RFID: Radio Frequency Identification
- GSM: Global System for Mobile Communications
- IEEE: Institute of Electrical and Electronics Engineers
- MIT: Massachusetts Institute of Technology
- EPM: Electronic Product Code
- IPSO: Independent Press Standards Organisation
- BLE: Bluetooth Low Energy
- IDC: International Data Corporation
- CES: Consumer Electronics Show
- IAB: Internet Architecture Board
- WPANs: Wireless Personal Area Networks
- CoAP: Constrained Application Protocol
- UDP: User Datagram Protocol
- DTLS: Datagram Transport Layer Security
- TLS: Transport Layer Security
- HTTP: HyperText Transfer Protocol
- IPv6: Internet Protocol version 6

- IPv4: Internet Protocol version 4
- QoS: Quality of Servise
- IOT G: Cisco Internet of Things Group
- BAN: Body Area Network
- PAN: Personal Area Network
- LAN: Local Area Network
- MAN: Metropolitan Area Network
- WAN: Wide Area Network
- GAN: Global Area Network
- UWB: Ultra Wideband Technology
- OFDM: Orthogonal Frequency-Division Multiplexing
- WPAN: Wireless Personal Area Network
- RF: RadioFrequency
- WSN: Wireless Sensor Network
- IBM: International Business Machines Corporation
- Li-Fi: Light-Fidelity
- VLC: Visible Light Communication
- BiDi: Bi-Directional
- XMPP: Extensible Messaging Presence Protocol
- AMP: Asynchronous Messaging Protocol
- RPC: Remote Procedure Call
- AMQP: Advanced Message Queuing Protocol
- JMS: Java Message Service
- SSL: Secure Sockets Layer
- RFID: Radio Frequency Identification
- DOS: Denial Of Service
- TLS: Transport Layer Security

- LPWAN: Low-Power Wide-Area Network
- NIST: National Institute of Standards and Technology
- AES: Advanced Encryption Standard

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 IoT και χρησιμότητά του στην καθημερινότητά μας

Το Internet of Things (IoT) είναι μία από τις κορυφαίες τεχνολογικές εξελίξεις της επόμενης δεκαετίας και θα επηρρεάσει πολλές πτυχές της κοινωνίας μας, μεταξύ αυτών τις επιχειρήσεις και την οικονομία. Το IoT ή διαδίκτυο των πραγμάτων είναι **ένα δίκτυο το οποίο αποτελείται από μηχανές που χρησιμοποιούνται στη βιομηχανία μέχρι φορητές συσκευές που χρησιμοποιούμε εμείς στην καθημερινότητά μας**. Η φιλοσοφία του IoT είναι: να συνδεθούν οι ηλεκτρονικές συσκευές ενός χρήστη μεταξύ τους (τοπικό δίκτυο) ή να τους δίνετε η δυνατότητα να συνδεθούν στο διαδίκτυο (παγκόσμιο ιστό). Οι συσκευές αυτές αφού συνδεθούν στο διαδίκτυο συλλέγουν και ανταλλάσσουν πληροφορίες. Ο όρος “Things” δεν είναι αυστηρά ορισμένος με την έννοια των “πραγμάτων”, αλλά αναφέρεται σε μία μεγάλη ποικίλια συσκευών, όπως π.χ. αυτοκίνητα με αισθητήρες, κάμερες, φώτα, συστήματα ασφάλεια κλπ (ότι δηλαδή διαθέτει ένα σύγχρονο αυτοκίνητο).

Η τεχνολογία καθημερινά επηρρεάζει ολοένα και περισσότερο την καθημερινότητά μας οπότε όλο και περισσότεροι άνθρωποι έχουν άμεση πρόσβαση σε συσκευές οι οποίες διαθέτουν σύστημα Wi-fi, Bluetooth και άλλα προηγμένα συστήματα. Αυτό σημαίνει ότι γίνεται εύπορο το έδαφος ώστε να διαδοθεί εύκολα και γρήγορα το IoT. Για παράδειγμα, ένα άτομο χρησιμοποιώντας το κινητό ή τον υπολογιστή του θα μπορεί να ελέγξει τις “έξυπνες” συσκευές του σπιτιού του (ψυγείο, κουζίνα, θερμοσίφωνας) από απόσταση, π.χ.από την εργασία του. [1]

Εικόνα 1: Αναπαράσταση των πραγμάτων που μπορούν να συνδεθούν μεταξύ τους [2]

Το IoT θα φέρει σημαντικές αλλαγές μεταξύ των οποίων είναι: ο τρόπος διοίκησης και λειτουργίας των επιχειρήσεων και οργανισμών, η επικοινωνία μηχανής με μηχανή (MTM), η επικοινωνία μιας μηχανής με μία ολόκληρη υποδομή συστημάτων, η επικοινωνία μιας μηχανής με το περιβάλλον καθώς και η επικοινωνία με οποιαδήποτε “έξυπνη” κινητή συσκευή μέσω αισθητήρων.

Σύμφωνα με την έκθεση της Intel “Rise of the Embedded Internet” “συσκευές σε δημόσιους και ιδιωτικούς χώρους θα αναγνωρίζουν τους κατοίκους μιας έξυπνης πόλης και θα προσαρμόζονται στις απαιτήσεις αυτών για την άνεση, την ασφάλεια, την ψυχαγωγία, το βελτιωμένο εμπόριο, την

εκπαίδευση, την εξοικονόμηση των πόρων, τη λειτουργική αποδοτικότητα και την προσωπική ευημερία”.

Κανείς δεν μπορεί να αμφισβητήσει το γεγονός ότι το Internet of Things αναπτύσσεται ταχύτατα και οι δυνατότητες που προσφέρει είναι τεράστιες, καθώς το δίκτυο για την επικοινωνία όλων αυτών των έξυπνων συσκευών και διαφόρων ηλεκτρονικών “πραγμάτων” δημιουργεί ένα παγκόσμιο νευρωνικό δίκτυο επικοινωνίας, το οποίο είναι βασισμένο στο Internet και το Cloud. Οι συσκευές αυτές καθώς και ο τρόπος επικοινωνίας τους μέσα από το cloud θα διεισδύσει σε κάθε πτυχή της ζωής μας λόγω της έξυπνης διαχείρισης και επεξεργασίας των πληροφοριών. Σαν αποτέλεσμα αυτού, μεγάλος όγκος πληροφοριών θα μεταφέρονται εντός του δικτύου και θα καταλήξουν σε συστήματα ή συσκευές στις οποίες μπορούμε να προγραμματίσουμε και να ελέγξουμε. Βασικός σκοπός είναι να συλλεχθούν αυτές οι πληροφορίες και να διευκολυνθεί ο τρόπος ζωής των ανθρώπων, να δημιουργηθούν νέες ευκαιρίες και υπηρεσίες προς όφελος του ανθρώπου και να μειωθεί όσο γίνεται η μόλυνση του περιβάλλοντος.

Όπως ήδη έχει αναφερθεί, οι δυνατότητες που προσφέρει το IoT είναι τεράστιες, με νέες ιδέες υλοποίησης και δυναμικά θα επηρρεάσει τις ζωές όλων μας. Για το λόγο αυτό, έχουν δημιουργηθεί οργανισμοί οι οποίοι θα βοηθήσουν στη μετάβαση αυτής της νέας εποχής του IoT όπως Alliance of IoT Innovations, Internet Security Releases Internet of Things και διάφοροι άλλοι οργανισμοί. Αποτελεί μία τεχνολογία η οποία έχει ως βασικό της σκοπό να αλλάξει το μέλλον, να φέρει σημαντικές αλλαγές στις αγορές, στον τομέα της υγείας και στη βιομηχανία. Όλα τα δεδομένα που θα συγκεντρώνονται μέσω της τεχνολογίας αυτής θα μπορούν να χρησιμοποιηθούν για να βελτιωθεί η ζωή των ανθρώπων, για να εντοπιστεί και να προβλεφθούν οι ανάγκες που αυτοί έχουν προτού καν εκδηλωθούν. [3]

Δεδομένων των παραπάνω, το Internet of Things θα διευκολύνει τους ανθρώπους στην καθημερινότητά τους, δεδομένου ότι αποτελεί νέα πηγή πληροφοριών, νέα επιχειρηματικά μοντέλα, νέες υπηρεσίες και νέα καινοτόμα προϊόντα σε πολλούς κλάδους. Ενδεικτικά, κάποιοι από τους κλάδους οι οποίοι θα επηρρεαστούν είναι:

- **Υγειονομική περίθαλψη και υπηρεσίες υγείας**

Εικόνα 2: Η ψηφιακή υγεία είναι το μέλλον για την υγειονομική περίθαλψη [4]

Πολλοί άνθρωποι παγκοσμίως ακόμη και σήμερα χρησιμοποιούν έξυπνες συσκευές για να παρακολουθούν από μόνοι τους την κατάσταση της υγείας τους χωρίς να χρειάζεται να μεταφερθούν σε κάποιο νοσοκομείο ή να επισκεφθούν κάποιο γιατρό. Εκτιμάται ότι στο άμεσο μέλλον στα νοσοκομεία η παρακολούθηση των ασθενών θα γίνεται μέσω monitor τα οποία θα είναι συνδεδεμένα σε ένα δίκτυο IoT. Με τον τρόπο αυτό, η υγειονομική περίθαλψη και οι υπηρεσίες υγείας θα είναι καλύτερες, άμεσες, θα εξοικονομηθεί χρόνος και το κόστος για τον ασθενή θα είναι σημαντικά μικρότερο. [5]

- **Μεταφορές**

Εικόνα 3: Παράδειγμα αυτοκινήτου το οποίο χρησιμοποιεί υπηρεσίες IoT [6]

Εταιρίες αυτοκινήτων όπως η Tesla και η BMW έχουν δημιουργήσει αυτοκίνητα τα οποία μπορούν να κινούνται αυτόματα ή με την επίβλεψη του ανθρώπου. Αξιοποιώντας την τεχνολογία αυτή, τα αυτοκίνητα έχοντας μια σύνδεση στο διαδίκτυο, συλλέγουν πληροφορίες για τη διαδρομή, την κίνηση στους δρόμους, τις κλιματολογικές συνθήκες και τη κατάσταση του οδοστρώματος. Συλλέγονται όλες οι παραπάνω πληροφορίες, επεξεργάζονται και αποφασίζεται ποια είναι η κατάλληλη ταχύτητα που καλό θα ήταν να μην ξεπεράσει ο οδηγός και τη βέλτιστη διαδρομή που πρέπει να ακολουθηθεί. [7]

- **Λιανικό εμπόριο**

Από τις λειτουργίες του IoT μπορούν να επωφεληθούν τόσο οι καταναλωτές όσο και τα καταστήματα. Οι επιχειρήσεις θα μπορούν να παρακολουθούν τα εμπορεύματά τους αυτόματα και θα ειδοποιούνται αμέσως για τα αποθέματά τους. Μέσω αισθητήρων και συστημάτων παρακολούθησης ο εργοδότης θα γνωρίζει ανά πάσα ώρα και στιγμή πόσοι καταναλωτές βρίσκονται στο κατάστημα αλλά και τι ενέργειες πραγματοποιούν στο κατάστημα. Θα του δίνετε δηλαδή η δυνατότητα να έχει τον πλήρη έλεγχο του καταστήματός του. Βασισμένη στο IoT έχει αναπτυχθεί τεχνολογία η οποία ανιχνεύει και ταυτόχρονα αναλύει τις ανθρώπινες εκφράσεις. Ανάλογα με τις εκφράσεις που έχουν οι καταναλωτές όταν βρίσκονται στο κατάστημα και κοιτάζουν τα προϊόντα του καταστήματος, καθώς και τι συηθίζουν να αγοράζουν, η επιχείρηση μπορεί να εξάγει πληροφορίες σχετικά με τις προτιμήσεις τους. Χρησιμοποιώντας αυτήν την τεχνολογία η διαφήμιση και η προώθηση των προϊόντων των επιχειρήσεων γίνεται πιο άμεσα και αποτελεσματικά. Από την μεριά των καταναλωτών, οι αγορές των

προϊόντων που επιθυμούν θα γίνουν γρηγορότερες αφού θα ενταχθούν νέοι τρόποι πληρωμής οι οποίοι θα κάνουν τις αγορές αυτοματοποιημένες. [8]

1.2 Ιστορική Αναδρομή

Η τεχνολογία δεν αναπτύχθηκε στα πρόθυμα της νέας γενιάς του IoT για να επιτρέψει την ασύγχρονη επικοινωνία μεταξύ των “έξυπνων” συσκευών αλλά είχε αρχίσει να υφίσταται σαν μία αόρατη σκέψη από το 1950.

1. Οι μηχανικοί της IBM είχαν την ανάγκη να ορίσουν ταυτότητες σε κάθε αντικείμενο και μηχάνημα που χρησιμοποιούσαν στην επιχείρηση. Η διαρκής ενασχόληση και οι πειραματισμοί με γραμμικά σχήματα, οδήγησαν στην ανακάλυψη των barcodes. Νέοι πειραματισμοί από μηχανικούς και επιστήμονες δημιούργησαν κινητές φορητές συσκευές τις οποίες μπορείς να φοράς στον καρπό σου (wearables). Η πρώτη συσκευή δημιουργήθηκε το 1955 από τον Edward O. Throrp ήταν ένα ρολόι το οποίο είχε τη δυνατότητα να προβλέψει τους κύκλους που έκαναν οι ρουλέτες στα καζίνα του Las Vegas. Τα αποτελέσματα αυτού ήταν υπερβολικά κερδοφόρα.

2. Το 1967 από τον Hubert Upton δημιουργήθηκε η πρώτη συσκευή σε σχήμα γυαλιών μυωπίας η οποία είχε ως σκοπό να βοηθήσει τα άτομα με ειδικές ανάγκες να διαβάσουν τα χείλη των ανθρώπων. Το 2011 η Google εμπνεύστηκε από την ιδέα του Hubert Upton και δημιούργησε το project “Google Glass” όπου περιλαμβάνει στοιχεία αυξημένης πραγματικότητας.

3. Το 1980 με τη δημιουργία του δικτύου ARPANET για την επικοινωνία και την ανταλλαγή δεδομένων ανάμεσα στις στρατιωτικές βάσεις των ΗΠΑ, στάλθηκε το πρώτο μήνυμα απομακρυσμένων υπολογιστών.

4. Το 1982 ήταν η εποχή του Internet και του πρωτοκόλλου TCP/IP, το οποίο πέρασε από τη διαδικασία να γίνει πρότυπο (Standart). Με το πρωτόκολλο TCP/IP ξεκίνησε μία νέα εποχή παγκοσμίου ιστού και δικτύων οι οποίοι συνδέονται μεταξύ τους, για να δημιουργηθεί το διαδίκτυο.

5. Η τεχνολογία RFID είναι η τεχνολογία η οποία μας επιτρέπει την ασύρματη αλλά παθητική ανάγνωση και εγγραφή δεδομένων σε συσκευές. Η τεχνολογία αυτή δημιουργήθηκε τον Ιανουάριο του 1973 από τον Mario Cardullo.

6. Δέκα χρόνια αργότερα, φοιτητές του Πανεπιστημίου Carnegie Mellon της Pennsylvania ανέπτυξαν την σκέψη να επικοινωνεί μία μηχανή με μία άλλη μηχανή.Εγκατέστησαν υπολογιστές για την παρακολούθηση της θερμοκρασίας από τερματικούς υπολογιστές στα μηχανήματα αυτόματων πολιτών που υπήρχαν στο Πανεπιστήμιο.

7. Το 1990 ο Mark Weiser, υπάλληλος της Xerox Parc δημοσίευσε ένα άρθρο όπου αφορούσε την εξέλιξη των υπολογιστών του 21ου αιώνα και εντός του άρθρου αυτού χρησιμοποίησε

όρους “καθολικών συστημάτων” και “ενσωματωμένα συστήματα επαυξημένης πραγματικότητας”.

8. Το 1995 η Siemens ανακοίνωσε το πρώτο chip το οποίο επιτρέπει σε συστήματα βιομηχανίας να επικοινωνούν μεταξύ τους με ασύσματο τρόπο και να εκτελούν εντολές. Επίσης, η IEEE ξεκίνησε το πρώτο διεθνές forum για φορητούς υπολογιστές.

9. Το 1999 το MIT δημιούργησε το πρώτο κέντρο ερευνών όπου περιελάμβανε σύγχρονα συστήματα και εκεί εξελίχθηκαν τα barcodes σε ένα νέο σύστημα το οποίο μπορούμε να αναγνωρίσει πληροφορίες πιο έξυπνα.Το σύστημα αυτό ονομάστηκε **EPM** (Electronic Product Code).

10. Το 2000 δημιουργήθηκε το πρώτο πρωτόκολλο επικοινωνίας “Machine to Machine”, για συσκευές οι οποίες είναι διασυνδεδεμένες στο διαδίκτυο.

11. Το 2005 μέλη από το πρόγραμμα Interaction Design Institude Ivrea κατασκευάστηκε τη πλατφόρμα του Arduino για μια φτηνή λύση μικροελεγκτή που προοριζόταν για τους φοιτητές.

12. Η ομάδα IPSO συντάχθηκε το 2008 με σκοπό να διαδόσουν το πρωτόκολλο IP σε οτιδήποτε αφορά “Internet of Things”.

13. Δύο χρόνια μετά, το Bluetooth αναβαθμίζεται και έρχεται στην αγορά ένα νέο stantard με ονομασία “Smart Bluetooth” (ή Bluetooth Low Energy – BLE), όπου επιτρέπει νέες δυνατότητες και εφαρμογές στους τομείς της υγείας, άθλησης και ψυχαγωγίας στο σπίτι να ενταχθούν στον κόσμο του IoT.

14. Το 2010 δημιουργήθηκε η υπηρεσία της Google “Street View” η οποία φωτογραφεί 360 μοιρών φωτογραφίες και αποτυπώνει γειτονιές και δρόμους σε ηλεκτρονική μορφή. Επίσης, είχε αποθηκευμένα πάρα πολλά δεδομένα από τα δίκτυα Wifi των ανθρώπων σε αυτές τις περιοχές. Οι εργαζόμενοι της Google συζητούσαν αυτήν την πληροφορία σαν μία νέα αρχή για την Google η οποία διχοτόμησε τις απόψεις των χρηστών του διαδικτύου αλλά και του φυσικού κόσμου. Την ίδια χρονιά, η κυβέρνηση της Κίνας ανακοίνωσε ότι το IoT θα αποτελεί προτεραιότητα στο σχέδιό τους.

15. Το 2011 η Gartner, η εταιρία της έρευνας της αγοράς που εφηύρε την “διαφημιστική εκστρατεία του κύκλου για τις αναδυόμενες τεχνολογίες” πρόσθεσε στη λίστα της το “Internet of Things”.

16. Το 2012 το θέμα της μεγαλύτερης ευρωπαϊκής διαδικτυακής διάσκεψης LeWeb ήταν το “Internet of Things”. Ταυτόχρονα, δημοφιλή περιοδικά που εστιάζουν στη τεχνολογία όπως το Forbes, το Fast Company και το Wired άρχισαν να χρησιμοποιούν στο λεξιλόγιό τους το IoT για να περιγράψουν το νέο αυτό φαινόμενο.

17. Το 2013 η IDC δημοσίευσε μία έκθεση που αναφέρει ότι το IoT θα στοιχίζει πολλά δισεκατομμύρια στην αγορά το 2020 και ο όρος IoT έφτασε στη μαζική συνειδητοποίηση της αγοράς, όταν η Google ανακοίνωσε την αγορά της Nest για $3,2 δις, μια εταιρία που κατασκεύαζε συσκευές για το IoT καθώς την ίδια στιγμή το Consumer Electronics Show (CES) στο Λας Βέγκας πραγματοποιήθηκε υπό το θέμα του IoT.

18. Το 2014 η Apple ανακοίνωσε το “HealthKit & HomeKit”, δυο πλατφόρμες ανάπτυξης υλοποιήσεων και την υποστήριξη της πλατφόρμας από τις νέες συσκευές, με σκοπό η ιδέα του έξυπνου σπιτιού και τρόπου ζωής να έρθει πιο κοντά στο σήμερα. Επίσης, η τεχνολογία iBeacon έφερε νέα πρότυπα στην αγορά των καταστημάτων και της πώλησης.

Από την ιστορική αυτή αναδρομή αξίζουν να αναφερθούν τα σημεία κλειδιά για την ανάπτυξη του Internet of Things τα οποία είναι: η τεχνολογία του **RFID** και συναφείς τεχνολογίες διευθυνσιοδότησης (που αναπτύχθηκαν πρώτα στο κέντρο Auto ID Lab) καθώς και οι δυνατότητες του **IPv6** οι οποίες θα επιτρέψουν σε κάθε υπολογιστή να έχει την δικιά του ξεχωριστή IP διεύθυνση, και να «εισέλθουν» στο κόσμο του IOT. [9]

1.3 Χαρακτηριστικά και απαιτήσεις του IoT

Τα βασικά χαρακτηριστικά τα οποία θα μπορούσαμε να πούμε ότι έχει το IoT και οι αντίστοιχες απαιτήσεις αυτού είναι:

- **Heterogeneit (Ανομοιογένεια):** Το IoT χαρακτηρίζεται από μεγάλη ανομοιογένεια επειδή επιτρέπει σύνδεση μεταξύ πολλών διαφορετικών συσκευών. Η διαχείριση και η υποστήριξη αυτών αποτελεί ένα από τα **βασικότερα χαρακτηριστικά** του IoT.

- **Scalability (Επεκτασιμότητα):** Πάρα πολλές συσκευές επικοινωνούν μεταξύ τους. Για να μπορέσει να λειτουργήσει σωστά το IoT οι μεγάλοι όγκοι των ανταλλασσόμενων δεδομένων, των πόρων και των λειτουργιών πρέπει να διαχειριστούν αποτελεσματικά.

- **Cost minimization (Ελαχιστοποίηση κόστους):** Οι σχεδιαστές μιας αρχιτεκτονικής IoT έχουν ως βασικό τους σκοπό να ελαχιστοποιήσουν το κόστος ανάπτυξης/συντήρησης, καθώς και την κατανάλωση ενέργειας.

- **Flexibility (Ευελιξία):** Η κατάσταση των συσκευών μεταβάλλεται συνέχεια (π.χ. συνδεδεμένο/αποσυνδεδεμένο) όποτε απαιτείται δυναμική διαχείριση και επαναπρογραμματισμός των συσκευών.

- **Quality of Service (QoS - Ποιότητα υπηρεσιών):** Όπως σε κάθε τεχνολογία και υπηρεσία, έτσι και στο IoT η εγγύηση υψηλής ποιότητας παρεχόμενων υπηρεσιών και εφαρμογών έχει μεγάλη σημασία, ιδιαίτερα όταν οι εφαρμογές αυτές χρησιμοποιούν real-time δεδομένα.

- **Secure environment (Ασφάλεια):** Η ασφάλεια στο IoT παίζει καθοριστικό ρόλο όπως και κάθε άλλη υπηρεσία η οποία χρησιμοποιεί δεδομένα χρηστών και απαιτεί σύνδεση στο

διαδίκτυο. Πρέπει δηλαδή να παρέχει ασφάλεια στις επικοινωνίες με ταυτοποίηση των συσκευών αλλά και των χρηστών, διατηρώντας την ακεραιότητα των δεδομένων και των συσκευών, έχοντας τα προσωπικά δεδομένα άκρως εμπιστευτικά. [10]

1.4 Συνδεσιμότητα

Το IoT βασίζεται στη διασύνδεση μικρών συσκευών ή συστημάτων που χρησιμοποιεί ένας χρήστης κατά μέσο όρο στην καθημερινή του ζωή. Όμως εκτός από την διασύνδεση αυτή, διαθέτει και τον κάταλληλο *εξοπλισμό* όπου θα έχει την δυνατότητα να διασυνδέσει τόσο τις συσκευές αυτές μεταξύ τους όσο και με τον κατασκευαστή των συστημάτων αυτών, με στόχο να προσφέρουν περισσότερες υπηρεσίες. Αυτό σημαίνει ότι μέσω του IoT τα συστήματα χρησιμοποιούν το διαδίκτυο για τη διασύνδεσή τους, είναι ανεξάρτητα μεταξύ τους και είναι διάστασης μικροτσίπ. Τα συστήματα αυτά είναι είτε smart συσκευές,είτε real time συστήματα, είτε συστήματα συγκέντρωσης πληροφοριών σε μεγάλες βάσεις δεδομένων.

Τα τρία κύρια μέρη ενός IoT είναι:

1. τα «πράγματα», όπου συλλέγουν πληροφορίες οπουδήποτε και οποιαδήποτε στιγμή χρησιμοποιώντας RFID τεχνολογία, αισθητήρες και κώδικα ,
2. τα δίκτυα επικοινωνιών που συνδέουν τα «πράγματα»,
3. τα υπολογιστικά συστήματα και οι εφαρμογές που επεξεργάζονται όσα δεδομένα ρέουν από και προς τα «πράγματα» όπως το cloud computing.

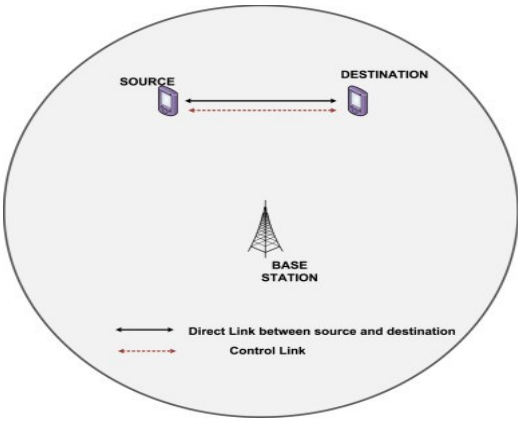
Η συνδεσιμότητα των τριών αυτών μερών του IoT πραγματοποιείται με τέσσερις τρόπους δικτύωσης (σύνδεσης και επικοινωνίας) όπως περιγράφονται σε έγγραφο του Internet Architecture Board - IAB (RFC 7452, Μάρτιος 2015 - https://tools.ietf.org/html/rfc7452) και παρουσιάζονται παρακάτω.

1.4.1 Σύνδεση συσκευή-προς-συσκευή (device-to-device communication)

Το μοντέλο αυτό επικοινωνίας συσκευή προς συσκευή αντιπροσωπεύεται από δύο ή περισσότερες συσκευές που συνδέονται άμεσα και επικοινωνούν μεταξύ τους χωρίς ενδιάμεσο server. Αυτές οι συσκευές συνδέονται με πολλούς τύπους δικτύων, συμπεριλαμβανομένων των δικτύων IP ή το Internet, χρησιμοποιώντας πρωτόκολλα όπως το Bluetooth, Z-Wave, ή ZigBee.

Το Bluetooth πρόκειται για μια ασύρματη τηλεπικοινωνιακή τεχνολογία μικρών αποστάσεων, ένα πρότυπο για ασύρματα προσωπικά δίκτυα υπολογιστών (Wireless Personal Area Networks, WPAN). Το Z-Wave είναι ένα πρωτόκολλο ασύρματων επικοινωνιών για εφαρμογές οικιακού αυτοματισμού. Χρησιμοποιεί χαμηλής ισχύος ραδιοκύματα. Ένα ακόμα πιο εξελιγμένο μέσο δικτύωσης από το Bluetooth είναι το *ZigBee*. Πρόκειται για ένα τυποποιημένο πρωτόκολλο χαμηλής κατανάλωσης ισχύος σε Wireless Personal Area Networks (WPANs).Η device-to-device επικοινωνία

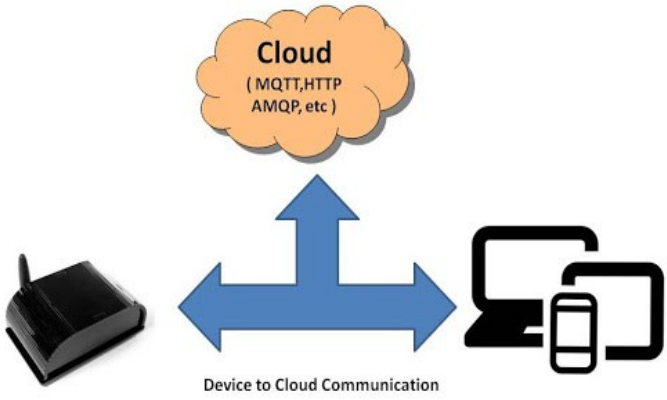
χρησιμοποιείται σε εφαρμογές όπως συστήματα οικιακού αυτοματισμού, που συνήθως χρησιμοποιούν μικρά πακέτα δεδομένων για επικοινωνία μεταξύ των συσκευών και με απαίτηση σχετικά χαμηλού ρυθμού μετάδοσης δεδομένων. [11]



Εικόνα 4: Σύνδεση συσκευή-προς-συσκευή (device-to-device communication) [14]

1.4.2 Σύνδεση συσκευής-προς-cloud (device-to-cloud communication)

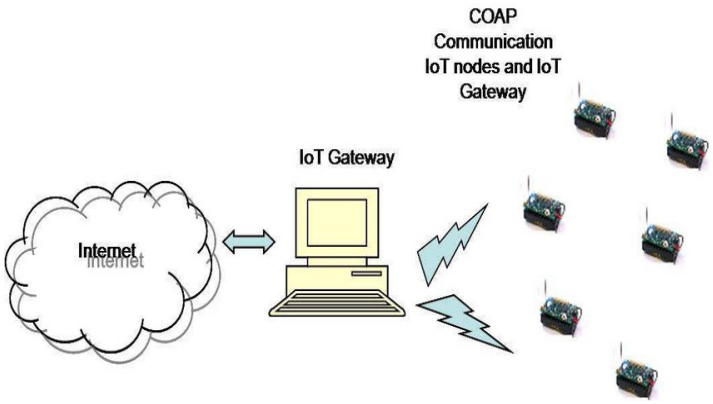
Η διασύνδεση στο IoT γίνεται εφαρμόζοντας τεχνολογίες, όπως το RFID και ασύρματους αισθητήρες, οι οποίες συλλέγουν τα δεδομένα που στη συνέχεια αξιοποιούνται από τα υπολογιστικά συστήματα. Αυτό έχει ως αποτέλεσμα την δημιουργία τεράστιων ποσοτήτων δεδομένων που θα πρέπει να αποθηκευτούν, να επεξεργαστούν και να παρουσιαστούν. Το cloud computing προσφέρει την υποδομή για τη συλλογή, ανάλυση, αποθήκευση και αποστολή πληροφοριών στον πελάτη. Έτσι επιτυγχάνεται η παροχή υπηρεσιών προς τους χρήστες που επιθυμούν την πρόσβαση σε εφαρμογές σε οποιοδήποτε χρόνο και μέρος. Η συσκευή IoT συνδέεται άμεσα με μια υπηρεσία cloud διαδικτύου, όπως ένας πάροχος υπηρεσίας εφαρμογής για την ανταλλαγή δεδομένων και τον έλεγχο ροής των πληροφοριών. [12]



Εικόνα 5: Σύνδεση συσκευής-προς-cloud (device-to-cloud-communication) [15]

1.4.3 Σύνδεση συσκευής με δίαυλο επικοινωνίας (device-to-gateway communication)

Σε αυτή την σύνδεση η συσκευή και ο πάροχος έρχονται σε επικοινωνία μέσω ενός διαύλου (gateway). Μια gateway συσκευή μπορεί να απορρίπτει, να αθροίζει και να ελέγχει τη μορφή των δεδομένων από μια ομάδα απλών αισθητήρων πριν τα στείλει κάπου αλλού. Για τη σύνδεση «πράγματος»/συσκευής με το gateway ακολουθούνται οι τρόποι που περιγράφηκαν παραπάνω. Η συνδεσιμότητα gateway-cloud πραγματοποιείται με τα πρωτόκολλα IPv4/IPv6. Προτιμάται το IPv6 γιατί έχει καλύτερη δυνατότητα αυτορρύθμισης συσκευών, καλύτερη ποιότητα υπηρεσιών (QoS) και μεγαλύτερη ασφάλεια από το Ipv4. [13]

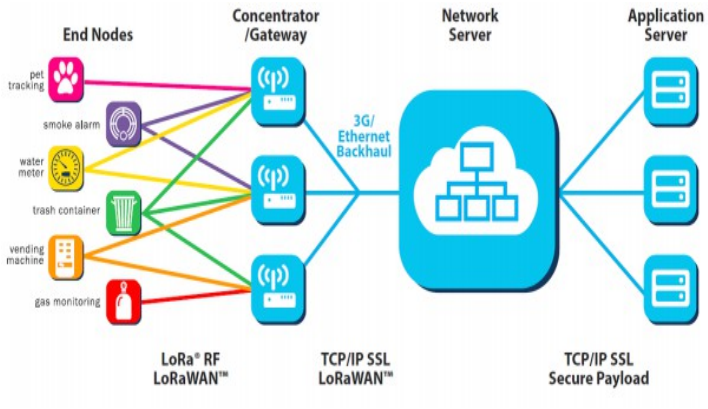


Εικόνα 6: Σύνδεση συσκευής με δίαυλο επικοινωνίας (device-to-gateway communication) [16]

Ένα παράδειγμα αυτού του τρόπου σύνδεσης είναι η LoRaWAN. Το LoRaWAN είναι ένα πρωτόκολλο ελέγχου πρόσβασης πολυμέσων (MAC) και αφορά δίκτυα ευρείας περιοχής. Έχει σχεδιαστεί για να επιτρέπει σε συσκευές χαμηλής ισχύος να επικοινωνούν με εφαρμογές συνδεδεμένες στο Internet μέσω ασύρματων συνδέσεων μεγάλης εμβέλειας. Το LoRaWAN μπορεί να αντιστοιχιστεί στο δεύτερο και στο τρίτο επίπεδο του μοντέλου OSI. Εφαρμόζεται πάνω από τη διαμόρφωση LoRa ή FSK σε βιομηχανικές, επιστημονικές και ιατρικές (ISM) ραδιοφωνικές ζώνες. Η τοπολογία της περιγράφεται ως εξής:

- **Node – end device** (κόμβος – τελική συσκευή): όπου πρόκειται για ένα αντικείμενο με μια ενσωματωμένη συσκευή επικοινωνίας χαμηλής ισχύος.
- **Gateway** (Πύλη): όπου είναι κεραίες οι οποίες λαμβάνουν εκπομπές από συσκευές λήξης και αποστέλλουν δεδομένα πίσω στις συσκευές λήξης.
- **Διακομιστής δικτύου** (Network Server): όπου είναι διακομιστές που δρομολογούν μηνύματα από τους κόμβους – τις τελικές συσκευές στη σωστή εφαρμογή και στη συνέχεια κάνουν την αντίθετη διαδικασία.
- **Εφαρμογή** (Application): οι εφαρμογές είναι ένα κομμάτι λογισμικού όπου εκτελούνται σε ένα διακομιστή. [21]

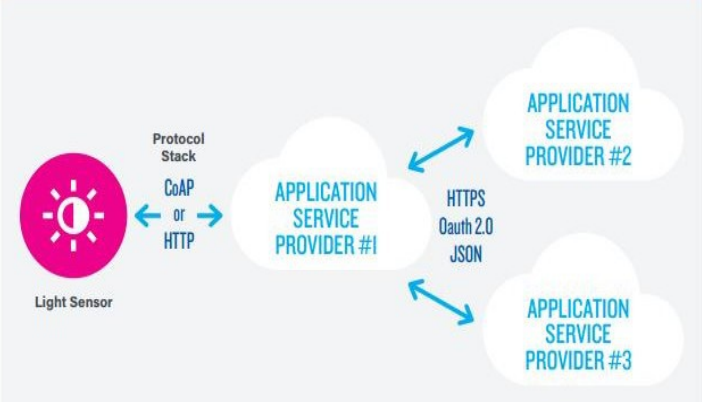
Ακολουθεί μία σχηματική αναπαράσταση της παραπάνω τοπολογίας:



Εικόνα 7: Σχηματική αναπαράσταση της LoRaWAN τοπολογίας [17]

1.4.4 Back – End Μοντέλο Ανταλλαγής Δεδομένων (Back-end Data - Sharing Model)

Το back-end μοντέλο ανταλλαγής δεδομένων αναφέρεται σε μια αρχιτεκτονική επικοινωνίας που επιτρέπει στους χρήστες να εξάγουν και να αναλύουν τα δεδομένα των «πραγμάτων» από μια υπηρεσία cloud, σε συνδυασμό με δεδομένα από άλλες πηγές.Για παράδειγμα, ένας εταιρικός χρήστης υπεύθυνος για ένα συγκρότημα γραφείων θα πρέπει να συλλέγει και να αναλύει τα δεδομένα κατανάλωσης ενέργειας και κοινής ωφέλειας που παράγονται από όλους τους αισθητήρες IoT και Internet-enabled συστήματα κοινής ωφελείας στις εγκαταστάσεις. Η back-end ανταλλαγή δεδομένων επιτρέπει στην εταιρεία να έχει εύκολη πρόσβαση και ανάλυση όλων των δεδομένων στο cloud που παράγεται από όλες τις συσκευές στο κτίριο. [19]



Εικόνα 8:Back-end Μοντέλο Ανταλλαγής Δεδομένων (Back-end Data-Sharing Model) [18]

1.5 “Εξυπνες” συσκευές

Η κύρια δυνατότητα μιας έξυπνης συσκευής είναι η **επεξεργασία δεδομένων** (η οποία επιτυγχάνεται από έναν μικροεπεξεργαστή και ποικίλες θύρες επικοινωνίας) για τον προγραμματισμό της. Η έννοια του «έξυπνου» προκύπτει από την δυνατότητα της συσκευής να επικοινωνεί ενσύρματα ή ασύρματα με τον χρήστη της συσκευής αυτής. Οι διάφοροι τρόποι ασύρματης επικοινωνίας και διαχείρισης της συσκευής αλλά και ο προγραμματισμός της για την αυτοματοποιημένη λειτουργία, είναι και ο κύριος λόγος χρήσης μιας έξυπνης συσκευής.

Η δυνατότητα των έξυπνων μηχανήματων είναι αντιστρόφως ανάλογη με την έννοια των επεξεργαστικά δυνατών. Δεν είναι σωστό να θεωρούμε ένα μηχάνημα “έξυπνο” αν προσφέρει (κατασκευαστικά) μεγάλες δυνατότητες σε ταχύτητα και επεξεργάζεται γρήγορα πληροφορίες. Για παράδειγμα, μια λευκή συσκευή δεν είναι αναγκασμένη να κάνει η ίδια υπολογισμούς, αλλά να είναι έξυπνη αρκετά ώστε να στείλει τα δεδομένα, μαζί με τις εργοστασιακές ρυθμίσεις και εξατομικευμένες επιλογές του χρήστη στο cloud προκειμένου να γίνει η επεξεργασία και να βγάλει αποτέλεσμα, χωρίς την παρέμβαση του χρήστη. Η εξέλιξη των δικτύων,του cloud networking καθώς το internet, θα πρέπει να εξελιχθούν σε πιο ασφαλή και γρήγορα, ενώ θα πρέπει να μειωθεί το κόστος και η κατανάλωση ενέργειας.

Η Ιδέα του Internet of things, περιλαμβάνει: το σπίτι που ζει ο άνθρωπος, την πόλη στην οποία ζει, το αμάξι (ή τα αμάξια) που έχει, ακόμα και δρόμους, με συσκευές να παρακολουθούν και να συλλέγουν δεδομένα και συμπεριφορές με σκοπό αυτές οι πληροφορίες να ενεργοποιούν ενέργειες και υπηρεσίες.Στην μέση αγορά, ο κάθε άνθρωπος έχει μια συσκευή smartphone στην κατοχή του, ενώ με το Internet of Things, ο αριθμός των έξυπνων συσκευών που θα περιλαμβάνει κάθε άνθρωπος θα αυξηθεί εκθετικά και δεν θα περιλαμβάνει μόνο μια συσκευή smartphone αλλά ότι συσκευή χρησιμοποιεί θα μετατραπεί σε έξυπνη. Έτσι η αγορά στον δυτικό κόσμο θα διχοτομηθεί και θα ξεπεράσει την αγορά των έξυπνων κινητών τηλεφώνων. Έως εκ τούτου, από την τεχνολογική σκοπιά

το Internet of Things, καθορίζεται από την δυνατότητα οι συσκευές να αλληλοεπιδρούν μεταξύ τους, με ολοκληρωμένα συστήματα και υποδομές και με αυτοματοποιημένο τρόπο να εκτελούν διάφορες ενέργειες. Αυτές οι συσκευές αποτελούν την ιδέα του έξυπνου. [20]

ΚΕΦΑΛΑΙΟ 2: ΤΕΧΝΟΛΟΓΙΕΣ ΚΑΙ ΠΡΩΤΟΚΟΛΛΑ

2.1 Ασύρματες Τεχνολογίες

Σε αυτήν την ενότητα θα παρουσιαστούν οι τεχνολογίες δικτύου και τα πρωτόκολλα που μπορούν να βοηθήσουν στην ανάπτυξη του IoT. Εφόσον η κάθε συσκευή ενδέχεται να χρειαστεί να επικοινωνήσει με άλλες σε οποιαδήποτε απόσταση και με διαφορετικό μέσο επικοινωνίας, υπάρχουν συγκεκριμένες κατάλληλες τεχνολογίες αναλόγως των αποστάσεων:

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

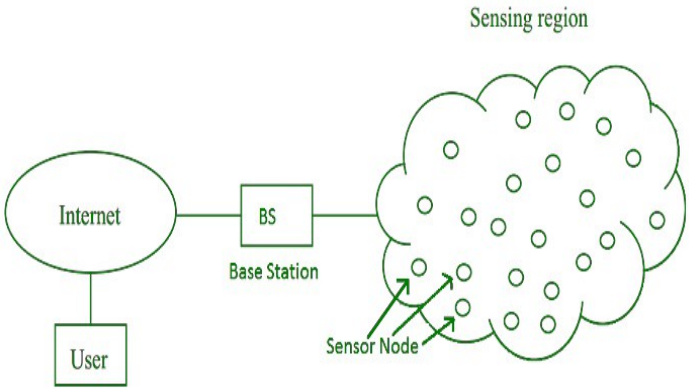
Οι ασύρματες τεχνολογίες (με τα πρωτόκολλα) για το IoT που θα αναπτυχθούν στην παρούσα εργασία είναι οι ακόλουθες: **ZigBee** (IEE 802.15.4), **WiMax** (IEE 802.16), **UWB** (IEE 802.15.3a), **Flash OFDM** κυψελωτά συστήματα (IEE 802.20).

- Το **ZigBee** είναι μια ασύρματη τεχνολογία που αναπτύχθηκε για να καλύψει τις ανάγκες για χαμηλό κόστος, χαμηλή ισχύς των ασύρματων δικτύων αισθητήρων. Συγκεκριμένα, το ZigBee που χρησιμοποιούν οι μικροί, χαμηλής ισχύος ψηφιακοί δέκτες για την επικοινωνία τους βασίζεται στο 802.15.4 πρότυπο της IEEE για τα ασύρματα προσωπικά τοπικά δίκτυα (WPAN), όπως για παράδειγμα τα ασύρματα ακουστικά που συνδέονται με τα κινητά τηλέφωνα. Το ZigBee στοχεύει στις εφαρμογές ραδιοσυχνότητας (RF) που απαιτούν ένα χαμηλό ρυθμό μεταφοράς δεδομένων, μεγάλη ζωή μπαταριών, και εξασφαλισμένη δικτύωση.
- Το **WiMAX** είναι μία τεχνολογία η οποία συνδέει διαδικτυακά (ασύρματα) η οποία λειτουργεί όπως το Wi-fi, μεγαλύτερης όμως εμβέλειας. Συγκεκριμένα, το Wi-Fi προσφέρει εμβέλεια επικοινωνίας μέχρι 100 μέτρα ενώ το WiMax μπορεί να φτάσει τα 35 χιλιόμετρα ή και παραπάνω. [23]
- Η **UWB** τεχνολογία είναι μια **νέα μορφή ασύρματης τεχνολογίας** όπου βασίζεται σε μεταβιβάσεις χαμηλής ισχύος και ωθήσεις (οι οποίες είναι κωδικοποιημένες) σε κοντινές αποστάσεις. Χρησιμοποιείται ευρέως σε ιατρικά συστήματα, σε συστήματα ασφάλειας, και γενικότερα σε εμπορικές και βιομηχανικές εφαρμογές.
- Η ανακάλυψη των **Flash OFDM** κυψελωτών ραδιοσυστημάτων βελτίωσε τις ασύρματες επικοινωνίες, αφού προσέφερε χρήση περισσότερων καναλιών, επικάλυψη ραδιοσυχνοτήτων. Οι πομποί και δέκτες χρειαζόταν πλέον λιγότερη ισχύ για την λειτουργία τους, κάτι που

σήμαινε μικρότερο κόστος, βάρος και μέγεθος, καθώς και λιγότερες παρεμβολές. Η κύρια ιδέα είναι ότι η γεωγραφική περιοχή που καλύπτει το σύστημα επικοινωνίας, να χωρίζεται σε **κυψέλες**. Κάθε κυψέλη χρησιμοποιεί ένα σύνολο συχνοτήτων που μπορεί να χρησιμοποιούν και άλλες κοντινές κυψέλες αλλά όχι οι γειτονικές της. [22]

Επιπλέον, με την ενσωμάτωση της τεχνολογίας IPv6 στο IoT, μπορούμε να αντιληφθούμε την από άκρο σε άκρο επικοινωνία με τον τρέχοντα εξοπλισμό του δικτύου και τη βελτίωση της αναμετάδοσης και της αποτελεσματικότητας του, χαρακτηριστικά που αυξάνουν περαιτέρω την ασφάλεια της μετάδοσης πληροφοριών.

Δίκτυο ασύρματων αισθητήρων - Wireless Sensor Network (WSN)

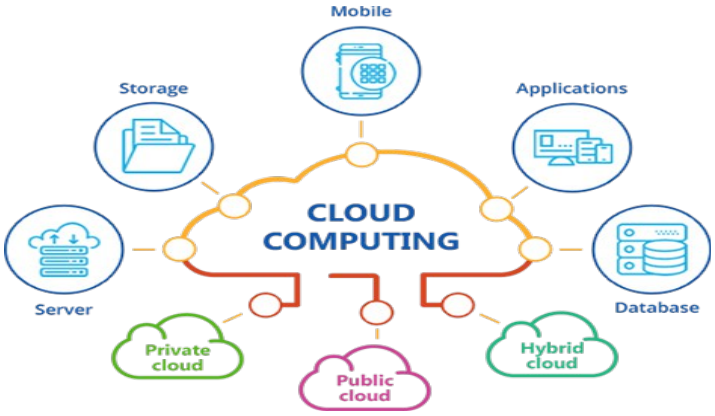


Εικόνα 9: Δίκτυο Ασύρματων Αισθητήτων [26]

Ιδιαίτερα σημαντική τεχνολογία του IoT αποτελεί το **Δίκτυο ασύρματων αισθητήρων** (Wireless Sensor Network (WSN)). Το WSN αποτελείται από ένα μεγάλο αριθμό μικροσκοπικών κόμβων αισθητήρων, με δυνατότητα ανίχνευσης των «πραγμάτων». Ο ρόλος των αισθητήρων είναι η παροχή ακατέργαστων πληροφοριών για επεξεργασία, μετάδοση, ανάλυση και ανατροφοδότηση πληροφοριών. Οι κόμβοι συλλέγουν και προωθούν τα δεδομένα στο σταθμό βάσης για την από κοινού παρακολούθηση των «πραγμάτων». Στα ασύρματα δίκτυα αισθητήρων υπάρχουν ένας ή περισσότεροι σταθμοί βάσης και αρκετοί κόμβοι αισθητήρων. Η βασική σύνθεση του κόμβου δικτύου αισθητήρων περιλαμβάνει τη *μονάδα επεξεργασίας*, τη *μονάδα επικοινωνίας* και τη *μονάδα ενέργειας*. Ο σταθμός βάσης χρησιμεύει ως επεξεργαστής δεδομένων που συνδέει το δίκτυο αισθητήρων με τον εξωτερικό κόσμο. [24]

2.2 Cloud Computing

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



Εικόνα 10: Cloud Computing [27]

Αν και το μέλλον του cloud computing είναι λιγότερο από σαφές, μερικά παραδείγματα της τρέχουσας πρακτικής προτείνουν πιθανές κατευθύνσεις:

- **Wordstar for the web**: Τα είδη των εφαρμογών παραγωγικότητας που προσέλκυαν αρχικά τους ανθρώπους σε προσωπικούς υπολογιστές πριν από 30 χρόνια εμφανίζονται τώρα ως υπηρεσίες λογισμικού. Τα προγράμματα των Εγγράφων Google είναι ένα παράδειγμα, συμπεριλαμβανομένου ενός επεξεργαστή κειμένου, ενός υπολογιστικού φύλλου και ενός εργαλείου για τη δημιουργία παρουσιάσεων τύπου PowerPoint. Μια άλλη επιχείρηση αυτού του είδους είναι το Buzzword, ένας επεξεργαστής κειμένου που βασίζεται στον ιστό, ο οποίος αποκτήθηκε από την Adobe Systems το 2007. Ένα άλλο πρόσφατο προϊόν της Adobe είναι το Photoshop Express, το οποίο έχει μετατρέψει το γνωστό πρόγραμμα χειραγώγησης εικόνων σε μια ηλεκτρονική υπηρεσία.
- **Enterprise computing in the cloud**: Το λογισμικό για σημαντικές επιχειρηματικές εφαρμογές (όπως η υποστήριξη πελατών, οι πωλήσεις και το μάρκετινγκ) εκτελέστηκε γενικά σε εταιρικούς διακομιστές, αλλά πολλές εταιρείες την παρέχουν τώρα ως υπηρεσία κατ 'απαίτηση.
- **Cloudy infrastructure**: Το Amazon.com παρέχει τις κατάλληλες υποδομές για την κατασκευή και τη συντήρηση του κέντρου δεδομένων. Έχει μεταφερθεί σε αυτήν την θέση του οικοσυστήματος του Διαδικτύου. Οι υπηρεσίες Amazon Web Services προσφέρουν αποθήκευση δεδομένων που κοστίζει το μήνα gigabyte και υπολογιστική χωρητικότητα από την ώρα CPU. Και τα δύο είδη πόρων διευρύνουν και συμβάλλουν ανάλογα με τις ανάγκες. Η IBM ανακοίνωσε σχέδια για την υποδομή "Blue Cloud". Και η Google δοκιμάζει το App Engine, το οποίο παρέχει φιλοξενία σε αγροκτήματα διακομιστών Google και ένα περιβάλλον λογισμικού επικεντρωμένο στη γλώσσα προγραμματισμού Python και το κατανεμημένο σύστημα αποθήκευσης Bigtable.
- **The cloud OS**: Για τις περισσότερες εφαρμογές cloud computing ολόκληρη η διεπαφή χρήστη βρίσκεται μέσα σε ένα μόνο παράθυρο σε ένα πρόγραμμα περιήγησης στο Web. Πολλές πρωτοβουλίες αποσκοπούν στην παροχή καλύτερης εμπειρίας χρήστη στις εφαρμογές

του Διαδικτύου. Μια προσέγγιση είναι να εκμεταλλευτεί το παράδειγμα του cloud-computing για να παρέχει όλες τις δυνατότητες ενός λειτουργικού συστήματος μέσα σε ένα πρόγραμμα περιήγησης. Το σύστημα eyeOS, για παράδειγμα, αναπαράγει τη γνωστή μεταφορική επιφάνεια εργασίας (με εικονίδια για αρχεία, φακέλους και εφαρμογές) τα οποία ζουν σε ένα παράθυρο του προγράμματος περιήγησης. Μια άλλη λύση θα παρακάμψει το πρόγραμμα περιήγησης Web, αντικαθιστώντας ένα πιο λειτουργικό σύστημα λογισμικού που λειτουργεί ως ξεχωριστή εφαρμογή στον υπολογιστή-πελάτη και επικοινωνεί απευθείας με διακομιστές στο cloud. Αυτή είναι η ιδέα πίσω από το AIR (πρώην Apollo) που δοκιμάστηκε από την Adobe Systems. Το Open-Laszlo, ένα έργο ανοιχτού κώδικα, λειτουργεί με τον ίδιο τρόπο.

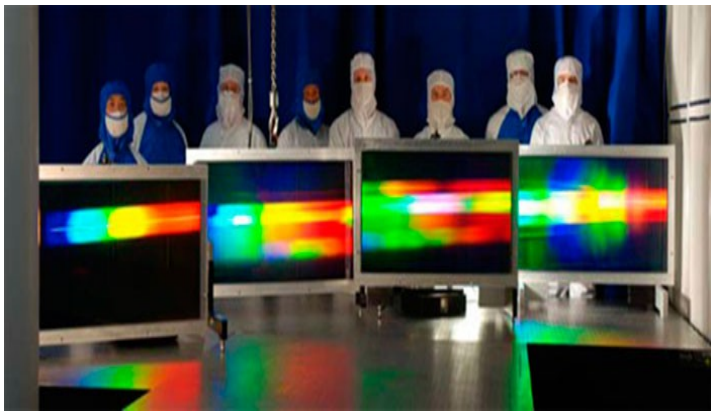
Τα οφέλη για τους τελικούς χρήστες από την χρήση του Cloud Computing είναι πολλά. Αρχικά, **θα μειωθεί σημαντικά το κόστος χρήσης λογισμικού** αφού η χρέωση γίνεται σύμφωνα με την *χρήση* και όχι κατά την *εγκατάσταση* όπως με το συμβατικό λογισμικό. Επίσης, χρησιμοποιώντας την διαδικτυακή δομή Cloud Computing **η χωρητικότητα αποθήκευσης δεδομένων γίνεται άπειρη**, οπότε δεν καθίσταται απαραίτητη η χρησιμοποίηση εξωτερικών σκληρών δίσκων για αποθήκευση δεδομένων. Ακόμη, λόγω του ότι πρόκειται για διαδικτυακή δομή, η πρόσβαση σε πληροφορίες είναι γρήγορη, άμεση και αποτελεσματική αφού η πληροφορία μπορεί να διαδοθεί σε οποιοδήποτε μέρος του κόσμου. Η χρήση μέσω της δομής αυτής είναι **ταχύτερη**, υπάρχει **ευελιξία** και **συμβατότητα** μεταξύ των δεδομένων, και το πιο σημαντικό από όλα είναι ότι εξασφαλίζεται η **ασφάλεια** των δεδομένων αυτών, κάτι το οποίο είχε απασχολήσει αρκετά τους χρήστες αρχικά. Η τεχνολογία αυτή μπορεί να χρησιμοποιηθεί και να εφαρμοστεί **χωρίς να απαιτείται η αγορά επιπλέον υλικού ή λογισμικού**, το ήδη υπάρχον υλικό και λογισμικό καλύπτει τις απαιτήσεις ενός μέσου χρήστη. Εκτός των άλλων όμως, σημαντικό παράγοντα στην τεχνολογία αυτή είναι και το real-time back-up δεδομένων όπου πραγματοποιείται *αυτόματα*, εξοικονομεί χρόνο για τον τελικό χρήστη και του παρέχει ασφάλεια σε περίπτωση διακοπής ρεύματος (όπου θα έχουν αποθηκευτεί τα δεδομένα που θα έχει στο Cloud). [25]

Εκτός των άλλων όμως, το IoT φαίνεται να είναι φιλικό και προς το περιβάλλον. Αν όλοι όσοι ασχολούνται αυτή τη στιγμή με την πληροφορική χρησιμοποιήσουν πλήρως (σε όλους τους τομείς, σε όλες τους τις συσκευές) την τεχνολογία αυτή, οι ατμοσφαιρικοί ρύποι στον πλανήτη θα μπορούσαν να μειωθούν έως και 5% συνολικά ή αλλιώς 2,5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO_2). Αξίζει να σημειωθεί ότι από την χρήση συστημάτων πληροφορικής η επιβάρυνση του περιβάλλοντος ενδέχεται να διπλασιαστεί την επόμενη δεκαετία, άρα η μείωση των ατμοσφαιρικών ρύπων σε όλο τον κόσμο θα μπορούσε να μειωθεί σε βάθος χρόνου έως και 5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO_2) ετησίως απλώς με την χρήση της τεχνολογίας Cloud Computing.

2.3 Οπτικές Τεχνολογίες

Οι ραγδαίες εξελίξεις στον τομέα των οπτικών τεχνολογιών, με τη μορφή τεχνολογιών όπως η Li-Fi και η BiDi της Cisco, θα μπορούσαν να είναι μια σημαντική ανακάλυψη στην ανάπτυξη του IoT.

Η Li-Fi (Light-Fidelity) τεχνολογία χρησιμοποιεί το ηλεκτρομαγνητικό φάσμα για τη μεταφορά δεδομένων. Αντί όμως για ραδιοσήματα, το Li- Fi μεταδίδει δεδομένα σε δυαδικό κώδικα χρησιμοποιώντας την τεχνολογία VLC (Visible Light Communication) που αξιοποιεί το φως από LED. Ομοίως, η Bi-Directional (BiDi) τεχνολογία δίνει ένα ethernet 40G για ένα μεγάλο εύρος συσκευών συνδεδεμένων στο δίκτυο IoT.



Εικόνα 11: Προηγμένες Οπτικές Τεχνολογίες [39]

Advanced Optical Technologies: προσφέρει πολυδιάστατο χαρακτηρισμό, χαρτογράφηση και αξιολόγηση πολύτιμων μικρο και νανο-δομικών υλικών για την πληρέστερη κατανόηση σύνθετων υλικών, συσκευών και σεναρίων και αναπτύσσει προσαρμοσμένους αισθητήρες για αμυντικούς και εμπορικούς πελάτες. [26]

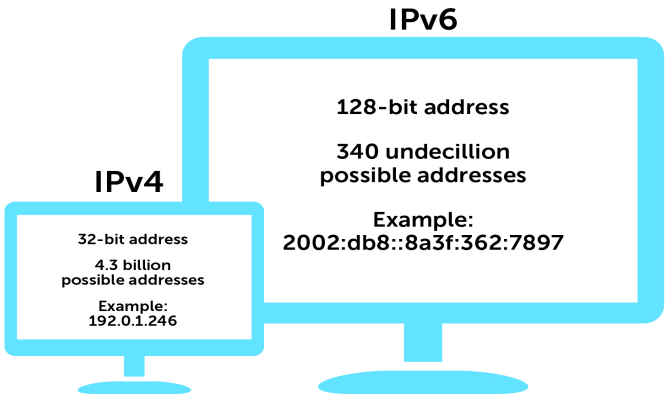
2.4 Πρωτόκολλα IP (IPv4, IPv6), UDP, TCP

Το IoT έχει ήδη πολύ μεγάλη απήχηση στους χρήστες, δεν θα μπορούσε όμως να την είχε αν δεν υπήρχαν και τα αντίστοιχα βασικά πρωτόκολλα που το συνοδεύουν. Πιο συγκεκριμένα, κάποια από τα βασικότερα πρωτόκολλα που χρημιποιούνται στην τεχνολογία αυτή είναι: το **IP** (Intenet Protocol), το **UDP** (User Datagram Protocol) και **TCP** (Trasmission Control Protocol) τα οποία θα αναλυθούν παρακάτω.

Το Πρωτόκολλο Διαδικτύου είναι ***ένα απο τα βασικότερα πρωτόκολλα επικοινωνίας*** για την μετάδοση πακέτων δεδομένων μέσα σε ένα δίκτυο. Βασική αρμοδιότητα αυτού είναι η δρομολόγηση των πακέτων και ο καθορισμός της μορφής των πακέτων που στέλνονται μέσω ενός δικτύου. Για την επικοινωνία μεταξύ δύο ή περισσότερων υπολογιστών απαιτείται η μεταφορά πακέτων μεταξύ τους. Το Πρωτόκολλο Διαδικτύου είναι υπεύθυνο να κάνει αυτή την προώθηση μέσω ενός ή περισσότερων δρομολογητών. Για το λόγο αυτό το IP καθίσταται απαραίτητο αφού οι αρμοδιότητες που έχει είναι βασικές για την επικοινωνία μεταξύ δύο ή περισσότερων υπολογιστών μέσω διαδικτύου.

Το Πρωτόκολλο IP λειτουργεί καλύτερα με το Πρωτόκολλο Ελέγχου Μετάδοσης (TCP), με αποτέλεσμα όλα τα πρωτόκολλα του Διαδικτύου να αναφέρονται απλά ως **TCP/IP**. Η πρώτη έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 (**IPv4**) η οποία χρησιμοποιείται ακόμα και σήμερα σε όλο το διαδίκτυο. Όμως, οι απαιτήσεις πλέον είναι μεγαλύτερες σε σχέση με πριν από 20 χρόνια μιας και όλο

και περισσότεροι άνθρωποι χρησιμοποιούν το διαδίκτυο καθημερινά. Αυτό έχει σαν αποτέλεσμα να υπάρχει μεγαλύτερη ανάγκη σε IP διευθύνσεις, ταχύτητα και εύρος ζώνης. Για το λόγο αυτό, αναπτύχθηκε η επόμενη έκδοση του πρωτοκόλλου, η έκδοση 6 (IPv6), η οποία χρησιμοποιείται πάρα πολύ παγκοσμίως όπως είναι αναμενόμενο.



Εικόνα 12: Το πρωτόκολλο IPv4 vs IPv6 [40]

Κάθε πακέτο IP, αποτελείται από μια **κεφαλίδα** και όλα τα υπόλοιπα είναι **δεδομένα**. Η κεφαλίδα αυτή περιέχει διάφορες πληροφορίες για τα δεδομένα που υπάρχουν στο πακέτο. Επίσης, υπάρχουν οι διευθύνσεις πηγής (IP source) και οι διευθύνσεις προορισμού (IP destination). Η διαδικασία προσθήκης της κεφαλίδας σε ένα πακέτο δεδομένων ονομάζεται **ενθυλάκωση**. Το IP είναι μια υπηρεσία η οποία δεν απαιτεί σύνδεση και είναι ανεξάρτητη από το υλικό που χρησιμοποιείται σε κάθε δίκτυο. [29]

Το IP δρομολογεί τα πακέτα και επιδιώκει να πάει κάθε ένα πακέτο στο προορισμό του, αλλά δεν εγγυάται ότι θα μπορέσει να αντιμετωπίσει προβλήματα όπως η απώλεια κάποιου πακέτου, η αλλοίωση της πληροφορίας, η επανάληψη κάποιου πακέτου, η αλλαγή στη σειρά των πακέτων και πιθανές καθυστερήσεις.

Για να αντιμετωπιστούν τα παραπάνω προβλήματα και να αποφευχθούν, χρειάζονται *πρόσθετα, υψηλότερα επίπεδα λογισμικού πρωτοκόλλων*. Η μόνη διαβεβαίωση που μπορεί να δώσει το πρωτόκολλο IP στην έκδοση 4 (IPv4), είναι μέσω του Header Checksum. Τα bit αυτά της κεφαλίδας θα “δείξουν” αν έχουν αλλάξει ή όχι κατά τη διάρκεια της μεταφοράς των πακέτων. Χρησιμοποιώντας το checksum, μπορεί να διαπιστωθεί εάν η κεφαλίδα έχει μεταφερθεί σωστά ή όχι, και ανάλογα με το αποτέλεσμα καθορίζεται αν το πακέτο θα απορριφθεί ή όχι. Στην επόμενη έκδοση του πρωτοκόλλου όμως που όπως ήδη αναφέρθηκε είναι το IPv6, δεν χρησιμοποιείται Header Checksum για πιο γρήγορη προώθηση των πακέτων δρομολόγησης στο δίκτυο. Αυτό σημαίνει ότι οι δύο αυτές εκδόσεις των πρωτοκόλλων έχουν διαφορετικές κεφαλίδες, άρα δεν μπορούν να συνεργαστούν. Όμως το IPv6 εξακολουθεί και θεωρείται επέκταση του Ipv4 ακόμα και ας έχουν διαφορετικές κεφαλίδες.[30]

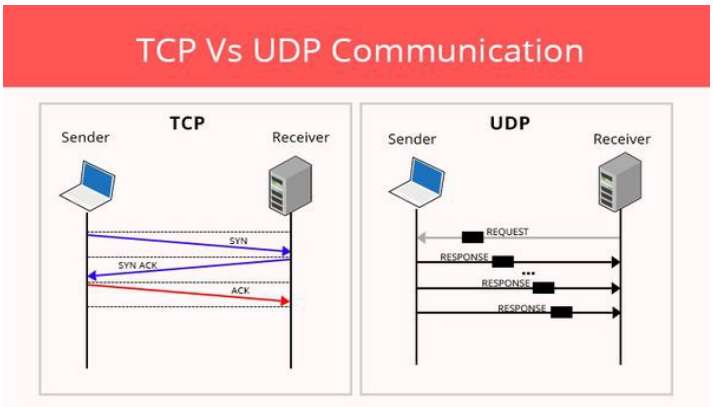
Τα πρωτόκολλα **TCP** και **UDP** είναι δύο επιπλέον πρωτόκολλα του διαδικτύου και χρησιμοποιούνται για την ανταλλαγή πληροφορίας μεταξύ υπολογιστών. Κάθε πακέτο TCP και UDP περιλαμβάνει δεδομένα και πληροφορία κατάλληλη για το αντίστοιχο πρωτόκολλο. Εκτός όμως από τα

δεδομένα αυτά, περιλάμβάνει και μια πικεφαλίδα στην οποία αναφέρονται όλα τα βασικά χαρακτηριστικά του πακέτου. Κάποια από τα χαρακτηριστικά αυτά είναι η θύρα (port) του αποστολέα και την θύρα του παραλήπτη. Όταν το πακέτο παραδοθεί στην κατάλληλη θύρα του παραλήπτη, τότε το παραλαμβάνει η αντίστοιχη εφαρμογή και χρησιμοποιεί τα δεδομένα που βρίσκονται μέσα σε αυτό. [31]

Το **TCP** παρέχει στις εφαρμογές έναν τρόπο να παραδίδουν (και να λαμβάνουν) μια ροή πακέτων πληροφοριών που έχουν παραγγελθεί και ελέγξει με σφάλμα μέσω του δικτύου. Το πρωτόκολλο User Datagram Protocol (**UDP**) χρησιμοποιείται από τις εφαρμογές για την παροχή πιο γρήγορης ροής πληροφοριών, εξαλείφοντας τον έλεγχο σφαλμάτων. Και τα δύο πρωτόκολλα βασίζονται στο πρωτόκολλο IP. Με άλλα λόγια, αν στέλνετε ένα πακέτο μέσω TCP ή UDP, αυτό το πακέτο αποστέλλεται σε μια διεύθυνση IP. [32] [33]

Το TCP είναι το πιο συχνά χρησιμοποιούμενο πρωτόκολλο στο Διαδίκτυο. Το TCP αφορά την **αξιοπιστία**, τα πακέτα που αποστέλλονται με TCP παρακολουθούνται, έτσι ώστε να μην χάνονται ή να διαβιβάζονται δεδομένα κατά τη μεταφορά. Αυτός είναι ο λόγος για τον οποίο οι λήψεις αρχείων δεν καταστρέφονται. Φυσικά, εάν ο παραλήπτης είναι εντελώς εκτός σύνδεσης, ο υπολογιστής θα εγκαταλείψει και εμφανιστεί ένα μήνυμα σφάλματος λέγοντας ότι δεν μπορεί να επικοινωνήσει με τον απομακρυσμένο κεντρικό υπολογιστή.

Το πρωτόκολλο UDP λειτουργεί παρόμοια με το TCP, αλλά **εκπέμπει όλα τα πράγματα ελέγχου σφαλμάτων**. Όλη η αμφίδρομη επικοινωνία εισάγει λανθάνουσα κατάσταση, επιβραδύνοντας την μετάδοση των πακέτων. Όταν μια εφαρμογή χρησιμοποιεί UDP, τα πακέτα αποστέλλονται στον παραλήπτη. Ο αποστολέας δεν περιμένει να βεβαιωθεί ότι ο παραλήπτης έλαβε το πακέτο, απλώς συνεχίζει να στέλνει τα επόμενα πακέτα. Εάν ο παραλήπτης χάσει μερικά πακέτα UDP εδώ και εκεί, χάνεται, ο αποστολέας δεν θα τα αποστείλει ξανά. Η απώλεια όλων αυτών των δαπανών σημαίνει ότι **οι συσκευές μπορούν να επικοινωνούν πιο γρήγορα**.



Εικόνα 13: Βασική διαφορά μεταξύ των πρωτοκόλλων TCP και UDP [41]

Το UDP χρησιμοποιείται όταν η ταχύτητα είναι επιθυμητή και η διόρθωση σφάλματος δεν είναι απαραίτητη. Για παράδειγμα, το UDP χρησιμοποιείται συχνά για ζωντανές εκπομπές και online

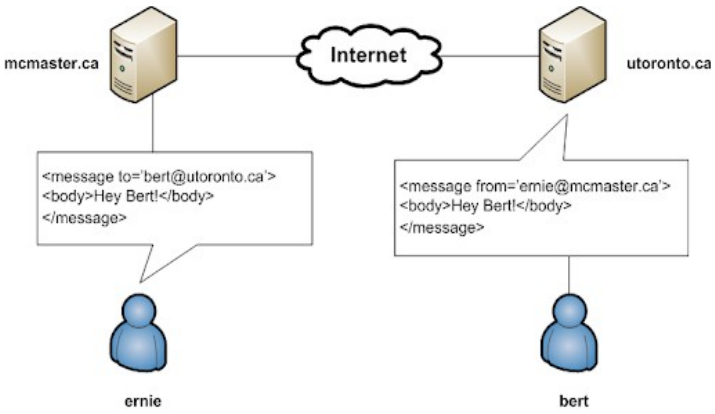
παιχνίδια. Για παράδειγμα, ας πούμε ότι βλέπετε μια ζωντανή ροή βίντεο, η οποία συχνά μεταδίδεται χρησιμοποιώντας UDP αντί TCP. Ο διακομιστής απλώς στέλνει μια σταθερή ροή πακέτων UDP σε υπολογιστές που παρακολουθούν. Εάν χάσετε τη σύνδεσή σας για λίγα δευτερόλεπτα, το βίντεο μπορεί να παγώσει ή να πάθει άλμα για λίγο και στη συνέχεια να μεταβεί στο τρέχον κομμάτι της εκπομπής. [34]

2.5 Πρωτόκολλα XMPP, AMP, AMQP

Το **XMPP** (Extensible Messaging Presence Protocol) πρόκειται για πρωτόκολλο για τη ροή στοιχείων XML σε ένα δίκτυο για την ανταλλαγή μηνυμάτων και πληροφοριών παρουσίας κοντά σε πραγματικό χρόνο. Αυτό το πρωτόκολλο χρησιμοποιείται κυρίως από εφαρμογές άμεσων μηνυμάτων όπως το WhatsApp. Τα **βασικά χαρακτηριστικά** του XMPP είναι τα ακόλουθα:

- Αποστολή και λήψη μηνυμάτων με άλλους χρήστες.
- Έλεγχος και κοινοποίηση παρουσίας.
- Διαχείριση συνδρομών προς και από άλλους χρήστες.
- Διαχείριση της λίστας επαφών.
- Αποκλεισμός επικοινωνίας μεσυγκεκριμένους χρήστες (μηνύματα, κοινοποίηση παρουσίας κ.λπ.).

Το πρωτόκολλο XMPP προήλθε από το πρωτόκολλο TCP (πρωτόκολλο ελέγχου μετάδοσης), χρησιμοποιώντας ροές XML ανοιχτού τύπου για μακροχρόνιες συνδέσεις TCP. Σε ορισμένες περιπτώσεις, το XMPP (θύρα 5222) δεν μπορεί να χρησιμοποιηθεί για εφαρμογές ιστού και χρήστες πίσω από περιορισμένα τείχη προστασίας, και για να ξεπεραστεί αυτό, η κοινότητα XMPP ανέπτυξε μια μεταφορά HTTP. Και καθώς ο πελάτης χρησιμοποιεί HTTP, τα περισσότερα τείχη προστασίας επιτρέπουν στους πελάτες να φέρονται και να δημοσιεύουν μηνύματα χωρίς κανένα πρόβλημα. Έτσι, σε σενάρια όπου η θύρα TCP που χρησιμοποιείται από το XMPP είναι αποκλεισμένη, ένας διακομιστής μπορεί να ακούει στη κανονική θύρα HTTP και η κίνηση μπορεί να γίνει χωρίς προβλήματα. [35]



Εικόνα 14: Το πρωτόκολλο XMPP χρησιμοποιώντας HTTP [42]

Το πρωτόκολλο ασύγχρονου μηνύματος (**AMP**) είναι ένα ευέλικτο πρωτόκολλο για την αποστολή πολλαπλών ασύγχρονων ζευγών αιτήσεων/απαντήσεων στην ίδια σύνδεση. Τα αιτήματα και οι απαντήσεις είναι και οι δύο συλλογές μη αντιστοιχισμένων ζευγών κλειδιών/τιμών. Το AMP δίνει τη δυνατότητα σε ένα πλούσιο σύνολο εφαρμογών του Διαδικτύου, που κυμαίνονται από τα παραδοσιακά API πελάτη-διακομιστή έως τα προσαρμοσμένα και αποτελεσματικά πρωτόκολλα RPC, στις κατανεμημένες τοπολογίες ανταλλαγής αλληλογραφίας μεταξύ ομότιμων χρηστών. Μόλις συνδεθεί, η συνομιλία AMP είναι συμμετρική, επιτρέποντας είτε στον πελάτη είτε στον εξυπηρετητή να εκκινήσει ένα ασύγχρονο αίτημα, υπό την προϋπόθεση ότι η άλλη πλευρά της σύνδεσης υλοποιεί ένα χειριστή γι 'αυτό. [36]

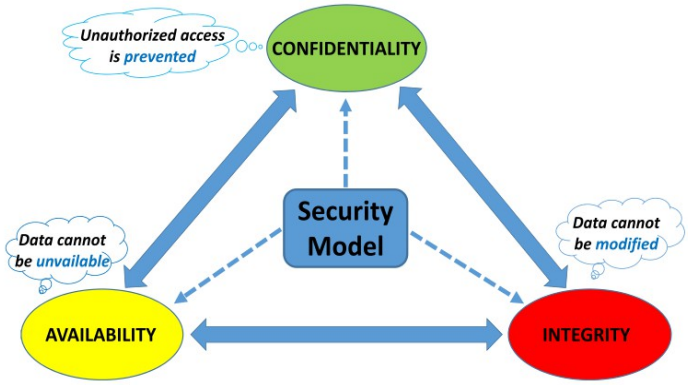
Το πρωτόκολλο Advanced Message Queuing Protocol (**AMQP**) είναι ένα ανοιχτό πρότυπο πρωτόκολλο εφαρμογής layer για middleware με γνώμονα τα μηνύματα. Βασικά χαρακτηριστικά του AMQP είναι: ο **προσανατολισμός του μηνύματος**, η **ουρά**, η **δρομολόγηση** (συμπεριλαμβανομένου του σημείου προς σημείο, η δημοσίευση και η εγγραφή), η **αξιοπιστία** των μηνυμάτων και η **ασφάλεια**. Προηγούμενες τυποποιήσεις του μεσαίου λογισμικού έχουν συμβεί σε επίπεδο API (π.χ. JMS) και έχουν επικεντρωθεί στην τυποποίηση της αλληλεπίδρασης του προγραμματιστή με διαφορετικές εφαρμογές του middleware και όχι στην παροχή διαλειτουργικότητας μεταξύ πολλαπλών υλοποιήσεων. Σε αντίθεση με το JMS, το οποίο ορίζει ένα API και ένα σύνολο συμπεριφορών που πρέπει να παρέχει μια υλοποίηση μηνυμάτων, το AMQP είναι ένα πρωτόκολλο επιπέδου σύρματος. Ένα πρωτόκολλο επιπέδου σύρματος είναι μια περιγραφή της μορφής των δεδομένων που αποστέλλονται μέσω του δικτύου ως ροή των byte. Κατά συνέπεια, κάθε εργαλείο που μπορεί να δημιουργήσει και να ερμηνεύσει μηνύματα που συμμορφώνονται με αυτό το μορφότυπο δεδομένων μπορεί να αλληλεπιδρά με οποιοδήποτε άλλο συμβατό εργαλείο ανεξάρτητα από τη γλώσσα εφαρμογής. [37]

ΚΕΦΑΛΑΙΟ 3: ΑΣΦΑΛΕΙΑ IoT

3.1 Θέματα ασφάλειας στο IoT

Όπως ήδη αναφέρθηκε, πολλές συσκευές συνδέονται στο διαδίκτυο, το οποίο όμως φιλοξενεί μεγάλους κινδύνους και τρωτά σημεία που θα μπορούσαν να καταστήσουν οποιαδήποτε συσκευή προσβάσιμη σε έναν κακόβουλο χρήστη. Καταγράφεται έντονη η ανάγκη για άμεση, αποτελεσματική καταγραφή και αναπαράσταση των δεδομένων που παράγονται, μεταφέρονται και μεταδίδονται από κόμβο σε κόμβο. Η ασφάλεια είναι απαραίτητη συνιστώσα στη διάδοση των τεχνολογιών και εφαρμογών IoT. Γι' αυτό το λόγο, τα «πράγματα» πρέπει να είναι σε θέση να επιβάλουν την δική τους ασφάλεια όσον αφορά τις εφαρμογές που υποστηρίζουν, την πρόσβαση στο δίκτυο, τις συσκευές και την χρήση από τους ιδιώτες. Σύμφωνα με τη θεωρία ένα ασφαλές δίκτυο παρέχει τα εξής χαρακτηριστικά :

1. **Πιστοποίηση** (Authentication): Πρόσβαση στην πληροφορία.
2. **Ακεραιότητα** (Integrity): Αξιόπιστη πληροφορία.
3. **Εμπιστευτικότητα** (Confidentiality): Απόκρυψη της πληροφορίας από τρίτους.



Εικόνα 15: Το τρίγωνο της ασφάλειας στο "Διαδίκτυο των Πραγμάτων" [43]

Η ακεραιότητα, η εμπιστευτικότητα και σε ορισμένες περιπτώσεις η πιστοποίηση, μπορούν να διασφαλιστούν με τη διαδικασία της **κρυπτογράφησης** στα πακέτα και τα σήματα που ανταλλάσσονται στο δίκτυο. [1]

Η ασφάλεια που παρέχουν οι τεχνολογίες IoT, είναι ο πιο καθοριστικός παράγοντας, ώστε να υιοθετηθούν ευρέως τεχνολογίες από τους τελικούς χρήστες. Εάν δεν υπάρξουν εγγυήσεις οι οποίες να αφορούν την εμπιστευτικότητα, την πιστοποίηση και την ακεραιότητα των ενδιαφερόμενων μελών, καμία IoT λύση, δεν θα ευδοκιμήσει. Σε αναπτύξεις IoT λύσεων, στα πρώιμα στάδια, όπου βασίζονταν μόνο στο RFID, οι λύσεις ασφαλείας παρέχονταν μόνο σε περίπτωση που παρουσιαζόταν ανάγκη και

δεν ήταν ενσωματωμένες εξ’ αρχής. Αυτό προκύπτει από το γεγονός ότι τέτοιες λύσεις αναπτύσσονταν με κάθετο τρόπο, όπου όλα τα στοιχεία ήταν υπό τον έλεγχο μίας ενιαίας διοικητικής οντότητας.

Στην περίπτωση ενός ανοιχτού IoT οικοσυστήματος, όπου τα ενδιαφερόμενα μέλη έχουν διαφορετικούς ρόλους, για παράδειγμα κάποια ομάδα από τα ενδιαφερόμενα μέλη έχει τους αισθητήρες ή τους actuators, κάποια άλλη ομάδα διαχειρίζεται και επεξεργάζεται τα δεδομένα που έχουν συλλεχθεί από τα προηγούμενα ενδιαφερόμενα μέλη και τέλος, μια διαφορετική ομάδα ανθρώπων θα παρέχει υπηρεσίες στους τελικούς χρήστες, οι οποίες θα βασίζονται στα δεδομένα που έχουν συλλεχθεί και επεξεργαστεί. Σε ένα τέτοιο μοντέλο δημιουργείται ένα πλήθος ζητημάτων ασφαλείας που πρέπει να επιλυθούν ώστε οι τεχνολογίες IoT να καταφέρουν να επικρατήσουν. Οι κυριότεροι παράγοντες που πρέπει να αντιμετωπιστούν είναι η **εμπιστευτικότητα** των δεδομένων,η **ιδιωτικότητα** και η **εμπιστοσύνη**. Οι εκτιμήσεις για την ασφάλεια είναι ορθογώνιες προς άλλους ερευνητικούς τομείς και εκτείνονται τόσο στην επικοινωνία/δικτύωση, πλατφόρμα/διαχείριση δεδομένων όσο και σε εφαρμογές/επίπεδα υπηρεσιών.

Όταν γίνεται λόγος για **αυτόνομη ασφάλεια** (autonomic security) πρέπει να έχουμε στο μυαλό μας τόσο τις έννοιες της *αυτοθεραπείας* και της *αυτοπροστασίας* όσο και τα χαρακτηριστικά και τις απαιτήσεις που υφίστανται σε οποιοδήποτε αυτόνομο σύστημα, καθώς επίσης και τη λειτουργία του κύριου βρόχου ελέγχου σε ένα γενικό αυτόνομο πλαίσιο. Σημαντικές έννοιες εδώ αποτελούν οι εξής:

1. **Αυτόνομη υπολογιστική** (Autonomic computing): Πρόκειται για μία έννοια η οποία ενώνει πολλούς τομείς των υπολογιστών με σκοπό τη δημιουργία συστημάτων αυτοδιαχείρισης. Σύμφωνα με έναν άλλον ορισμό πρόκειται για ένα έξυπνο σύστημα ή σύστημα συστημάτων όπου τα δεδομένα που έχουν αποκτηθεί μέσω ανίχνευσης ή παρακολούθησης διαφορετικών δυνατοτήτων χρησιμοποιείται εποικοδομητικά σε μία γενικότερη αυτόνομη διαδικασία λήψης αποφάσεων.

Ένα αυτόνομο υπολογιστικό σύστημα πρέπει να ρυθμίζει και να επαναρυθμίζει τον ίδιο του ‘τον εαυτό’ ανάλογα με τις εκάστοτε συνθήκες, οι οποίες μπορεί πολλές φορές να καθίστανται απρόβλεπτες. Η ρύθμιση του συστήματος θα πρέπει σε κάθε περίπτωση να συμβαίνει αυτομάτως μέσω δυναμικών και συνεχόμενων προσαρμογών στο διαρκώς μεταβαλλόμενο περιβάλλον. Με στόχο τη μακροπρόθεσμη επάρκεια, κάθε δίκτυο και σύστημα στο IoT θα πρέπει να επιτυγχάνει κάποιο είδος αυτόνομης συμπεριφοράς, με απουσία δηλαδή της ανθρώπινης παρέμβασης. Επιπλέον, στόχος-πρόκληση κάθε αυτόνομου συστήματος αποτελεί ο διαχωρισμός ρόλων μεταξύ των συστατικών στοιχείων χωρίς παράλληλα να θυσιαστεί κάποιο κομμάτι της λειτουργικότητας. Η παρουσία μίας κεντρικής αρχής αποτελεί επιτακτική προϋπόθεση, καθώς επιτρέπει την ελεγχόμενη διαχείριση των εμπλεκόμενων μερών.

Η **αυτόνομη υπολογιστική** ασχολείται με τη διαχείριση των πηγών του υπολογιστή με τρόπο τέτοιο, ώστε να ελαχιστοποιηθεί η παρέμβαση του χρήστη. Η έννοια της **αυτονομίας** χρησιμοποιεί μία

τεχνολογία με σκοπό τη διαχείριση και τη βελτιστοποίηση της λειτουργικότητας κάποιας άλλης τεχνολογίας, έτσι ώστε να μειωθεί η ανάγκη χειροκίνητης παρέμβασης στα υπόλοιπα συστήματα.

2. Ο όρος «**Self-* (self-star)**» αναφέρεται στο σύνολο των περιπτώσεων αυτοοργανισμού, αυτοεπίγνωσης, αυτοπροσαρμογής, αυτοσχεδιασμού, αυτοκατασκευής και αυτοδιόρθωσης. Η φιλοσοφία του έγκειται στην περιγραφή των απαραίτητων ποιοτικών χαρακτηριστικών που συνθέτουν τη συμπεριφορά ενός αυτόνομου στοιχείου. Σημαντικές έννοιες εδώ αποτελούν η **αυτοθεραπεία** (self-healing)και η **αυτοπροστασία** (self-protection). Η πρώτη αναφέρεται *στην ικανότητα ενός συστήματος να ανακαλύπτει τις αιτίες σε περίπτωση αποτυχίας χωρίς την ανθρώπινη επίβλεψη*, ενώ η δεύτερη *στη δυνατότητα για αναγνώριση και προστασία των συστατικών στοιχείων του συστήματος από τυχαίες επιθέσεις*.

Αξιοσημείωτο είναι το γεγονός ότι στο IoT ίσως να μην τυγχάνει εφαρμογής η δεύτερη έννοια, καθώς οι κόμβοι μπορεί να ακολουθούν διαρκώς διαδικασίες σύνδεσης και αποσύνδεσης από ένα δίκτυο. Η αυτόνομη υπολογιστική εφαρμόζεται μέσω της χρήσης του κυκλώματος ελέγχου “MAPE” που έλαβε το όνομά του από τα αρχικά των τεσσάρων ακόλουθων λέξεων που ταυτόχρονα αποτελούν τα ξεχωριστά μέρη της αρχιτεκτονικής του κυκλώματος ελέγχου με βάση τη λειτουργικότητα.

- **Monitor** (Παρακολούθηση): Η μονάδα παρακολούθησης είναι υπεύθυνη για τη συλλογή λεπτομερών εσωτερικών πληροφοριών από ένα στοιχείο. Αυτές οι λεπτομέρειες περιλαμβάνουν τα δεδομένα που έχουν αποκτηθεί από το περιβάλλον, καθώς και τα δεδομένα που σχετίζονται με το ίδιο το στοιχείο.
- **Analyze** (Ανάλυση): Η μονάδα ανάλυσης παρέχει μηχανισμούς που δημιουργήθηκαν με βάση τις λεπτομερείς εσωτερικές πληροφορίες και που μπορούν να χρησιμοποιηθούν σε σύνθετες καταστάσεις, επιτρέποντας στην κεντρική αρχή να λαμβάνει γνώση για το περιβάλλον. Η εν λόγω μονάδα δύναται επίσης να προβλέψει μελλοντικές καταστάσεις.
- **Plan** (Σχεδιασμός): Η μονάδα σχεδιασμού παρέχει μηχανισμούς οι οποίοι καθοδηγούν κάθε είδους ενέργεια-δράση που απαιτείται για την επίτευξη των στόχων του συστήματος με τη βοήθεια πολιτικών, κανόνων και κανονισμών υψηλού επιπέδου. Επίσης, σχεδιάζει τις μετέπειτα ενέργειες, λαμβάνοντας υπόψιν και τους περιορισμούς που έχουν τεθεί στο σύστημα.
- **Execute** (Εκτέλεση): Η μονάδα εκτέλεσης ελέγχει την εφαρμογή του προγραμματισμένου σχεδίου με την υποστήριξη ενός είδους ανατροφοδότησης.

Οι αυτόνομες εφαρμογές προϋποθέτουν σε κάθε περίπτωση την εκτέλεση αυτόνομης διαχείρισης, καθώς και την πηγή διαχείρισης. Στο IoT λόγω της ετερογένειας δεν είναι δυνατό να υποδειχθεί ο καλύτερος συνδυασμός των αυτόνομων φορέων (autonomic agents). Για το λόγο αυτό, υφίστανται διαφορετικά πλαίσια αυτονομίας τα οποία ποικίλλουν (από τελικά δίκτυα έως πρωτόκολλα υψηλότερου επιπέδου). Οι αισθητήρες πραγματοποιούν συλλογές ακατέργαστων δεδομένων, που παραδοσιακά περιορίζονται σε συναφή σύνολα δεδομένων με τους χρόνους ανταπόκρισης, τα δίκτυα

και τη χρήση δίσκων, τη μνήμη και τη χρησιμοποίηση CPU. Στην περίπτωση του IoT, οι αισθητήρες δρουν ως το κέντρο των πληροφοριών, ανιχνεύοντας το περιβάλλον για φυσικά δεδομένα, προσδίδοντας έτσι σε αυτά μία περιβαλλοντική φύση. [38]

3.2 Απειλές στην ασφάλεια του IoT

Για να εξασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα στο IoT δημιουργήθηκε η ανάγκη βελτιστοποίησης των υπολογιστικών πόρων από αισθητήρες. Διαφορετικά επίπεδα επεξεργασίας παρουσιάζουν δυσκολία στο συντονισμό εμπλεκομένων μέτρων με αποτέλεσμα την ύπαρξη τρωτών σημείων. Μερικά από τα **πιθανά προβλήματα** που σχετίζονται με το IoT έχουν ως ακολούθως:

- **Γενικά** (εικονικές και φυσικές απειλές)

Σε ένα IoT τα θέματα ασφάλειας εστιάζονται στις εικονικές και στις φυσικές απειλές. Οι φυσικές απειλές αυξάνονται όσο περισσότερα «πράγματα» συνδέονται στο δίκτυο. Οι εικονικές απειλές είναι παρόμοιες με τις απειλές σε οποιοδήποτε άλλο IT-περιβάλλον. Η ανάλυση γίνεται σε τρία σημεία ενός IoT, στον τρόπο συνδεσιμότητας των «πραγμάτων», στα ίδια τα «πράγματα» και στην πύλη (gateway) (το κεντρικό σημείο συλλογής δεδομένων από διάφορους αισθητήρες) που θεωρούνται ευάλωτα στις επιθέσεις. [44]

Όσον αφορά στην επικοινωνία σε ένα δίκτυο πραγμάτων σημαντικές απειλές κρίνονται **η παρεμβολή** και **η υποκλοπή σήματος**. Παρεμβολή συμβαίνει όταν η ροή της κυκλοφορίας των δεδομένων που προορίζονταν για τη σύνδεση, με κάποιο τρόπο διαταράσσεται ή εξαλείφεται τελείως λόγω άλλων ανεπιθύμητων ροών που καταλαμβάνουν τη φυσική σύνδεση. Ένα παράδειγμα είναι όταν εμφανίζεται μια επίθεση άρνησης υπηρεσίας η οποία μπορεί να είναι καταστροφική σε ένα περιβάλλον IoT που απαιτεί διαρκή επικοινωνία των «πραγμάτων». Παρεμβολή μπορεί επίσης να γίνει σε ένα φυσικό επίπεδο, για παράδειγμα με μπλοκάρισμα της ασύρματης επικοινωνίας μεταξύ των κόμβων.

Εικόνα 16: Απειλές στην ασφάλεια του IoT [51]

Υποκλοπή σήματος μπορεί να γίνει σε διάφορα στάδια στην αλυσίδα της επικοινωνίας ανάλογα με το ποια συσκευή οι επιτιθέμενοι είναι σε θέση να ακούσουν, να αναμεταδώσουν κρυφά τα δεδομένα και σε ορισμένες περιπτώσεις να τροποποιήσουν την επικοινωνία μεταξύ δύο μερών. Η επίθεση αυτή του **ενδιάμεσου κόμβου** (Man in the middle attack) και έχει ως στόχο την κλοπή ή την αλλαγή πληροφοριών μεταξύ της επικοινωνίας. Επιτυγχάνεται με το να στείλει ο επιτιθέμενος δυο

binding updates, ένα στον στόχο (π.χ πελάτη) και ένα στον server με τον όποιο επικοινωνεί.Αυτό γίνεται με τέτοιο τρόπο όπου αλλάζει η ροή της πληροφορίας που ανταλλάσσουν μεταξύ τους με αποτέλεσμα να έχει πρόσβαση στο περιεχόμενο των μηνυμάτων τους. [45]

Εικόνα 17: Επίθεση "Man-in-the-middle" [52]

Σε μία IoT-συσκευή υπάρχουν κυρίως απειλές σε μορφή εισβολής ή/και εκμετάλλευσης στο εικονικό επίπεδο. Υπάρχει η δυνατότητα της εισβολής, όταν υπάρχει ανεπαρκής ή ανύπαρκτη ταυτότητα και εξουσιοδότηση για την πρόσβαση σε ένα σύστημα, συσκευή ή στα δεδομένα. Εκμετάλλευση υφίσταται το IoT-περιβάλλον κάθε φορά που ένας χρήστης έχει πρόσβαση σε ένα στοιχείο (συσκευή ή πύλη). Μπορεί να έχει τη μορφή της ανάγνωσης πληροφοριών, καταστρέφοντας τα ή παρεμβαίνοντας στην επικοινωνία. Όπως φαίνεται, οι φυσικές απειλές στα «πράγματα» επηρεάζουν σε μεγάλο βαθμό την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Η διαπραγμάτευση εμπιστοσύνης βασίζεται σε peer–to –peer αλληλεπιδράσεις και αποτελείται από επαναληπτική δημοσιοποίηση ψηφιακών πιστοποιητικών με σκοπό την επαλήθευση και την παγίωση αμοιβαίας εμπιστοσύνης. Ακεραιότητα δεδομένων περιλαμβάνει την προστασία σημαντικών δεδομένων κατά τη μετάδοση τους καθώς υπάρχει ο κίνδυνος οι hackers να χρησιμοποιούν μεθόδους παρακολούθησης. Η πύλη, ως ένα εκτεταμένο δίκτυο, περιέχει πολλούς αισθητήρες ή συσκευές που επικοινωνούν μεταξύ τους μέσω αυτής. Βασική απειλή είναι **η τροποποίηση μεγάλων ποσοτήτων δεδομένων** που μεταφέρονται από αυτήν.

Για τη προστασία από τις παραπάνω απειλές έχουν αναπτυχθεί δυο τρόποι σύνδεσης, η e**nd-to-end** και η **hop-by-hop** σύνδεση. Η end-to-end επικοινωνία σημαίνει ότι μόνο τα τελευταία σημεία της σύνδεσης έχουν τη δυνατότητα να παρουσιάζουν τα δεδομένα σε μορφή απλού κειμένου ενώ τα ενδιάμεσα πράγματα φέρουν τα δεδομένα κρυπτογραφημένα. Με αυτό τον τρόπο ο εισβολέας δεν μπορεί να παραποιήσει τα μηνύματα που διαβιβάζονται στους διάφορους κόμβους. Με τη hop-by- hop προστασία τα δεδομένα που αποστέλλονται από μια συσκευή αποκρυπτογραφούνται, όταν πρόκειται για την πύλη, και στη συνέχεια κρυπτογραφούνται με τα κλειδιά της πύλης πριν από τη διαβίβαση. Με τον τρόπο αυτό μόνο η πύλη μπορεί να διαχειριστεί τα κλειδιά για αυτές τις συσκευές.

- **Μη εξουσιοδοτημένη πρόσβαση σε RFID**

Μια μη εξουσιοδοτημένη πρόσβαση σε ετικέτες που περιέχουν τα δεδομένα ταυτοποίησης είναι ένα σημαντικό ζήτημα του IoT. Όχι μόνο η ετικέτα μπορεί να διαβαστεί από έναν οποιοδήποτε αναγνώστη αλλά μπορεί ακόμη και να τροποποιηθεί ή ενδεχομένως να καταστραφεί. Μερικές από τις απειλές των RFID περιλαμβάνουν κακόβουλη τροποποίηση δεδομένων, πλαστή ταυτότητα ετικέτας,

απενεργοποίηση και αποκόλληση ετικέτας, παρακολούθηση, μπλοκάρισμα, παρεμβολή και πλαστή ταυτότητα αναγνώστη.

Πιο συγκεκριμένα, ο επιτιθέμενος προσπαθεί να εξαπατήσει τον αναγνώστη στο να δεχτεί μια άλλη ετικέτα RFID από την δική του. Ο επιτιθέμενος αποκτά τον σειριακό αριθμό της ετικέτας RFID και ουσιαστικά την κλωνοποιεί και την εισάγει στο σύστημα με στοπό να το εξαπατήσει. Κατά τη φάση της παρακολούθησης, ότι δεδομένα ανταλλάσσονται στην επικοινωνία μεταξύ του αναγνώστη και της ετικέτας υποκλέπτονται και αποκωδικοποιούνται. Κατά τη φάση του μπλοκαρίσματος, μια ειδικά κατασκευασμένη ετικέτα δίνει την εντύπωση στον αναγνώστη ότι πολύ μεγάλος αριθμός ετικετών διαβάζονται ταυτόχρονα, οπότε ο αναγνώστης αυτο-μπλοκάρεται λόγω της σύγχυσης που δημιουργείται. [46]

- **Παραβίαση ασφάλειας των κόμβων δικτύου αισθητήρων**

Τα ασύρματα δίκτυα αισθητήρων είναι ευάλωτα σε διάφορους τύπους επιθέσεων, μερικές από τις πιο πιθανές επιθέσεις είναι το Jamming, η αλλοίωση, το Sybil, flooding, οι οποίες συνοψίζονται παρακάτω:

1. **Jamming**: Η επίθεση Jamming παρεμποδίζει το σύνολο του δικτύου παρεμβαίνοντας στις συχνότητες των κόμβων αισθητήρων.
2. **Αλλοίωση:** Είναι η μορφή της επίθεσης στην οποία τα δεδομένα μπορούν να τροποποιηθούν από τον επιτιθέμενο.
3. **Sybil επίθεση:** Σε μια επίθεση Sybil ένας κόμβος παρουσιάζει πολλές (διαφορετικές μεταξύ τους) ταυτότητες στους άλλους κόμβους στο δίκτυο.
4. **Flooding:** Η επίθεση Flooding αφορά τη πλημμύρα των πακέτων σε μία σύνδεση στο δίκτυο όπου δημιουργεί προβλήματα στη ροή των δεδομένων. Αυτό σημαίνει ότι μπορεί να προκαλέσει διαταραχή στο κατέβασμα των αρχείων από το δίκτυο, ροή αντίθετη της κανονικής με αποτέλεσμα την υπερχείλιση. Πρόκειται για ένα είδος επίθεσης DOS (denial of service).[47]

3.3 Ασφάλεια συσκευών

Η ασφάλεια των συσκευών στο Ίντερνετ των πραγμάτων πρέπει να παρέχεται σε όλη τη διάρκεια του κύκλου ζωής της συσκευής και αφορά:

1. Ασφαλής εκκίνηση: Κάθε φορά που η συσκευή συνδέεται θα πρέπει να διασφαλίζεται η αυθεντικότητα και η ακεραιότητα του λογισμικού της με τη χρησιμοποίηση ψηφιακών υπογραφών.
2. Πρόσβαση: Απαραίτητη είναι η πρόσβαση στη συσκευή μόνο των πόρων που χρειάζονται για να κάνουν τη δουλειά τους παρέχοντας διαπιστευτήρια ότι η πρόσβαση θα είναι η ελάχιστη

που απαιτείται για να εκτελεστεί μια λειτουργία, προκειμένου να ελαχιστοποιηθεί η παραβίαση της ασφάλειας.

3. Ταυτότητας συσκευής: Όταν η συσκευή είναι συνδεδεμένη στο δίκτυο, θα πρέπει να πιστοποιείται πριν από τη λήψη ή τη μετάδοση δεδομένων.
4. Firewalls και IPS: Η συσκευή χρειάζεται επίσης ένα τείχος προστασίας και το δικό του πρωτόκολλο επικοινωνίας με άλλες συσκευές.
5. Ενημερώσεις: οι συσκευές θα πρέπει να είναι σε θέση να κάνουν ενημερώσεις. [38]

Εικόνα 18: Ασφάλεια συσκευών [53]

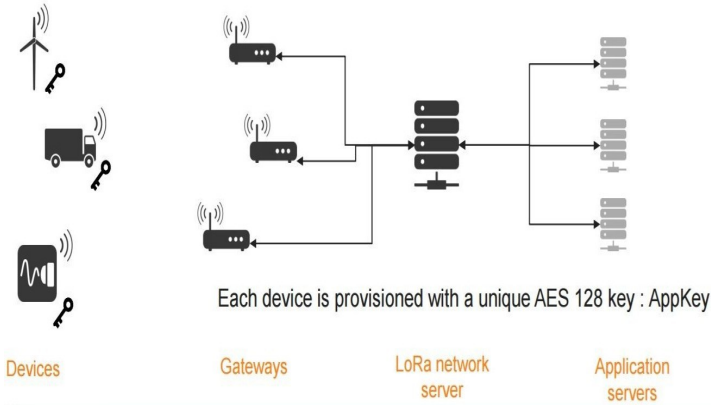
3.4 Ασφάλεια LoRaWAN

Η ασφάλεια LoRaWAN έχει σχεδιαστεί για να ικανοποιεί τα γενικά κριτήρια σχεδιασμού LoRaWAN: **χαμηλή κατανάλωση ενέργειας, χαμηλή πολυπλοκότητα υλοποίησης, χαμηλό κόστος και υψηλή κλιμάκωση**. Καθώς οι συσκευές αναπτύσσονται στο πεδίο για μεγάλα χρονικά διαστήματα (έτη), η ασφάλεια πρέπει να είναι ανθεκτική στο μέλλον. Ο σχεδιασμός ασφάλειας LoRaWAN ακολουθεί τις σύγχρονες αρχές: τη χρήση τυποποιημένων αλγόριθμων και την ασφάλεια από το ένα στο άλλο. Οι βασικές ιδιότητες που υποστηρίζονται στην ασφάλεια LoRaWAN είναι η αμοιβαία πιστοποίηση ταυτότητας, η προστασία ακεραιότητας και η εμπιστευτικότητα.

Ο αμοιβαίος έλεγχος ταυτότητας δημιουργείται μεταξύ μιας τελικής συσκευής LoRaWAN και του δικτύου LoRaWAN ως μέρος της διαδικασίας σύνδεσης στο δίκτυο. Αυτό εξασφαλίζει ότι μόνο γνήσιες και εγκεκριμένες συσκευές θα ενωθούν σε γνήσια και αυθεντικά δίκτυα. Το LoRaWAN MAC και τα μηνύματα εφαρμογών προέρχονται από την αυθεντικότητα, προστατεύονται από την ακεραιότητα, προστατεύονται με επανάληψη και κρυπτογραφούνται. Αυτή η προστασία, σε συνδυασμό με την αμοιβαία αναγνώριση, εξασφαλίζει ότι η κυκλοφορία του δικτύου δεν έχει αλλάξει, προέρχεται από μια νόμιμη συσκευή, δεν είναι κατανοητή για τις υποκλοπές και δεν έχει καταγραφεί και επαναληφθεί από μη εξουσιοδοτημένους χρήστες. Η ασφάλεια LoRaWAN εφαρμόζει περαιτέρω κρυπτογράφηση από άκρο σε άκρο για εφαρμογή στα φορτία που ανταλλάσσονται μεταξύ των τελικών συσκευών και των διακομιστών εφαρμογών.

Το LoRaWAN είναι ένα από τα λίγα δίκτυα IoT που εφαρμόζουν κρυπτογράφηση από άκρο σε άκρο. Σε ορισμένα παραδοσιακά κυψελοειδή δίκτυα, η κυκλοφορία κρυπτογραφείται μέσω της διασύνδεσης του αέρα, αλλά μεταφέρεται ως απλό κείμενο στο κεντρικό δίκτυο του φορέα

εκμετάλλευσης. Κατά συνέπεια, οι τελικοί χρήστες επιβαρύνονται με την επιλογή, την ανάπτυξη και τη διαχείριση ενός πρόσθετου επιπέδου ασφάλειας (που γενικά εφαρμόζεται από κάποιο είδος VPN ή ασφάλειας κρυπτογράφησης επιπέδου εφαρμογής όπως το TLS). Αυτή η προσέγγιση δεν είναι κατάλληλη για τα LPWAN, όπου τα στρώματα ασφαλείας που βρίσκονται πάνω από την κορυφή προσθέτουν σημαντική πρόσθετη κατανάλωση ενέργειας, πολυπλοκότητα και κόστος.



Εικόνα 19: Ασφάλεια LoRaWAN [54]

Οι μηχανισμοί ασφαλείας που αναφέρθηκαν προηγουμένως βασίζονται στους δοκιμασμένους και τυποποιημένους κρυπτογραφικούς αλγόριθμους AES. Αυτοί οι αλγόριθμοι έχουν αναλυθεί από την κρυπτογραφική κοινότητα εδώ και πολλά χρόνια, έχουν εγκριθεί από το NIST και έχουν υιοθετηθεί ευρέως ως η καλύτερη πρακτική ασφάλειας για περιορισμένους κόμβους και δίκτυα. Κάθε συσκευή LoRaWAN είναι εξατομικευμένη με ένα μοναδικό κλειδί AES 128 bit (που ονομάζεται AppKey) και ένα παγκοσμίως μοναδικό αναγνωριστικό (DevEUI με βάση το EUI-64), και τα δύο χρησιμοποιούνται κατά τη διάρκεια της διαδικασίας επαλήθευσης της συσκευής. Η κατανομή των αναγνωριστικών EUI-64 απαιτεί από τον εκχωρητή να έχει ένα οργανικά μοναδικό αναγνωριστικό από την αρχή εγγραφής του IEEE. Τα δίκτυα LoRaWAN ταυτοποιούνται ταυτόχρονα με ένα παγκόσμιο μοναδικό αναγνωριστικό 24 bit που έχει ανατεθεί από το LoRa Alliance ™.

Τα φορτία εφαρμογών LoRaWAN ™ είναι πάντα κρυπτογραφημένα από άκρο σε άκρο μεταξύ της τελικής συσκευής και του διακομιστή εφαρμογών. Η προστασία ακεραιότητας παρέχεται με τη μορφή του hop-by-hop: ένα χτύπημα στον αέρα μέσω της προστασίας ακεραιότητας που παρέχεται από το πρωτόκολλο LoRaWAN και του άλλου hop μεταξύ του δικτύου και του διακομιστή εφαρμογών χρησιμοποιώντας ασφαλή λύσεις μεταφοράς όπως HTTPS και VPN. [48]

3.5 Ασφάλεια στις Οπτικές Τεχνολογίες

Όπως αναφέρθηκε και στο προηγούμενο κεφάλαιο, οι ραγδαίες εξελίξεις στον τομέα των οπτικών τεχνολογιών, με τη μορφή τεχνολογιών όπως η Li-Fi και η BiDi της Cisco, θα μπορούσαν να είναι μια σημαντική ανακάλυψη στην ανάπτυξη του IoT. Μία από τις ελλείψεις του Li-Fi μπορεί επίσης να θεωρηθεί ως δύναμη. Επειδή χρησιμοποιεί το φάσμα ορατού φωτός, το Li-Fi δεν μπορεί να διεισδύσει σε τοίχο. Σε πολλά σενάρια αυτό είναι ένα πρόβλημα, αλλά για ασφαλείς συνδέσεις είναι ένα πλεονέκτημα. Ο Haas δήλωσε ότι τα άτομα που ενδιαφέρονται για την ασφάλεια, ιδιαίτερα τον

στρατό, όπως η ιδέα να είναι σε θέση να δημιουργήσουν ένα ασύρματο δίκτυο το οποίο μπορεί να κλειδωθεί σε μια αίθουσα, εφόσον οι τοίχοι δεν έχουν παράθυρα.

Ο Oswal επισημαίνει ότι “η Cisco βρίσκεται ακόμα σε εξερευνητική φάση με τη Li-Fi και δεν έχει λάβει καμία απόφαση για το τι θα κάνει εμπορικά με την τεχνολογία. Η εταιρεία πιστεύει ότι οι εγκαταστάσεις Li-Fi θα ξεκινήσουν σε εξειδικευμένες αγορές όπου η ασφάλεια και η ασφάλεια είναι καθοριστικής σημασίας”. [49]

3.6 Ασφάλεια Cloud Computing

Για όλες τις υπηρεσίες cloud, έτσι και για την ασφάλεια cloud computing, έχουν εφαρμοστεί κάποιοι μέθοδοι οι οποίοι φαίνεται να λειτουργούν καλά. Μία μέθοδος είναι η καλή χρήση δικαιωμάτων των χρηστών (π.χ. Admin) με ισχυρούς κωδικούς πρόσβασης, μία άλλη είναι η είναι η μέθοδος SSL και άλλοι. Σημαντικό ρόλο παίζουν και οι πιστοποιήσεις από προμηθευτές cloud υπηρεσιών όπου το επίπεδο ασφαλείας γίνεται πολύ ανώτερο και δυσκολότερο να παραβιαστεί. Οι cloud υπηρεσίες χρησιμοποιούν αλγορίθμους κρυπτογράφησης οι οποίοι έχουν θεωρηθεί ότι είναι δύσκολο να παραβιαστούν, κάνουν δηλαδή δύσκολη τη δουλειά του παραβάτη.

Εικόνα 20: Ασφάλεια Cloud Computing [55]

Επιπλέον, για επαγγελματική χρήση τα επίπεδα της ασφάλειας είναι αυστηρότερα μιας και απαιτείται η αγορά μιας υπηρεσίας, η οποία θα προσφέρει υψηλά επίπεδα ασφάλειας στον επαγγελματία. Ακόμη, σε τέτοιες περιπτώσεις πρέπει να ληφθεί υπόψη πως το cloud δεν είναι μόνο λογισμικό, είναι και οι υπηρεσίες που παρέχονται από τον πάροχο. Κάποιες τέτοιες υπηρεσίες ενός λογισμικού οι οποίες πρέπει να παρέχονται από τον πάροχο είναι: ενημερώσεις σε νέες εκδόσεις, οι νέες εκδόσεις για το σύστημα λογισμικού (για οποιοδήποτε λειτουργικό σύστημα υποστηρίζουν), το καθημερινό backup για διαφύλαξη των αρχείων, ο έλεγχος υγείας (health- checks) όλων των επιμέρους συστημάτων, η συντήρηση των servers, έτσι ώστε να διατηρηθεί η ακεραιότητα των επιπέδων ασφαλείας.

Τα επίπεδα ασφάλειας όμως αυτά μπορεί να μην είναι αρκετά για τα επαγγελματικά δεδομένα τα οποία είναι υψίστης σημασίας να παραμένουν εμπιστευτικά. Αυτό σημαίνει ότι όσο ασφαλές και αν είναι το cloud σήμερα, δεν είναι η καλύτερη λύση που θα μπορούσε να βρει ένα επαγγελματίας σε ότι

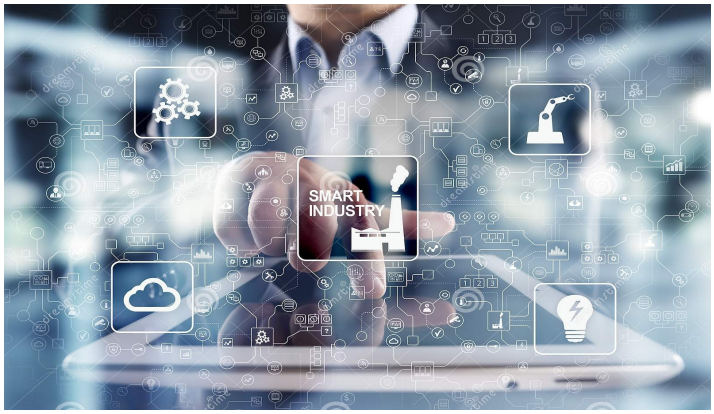
αφορά τα δεδομένα της δουλειάς του. Ειδικά στη σημερινή εποχή όπου η εταιρική κατασκοπία και ο ανταγωνισμός βρίσκονται σε έξαρση, μια αδυναμία στην προστασία των επαγγελματικών δεδομένων είναι αρκετή για να στοχοποιηθεί και να υποκλεπτούν τα δεδομένα της επιχείρησης. Αξίζει να σημειωθεί επίσης ότι στις σύγχρονες εποχές η πρόσβαση στο διαδίκτυο είναι εύκολη και άμεση σε οποιοδήποτε σημείο και αν βρισκόμαστε. Αυτό βρίσκει εύπορο έδαφος για την υποκλοπή και την παραβίαση δεδομένων. Αυτό σημαίνει ότι η χρήση του Cloud Computing είναι καλό να εφαρμόζεται και να χρησιμοποιείται ωστόσο καλό θα ήταν να αποφεύγεται όταν πρόκειται για επαγγελματικούς σκοπούς. [50]

ΚΕΦΑΛΑΙΟ 4: ΠΕΔΙΑ ΕΦΑΡΜΟΓΗΣ

Η ανάμειξη της τεχνολογίας IoT με το Cloud Computing, τα Big Data (ανάλυση τεράστιων όγκων δεδομένων) και των φορητών συσκευών (ηλεκτρονικές συσκευές που χρησιμοποιούν οι χρήστες) δημιουργεί ένα έξυπνο περιβάλλον όπου μπορούν να συνδεθούν όλες οι συσκευές μεταξύ τους και να δημιουργηθούν νέες υπηρεσίες και να δωθούν νέες δυνατότητες σε συνδυασμό με τις υπάρχουσες τεχνολογίες. Ερευνώντας την εφαρμογή του IoT στο πεδίο της αγοράς διαπιστώνεται ότι απευθύνεται *σε κάθε επιχειρηματικό κλάδο* όπως βιομηχανική παραγωγή, κατασκευές, μεταφορές, διαχείριση ενέργειας, εφοδιαστική αλυσίδα κ.α.

4.1 Έξυπνη Βιομηχανία

Το IoT στη βιομηχανία παρέχει αυτόματες διαδικασίες αναγνώρισης προϊόντων μέσω ετικετών ραδιοσυχνοτήτων RFID, συντήρησης των μηχανημάτων μέσω των συνδεδεμένων αισθητήρων επιτρέποντας την παρακολούθηση σε πραγματικό χρόνο, της καλής λειτουργίας και της απόδοσης του εξοπλισμού του εργοστασίου και παραγωγή προϊόντων. [56]



Εικόνα 21:Smart Industry [63]

4.2 Έξυπνη Γεωργία, Αυτοκινητοβιομηχανία

Στο τομέα της κτηνοτροφίας το IoT χρησιμεύει στην παρακολούθηση της αλυσίδας προσφοράς τροφίμων, στην παρακολούθηση των ζώων, στην φυτοπροστασία με σκοπό τον έλεγχο των συνθηκών των φυτών προκειμένου να παρθεί η μέγιστη απόδοση καλλιεργειών καθώς και την παρακολούθηση της φάρμας των ζώων για να διασφαλιστεί η επιβίωση και η υγεία των ζώων.

- **Έξυπνο σύστημα άρδευσης.**

Το έξυπνο σύστημα άρδευσης είναι υπεύθυνο να ενημερώνει τον χρήστη (τον γεωργό) καθημερινά για τη συχνότητα του ποτίσματος, σύμφωνα με την υγρασία του εδάφους και τις μετεωρολογικές προγνώσεις. Για να μετρηθεί η υγρασία του εδάφους χρησιμοποιούνται μετρητές υγρασίας. Οι μετρητές υγρασίας συνδέονται ανά ομάδες μέσω καλωδίων με κεραίες, οι οποίες

μεταδίδουν τα δεδομένα ασύρματα σ’ έναν server. Εκεί το αντίστοιχο λογισμικό επεξεργάζεται τις μετρήσεις για την υγρασία στο έδαφος συνδυάζοντάς τες με τις πληροφορίες για τις καιρικές συνθήκες που θα επικρατήσουν στο χωράφι τις επόμενες ώρες. Το λογισμικό συμβουλεύεται επίσης ένα ηλεκτρονικό αρχείο που περιέχει στοιχεία για τη συγκεκριμένη καλλιέργεια όπου είναι εγκατεστημένο το σύστημα. Τα στοιχεία αυτά έχουν να κάνουν με το πόσο νερό χρειάζεται η εν λόγω καλλιέργεια στις διάφορες φάσεις ανάπτυξής της, αφού οι ανάγκες σε άρδευση μεταβάλλονται ανάλογα με την ηλικία των φυτών. Από όλα τα παραπάνω, οι αλγόριθμοι μπορούν να συμπεράνουν αν το χωράφι χρειάζεται ή όχι πότισμα και πόσο, εμφανίζοντας τις σχετικές πληροφορίες στον υπολογιστή ή το τηλέφωνο του χρήστη.

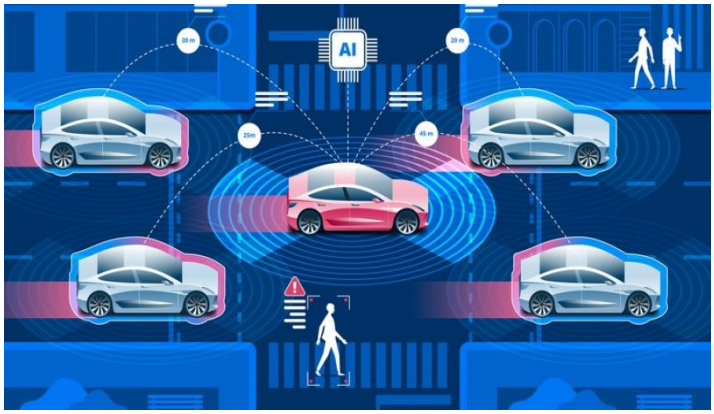
Εικόνα 22: Χρησιμοποίηση ενός κινητού τηλεφώνου για καλλιέργεια σοδιάς [64]

- **Το Internet of Things στο αμπέλι**

Το έξυπνο σύστημα καταγράφει τα θρεπτικά συστατικά του χώματος, την υγρασία και τη θερμοκρασία εδάφους και αέρα, την ένταση των ανέμων, την ώρα και την ένταση της ηλιοφάνειας και μεταδίδει τα δεδομένα στο Cloud. Μέσω ειδικής εφαρμογής ο καλλιεργητής παρακολουθεί τα πάντα στην οθόνη του κινητού του. [57]

Στη συνέχεια, θα αναφερθούμε για την εφαρμογή του IoT στις αυτοκινητοβιομηχανίες. Ο στόχος του έξυπνου αυτοκινήτου είναι η σύνδεση του αυτοκινήτου στο σύστημα IoT, και ο διαμοιρασμός δεδομένων και πληροφοριών μεταξύ των συσκευών, με στόχο την δημιουργία καλύτερων εμπειριών για τους χρήστες, είτε βρίσκονται στον δρόμο, είτε στο σπίτι τους. Για παράδειγμα, η εταιρεία κατασκευής ελαστικών Continental δημιούργησε μια σειρά αισθητήρων που θα βρίσκονται ενσωματωμένοι στα ελαστικά του αυτοκινήτου και θα ελέγχουν την πίεση του αέρα, το φορτίο και την κατάσταση του ελαστικού πέλματος. Το «έξυπνο» αυτό σύστημα παρακολουθεί τις αλλαγές στην κατάσταση των ελαστικών με το πέρασμα του χρόνου και έχει τη δυνατότητα να ειδοποιεί τον οδηγό όταν τα λάστιχα χρειάζονται αντικατάσταση. Σημαντική διευκόλυνση κάθε οδηγού και κυρίως στις μεγάλες πόλεις αποτελεί ο αισθητήρας στάθμευσης ο οποίος είναι τοποθετημένος στο οδόστρωμα και προειδοποιεί τον οδηγό αν η θέση parking είναι ελεύθερη. Επιπρόσθετα, αισθητήρες στο μπροστινό και στο πίσω μέρος του αυτοκινήτου βοηθούν στη

συνεργασία οχήματος με όχημα ώστε να κρατιούνται οι κατάλληλες αποστάσεις. Τέλος οδικές υπηρεσίες πληροφοριών μπορούν να παρέχονται. [58]



Εικόνα 23: Ικανότητα αυτοκινήτου να αναγνωρίζει τους ανθρώπους και άλλα αυτοκινήτα γύρω του [65]

4.3 Ο τομέας της έξυπνης ενέργειας (SmartGrids)

Ο τομέας της έξυπνης ενέργειας περιλαμβάνει τα έξυπνα δίκτυα, τους έξυπνους μετρητές, το έξυπνο νερό, αλλά και την έξυπνη διαχείριση σκουπιδιών. Η αποκομιδή των απορριμμάτων αποτελεί ένα διαχρονικό πρόβλημα στα μεγάλα αστικά κέντρα, ιδιαίτερα σε περιοχές με πολύ πυκνό πληθυσμό. Σε μία έξυπνη πόλη, οι κάδοι έχουν ενσωματωμένους αισθητήρες, ώστε να ειδοποιούνται αυτόματα οι αρμόδιοι φορείς όταν υπάρχει ανάγκη. Τα ευφυή συστήματα μέτρησης συλλέγουν όλες τις απαιραίτητες πληροφορίες και εξάγουν συμπεράσματα.

Εικόνα 24: Smart Energy [66]

Αυτό το έξυπνο δίκτυο είναι ένα δισδιάστατο δίκτυο παροχής ηλεκτρικής ενέργειας όπου συνδυάζει πληροφορίες από τους χρήστες με σκοπό την αποτελεσματική και οικονομικότερη παροχή ηλεκτρικής ενέργειας. Σκοπός αποτελεί η έξυπνη παραγωγή, διανομή και χρήση της ενέργειας. [59]

4.4 Εφαρμογές του IoT στον ιατρικό κλάδο

Η παρακολούθηση του ιστορικού της υγείας των ανθρώπων είναι μια άλλη εφαρμογή του IoT. Το IoT στην ιατρικό τομέα αποκτά ιδιαίτερη σημασία μιας και μπορεί να βοηθήσει τον άνθρωπο

στη βελτίωση της υγείας του άρα και της ζωής του γενικότερα. Πιο συγκεκριμένα, θα παρέχεται η δυνατότητα μέσω αισθητήρων να παρακολουθείται η κατάσταση της υγείας του χρήστη σε σημεία ζωτικής σημασίας του ανθρώπου (π.χ. Υπολογισμός του σφυγμού, της θερμοκρασίας, της πίεσης). Επίσης, θα παρέχεται η δυνατότητα παρακολούθησης της φαρμακευτικής αγωγής του ασθενή, έτσι ώστε να είναι πιο άμεση η ενημέρωση του γιατρού. Τα συστήματα αυτά μπορούν να χρησιμοποιηθούν στα νοσοκομεία, στο σπίτι του ασθενή, στα ιατρεία καθώς και στη φροντίδα ηλικιωμένων. Με την επέκταση ηλεκτρονικών αυτών υπηρεσιών, που χρησιμοποιούνται άμεσα από τους πολίτες, έχουν ως στόχο την βελτίωση της καθημερινότητας των ανθρώπων κάνοντας την πιο λειτουργική και αποδοτική. [60]

Εικόνα 25: Εφαρμογή του Internet of Things στην ιατρική και την υγεία [67]

4.5 Έξυπνες πόλεις

Οι ευφυείς πόλεις υπόσχονται μέγιστη **ασφάλεια** και **αποτελεσματικότητα** για το σύνολο των κατοίκων τους. Αισθητήρες τοποθετημένοι στα αυτοκίνητα, τα φώτα των οδικών αξόνων, ακόμα και στους κάδους απορριμμάτων συλλέγουν δεδομένα με στόχο τη μείωση του ενεργειακού κόστους και την παροχή καλύτερων υπηρεσιών σε άτομα και επιχειρήσεις. Αφορά κυρίως τη βελτίωση των πόλεων στην επίλυση προβλημάτων. Παρακάτω θα δοθούν τρία παραδείγματα ο *έξυπνος φωτισμός*, η *έξυπνη εξυπηρέτηση ατόμων με ειδικές ανάγκες* και οι *έξυπνες στάσεις* δείχνοντας την υψηλή σημασία της εξέλιξης και της χρήσης του IoT.

- **Έξυπνη φωταγώγηση (Smart Lighting)**

Η εξύπνη φωταγώγηση πρόκειται να χρησιμοποιηθεί στη διαχείριση της δημόσιας φωταγώγισης. Θα συλλέγονται δεδομένα από αισθητήρες φωτός, βροχής και κίνησης και σύμφωνα με τα δεδομένα αυτά θα καθορίζεται το άναμμα και το σβήσιμο της δημόσιας φωταγώγησης.Κάποιες επιπλέον δυνατότητες που θα μπορούσαν να εφαρμοστούν είναι να διαφοροποιείται το σύστημα σε κατοικημένες και σε μη κατοικημένες περιοχέςκαθώς επίσης και η προσαρμοσμένη συμπεριφορά του συστήματος σε περιπτώσεις έκτακτης ανάγκης. Επίσης, σε κάθε συσκευή θα υπάρχουν αισθητήρες φωτός, κίνησης και υγρασίας για τη ρύθμιση των λαμπτήρων, ενώ κάθε επιμέρους συσκευή θα συνδέεται σε ένα gateway, όπου θα γίνεται η αποστολή των δεδομένων που έχουν συλλεχθεί από τους

αισθητήρες. Αυτό θα συμβεί έτσι ώστε να πραγματοποιηθεί η συγκέντρωσή τους σε βάση δεδομένων, η επεξεργασία και η παροχή ή η παρουσίασή τους σε οποιοδήποτε το επιθυμεί.

Εικόνα 26: Απεικόνιση μιας έξυπνης πόλης [68]

- **Οι πόλεις με IoT εξυπηρετούν τα άτομα με ειδικές ανάγκες**

Επιπλέον, οι πόλεις με την τεχνολογία IoT είναι πολύ φιλικές για τα άτομα με ειδικές ανάγκες. Για παράδειγμα, τα κινητά αξιοποιώντας την beacon τεχνολογία θα παρέχουν οδηγίες στους χρήστες που έχουν προβλήματα στην όραση για το πώς θα φτάσουν στον προορισμό τους. Επίσης, θα δίνεται η δυνατότητα σε ένα άτομο με κινητικά προβλήματα που μετακινείται χρησιμοποιώντας το αναπηρικό του αμαξίδιο, να ενημερώνεται (μέσω του κινητού του τηλεφώνου) για δρόμους που είναι κατάλληλοι για άτομα με αμαπηρικό αμαξίδιο. Επίσης, θα δίνεται η δυνατότητα σε άτομα με ειδικές ανάγκες να ενημερώνονται για όλα τα εστιατόρια, ξενοδοχεία, super market κλπ όπου διαθέτουν θέσεις παρκαρίσματος για άτομα με ειδικές ανάγκες. Με τον τρόπο αυτό, η ζωή των ανθρώπων αυτών θα γίνει ευκολότερη και καλύτερη.

- **Έξυπνες στάσεις**

Οι «έξυπνες» στάσεις θα παρέχουν ακριβής πληροφόρηση, με ακρίβεια δευτερολέπτου, σε ότι αφορά τα δρομολόγια. Αυτό αποτελεί μία πολύ βασική λειτουργία για τις σύγχρονες κοινωνίες, αφού οι ρυθμοί ζωής είναι πολύ πιο γρήγοροι σε σχέση με παλαιότερα και η ακρίβεια δευτερολέπτου καθίσταται ιδιαίτερα σημαντική. Πολλά άτομα στις σύγχρονες κοινωνίες χρησιμοποιούν στην καθημερινή τους ζωή τα μέσα μαζικής μεταφοράς, αντί για δικός τους μεταφορικό μέσο, οπότε οι “έξυπνες” στάσεις θα έχουν καθοριστική σημασία στη ζωή αυτών των ανθρώπων.

Τέλος, εντός του μέσου μαζικής μεταφοράς θα δίνεται η δυνατότητα να ενημερώνεται ο επιβάτης για την τοποθεσία του οχήματος εκείνη τη στιγμή, για τις επόμενες στάσεις που πρόκειται να ακολουθήσουν, για την πορεία της διαδρομής συνολικά καθώς και για κάποιες σημαντικές ανακοινώσεις υψίστης σημασίας. [61]

Εικόνα 27: Απεικόνιση μιας έξυπνης στάσης [69]

4.6 Έξυπνο σπίτι/Οικιακοί αυτοματισμοί

Το έξυπνο σπίτι αφορά την σύνδεση όλων των λευκών συσκευών του σπιτιού αλλά και των ηλεκτρονικών συσκευών μέσω διαδικτύου και την αποδοτική διασύνδεσή τους. Εκτός αυτού όμως, ανάλογα με τις καθημερινές ανάγκες και συνήθειες που έχει ο εκάστοτε χρήστης (ιδιοκτήτης του σπιτιού) δίνεται η δυνατότητα να αυτοματιστούν οι παραπάνω συσκευές με την ομαδοποίηση και την οργάνωση της λειτουργίας της οικίας του χρήστη. Επίσης, υπάρχει δυνατότητα ο χρήστης να μπορεί να παρακολουθεί και να διαχειρίζεται όλους τους χώρους και τις εγκαταστάσεις της οικίας του με οποιοδήποτε τρόπο επικοινωνίας όπως μέσω σταθερού τηλεφώνου, κινητού τηλεφώνου και διαδικτύου.

Κάποιες από τις **λειτουργίες ενός έξυπνου σπιτιού** είναι:

- Έλεγχος φωτισμού
- Κεντρικό σύστημα συναγερμού και θέρμανσης
- Κεντρικό σύστημα διανομής εικόνας και ήχου
- Δίκτυο οικιακών συσκευών: με τη χρήση της «έξυπνης» πρίζας προσαρμόζεται και ρυθμίζεται απλά και εύκολα η λειτουργία των συσκευών. Ουσιαστικά με το πάτημα ενός κουμπιού π.χ. από το κινητό μας τηλέφωνο μέσω Wi-Fi μπορούμε να συνδέσουμε οτιδήποτε: από καφετιέρα μέχρι τηλεόραση και λαμπτήρες και έτσι να ελέγχουμε πότε θα ενεργοποιηθεί ή θα απενεργοποιηθεί η κάθε συσκευή που βρίσκεται στο σπίτι μας.
- Απομακρυσμένη παρακολούθηση κλειδαριών
- Διαχείριση ενέργειας
- Σύστημα ποτίσματος
- Έλεγχος ζεστού νερού
- Έλεγχος ψυγείου – Έξυπνα ψυγεία. [62]

ΚΕΦΑΛΑΙΟ 5: ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερέροντας, το IoT στις μέρες μας παίζει καθοριστικό ρόλο, μιας και ήδη έχουν αρχίσει να εφαρμόζονται πολλά από τα αναφερόμενα πεδία εφαρμογής του IoT, όπως παραδείγματος χάριν: το έξυπνο σπίτι, οι έξυπνες στάσεις λεωφορείων, η έξυπνη ενέργεια κλπ και ενδέχεται να εξελιχθεί ακόμα περισσότερο τα επόμενα χρόνια. Το IoT εφαρμόζεται τα τελευταία χρόνια όμως είχε αρχίσει να υφίσταται από τις αρχές του 1950. Κάθε δεκαετία φαίνεται ότι χρησιμοποιεί όλο και περισσότερα πεδία εφαρμογής (από τις αρχές του 1950 έως σήμερα). Το “Διαδίκτυο των πραγμάτων” έχει ως βασικό σκοπό του να **διευκολύνει την ζωή των ανθρώπων** όπου λόγω των ραγδαίων εξελίξεων και των γρήγορων ρυθμών ζωής δυσκολεύονται να έρθουν αντιμέτωποι με προβλήματα της καθημερινότητάς τους.

Όπως και σε οποιαδήποτε άλλη τεχνολογία, καθοριστικό ρόλο παίζει και η **ασφάλεια**. Από την πρώτη στιγμή που εμφανίστηκε το IoT δώθηκε ιδιαίτερη έμφαση στην ασφάλεια που θα παρέχει στους χρήστες από κάθε άποψη. Η επιτυχία σε οποιαδήποτε τεχνολογία βασίζεται στη δυνατότητα που θα παρέχει στην ασφάλεια των χρηστών, για αυτό και το IoT έχει ακόμη και στις μέρες μας τόσο υψηλή απήχηση, και ενδέχεται να έχει ακόμα μεγαλύτερη στο μέλλον. Για αυτό και η ασφάλεια διασφαλίστηκε σε κάθε κλάδο της τεχνολογίας αυτής.

Το IoT δεν θα είχε λόγω ύπαρξης αν δεν υπήρχαν τα αντίστοιχα πρωτόκολλα ώστε να μπορέσουν να το υποστηρίξουν. Τα πιο σημαντικά πρωτόκολλα που χρησιμοποιούνται γενικότερα στο διαδίκτυο και εφαρμόζονται και στο IoT είναι το IP, το TCP, το UDP καθώς και όχι και τόσο γνωστά πρωτόκολλα αλλά εξίσου σημαντικά ,όπως είναι το XMPP, το AMP και το AMQP. Τέλος, αξίζει να σημειωθεί ότι τα πρωτόκολλα παρουσιάζουν πολλές διαφορές αλλά και ομοιότητες μεταξύ τους, αλλά όλα αυτά σε συνδυασμό μπορούν να χρησιμοποιηθούν αποδοτικά για την καλύτερη επικοινωνία και αξιοποίηση των πόρων για το IoT, οπότε και για την βελτίωση του τρόπου ζωής και υγείας των ανθρώπων.

Βιβλιογραφία

[1]:Διαδίκτυο των πραγμάτων

[3]:https://www.researchgate.net/profile/Muhammad_Farooq75/publication/273693976_A_Review_on_Internet_of_Things_IoT/links/5508ac290cf26ff55f83af53.pdf

[5]:Το internet of things στον τομεα της υγείας

[7]:IoT in Transportation: Benefits, Challenges and Uses

[8]:Πώς αλλάζει το λιανικό εμπόριο η τεχνητή νοημοσύνη

[9]:IoT History Paper by Tasos Reality - issuu

[10]:(PDF) Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges

[11]:Device-to-device

[12]:Overview of Internet of Things | Solutions

[13]:IoT devices and gateways

[19]:Back-End Data-Sharing Model [10] | Download Scientific Diagram

[20]:What is IoT devices (internet of things devices)? - Definition from WhatIs.com

[21]:LoRaWAN Architecture

[22]:Internet of things

[23]:WiMAX

[24]:Ασύρματο δίκτυο αισθητήρων

[25]:Communications of the ACM

[28]:Optical networking

[29]:IPv4

[30]:IPv6

[31]:4A-4 TCP and UDP Performance over a Wireless LAN

[32]:TCP vs. UDP: Understanding the Difference

[33]:Πρωτόκολλο Ελέγχου Μεταφοράς

[34]:UDP

[35]:Extensible Messaging and Presence Protocol

[36]:https://amp-protocol.net/

[37]:Advanced Message Queuing Protocol

[38]:Ασφάλεια στο διαδίκτυο των πραγμάτων (IoT)

[44]:Το Internet of Things απειλεί την ασφάλεια

[45]:Επίθεση man-in-the-middle

[46]:Radio-frequency identification

[47]:Ασφάλεια στα Δίκτυα Ασυρμάτων Αισθητήρων

[48]:LoRaWAN™ SECURITY

[49]:Optical Network Security

[50]:http://okeanis.lib2.uniwa.gr/xmlui/bitstream/handle/123456789/4344/cse_32895.pdf?sequence=1&isAllowed=y

[56]:Τι να περιμένουμε από τη βιομηχανία του Internet of Things

[57]:Η σημασία των τεχνολογιών IoT στην έξυπνη γεωργία

[58]:IoT - The future DNA of Automobile Industry

[59]:Smart grid

[60]:Το internet of things στον τομεα της υγείας

[61]:Smart city

[62]:Smart home technology

Εικόνες:

[2]:https://www.google.com/search?q=IOT&safe=active&sxsrf=ALeKk00T8ylYFPXjw-fD16DQ_cgG-x-fEg:1584982742174&source=lnms&tbm=isch&sa=X&ved=2ahUKEwij6cnqiLHoAhUxVd8KHVqoCFEQ_AUoAnoECBMQBA&biw=1533&bih=748#imgrc=7lWBp5648v4CtM (Εικόνα 1)

[4]:https://www.google.com/search?q=%CF%85%CE%B3%CE%B5%CE%B9%CE%BF%CE%BD%CE%BF%CE%BC%CE%B9%CE%BA%CE%B7+%CF%80%CE%B5%CF%81%CE%B9%CE%B8%CE%B1%CE%BB%CF%88%CE%B7+%CE%BA%CE%B1%CE%B9+%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%B9%CE%B5%CF%82+%CF%85%CE%B3%CE%B5%CE%B9%CE%B1%CF%82&safe=active&sxsrf=ALeKk02CvA70xw-u4w4vcL4RdG_hBzrS4Q:1584983063081&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjOq8yDirHoAhVnhuAKHSugAdwQ_AUoA3oECA0QBQ&biw=1533&bih=748#imgrc=ptX9OxDBFHteVM (Εικόνα 2)

[6]:https://www.google.com/search?q=%CE%B1%CF%85%CF%84%CE%BF%CE%BA%CE%B9%CE%BD%CE%B7%CF%84%CE%B1+iot&tbm=isch&ved=2ahUKEwioofCWi7HoAhUWklkKHWTuBV0Q2-cCegQIABAA&oq=%CE%B1%CF%85%CF%84%CE%BF%CE%BA%CE%B9%CE%BD%CE%B7%CF%84%CE%B1+iot&gs_l=img.3...1962.2610..2850...0.0..0.276.539.2-2.....0....1..gws-wiz-img.8DXDP6v1S3I&ei=S-14XujPOZak5gLk3JfoBQ&bih=748&biw=1533&safe=active#imgrc=rW1ONifHMIP1HM (Εικόνα 3)

[14]:https://www.google.com/search?q=device+to+divice+communication&tbm=isch&ved=2ahUKEwiaxuqojbHoAhWR11kKHY35Dr8Q2-cCegQIABAA&oq=device+to+divice+communication&gs_l=img.3...4567.12284..12519...0.0..0.336.7839.1j0j25j3.....0....1..gws-wiz-img.....0..0i131j0j0i30j0i19j0i8i30j0i24.TSAEZy5BHcY&ei=iu94XprZHJGv5wKN87v4Cw&bih=748&biw=1533&safe=active#imgrc=L929hIKQPosvQM (Εικόνα 4)

[15]:https://www.google.com/search?q=device+to+cloud+communication&tbm=isch&ved=2ahUKEwiciPuvjbHoAhUGR1kKHXnyBsYQ2-cCegQIABAA&oq=device+to+cloud+communication&gs_l=img.3..0i7i30.201852.205320..205493...3.0..0.352.2566.2-7j2.....0....1..gws-wiz-img.....0i8i30.Ow6gnNFAdF0&ei=me94XtzXGYaO5QL55JuwDA&bih=748&biw=1533&safe=active#imgrc=Bbr7WGFfhaMbHM (Εικόνα 5)

[16]:https://www.google.com/search?q=device+with+gateway+communication&tbm=isch&ved=2ahUKEwior4CTjrHoAhXG1lkKHTU0BqAQ2-cCegQIABAA&oq=device+with+gateway+communication&gs_l=img.3...215058.222047..222331...3.0..0.330.5291.2-17j2.....0....1..gws-wiz-img.....0i7i30j0i7i5i30j0i8i7i30j0i19j0i7i30i19j0i7i5i30i19j0i5i30i19.lQnpI0ogsSE&ei=afB4XujWB8at5wK16JiACg&bih=748&biw=1533&safe=active#imgrc=uKpryN2zlRCawM (Εικόνα 6)

[17]:https://www.google.com/search?q=LoRaWAN+Architecture&safe=active&sxsrf=ALeKk01KyqUXZGbpBfWAM6jNYGN_i-kIVg:1584985950429&source=lnms&tbm=isch&sa=X&ved=2ahUKEwisl7LklLHoAhX4hHIEHTHkD5YQ_AUoAXoECAsQAw&biw=1533&bih=748#imgrc=-9JVvxFnyEd2TM (Εικόνα 7)

[18]:https://www.google.com/search?q=Back+%E2%80%93+End+%CE%9C%CE%BF%CE%BD%CF%84%CE%AD%CE%BB%CE%BF+%CE%91%CE%BD%CF%84%CE%B1%CE%BB%CE%BB%CE%B1%CE%B3%CE%AE%CF%82+%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD+(Back-end+Data+-+Sharing+Model)&safe=active&sxsrf=ALeKk01GtMsFoGDscl4BASFcIX48WMQfXw:1584984596269&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjI5tbej7HoAhXFhOAKHeCYBjEQ_AUoAXoECAwQAw&biw=1533&bih=748#imgrc=zKYu2CTRv4Z4KM (Εικόνα 8)

[26]:https://www.google.com/search?q=WSN&safe=active&sxsrf=ALeKk01jSa_pIfDcZuvP4q54SV8YojP23g:1585058403953&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjPlPbYorPoAhUPmhQKHfdiDckQ_AUoAXoECAwQAw#imgrc=DzvOl2PFMPyTlM (Εικόνα 9)

[27]:https://www.google.com/search?q=cloud+computing&tbm=isch&ved=2ahUKEwjl5sfZorPoAhVG6aQKHdBOBnoQ2-cCegQIABAA&oq=cloud+computing&gs_l=img.3..0l2j0i30l8.324144.327112..327231...0.0..0.137.1899.3j14.....0....1..gws-

wiz-img.....0..0i131j0i67.9vDkJ5EzkII&ei=ZRJ6XqWgEcbSkwXQnZnQBw&safe=active#imgrc=iE8WM1k5jKVK4M (Εικόνα 10)

[39]:https://www.google.com/search?q=optical+technologies&safe=active&hl=el&sxsrf=ALeKk03JuOGHG95pdffXpu5ycDNT_BVcZg:1585061064559&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiE48zNrLPoAhWvShUIHQ7sB-wQ_AUoAXoECAsQAw&biw=1533&bih=748#imgrc=dlToJ7c67jPGeM (Εικόνα 11)

[40]:https://www.google.com/search?q=ipv4%2C+ipv6+protocol&tbm=isch&ved=2ahUKEwjW_abxwbXoAhULgFkKHbXJA1wQ2-cCegQIABAA&oq=ipv4%2C+ipv6+protocol&gs_l=img.3..0i8i30l2j0i24.1914.6472..6827...0.0..0.368.4487.2-13j3.....0....1..gws-wiz-img.....0j0i7i30j0i8i7i30j0i19j0i7i30i19j0i8i30i19.MAhv9FGtzSk&ei=iD97XtaZA4uA5gK1k4_gBQ&bih=748&biw=1533&safe=active#imgrc=-ktwiHWCCSX3ZM (Εικόνα 12)

[41]:https://www.google.com/search?q=UDP+TCP+&tbm=isch&ved=2ahUKEwjhp_H2wbXoAhWWFFkKHXl9As4Q2-cCegQIABAA&oq=UDP+TCP+&gs_l=img.3..0i19l10.187508.191938..192139...1.0..1.436.2774.3j0j7j1j1.....0....1..gws-wiz-img.....0..0j0i131j0i3j0i67j0i30.A3PoAznjLNQ&ei=kz97XqGSLpap5AL5-onwDA&bih=748&biw=1533&safe=active#imgrc=DLWq4aHdtZ-zFM (Εικόνα 13)

[42]:https://www.google.com/search?q=XMPP+PROTOCOL&tbm=isch&ved=2ahUKEwjP55rWxbXoAhWiV98KHeCJBn8Q2-cCegQIABAA&oq=XMPP+PROTOCOL&gs_l=img.3..0i19l4.858.3830..3999...2.0..0.301.2757.2-9j1.....0....1..gws-wiz-img.-DG6kmpHRok&ei=gEN7Xs-nO6Kv_Qbgk5r4Bw&bih=748&biw=1533&safe=active#imgrc=AvWc7DXJjMImEM (Εικόνα 14)

[43]:https://www.google.com/search?q=CIA+security+iot&tbm=isch&ved=2ahUKEwiPxZ395L_oAhVmMOwKHaiGBNcQ2-cCegQIABAA&oq=CIA+security+iot&gs_lcp=CgNpbWcQA1DAC1jAC2DUC2gAcAB4AIABAIgBAJIBAJgBAKABAaoBC2d3cy13aXotaW1n&sclient=img&ei=gaKAXs-AKubgsAeojZK4DQ&bih=748&biw=1533&safe=active#imgrc=JuqN5ggDmNA63M (Εικόνα 15)

[51]:https://www.google.com/search?q=security+threat+iot&tbm=isch&ved=2ahUKEwjVn5uW5r_oAhXGNuwKHZvIAqwQ2-cCegQIABAA&oq=security+threat+iot&gs_lcp=CgNpbWcQAzIGCAAQCBAeOgQIABATUJRBWOtEYOxFaABwAHgAgAGaAYgBtQOSAQMwLjOYAQCgAQGqAQtnd3Mtd2l6LWltZw&sclient=img&ei=wqOAXtW2H8btsAebkYvgCg&bih=748&biw=1533&safe=active#imgrc=bvOjzDfzV8-sAM (Εικόνα 16)

[52]:https://www.google.com/search?q=man+in+the+middle&tbm=isch&ved=2ahUKEwjr8aSR57_oAhUah6QKHQHfBQUQ2-cCegQIABAA&oq=man+in+the+middle&gs_lcp=CgNpbWcQAzICCAAyAggAMgQIABAeMgQIABAeMgQIABAeMgQIABAeMgQIABAeMgQIABAeOgUIABCDAToGCAAQBRAeUNXTAliL6AJgnOkCaABwAHgAgAG9AYgB3hKSAQQwLjE2mAEAoAEBqgELZ3dzLXdpei1pbWc&sclient=img&ei=xKSAXuv_JZqOkgWBvpco&bih=748&biw=1533&safe=active#imgrc=MNWSERcZnAoo1M (Εικόνα 17)

[53]:https://www.google.com/search?q=%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1+%CF%83%CF%85%CF%83%CE%BA%CE%B5%CF%85%CF%8E%CE%BD&tbm=isch&ved=2ahUKEwji4IOo57_oAhWZ7qQKHTvkDisQ2-cCegQIABAA&oq=%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1+%CF%83%CF%85%CF%83%CE%BA%CE%B5%CF%85%CF%8E%CE%BD&gs_lcp=CgNpbWcQAzoCCAA6BQgAEIMBOgQIABBDOgQIABATOgYIABAIEB46BAgAEBg6BggAEAUQHlD-kwdYj74HYOPDB2gIcAB4AIABkwOIAdcikgEKNC4yMy4xLjEuMZgBAKABAaoBC2d3cy13aXotaW1nsAEA&sclient=img&ei=9KSAXuKWE5ndkwW7yLvYAg&bih=748&biw=1533&safe=active#imgrc=V0IuXFJlP7wVxM(Εικόνα 18)

[54]:https://www.google.com/search?q=lorawan+security&safe=active&sxsrf=ALeKk02mnkh4XK1_jYIxJfgtzRkcAg11oQ:1585490622534&source=lnms&tbm=isch&sa=X&ved=2ahUKEwje-ebq7L_oAhVM5eAKHUu5AUYQ_AUoAXoECAsQAw&biw=1533&bih=748#imgrc=ZyHr7nuhrCFaTM (Εικόνα 19)

[55]:https://www.google.com/search?q=cloud+computing+security&safe=active&sxsrf=ALeKk02LUyHSICvPZ47_dAPIRQgmakVGzA:1585485549825&source=lnms&tbm=isch&sa=X&ved=2ahUKEwjJp_n32b_oAhXZQRUIHRdwDPwQ_AUoAXoECA0QAw&biw=1533&bih=748#imgrc=wDxkKT6PiZMSCM(Εικόνα 20)

[63]:https://www.google.com/search?q=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B2%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%AF%CE%B1&safe=active&sxsrf=ALeKk02WyREYqFfORShynsdAeOlQ3S0X1A:1586719223676&source=lnms&tbm=isch&sa=X&ved=2ahUKEwixxb3dzePoAhVOPJoKHbbwCzQQ_AUoAXoECAsQAw&biw=1533&bih=748#imgrc=kMa_EGHVRk0JTM (Εικόνα 21)

[64]:https://www.google.com/search?q=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B3%CE%B5%CF%89%CF%81%CE%B3%CE%AF%CE%B1&tbm=isch&ved=2ahUKEwi5n6HezePoAhWi1-AKHWrgBbwQ2-cCegQIABAA&oq=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B3%CE%B5%CF%89%CF%81%CE%B3%CE%AF%CE%B1&gs_lcp=CgNpbWcQAzIECAAQGDoCCAA6BAgAEB5Q2dycAljQ-ZwCYNr6nAJoBHAAeAGAAbcBiAH5DZIBBDAuMTKYAQCgAQGqAQtnd3Mtd2l6LWltZw&sclient=img&ei=-WmTXvm-EqKvgwfqwJfgCw&bih=748&biw=1533&safe=active#imgrc=yd7CYAM7AB8JmM (Εικόνα 22)

[65]:https://www.google.com/search?q=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B1%CF%85%CF%84%CE%BF%CE%BA%CE%B9%CE%BD%CE%B7%CF%84%CE%BF%CE%B2%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%AF%CE%B1&tbm=isch&ved=2ahUKEwjk3u-R3-PoAhUMQhoKHbfBCtwQ2-cCegQIABAA&oq=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B1%CF%85%CF%84%CE%BF%CE%BA%CE%B9%CE%BD%CE%B7%CF%84%CE%BF%CE%B2%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%AF%CE%B1&gs_lcp=CgNpbWcQAzoECAAQGDoCCAA6BAgAEB5Q95IKWP3nCmD-6ApoAXAAeACAAdEBiAHCHpIBBjAuMjYuMZgBAKABAaoBC2d3cy13aXotaW1n&sclient=img&ei=OHyTXuTiOYyEabeDq-AN&bih=748&biw=1533&safe=active#imgrc=r9bApVfV07vqHM (Εικόνα 23)

[66]:https://www.google.com/search?q=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B5%CE%BD%CE%AD%CF%81%CE%B3%CE%B5%CE%B9%CE%B1&tbm=isch&ved=2ahUKEwj7kZbn3-PoAhUY44UKHVl6C7gQ2-cCegQIABAA&oq=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CE%B5%CE%BD%CE%AD%CF%81%CE%B3%CE%B5%CE%B9%CE%B1&gs_lcp=CgNpbWcQAzoFCAAQgwE6AggAOgQIABAYOgQIABBDOgQIABAeUPH7CljFmAtgrZkLaAJwAHgAgAGmAYgBsRKSAQQwLjE2mAEAoAEBqgELZ3dzLXdpei1pbWc&sclient=img&ei=63yTXrvwMpjGlwTZ9K3ACw&bih=748&biw=1533&safe=active#imgrc=PjfZzTiGFHTKCM (Εικόνα 24)

[67]:https://www.google.com/search?q=%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82+%CF%84%CE%BF%CF%85+iot+%CF%83%CF%84%CE%BF%CE%BD+%CE%B9%CE%B1%CF%84%CF%81%CE%B9%CE%BA%CF%8C+%CF%84%CE%BF%CE%BC%CE%AD%CE%B1+%CE%BA%CE%B1%CE%B9+%CF%84%CE%B7%CE%BD+%CF%85%CE%B3%CE%B5%CE%AF%CE%B1&tbm=isch&ved=2ahUKEwjL-Ku_4OPoAhVSaBoKHSMQDicQ2-cCegQIABAA&oq=%CE%B5%CF%86%CE%B1%CF%81%CE%BC%CE%BF%CE%B3%CE%AD%CF%82+%CF%84%CE%BF%CF%85+iot+%CF%83%CF%84%CE%BF%CE%BD+%CE%B9%CE%B1%CF%84%CF%81%CE%B9%CE%BA%CF%8C+%CF%84%CE%BF%CE%BC%CE%AD%CE%B1+%CE%BA%CE%B1%CE%B9+%CF%84%CE%B7%CE%BD+%CF%85%CE%B3%CE%B5%CE%AF%CE%B1&gs_lcp=CgNpbWcQAzoECAAQQzoCCAA6BAgAEAM6BQgAEIMBOgQIABAYOgQIABAeOgYIABAFEB5QofkKWPzGC2CLyAtoA3AAeAGAAZUDiAHbPpIBCjEuNTEuMS4wLjGYAQCgAQGqAQtnd3Mtd2l6LWltZ7ABAA&sclient=img&ei=pH2TXsuWLdLQaaOguLgC&bih=748&biw=1533&safe=active#imgrc=Cxwlj4ehIiCKEM&imgdii=-IfMH5HPhaoh_M (Εικόνα 25)

[68]:https://www.google.com/search?q=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CF%80%CF%8C%CE%BB%CE%B7&tbm=isch&ved=2ahUKEwjdiZH54ePoAhUS_hoKHZuABqsQ2-cCegQIABAA&oq=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CF%80%CF%8C%CE%BB%CE%B7&gs_lcp=CgNpbWcQAzIECAAQGDoFCAAQgwE6AggAOgQIABBDOgQIABAeUPggWNwwYKsyaABwAHgAgAGRAogBrA-SAQUwLjkuMpgBAKABAaoBC2d3cy13aXotaW1n&sclient=img&ei=Kn-TXt3MFpL8a5uBmtgK&bih=748&biw=1533&safe=active#imgrc=5udmt9BH13eGYM (Εικόνα 26)

[69]:https://www.google.com/search?q=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CF%80%CF%8C%CE%BB%CE%B7&tbm=isch&ved=2ahUKEwjdiZH54ePoAhUS_hoKHZuABqsQ2-cCegQIABAA&oq=%CE%AD%CE%BE%CF%85%CF%80%CE%BD%CE%B7+%CF%80%CF%8C%CE%BB%CE%B7&gs_lcp=CgNpbWcQAzIECAAQGDoFCAAQgwE6AggAOgQIABBDOgQIABAeUPggWNwwYKsyaABwAHgAgAGRAogBrA-SAQUwLjkuMpgBAKABAaoBC2d3cy13aXotaW1n&sclient=img&ei=Kn-TXt3MFpL8a5uBmtgK&bih=748&biw=1533&safe=active#imgrc=KEkWjsS5YdeaqM (Εικόνα 27)