ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Ανάπτυξη διάταξης ασφαλούς ασύρματου κόμβου για εφαρμογές IIoT βασισμένου σε τεχνολογίες LPWAN

Αδαμαντίδης Κωνσταντίνος Αλέξανδρος
ΑΜ: 50107086

Επιβλέπων Καθηγητής

Παναγιώτης Παπαγέωργας
Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, Σεπτέμβριος, 2022

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

Development of a secure wireless node for IIoT applications based on LPWAN technologies

Adamantidis Konstantinos Alexandros
50107086

Supervisor

Panagiotis Papageorgas

Associate Professor

ATHENS-EGALEO, SEPTEMBER, 2022

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

(Ονοματεπώνυμο), (βαθμίδα)	(Ονοματεπώνυμο), (βαθμίδα)	(Ονοματεπώνυμο), (βαθμίδα)
Παναγιώτης Παπαγέωργας Καθηγητής  Digitally signed by Panagiotis Papageorgas Date: 2022.10.09 19:26:20 +03'00' (Υπογραφή)	Σταύρος Καμινάρης Καθηγητής Stavros Kaminaris Digitally signed by Stavros Kaminaris Date: 2022.10.10 12:53:53 +03'00' (Υπογραφή)	Δημήτριος Πυρομάλης Επίκουρος Καθηγητής Dimitrios Pyromalis Digitally signed by Dimitrios Pyromalis Date: 2022.10.10 10:29:21 +03'00' (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Αδαμαντίδης Κωνσταντίνος Αλέξανδρος του Σάββα , με αριθμό μητρώου 50107086 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι 01/1/2023 και έπειτα από αίτησή μου στη Βιβλιοθήκη και έγκριση του επιβλέποντος καθηγητή.»

Ο Δηλών

Κωνσταντίνος Αλέξανδρος Αδαμαντίδης

Κ. Α. Αδαμαντίδης

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία, εκπονήθηκε στα πλαίσια του προπτυχιακού διπλώματος, Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών του πανεπιστημίου Δυτικής Αττικής. Η εκπόνηση της διπλωματικής εργασίας έγινε υπό την επίβλεψη του καθηγητή Παναγιώτη Παπαγέωργα.

Με αυτή την αφορμή λοιπόν θα ήθελα να τον ευχαριστήσω θερμά για την επίβλεψη αυτής της διπλωματικής εργασίας, και για την αμέριστη συμπαράστασή του καθ' όλη τη διάρκεια της εκπόνησης. Ήταν πάντα διαθέσιμος στο να μου προσφέρει απλόχερα τις γνώσεις και την εμπειρία του πάνω στο θέμα καθώς και να προβαίνει στις απαραίτητες κριτικές ώστε να φτάσει στην τελική της μορφή.

Θα ήθελα ακόμη να ευχαριστήσω θερμά όλους τους συναδέλφους συμφοιτητές μου, οι οποίοι με τα σχόλια, τις κριτικές και τις γνώσεις τους, στάθηκαν δίπλα μου στην αντιμετώπιση των δυσκολιών.

Τέλος ευχαριστίες θέλω να απευθύνω και προς την οικογένειά μου, για την στήριξή τους όλα αυτά τα χρόνια κατά την πραγμάτωση των στόχων μου.

Περίληψη

Η συνεχώς αυξανόμενη συνδεσιμότητα συσκευών στο Διαδίκτυο, αποτελεί στις μέρες μας ένα κρίσιμο θέμα σε διάφορους τομείς της ζωής. Το Διαδίκτυο των Πραγμάτων (IoT) είναι μια έννοια με την οποία περιγράφουμε με απλά λόγια ένα δίκτυο επικοινωνίας αντικειμένων, τα οποία ανταλλάσσουν δεδομένα. Αυτό γίνεται με την προσθήκη ηλεκτρονικών μέσων, λογισμικού και αισθητήρων στα αντικείμενα αυτά, δίνοντάς τους έτσι την δυνατότητα να συλλέγουν δεδομένα από το περιβάλλον τους μέσω απομακρυσμένης πρόσβασης και ελέγχου. Το IoT έχει πληθώρα χρήσεων στο τομέα της ιατρικής περίθαλψης, στο εμπόριο, στο καταναλωτικό τομέα καθώς και στον τομέα παραγωγής που θα μας απασχολήσει στην παρούσα διπλωματική.

Στη βιομηχανική παραγωγή λοιπόν βλέπουμε ότι το Industrial Internet of Things (IIoT) σε συνδυασμό με το Industry 4.0 αναπτύσσονται με ταχείς ρυθμούς και συναντώνται σε όλα τα στάδια μιας παραγωγικής διαδικασίας. Έρευνες δείχνουν ότι πάνω από το 90% των εταιρειών εφάρμοσαν τεχνολογίες IIoT μέχρι το τέλος του 2021.

Με την χρήση του IIoT επομένως, η εποπτεία και ο έλεγχος ενός εργοστασίου περνά σε αυτοματοποιημένα συστήματα, τα οποία απαιτούν ολοένα και λιγότερο την συμμετοχή του ανθρώπινου παράγοντα στην παραγωγική διαδικασία καθώς αυτόματοι, ασύρματοι κόμβοι συλλέγουν και επεξεργάζονται δεδομένα σε πραγματικό χρόνο με στόχο την αύξηση της αποδοτικότητας και ποιότητας των κατασκευαστών.

Η κάλυψη της ασύρματης επικοινωνίας των κόμβων με το IIoT επιτυγχάνεται μέσω της τεχνολογίας Low Power Wide Area Network (LPWAN). Μια τεχνολογία, ασύρματου δικτύου ευρείας περιοχής χαρακτηριστικό της οποίας είναι η μετάδοση δεδομένων σε μεγάλες αποστάσεις με την ελάχιστη δυνατή χρήση ενέργειας. Μια τεχνολογία LPWAN που χρησιμοποιείται τα τελευταία χρόνια στη χώρα μας, είναι η Narrowband-IoT (NB-IoT), η οποία χρησιμοποιεί αδειοδοτημένες ζώνες συχνοτήτων έχοντας σαν κύριο προτέρημα έναντι των άλλων τεχνολογιών την ασφαλέστερη μετάδοση δεδομένων.

Κατά την μετάδοση δεδομένων των ασύρματων κόμβων μέσω της παραπάνω τεχνολογίας εγείρεται το ζήτημα της ασφάλειας και της ακεραιότητας των δεδομένων αυτών, πράγμα που αποτελεί ένα από τα σημαντικότερα ζητήματα στις ασύρματες επικοινωνίες στο IoT. Στη παρούσα εργασία για την επίτευξη της ασφάλειας του κόμβου χρησιμοποιήθηκε πρωτόκολλο εφαρμογής MQTT και το πρωτόκολλο ασφάλειας TLS/SSL όπου με τη χρήση certificates προσφέρεται μία ασφαλής επικοινωνία μεταξύ κόμβου και IoT.

Τέλος θα ασχοληθούμε με την υλοποίηση ενός ασφαλούς ασύρματου κόμβου με τη χρήση ενός μικροελεγκτή arduino, ο οποίος χρησιμοποιώντας το πρωτόκολλο επικοινωνίας NB-IoT και το πρωτόκολλο ασφάλειας TLS/SSL και το πρωτόκολλο εφαρμογής MQTT, έχει προγραμματιστεί να στέλνει μετρήσεις ενός αισθητήρα έχοντας στόχο την ασφαλή και ακέραια μεταφορά δεδομένων σε περιβάλλον IIoT

Λέξεις -Κλειδιά

Ασφάλεια κόμβου, IoT, IIoT, LPWAN, NB-IoT, TLS/SSL, MQTT, LTE, Microcontroller, SIM7000

Abstract

The continuously increasing connectivity of devices to the Internet is nowadays a critical issue in various areas of life. The Internet of Things (IoT) is a meaning that describes in simple terms a network of communicating objects that exchange data. This is done by adding electronic media, software and sensors to these objects, thus enabling them to collect data from their environment through remote access and control. Finally, the IoT has a plenty of uses in the healthcare, commerce, consumer and manufacturing sectors that will be the focus of this thesis.

In industrial production we see that the Industrial Internet of Things (IIoT) in combination with Industry 4.0 are developing rapidly and are encountered at all stages of a production process. Research shows that more than 90% of companies have implemented IIoT technologies by the end of 2021.

With the use of IIoT therefore, the supervision and control of a factory is moving to automated systems, which increasingly require less and less human involvement in the production process as automatic, wireless nodes collect and process data in real time to increase manufacturers' efficiency and quality.

The wireless communication coverage of the nodes with IIoT is achieved through Low Power Wide Area Network (LPWAN) technology. A technology, wireless wide area network characteristic of which is the transmission of data over long distances with minimal power usage. One LPWAN technology used in recent years in our country is Narrowband-IoT (NB-IoT), which uses licensed frequency bands having as main advantage over other technologies the more secure data transmission.

During the transmission of wireless node data via the above technology, the issue of security and integrity of this data arises, which is one of the most important issues in wireless communications in IoT. In this paper in order to achieve node security, MQTT application protocol and TLS/SSL security protocol was used to achieve node security where using certificates a secure communication between node and IoT is offered.

Finally, we will deal with the implementation of a secure wireless node using an arduino microcontroller, which using the NB-IoT communication protocol and the TLS/SSL security protocol and the MQTT application protocol, has been programmed to send measurements of a sensor aiming at secure and integral data transfer in an IIoT environment.

Keywords

IoT, IIoT, NB-IoT, Security, LPWAN, MQTT, LTE, Arduino, SIM7000, Sensor networks, Node-red.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Σχημάτων

Κατάλογος Εικόνων

Αλφαβητικό Ευρετήριο

1) LPWAN Low-power wide-area network
2) PSM power saving mode
3) eDRx extended Discontinuous Reception
4) VoLTE voice over LTE
5) UE user equipment
6) EPS Evolved Packet System
7) NPUSCH Narrowband Physical Upink Shared Channel
8) NPRAC Narrowband Physical Random-Accesss Channel
9) SC-FDMA Single-Carrier Frequency Division Multiple Access
10) NPBCH Narrowband Physical Broadcast Channel
11) NPDCCH Narrowband Physical Downlink Control Channel
12) NPDSCH Narrowband Physical Downlink Shared Channel
13) OFDM Orthogonal Frequency Division Multiplexing
14) TLS Transport Layer Security
15) SSL Secure Sockets Layer
16) TCP transmission Control Protocol
17) HTTP Hypertext Transfer Protocol
18) D2D Device to device
19) QoS Quality of Service
20) IIoT Industrial Internet of Things
21) IoT Internet of Things
22) MaaS Manufacturing as a Service
23) PaaS Product as a Service
24) GNSS Globan navigation satellite system
25) DSSS Direct Sequence Spread Spectrum
26) BFSK binary frequency shift keying
27) IP Internet Protocol
28) PDP packet data protocol
29) APN access point name

ΕΙΣΑΓΩΓΗ

Πρόβλημα- Σημαντικότητα του θέματος

Η παρούσα εργασία έχει ως βασικό αντικείμενο, την μελέτη των ασύρματων δικτύων μεγάλης εμβέλειας χαμηλής ισχύος (LPWAN) καθώς και την υλοποίηση ασφαλούς ασύρματου κόμβου που εξυπηρετεί την ανάγκη βελτιστοποίησης των συστημάτων παρακολούθησης του αυτοματισμού στο τομέα της βιομηχανίας λαμβανομένου υπόψι ότι βρισκόμαστε στην εποχή του Industry 4.0.

Σκοπός – Στόχος

Στόχος της εργασίας είναι, να δείξουμε τα βήματα όπου μια υλοποίηση ασύρματου κόμβου μπορεί να στείλει δεδομένα με ασφάλεια σε περιβάλλον IIoT.

Δομή

Θα ξεκινήσουμε λοιπόν στο πρώτο κεφάλαιο να αναλύσουμε τα μοντέλα επικοινωνίας μιας IoT συσκευής καθώς και την αρχιτεκτονική του διαδικτύου των πραγμάτων (IoT).

Έπειτα θα περάσουμε σε μια ιστορική αναδρομή της βιομηχανικής επανάστασης για να καταλήξουμε στην τέταρτη βιομηχανική επανάσταση (Industry 4.0) με την οποία ορίζεται η ενσωμάτωση λογισμικού αλλά και ενός δικτύου από αισθητήρες σε μηχανές της βιομηχανίας για να επιτευχθεί η παρακολούθηση και ο απομακρυσμένος έλεγχος μηχανών παραγωγής. Το μέσο με το οποίο μια μηχανή παραγωγής του βιομηχανικού τομέα επικοινωνεί με το διαδίκτυο, ονομάζεται Βιομηχανικό Διαδίκτυο των Πραγμάτων (IIoT) το οποίο δεν είναι άλλο από μια εφαρμογή ενός συστήματος Internet of Things στον βιομηχανικό και παραγωγικό κλάδο, το οποίο σε συνδυασμό με την χρήση έξυπνων αισθητήρων παρέχει υψηλό επίπεδο επικοινωνίας με τις μηχανές για την διασφάλιση της ποιότητας και ασφάλειας της διαδικασίας.

Στο επόμενο κεφάλαιο θα παρουσιάσουμε τα χαρακτηριστικά μερικών ασύρματων πρωτόκολλων επικοινωνίας LPWAN όπως NB-IoT, LoRa, Sigfox, LTE-M, καθώς και τα πλεονεκτήματα που παρουσιάζει το καθένα απ αυτά. Από τα παραπάνω πρωτόκολλα επικοινωνίας, επιλέξαμε για την υλοποίηση ασύρματου κόμβου το πρωτόκολλο NB-IoT που φαίνεται να υπερτερεί σε ασφάλεια έναντι των άλλων πρωτοκόλλων.

Η ασφάλεια του ασύρματου κόμβου, αναλύεται στο όγδοο κεφάλαιο και αποτελεί ένα από τα σημαντικότερα ζητήματα στο χώρο του IoT καθώς πολλές συσκευές IoT διαχειρίζονται κρίσιμα δεδομένα στα οποία πρέπει να υπάρχει πρόσβαση μόνο από εξουσιοδοτημένο προσωπικό. Συνεπώς μια ασφαλής επικοινωνία προϋποθέτει ότι οι απεσταλμένες πληροφορίες θα φθάσουν με ασφάλεια και ακεραιότητα δίχως να έχουν

υποστεί κάποια τροποποίηση ή υποκλοπή. Για να επιτύχουμε αυτό τον στόχο χρησιμοποιούμε διάφορα πρωτόκολλα ασφάλειας και τεχνικές κρυπτογράφησης τις οποίες θα αναλύσουμε περαιτέρω.

Τέλος στο ένατο κεφάλαιο παρουσιάζουμε μια υλοποίηση ασύρματου κόμβου με πρωτόκολλο επικοινωνίας NB-IoT και πρωτόκολλο ασφάλειας TLS/SSL που αναλύσαμε σε προηγούμενο κεφάλαιο καθώς και όλα τα υλικά και τον απαραίτητο προγραμματισμό τους προκειμένου να δείξουμε τον τρόπο ασφαλούς μετάδοσης δεδομένων από έναν ασύρματο κόμβο.

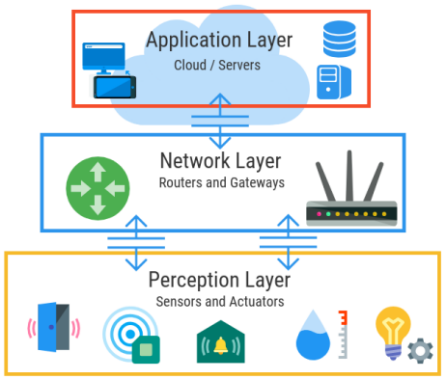
ΚΕΦΑΛΑΙΟ 1: Διαδίκτυο των πραγμάτων (Internet of Things - IoT)

1.1 Ορισμός

Ο όρος Internet of Things χρησιμοποιήθηκε πρώτη φορά στα τέλη της δεκαετίας του 1990 από έναν βρετανό πρωτοπόρο επιστήμονα τον Kevin Ashton, ο όποιος ήταν ένας από τους ιδρυτές του Auto-ID center στο MIT και μέρος μιας ομάδας που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το Διαδίκτυο μέσω μιας ετικέτας RFID (ραδιοσυχνοτήτων), έχοντας ως στόχο την μέτρηση αλλά και τον εντοπισμό προϊόντων χωρίς να είναι απαραίτητη η ανθρωπινή παρέμβαση [3].

Εναλλακτικά με τον όρο διαδίκτυο των πραγμάτων (IoT), ορίζουμε την σύνδεση κάποιων αντικειμένων που χρησιμοποιεί ο άνθρωπος στην καθημερινότητά του με το διαδίκτυο. Η σύνδεση των αντικειμένων με το διαδίκτυο, έχει ως στόχο τον απομακρυσμένο έλεγχο αλλά και την αλληλεπίδραση τους από τον άνθρωπο. Ως αντικείμενα (Things), ορίζουμε τις συσκευές όπου μπορούν να ελεγχθούν μέσω υπολογιστή η κινητού δηλαδή ένα σύνολο αισθητήρων και ελεγκτών που βρίσκονται ενσωματωμένοι πάνω στις συσκευές. Επιπλέον σαν αντικείμενα μπορούμε να θεωρήσουμε και κάποια μηχανήματα στην βιομηχανία . Τέλος, τα αντικείμενα μπορούν να είναι συνδεδεμένα με το διαδίκτυο είτε ενσύρματα είτε ασύρματα συνδυάζοντας διάφορα πρωτόκολλα επικοινωνίας και ασφάλειας[4] .

1.2 Αρχιτεκτονική IoT



Εικόνα 1. Αρχιτεκτονική τριών επίπεδων IoT [4]

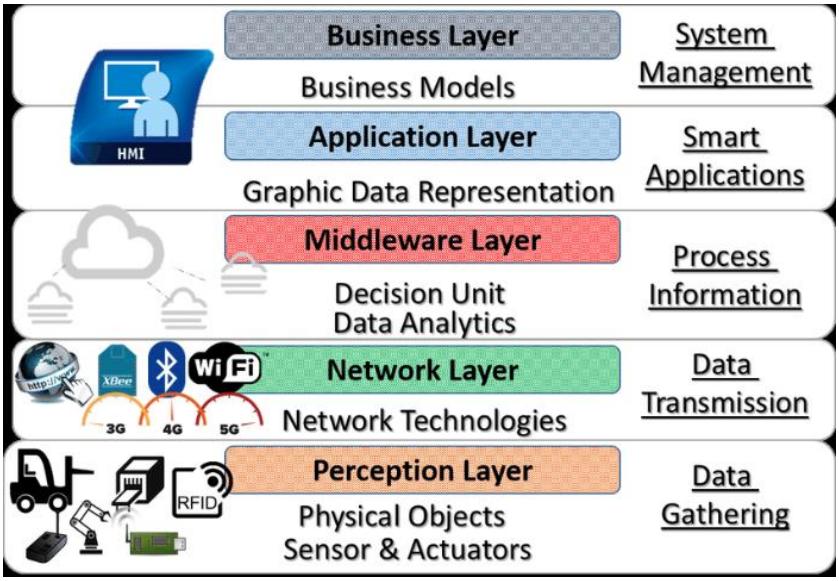
Η επικρατέστερη αρχιτεκτονική συμφώνα με τον Domingo και την Jia διαχωρίζεται σε τρία βασικά επίπεδα :α) το επίπεδο αντίληψης, β) το επίπεδο δικτύου και γ) το επίπεδο υπηρεσιών[4],[20] .

A. **Perception layer (Επίπεδο αντίληψης) :** Στο IoT οι συσκευές μπορούν να συνδεθούν σε ένα δίκτυο ώστε να μπορούν να ελεγχθούν από απόσταση. Έτσι, σκοπός αυτού του επίπεδου είναι η αναγνώριση αντικειμένων και η συλλογή πληροφοριών που μπορούν να ανταλλάσουν αυτόματα πληροφορίες μεταξύ άλλων συσκευών. Το επίπεδο αντίληψης περιλαμβάνει συσκευές που εξοπλίζονται με RFID κάρτες , ενσωματωμένους αισθητήρες , κάμερες , ενεργοποιητές ή ακόμα και GPS. Οι τεχνολογίες αυτές βοηθούν στην ανάπτυξη της ικανότητας του IoT να αντιλαμβάνεται και να αναγνωρίζει πράγματα ή ακόμη και το περιβάλλον. Τέλος σε ορισμένους τομείς της βιομηχανίας, σε κάθε συσκευή ή υπηρεσία που μπορεί να χρειαστεί, αποδίδεται ένα μοναδικό αναγνωριστικό (UUID) που μπορεί να αναγνωριστεί και να ανακτηθεί εύκολα η κάθε συσκευή κάνοντας τα UUID απαραίτητα σε ένα μεγάλο δίκτυο IoT [4],[20].

B. **Network Layer (Επίπεδο δικτύου) :** Ο βασικός ρόλος αυτού του επίπεδου είναι η σύνδεση, η ορθή δρομολόγηση και η μετάδοση των πακέτων όλων των συσκευών και των υπηρεσιών σε ένα δίκτυο. Το επίπεδο δικτύωσης περιλαμβάνει τεχνολογίες δικτύων όπως ασύρματα ή ενσύρματα πρωτοκόλλα επικοινωνίας και τοπικά δίκτυα (LAN). Τα πιο γνωστά πρωτοκόλλα που χρησιμοποιούνται για την μετάδοση, είναι το WiFi ,3G/4G , Bluetooth , Ethernet. Τέλος μπορεί να συγκεντρώνει πληροφορίες ώστε να πραγματοποιεί επεξεργασία και αποθήκευση σε έναν μεγάλο όγκο δεδομένων [4],[20]

C. **Application Layer (επίπεδο εφαρμογής) :** Το επίπεδο εφαρμογής, περιέχει ένα ενδιάμεσο λογισμικό που παρέχει λειτουργίες για την ενσωμάτωση υπηρεσιών και εφαρμογών στο IoT και στο οποίο γίνεται η επεξεργασία δεδομένων από το επίπεδο δικτύου. Το ενδιάμεσο λογισμικό (middleware) περιέχει εφαρμογές που ο χρήστης μπορεί να ελέγξει και να παρακολουθήσει τα έξυπνα αντικείμενα που βρίσκονται στο επίπεδο αντίληψης το όποιο λειτουργεί σαν ενδιάμεσος συνδετικός κρίκος μεταξύ επίπεδου εφαρμογής και δικτύου. Πολλοί υποστηρίζουν ότι το ενδιάμεσο λογισμικό μπορεί να γίνει και ένα ξεχωριστό επίπεδο[4] .

Η International Telecommunica- tion Union υποστηρίζει ότι η αρχιτεκτονική ενός IoT αποτελείται από πέντε διαφορετικά στρώματα τα οποία προσθέτουν δύο ακόμη επίπεδα, μαζί με τα παραπάνω: δ) το επίπεδο ενδιάμεσου λογισμικού και ε) το επίπεδο επιχείρησης.



Εικόνα 2 Αρχιτεκτονική πέντε επίπεδων IoT [20]

D. **Middleware Layer (Επίπεδο Ενδιάμεσου Λογισμικού) :** Το επίπεδο αυτό περιέχει το λογισμικό με το όποιο οι εφαρμογές έχουν πρόσβαση στα δεδομένα τα όποια προέρχονται από τα έξυπνα αντικείμενα . Ακόμη σε αυτό το επίπεδο πραγματοποιούνται λειτουργίες όπως αποθήκευση και επεξεργασία δεδομένων από τις συσκευές . Τέλος το middleware layer αποτελεί συνδετικό κρίκο του επίπεδου εφαρμογής με το επίπεδο δικτύου και παράλληλα ενσωματώνει και τις πλατφόρμες λογισμικού οι οποίες αποτελούν ένα τμήμα αυτού του επίπεδου[20] .

E. **Business Layer (Επίπεδο Επιχείρησης):** Το επίπεδο επιχείρησης, προσφέρει υπηρεσίες όπως, δημιουργία διαγραμμάτων ροής και γραφημάτων καθώς και ανάλυσης των αποτελεσμάτων και του τρόπου βελτίωσης της συσκευής παίρνοντας ως αντάλλαγμα ένα χρηματικό αντίτιμο[20].

1.3 Μοντέλα επικοινωνίας

1.3.1 Device to device

Στο μοντέλο επικοινωνίας, δύο ή περισσότερων IoT συσκευών, η σύνδεσή τους μπορεί να γίνει, χωρίς να υπάρχει απαραίτητα χρήση ενός ενδιάμεσου application server. Οι συσκευές αυτής της κατηγορίας επικοινωνούν μέσω του διαδικτύου, με χρήση της IP διεύθυνσης αλλά και με διάφορα πρωτόκολλα επικοινωνίας όπως το Bluetooth , το ZigBee , το Z-WAVE και το RFID . Η επιλογή του κάθε πρωτόκολλου γίνεται ανάλογα με την κάθε εφαρμογή για την ανταλλαγή μηνυμάτων. Τα πρωτόκολλα που χρησιμοποιούνται για αυτήν την κατηγορία επικοινωνίας, χρησιμοποιούν μικρό ρυθμό μετάδοσης δεδομένων και τα συναντάμε σε οικιακούς αυτοματισμούς που δεν χρειάζονται ιδιαίτερες απαιτήσεις, παραδείγματος χάριν έξυπνες πρίζες , διακόπτες φωτισμού , λαμπτήρες ,θερμοστάτες και κλιματιστικά. Τέλος η επιλογή της κάθε συσκευής πρέπει να γίνει με βάση το κάθε πρωτόκολλο διότι αρκετές εταιρίες χρησιμοποιούν τα δικά τους πρωτόκολλα με κίνδυνο ασυμβατότητας μεταξύ των συσκευών [22].

Εικόνα 3 Μοντέλο επικοινωνίας Device to Device [12]

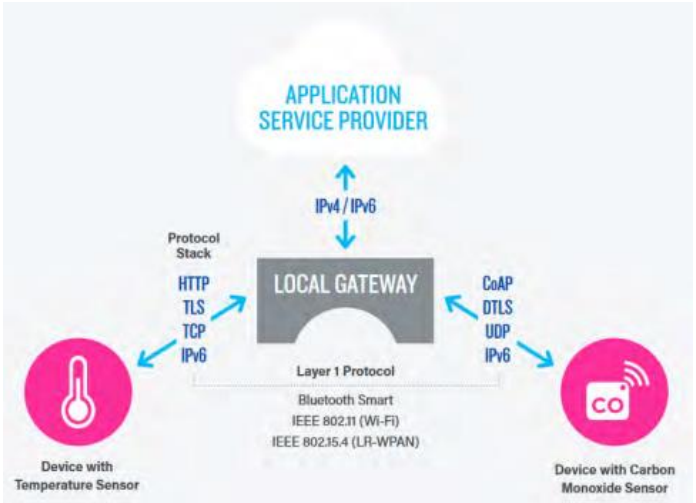
1.3.2 Device to cloud

Στο μοντέλο επικοινωνίας device to cloud, η σύνδεση της IoT συσκευής με το cloud γίνεται με την σύνδεσή της στο διαδίκτυο για την διαχείριση και τον έλεγχο κυκλοφορίας των μηνυμάτων και την ανταλλαγή δεδομένων. Χρησιμοποιώντας ασύρματες ή ενσύρματες μεθόδους, όπως το Wi-Fi και το Ethernet, κάθε συσκευή αποκτά μια μοναδική διεύθυνση δικτύου IP και τα δεδομένα πηγαίνουν σε ένα cloud. Οι συσκευές αυτής της κατηγορίας χρησιμοποιούνται για απομακρυσμένο έλεγχο και για ανάλυση δεδομένων για την χρήση τους . Για παράδειγμα ένας έξυπνος θερμοστάτης τον οποίο μπορούμε να τον ελέγξουμε απομακρυσμένα, μπορεί να μεταδίδει δεδομένα σε ένα cloud, ώστε να γίνεται μια ανάλυση κατανάλωσης ενεργείας του σπιτιού [22] .

Εικόνα 4 Μοντέλο επικοινωνίας Device to Cloud [12]

1.3.3 Device to Gateway

Η σύνδεση της IoT συσκευής και της cloud υπηρεσίας, γίνεται μέσω μιας ALG υπηρεσίας, στην οποία υπάρχει μια ενδιάμεση συσκευή gateway και ένα application software τα οποία λειτουργούν ως μεσολαβητής. Όταν η σύνδεση των συσκευών δεν γίνεται μέσω διαδικτύου, χρησιμοποιούνται τα πρωτόκολλα επικοινωνίας Bluetooth και το ZigBee (εκτός του ZigBee 3.0) παρέχοντας έτσι ασφάλεια. Για παράδειγμα, ένα μοντέλο device to gateway είναι σε μια βιομηχανία που χρησιμοποιεί κόμβους, οι κόμβοι στέλνουν τα δεδομένα τους στις πύλες GWs, και τα GWs στέλνουν τα δεδομένα στο cloud . Οι πύλες IoT έχουν σχεδιαστεί για την ταυτόχρονη εκτέλεση πολλών εργασιών, όπως από ένα απλό φιλτράρισμα δεδομένων έως την δυνατότητα οπτικοποίησης των αποθηκευμένων δεδομένων και τον έλεγχο της συσκευής καθώς και την κρυπτογράφηση δεδομένων IoT[22].

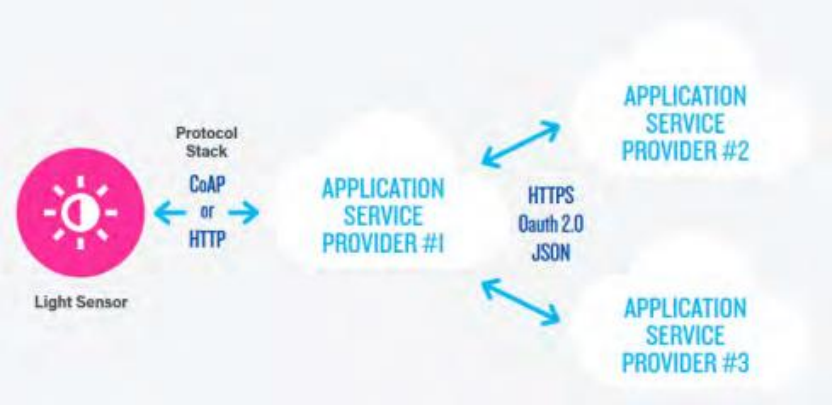


Εικόνα 5 Μοντέλο επικοινωνίας Device to Gateway [12]

Μια πύλη IoT μπορεί να εκτελέσει τις ακόλουθες λειτουργίες [23]:

- Διαγνωστικά ελέγχου του συστήματος
- Επικοινωνίες από συσκευή σε συσκευή
- Συγκέντρωση δεδομένων
- Προεπεξεργασία δεδομένων, καθαρισμό και φιλτράρισμά τους
- Προσωρινή αποθήκευση δεδομένων και ροής
- Διευκόλυνση της επικοινωνίας με πιο παλιές συσκευές που δεν είναι συνδεδεμένες στο δίκτυο
- Ασφάλεια δικτύου

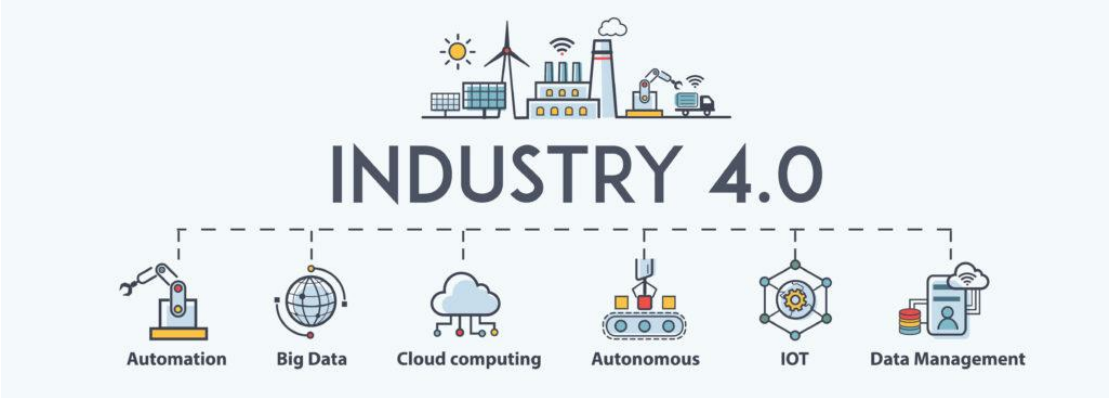
1.3.4 Back End Data Sharing



Εικόνα 6 Μοντέλο επικοινωνίας Back End Data Sharing [12]

Το Back End Data Sharing είναι μια cloud υπηρεσία που σε συνδυασμό με το μοντέλο device to cloud δίνει την δυνατότητα στους χρηστές να εξάγουν δεδομένα που βρίσκονται στο cloud αλλά και να κάνουν ανάλυση στα δεδομένα που προέρχονται από έξυπνες υπηρεσίες . Το Back End Data Sharing χρησιμοποιεί κλειδιά cloud APIs για να μπορέσει η συσκευή να στείλει δεδομένα στο cloud [22] .

ΚΕΦΑΛΑΙΟ 2: Industry 4.0



Εικόνα 7 INDUSTRY 4.0 [61]

2.1 Ορισμός Industry 4.0

Ένας ορισμός του Industry 4.0, η αλλιώς τέταρτη βιομηχανική επανάσταση ορίζεται η ενσωμάτωση λογισμικού αλλά και ενός δικτύου από αισθητήρες σε μηχανές της βιομηχανίας για να επιτευχθεί η παρακολούθηση, ο απομακρυσμένος έλεγχος αλλά και η ικανότητα ελάττωσης της παράγωγης λόγο προβλέψεων. Το Industry 4.0 περιλαμβάνει κάποιες βασικές έννοιες, όπως το Διαδίκτυο των Πραγμάτων (Internet of Things) , το Cloud Computing, τα Μαζικά Δεδομένα (Big Data), Κυβερνοφυσικά Συστήματα (Cyber Psychical Systems - CPS) και την γνωστική υπολογιστική[26][27].

2.2 Εφαρμογή του Industry 4.0

Για την εφαρμογή του Industry 4.0 πρέπει να ληφθούν υπόψη τα τρία ακόλουθα χαρακτηριστικά: α) κάθετη ολοκλήρωση β) ψηφιακή ολοκλήρωση γ) οριζόντια ολοκλήρωση[30].

1. Η κάθετη ολοκλήρωση και δικτύωση στα συστήματα παράγωγης της βιομηχανίας συγχωνεύει επιμέρους τμήματα της βιομηχανίας για την λήψη αποφάσεων. Τα δεδομένα διαμοιράζονται από την ανάπτυξη των προϊόντων σε διαφορές μονάδες όπως η παράγωγη και το μάρκετινγκ, διασφαλίζοντας ότι όλες οι μονάδες ενός εργοστασίου επικοινωνούν μεταξύ τους σε πραγματικό χρόνο [30].

2. Η ψηφιακή ολοκλήρωση της μηχανής από άκρο σε άκρο παρέχει λειτουργίες διαχείρισης του κύκλου ζωής και την ψηφιοποίηση ενός προϊόντος. Τα

προϊόντα παρακολουθούνται από διάφορους οργανισμούς σε διάφορα στάδια παράγωγης για να εξασφαλιστεί η επίτευξη του προϊόντος [30].

3. Τέλος η οριζόντια ολοκλήρωση επιτρέπει στις εταιρίες να συνεργάζονται με άλλες επιχειρήσεις, όπως προμηθευτές και πελάτες. Έτσι μια τέτοια ολοκλήρωση μπορεί να προσφέρει μια πλήρως ολοκληρωμένη αλυσίδα εφοδιασμού . Οι επιχειρήσεις χρησιμοποιούν το επίπεδο ολοκλήρωσης για να διατηρούν επιχειρηματικές στρατηγικές, επιχειρηματικά μοντέλα και αλυσίδες αξίας [30].

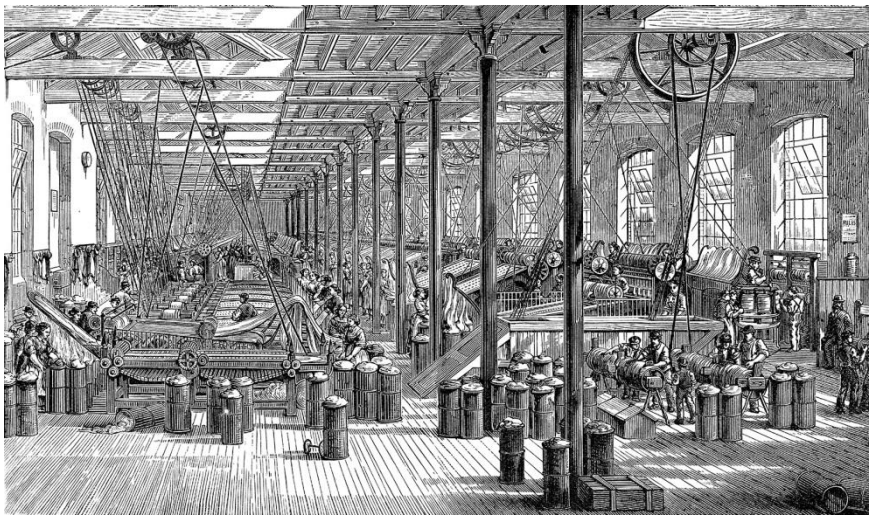
Τα επίπεδα ενσωμάτωσης του Industry 4.0 σε συνδυασμό με τις τεχνολογίες IoT και IIoT καθιστούν την μετατροπή των βιομηχανιών σε ¨έξυπνες¨ επιχειρήσεις. Το IoT προσφέρει την σύνδεση των μηχανών με το διαδίκτυο ενσύρματα η ασύρματα τοποθετώντας αισθητήρες και ενεργοποιητές για την παρακολούθηση και το χειρισμό των διαδικασιών. Το IIOT συνδέεται άμεσα με το IoT αφού όταν το διαδίκτυο των πραγμάτων εφαρμόζεται στην βιομηχανικά αναφέρεται ως IIoT . Το IoT παρέχει έναν μεγάλο όγκο δεδομένων (Big Data) για την συλλογή και την ανάλυση. Έτσι με βάση τα δεδομένα μπορεί να εφαρμοστεί η τεχνητή νοημοσύνη και η προσομοίωση των φυσικών διεργασιών πριν την παράγωγη σε πραγματικό επίπεδο για την αξιολόγηση των πραγμάτων. Ο συνδυασμός των τεχνολογιών της τεχνητής νοημοσύνης και των επίπεδων ολοκλήρωσης οδηγούν στο Cyber Physical Systems (CPS).[30] Τα CPS συστήματα είναι αυτόνομα και μπορούν να λαμβάνουν μονά τους αποφάσεις, έτσι η επίτευξη των CPS δημιουργεί μια πλήρως ολοκληρωμένη επιχείρηση η οποία μπορεί να συμμετέχει σε έναν κυβερνητικό κόσμο [30].

2.3 Ιστορική ανάδρομη

2.3.1 Πρώτη βιομηχανική επανάσταση

Η βιομηχανική επανάσταση σηματοδοτεί την έναρξη της βιομηχανικής εποχής. Με τον όρο αυτό εννοούμε μια διαδικασία που μετασχηματίζει την αγροτική παραγωγή σε βιομηχανική, περνώντας με αυτό τον τρόπο από την χειρωνακτική εργασία των ανθρώπων στην χρήση ατμομηχανών. Η πρώτη βιομηχανική επανάσταση ξεκίνησε περίπου στα μέσα του δεκάτου όγδοου αιώνα το 1760 στην μεγάλη Βρετάνια και στην συνέχεια άρχισε να επεκτείνεται στο Ηνωμένο Βασίλειο και πολύ γρήγορα στην Ευρώπη και στις ΗΠΑ. Έτσι ξεκίνησε και ο οικονομικός μετασχηματισμός στην Ευρώπη από το 1780 έως το 1850 που οφειλόταν στην πρώτη βιομηχανική επανάσταση. Παράλληλα η βιομηχανική επανάσταση φαίνεται να είχε πολλαπλά οφέλη στην τεχνολογική πρόοδο, στον οικονομικό και κοινωνικό τομέα και βελτίωση της καθημερινότητας και ποιότητας ζωής των ανθρώπων. Συνοψίζοντας

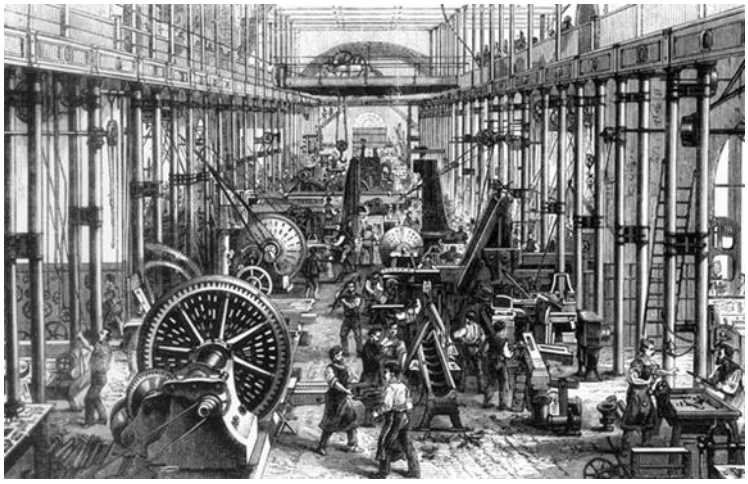
με την πρώτη βιομηχανική επανάσταση έχουμε την δημιουργία πρώτων υλών, όπως του σιδήρου και του χάλυβα αλλά και του άνθρακα που ήταν απαραίτητος για την χρήση στις μηχανές[28] .



Εικόνα 8 Πρώτη βιομηχανική επανάσταση [45]

2.3.2 Δεύτερη βιομηχανική επανάσταση

Η δεύτερη βιομηχανική επανάσταση ξεκίνησε στα τέλη του 19^{ου} αιώνα έως τις αρχές του 20^{ου} αιώνα και είναι γνωστή και ως τεχνολογική επανάσταση κατ την οποία άρχισε να γίνεται μαζική παράγωγη προϊόντων με την ανακάλυψη του ηλεκτρισμού. Η δεύτερη επανάσταση χαρακτηρίστηκε από την κατασκευή σιδηροδρομικών γραμμών και άρχισε να αναπτύσσεται η παράγωγη χάλυβα και σιδήρου. Η χρήση των σιδηρόδρομων βοήθησε στην φθηνή μεταφορά υλικών και προϊόντων και αργότερα άρχισαν να επεκτείνονται αφού ο άνθρακας ήταν φθηνός για την λειτουργία των ατμομηχανών. Παράλληλα η Γερμάνια , η Γαλλία , οι ΗΠΑ και η Ιαπωνία ξεκίνησαν και την βαριά βιομηχανία λόγο του σιδηρού και της ευρεία χρήσης μηχανημάτων στην παράγωγη. Τέλος άρχισαν να χρησιμοποιούνται σύγχρονες παραγωγικές μέθοδοι για τη λειτουργία επιχειρήσεων μεγάλης κλίμακας σε τεράστιες περιοχές[28].



Εικόνα 9 Δεύτερη βιομηχανική επανάσταση [46]

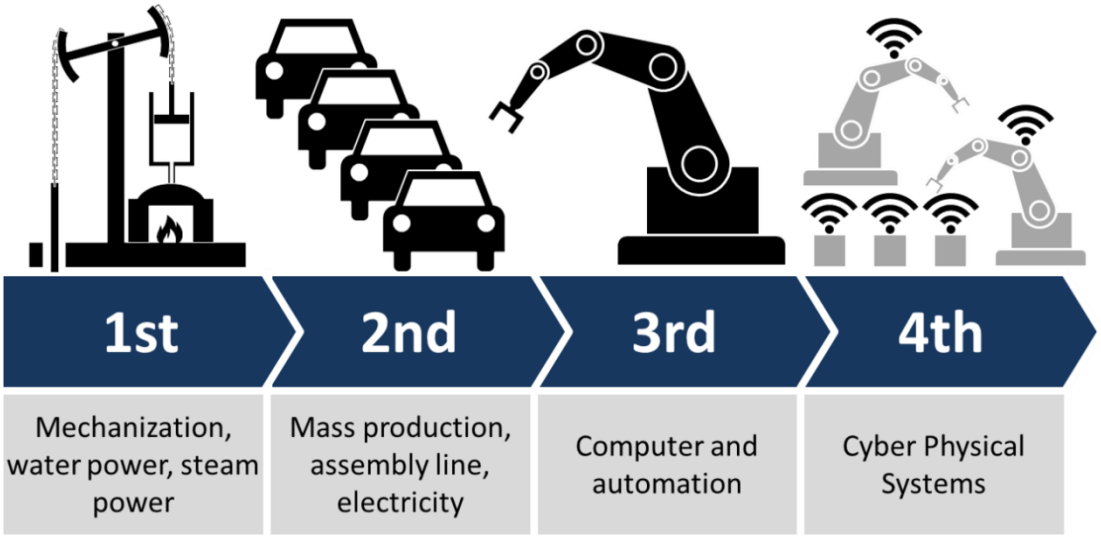
2.3.3 Τρίτη βιομηχανική επανάσταση

Η τρίτη βιομηχανική επανάσταση στηρίχτηκε στις προηγούμενες επαναστάσεις και έφερε την εισαγωγή της ψηφιακής τεχνολογίας , των υπολογιστών και του διαδικτύου. Ξεκίνησε από τις αρχές της δεκαετίας του 1950, αφού τέλειωσε ο δεύτερος παγκόσμιος πόλεμος , καθώς ο πρώτος και ο δεύτερος παγκόσμιος πόλεμος δεν επέτρεψαν την είσοδο της ανάπτυξης της τεχνολογίας και της παράγωγης. Παράλληλα παρατηρήθηκε ότι οι χώρες που είχαν εκβιομηχανιστεί είχαν μεγάλες οικονομικές επιπτώσεις. Τέλος η καθημερινότητα των ανθρώπων άρχισε να αναβαθμίζεται αφού εισήλθαν πιο πρακτικά και μικρότερα προϊόντα και το ανθρώπινο δυναμικό στις βιομηχανίες άρχισε να μειώνεται [28].

Εικόνα 10 Τρίτη βιομηχανική επανάσταση[47]

2.3.3 Τέταρτη βιομηχανική επανάσταση

Η τέταρτη βιομηχανική επανάσταση η αλλιώς Industry 4.0 φέρνει την χρήση του IoT μέσα στις βιομηχανίες και κατευθύνεται προς την πλήρη ψηφιοποίησή τους (Ψηφιακά Δίδυμα-Digital Twins). Ξεκίνησε το 2013 όπου η γερμανική κυβέρνηση εξηγούσε την στρατηγική που θα ακολουθούταν τα επόμενα χρόνια στις βιομηχανίες και την ανάγκη της σύνδεσης του internet με την βιομηχανική παράγωγη . Το IoT χρησιμοποιεί κάποια συστήματα όπως αισθητήρες οι όποιοι, συλλέγουν μεγάλες ποσότητες δεδομένων για ανάλυση αλλά και βελτίωση των προϊόντων. Ακόμη το Industry 4.0 ενσωμάτωσε την τεχνητή νοημοσύνη μέσα στις βιομηχανίες κάνοντας τις μηχανές να χρησιμοποιούν συστήματα αυτοβελτιστοποίησης και αυτορρύθμισης για να αυξήσουν την παράγωγη [28],[29].



Εικόνα 11 Βιομηχανικές επαναστάσεις [48]

2.4 Σχεδιασμός Industry 4.0

Το Industry 4.0 περιλαμβάνει την έννοια του ¨έξυπνου εργοστάσιου ¨ εννοώντας την ύπαρξη ενός δικτύου κατά μήκος της βιομηχανίας στο οποίο οι πληροφορίες της παραγωγικής διαδικασίας και του κύκλου ζωής των προϊόντων είναι διαθέσιμες. Κάθε μηχάνημα μπορεί να λειτουργεί αυτόνομα και συνεκτικά με ταυτόχρονη ύπαρξη ελέγχου μεταξύ των μηχανημάτων.

Σκοπός του Industry 4.0 είναι η διασύνδεση όλων των μηχανημάτων μεταξύ τους. Το Industry 4.0 περιλαμβάνει έξι βασικές αρχές σχεδιασμού προκειμένου να αξιοποιηθούν πλήρως τα οφέλη της βιομηχανίας 4.0 που έχουν να κάνουν με την αυτοματοποίηση των διαδικασιών και την ψηφιοποίηση της παραγωγικής διαδικασίας. Οι αρχές σχεδιασμού για να μπορέσει να υλοποιηθεί είναι: η

διαλειτουργικότητα (interoperability), η εικονοποίηση (virtualization), η αποκεντροποίηση (decentralization), η ικανότητα πραγματικού χρόνου (real-time capability), η δομοστοιχειοθέτηση (modularity) και ο προσανατολισμός στην υπηρεσία (service orientation) [26][27].

- Διαλειτουργικότητα (interoperability) : η διαλειτουργικότητα αποτελεί την πρώτη αρχή του σχεδιασμού η όποια αναφέρεται στην ικανότητα των συσκευών , του εξοπλισμού , και των ανθρώπων να επικοινωνούν μεταξύ τους καθώς και για το διαμοιρασμό των δεδομένων όπου μπορεί να επιτευχθεί μέσω του IoT [26] [27].

- Εικονικοποίηση (Virtualization): Μας δίνει την δυνατότητα να κάνουμε προσομοίωση στις παραγωγικές διεργασίες των μηχανημάτων μέσα σε μια βιομηχανία σε εικονικά μοντέλα ή σε μοντέλα προσομοίωσης . Με την βοήθεια των αισθητήρων που είναι ενσωματωμένοι στα μηχανήματα, τα δεδομένα που λαμβάνονται, συλλέγονται δίνοντάς μας πληροφορίες για το μηχάνημα . Με αυτόν τον τρόπο δημιουργείται ένα εικονικό αντίγραφο της φυσικής λειτουργίας του κάθε μηχανήματος, το Ψηφιακό Δίδυμο (Digital Twin). Έτσι το εικονικό αντίγραφο βοήθα στην βελτιστοποίηση της απόδοσης του μηχανήματος αφού μπορεί να γίνει παρακολούθηση των παραμέτρων από μηχανικούς και σχεδιαστές, κάνοντας διάφορες παραμετροποιήσεις σε ένα εικονικό περιβάλλον χωρίς να σταματήσει ή να επηρεαστεί η φυσική διαδικασία. Τέλος η εικονοποίηση μπορεί να λειτουργήσει και σαν περιβάλλον παρακολούθησης των φυσικών μηχανημάτων αφού επιτρέπουν στους χείριστες να βλέπουν την κατάσταση του μηχανήματος σε πραγματικό χρόνο, να αναλύουν την απόδοση, και να εντοπίζουν διάφορα προβλήματα [26] [27].

- Αποκεντροποίηση (Decentralization): η αποκέντρωση είναι ένα πολύ σημαντικό χαρακτηριστικό μιας επιχείρησης αφού προσφέρει την δυνατότητα ευελιξίας και ευκαμψίας στην παράγωγη . Έτσι ως αποκέντρωση ορίζουμε την ικανότητα των κυβερνο-φυσικών συστημάτων (CPS) να λαμβάνουν αυτόνομες αποφάσεις χωρίς να υπάρχει εντολή από κάποιον έλεγχο για την εξυπηρέτηση της παραγωγικής διαδικασίας. Οι τεχνολογίες που υποστηρίζουν την αποκέντρωση είναι τα CPS, το IoT , οι έξυπνοι αισθητήρες , οι έξυπνοι ενεργοποιητές και η τεχνητή νοημοσύνη που μπορούν να επικοινωνούν και να μοιράζονται πληροφορίες για τον έλεγχο την παραγωγικής διαδικασίας [26] [27].

- Ικανότητα πραγματικού χρόνου (real-time capability) : είναι μια από τις βασικότερες αρχές σχεδιασμού όπου η επιχείρηση μπορεί να συλλέγει , να μεταφέρει , να αναλύει και να παρακολουθεί τα δεδομένα σε πραγματικό χρόνο. Η επεξεργασία και η ανάλυση των δεδομένων σε πραγματικό χρόνο

βοήθα στην διαδικασία λήψης αποφάσεων και στην βελτίωση της παράγωγης. Ακόμη μπορεί να γίνει ανίχνευση βλαβών και αναζήτηση λύσεων για την αντιμετώπιση προβλημάτων πράγμα που αυξάνει την παραγωγικότητα[26] [27].

- Δομοστοιχειοθέτηση (Modularity): είναι η ικανότητα προσαρμογής κάθε έξυπνου εργοστασίου σε διάφορες μελλοντικές καταστάσεις, είτε αυτές οφείλονται σε εσωτερικές είτε σε εξωτερικές ανάγκες. Με αυτόν τον τρόπο γίνεται εξοικονόμηση στον χρόνο κατασκευής των προϊόντων και υπάρχει γρήγορη και αποτελεσματική ανταπόκριση στην ζήτηση. Τέλος η δομοστοιχειοθέτηση υποστηρίζει την χρήση <<αρθρωτών>> συστημάτων παράγωγης που απλοποιούν την διαδικασία παράγωγης [26] [27].

- Προσανατολισμός στην υπηρεσία (service orientation) : Η νέα επιχειρηματική στρατηγική προσφέρει ολοκληρωμένες λύσεις στους πελάτες των προϊόντων. Οι βιομηχανίες εκτός από την δημιουργία προϊόντων πρέπει να επικεντρωθούν και στον προσανατολισμό στις υπηρεσίες , αυτό επιτυγχάνεται με την ενσωμάτωση έξυπνων εργαλείων με την βοήθεια του διαδικτύου των υπηρεσιών (IoS-Internet of Services). Έτσι οι βιομηχανίες προσφέρουν υπηρεσίες μέσω της πλατφόρμας IoS όπου οι πελάτες πληρώνουν μια συνδρομή [26] [27].

ΚΕΦΑΛΑΙΟ 3: Industrial Internet of Things

Το Industrial Internet of Things (Βιομηχανικό Διαδίκτυο των Πραγμάτων) είναι η εφαρμογή ενός συστήματος Internet of Things στον βιομηχανικό, στον παραγωγικό κλάδο και σε έξυπνες μηχανές, στα οποία με την χρήση έξυπνων αισθητήρων παρέχεται υψηλό επίπεδο επικοινωνίας για να διασφαλιστεί η ποιότητα και η ασφάλεια της διαδικασίας, με τρόπο που η ανθρώπινη αλληλεπίδραση δεν μπορεί από μόνη της να επιτύχει [23]. Το IIoT συχνά παρομοιάζεται με το IoT, ωστόσο ένα σύστημα IoT περιλαμβάνει πιο γενικές εφαρμογές και στοχεύει στην διασύνδεση συσκευών με το διαδίκτυο, όπως σε εφαρμογές στην γεωργία ή σε οικιακούς αυτοματισμούς, ενώ το IIoT εστιάζει σε βιομηχανικές εφαρμογές για την διασύνδεση μηχανών.

Στην βιομηχανία, η επικοινωνία των μηχανών είναι κρίσιμη, αφού μια βλάβη σε ένα μηχάνημα ή μια διακοπή στο ρεύμα μπορεί να προκαλέσει απειλή σε ανθρώπινες ζωές. Έτσι το IIoT στοχεύει στην ενίσχυση των παραγωγικών διαδικασιών καθώς τα μηχανήματα είναι εξοπλισμένα με αισθητήρες και ενεργοποιητές που μπορούν να ελέγξουν την τρέχουσα κατάσταση του κάθε μηχανήματος. Επομένως το IoT στην βιομηχανία αποτελεί ένα ελέγξιμο σύστημα DCS που στηρίζεται στον αυτοματισμό και στην βελτιστοποίηση του ελέγχου στην διαδικασία παράγωγης, χρησιμοποιώντας την τεχνολογία cloud computing. Ακόμη υπάρχει επικοινωνία machine-to-machine, τεχνητή νοημοσύνη, edge computing, κυβερνοασφάλεια (cyber security), big data , RFID κ.α. Τέλος το IIoT είναι άμεσα συνδεδεμένο με το Industry 4,0, καθώς με την χρήση έξυπνων αισθητήρων και ενεργοποιητών γίνεται ανάλυση των δεδομένων σε ένα σύστημα , σε πραγματικό χρόνο [23] [24].

Εικόνα 12 Industrial Internet of Things[49]

3.1 Πλεονεκτήματα και οφέλη του IIoT

Η εγκατάσταση ενός δικτύου IoT στην βιομηχανία προαπαιτεί ότι όλες οι μηχανές είναι πλήρως διασυνδεδεμένες μεταξύ τους και διαθέτουν αισθητήρες και ενεργοποιητές. Συνεπώς εάν γίνει σωστή μελέτη στην διασύνδεση αυτής της υποδομής, το IIoT υπόσχεται μεγάλα οφέλη σε μια εταιρία. Πριν την ένταξη του όρου Industry 4.0, τα βιομηχανικά δίκτυα ακολουθούσαν δυο συστήματα: α) το σύστημα της επιχειρησιακής τεχνολογίας (OT) και β) το σύστημα των εταιρικών πληροφοριών (IT), μετά την τεχνολογική πρόοδο όμως τα δυο αυτά συστήματα ενώθηκαν και έφεραν μεγάλα οφέλη στις βιομηχανίες [23][25] .

- Προγνωστική συντήρηση μηχανημάτων: ένα από τα μεγαλύτερα οφέλη που προσφέρει το IIoT, είναι η προγνωστική συντήρηση των μηχανημάτων . Τα μηχανήματα στέλνουν δεδομένα από τους αισθητήρες που έχουν ενσωματωμένους και η επιχείρηση τα συλλέγει και τα αναλύει σε πραγματικό χρόνο. Έτσι μπορεί γίνει πρόβλεψη σε τυχόν βλάβες και να ειδοποιηθούν τα αρμόδια τμήματα ώστε να γίνει πρόωρη συντήρηση του μηχανήματος πριν εμφανιστεί κάποιο πρόβλημα. Με αυτόν τον τρόπο η επιχείρηση μειώνει σημαντικά τον χρόνο διακοπής λειτουργίας της μηχανής, κάνοντας εξοικονόμηση χρόνου[23] .

- Απομακρυσμένος έλεγχος μηχανημάτων: Η δυνατότητα που δίνει ο απομακρυσμένος έλεγχος μέσω εφαρμογών, βοήθα στην μείωση της ανθρώπινης παρέμβασης καθώς κάθε μηχάνημα μπορεί να ελέγχεται εξ αποστάσεως και να ελαχιστοποιείται η ανθρώπινη παρέμβαση. Έτσι παρέχεται μεγαλύτερη ασφάλεια κατά την ολοκλήρωση της παραγωγικής διαδικασίας [23] .

- Κόστος λειτουργιάς: Η άμεση επικοινωνία που προσφέρει το IIoT μεταξύ των μηχανών βοήθα στην μείωση του κόστους λειτουργίας καθώς βελτιστοποιείται η παραγωγική διαδικασία. Ακόμη, λόγο της αυτοματοποιημένης παράγωγης γίνεται μείωση της ανθρώπινης παρέμβασης και έτσι αποφεύγονται τα ανθρώπινα σφάλματα που μπορούν να δημιουργηθούν και να αυξήσουν τις δαπάνες της εταιρίας .

- Διαχείριση εγκαταστάσεων: Οι κατασκευαστές με την βοήθεια των συστημάτων διαχείρισης, μπορούν να παρακολουθούν την τρέχουσα κατάσταση κάθε στοιχείου και την διαχείριση του εφοδιασμού των προϊόντων. Τέλος, μέσω των αισθητήρων μπορούν να ελεγχθούν διάφορες καταστάσεις μέσα σε μια βιομηχανία όπως υψηλή θερμοκρασία , κραδασμοί , αλλαγές στην τάση τροφοδοσίας για την προστασία των μηχανημάτων .

ΚΕΦΑΛΑΙΟ 4: Ασύρματες τεχνολογίες μικρής εμβελείας (Short-Range Wireless Solutions)

Οι ασύρματες τεχνολογίες μικρής εμβελείας εξυπηρετούν εφαρμογές μικρής απόστασης μεταξύ των συσκευών και των πυλών όπου η απόσταση των συσκευών δεν ξεπερνά τα 150 μέτρα . Σε αυτό το κεφάλαιο θα κάνουμε μια σύντομη ανασκόπηση στις ασύρματες τεχνολογίες μικρής εμβελείας για να παρουσιάσουμε στο επόμενο κεφάλαιο τις διαφορές με τα δίκτυα LPWAN . Κάποιες από αυτές τις τεχνολογίες, είναι οι παρακάτω : RFID , ZigBee και το Z-WAVE.

4.1 Radio Frequency Identification (RFID)

Εικόνα 13 Λογότυπο RFID ετικέτας [50]

Το RFID είναι μια πρωτοποριακή τεχνολογία η οποία χρησιμοποιεί ετικέτες για την αναγνώριση αντικειμένων του IoT . Οι ετικέτες περιέχουν αναμεταδότες και εκπέμπουν μηνύματα στους ειδικούς αναγνώστες RFID, χρησιμοποιώντας την ειδική τεχνολογία αναγνώρισης ραδιοσυχνοτήτων (Radio Frequency Identification). Οι ετικέτες RFID αποθηκεύουν ένα μοναδικό αναγνωριστικό. Για παράδειγμα έναν κωδικό πελάτη ή έναν κωδικό SKU (stock-keep-ing unit) ενός προϊόντος. Ο αναγνώστης αντλεί πληροφορίες σχετικά με τον μοναδικό αριθμό αναγνώρισης από μια βάση δεδομένων και ενεργεί. Κάποιες ετικέτες RFID έχουν ενσωματωμένη μνήμη στην όποια αποθηκεύονται πληροφορίες από διαφόρους αναγνώστες.

Υπάρχουν δυο κατηγορίες ετικετών: α) οι ενεργές και β) οι παθητικές ετικέτες που διαφέρουν στην πηγή ηλεκτρικής τους ενεργείας . α) Οι ενεργές ετικέτες RFID έχουν δική τους πηγή ενεργείας , συνήθως μια μπαταρία ενώ οι παθητικές ετικέτες λαμβάνουν ενεργεία από τον αναγνώστη. Έτσι και οι αναγνώστες των ετικετών χωρίζονται αντίστοιχα σε δυο κατηγορίες σε ενεργούς και παθητικούς ανάλογα με

την κατηγορία ετικετών που διαβάζουν [32]. Η τεχνολογία που εκτελεί την αναγνώριση της ετικέτας ονομάζεται RFID EPC-GEN2. Σε μια σύνδεση μηχανής με μηχανή (M2M) ο αναγνώστης της ετικέτας, στέλνει ένα σήμα στην ετικέτα και λαμβάνει ένα ανακλώμενο σήμα. Οι ενεργές ετικέτες επειδή διαθέτουν την δική τους πηγή ενεργείας, εκπέμπουν ένα ισχυρότερο σήμα, το οποίο οι αναγνώστες μπορούν το λαμβάνουν από μεγαλύτερη απόσταση . Έτσι οι ετικέτες αυτής της κατηγορίας χρησιμοποιούνται για εφαρμογές παρακολούθησης αντικειμένων σε μεγάλες αποστάσεις, διότι παρέχουν μεγαλύτερη ακρίβεια και έχουν μέγεθος σαν μια τράπουλα. Κατά την χρήση τους μπορούν να εκπέμπουν συνεχώς ένα σήμα, είτε να παραμείνουν σε αδράνεια μέχρι να βρεθούν στην εμβέλεια ενός δέκτη. Η συχνότητα που εκπέμπουν είναι 455MHz ,2.4GHz ή 5.8GHz και η εμβέλεια που μπορούν να στείλουν είναι από 20 έως 100 μέτρα απόσταση. Αντίθετα οι παθητικές ετικέτες είναι πολύ φθηνές και λόγο των νέων τεχνολογιών γίνονται συνεχώς φθηνότερες. Το μέγεθος τους είναι πολύ μικρότερο σε σχέση με τις ετικέτες της άλλης κατηγορίας και η εμβέλεια είναι πολύ μικρή [32].

Β) Οι παθητικές ετικέτες είναι σχεδιασμένες να καταναλώνουν πολύ χαμηλές τιμές ενεργείας διότι η τροφοδοσία τους γίνεται από έναν υποδοχέα (scavenger). Το κόστος σχεδίασης και κατασκευής πρέπει να είναι πολύ χαμηλό, γιατί σε εφαρμογές αναγνώρισης IoT, όπως για παράδειγμα σε μια αποθήκη, πρέπει να υπάρχουν παρά πολλές ετικέτες με μεγάλο κόστος. Τα συστήματα RFID λειτουργούν σε διάφορες ζώνες συχνοτήτων: (α) Στην χαμηλή ζώνη συχνοτήτων (LF) λειτουργούν στα 125 – 134.2 KHz, (β) Στην υψηλή ζώνη συχνοτήτων (HF) λειτουργούν στα 13.56 MHz, (γ) ενώ για τις ζώνες Ultra High Frequency (UHF), βάση του πρωτοκόλλου EPC-GEN2, λειτουργούν σε 850 – 960MHz[33].

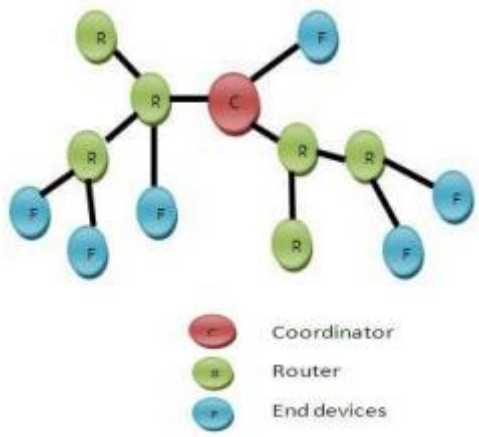
4.2 ZigBee

Εικόνα 14 Λογότυπο ZigBee [51]

Το ZigBee είναι ένα πρωτόκολλο επικοινωνίας που δημιουργήθηκε από την ZigBee alliance το οποίο έχει βασιστεί στην προδιαγραφή IEEE 802.15.4. Το ZigBee ορίζει τα επίπεδα του δικτύου και της ασφάλειας εφαρμογής ενώ το IEEE 802.15.4 ορίζει τα φυσικά στρώματα . Η ισχύς που χρειάζεται για το ZigBee είναι περίπου της τάξης των 1mW και μπορεί να παρέχει εμβέλεια έως 150 μετρά σε εξωτερικούς χώρους χωρίς εμπόδια με την τεχνική DSSS (Direct Sequence Spread Spectrm). Στην Ευρώπη λειτούργει στην ζώνη ISM 868 MHz και στην παγκόσμια διαθέσιμη ζώνη των 2.4GHz με ρυθμό δεδομένων 20 kbps [37][36]. Το πρότυπο IEEE 802.15.4 χρησιμοποιεί διευθύνσεις 16 και 64 bit και μπορεί να υποστηρίξει θεωρητικά έως και 65.000 κόμβους σε κάθε δίκτυο, ενώ η απόσταση του κάθε κόμβου μπορεί να είναι έως και 50 μέτρα, ώστε να μπορεί να γίνει αναμετάδοση των δεδομένων σε άλλους κόμβους . Έτσι μπορεί να δημιουργηθεί ένα πολύ μεγάλο δίκτυο με ευρεία κάλυψη.

Το πρότυπο IEEE 802.15.4 ορίζει δυο τύπους τελικών συσκευών: α) συσκευές πλήρους λειτουργίας (FFD) και Β) συσκευές μειωμένης λειτουργίας (RFD). Οι συσκευές της πρώτης κατηγορίας, μπορούν να εκτελούν όλες τις διαθέσιμες λειτουργίες, όπως ο μηχανισμός δρομολόγησης, ο συντονισμός εργασιών και η ανίχνευση της εργασίας. Η τροφοδοσία μιας FFD συσκευής γίνεται με την τροφοδότηση εναλλασσομένου ρεύματος, γιατί πρέπει πάντα να είναι ενεργή για να εξυπηρετεί τις υπόλοιπες τελικές συσκευές. Αντίθετα οι συσκευές της δεύτερης κατηγορίας που έχουν περιορισμένες λειτουργίες συνδέονται με τις FFD συσκευές και δεν μπορούν να δρομολογήσουν. Οι συσκευές της δεύτερης κατηγορίας, οι RFD είναι συνήθως συσκευές που περιλαμβάνουν αισθητήρες, ενεργοποιητές και καταγράφουν διάφορες μετρήσεις όπως θερμοκρασία και πίεση. Η τροφοδοσία τους γίνεται με μπαταρία.

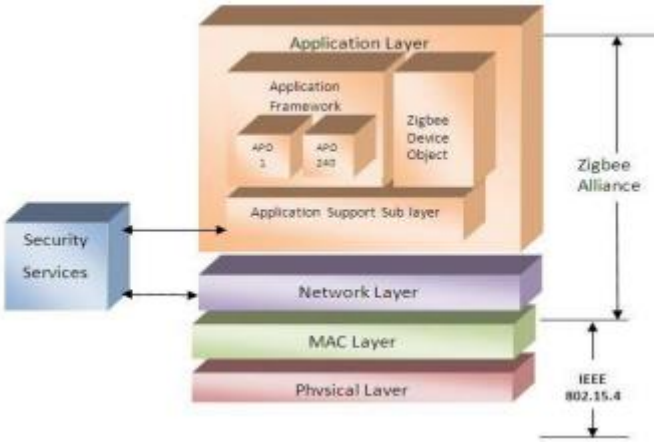
Το ZigBee υποστηρίζει τρεις κατηγορίες κόμβων: i) τους συντονιστές, ii) τους δρομολογητές και iii) τις τελικές συσκευές . i) Οι συντονιστές είναι υπεύθυνοι για την ρύθμιση των παραμέτρων ενός δικτύου όπως το κανάλι της συχνότητας, το μοναδικό αναγνωριστικό κάθε συσκευής και τον καθορισμό άλλων λειτουργικών παραμέτρων. Ακόμη μπορεί να αποθηκεύουν πληροφορίες και τα κλειδιά για την ασφάλεια του δικτύου. Οι συντονιστές λειτουργούν και σαν γέφυρα για την επικοινωνία με αλλά δίκτυα. Ii) Οι δρομολογητές βοηθούν στην αναμετάδοση δεδομένων σαν ενδιάμεσοι κόμβοι. Επίσης, μπορούν να συνδεθούν σε ένα υπάρχον δίκτυο ή να δεχθούν συνδέσεις από άλλες συσκευές. Με αυτόν τον τρόπο μπορεί να γίνει επέκταση του δικτύου ZigBee. Iii) Οι τελικές συσκευές είναι κόμβοι που λειτουργούν με μπαταρία και μπορούν να συλλέγουν πληροφορίες από αισθητήρες ή να λειτουργούν σαν ενεργοποιητές. Οι τελικές συσκευές δεν μπορούν να κάνουν αναμετάδοση σε δεδομένα από άλλες συσκευές. Λόγω της έλλειψης αυτής της λειτουργίας έχουν χαμηλό κόστος κατασκευής . Τέλος, κάθε τελική συσκευή μπορεί να έχει έως και 240 τελικούς κόμβους που να μοιράζονται την ίδια συχνότητα και να εξυπηρετούν διαφορετικές εφαρμογές[36][37].



Εικόνα 15 Δίκτυο ZigBee [36]

4.2.1 Αρχιτεκτονική ZigBee

Το ZigBee βασίζεται στην αρχιτεκτονική πρότυπου IEEE 802.15.4 η οποία ορίζει δυο επίπεδα: α) το φυσικό επίπεδο και β) το επίπεδο έλεγχου πρόσβασης. Η ZigBee alliance ορίζει αλλά δυο επίπεδα: (γ) το επίπεδο δικτύου και (δ) το επίπεδο εφαρμογής, τα οποία θα αναλύσουμε παρακάτω [36].



Εικόνα 16 Στοίβα πρωτόκολλων ZigBee [36]

Α) Το φυσικό επίπεδο του πρότυπου IEEE 802.15.4 είναι το στρώμα που ελέγχει τον δέκτη και χειρίζεται τις εργασίες που έχουν να κάνουν με την πρόσβαση στο υλικό του ZigBee, όπως η επιλογή καναλιού, η ποιότητα της σύνδεσης και η ανίχνευση ενεργείας. Υποστηρίζει τρεις ζώνες συχνοτήτων: την ζώνη 2,45GHz που περιέχει 16 κανάλια με ρυθμό μετάδοσης 250Kbps και χρησιμοποιείται παγκόσμια, την ζώνη 915MHz που περιέχει 10 κανάλια και ρυθμό μετάδοσης 40Kbps που χρησιμοποιείται στις ΗΠΑ και την ζώνη 866 MHz που περιέχει 1 κανάλι με ρυθμό μετάδοσης 20Kbps που χρησιμοποιείται στην Ευρώπη. Και οι τρεις ζώνες συχνοτήτων χρησιμοποιούν το Direct Spread Spectrum Sequencing (DSSS)[36].

Β) Το στρώμα MAC είναι υπεύθυνο για την διασύνδεση του επίπεδου δικτύου και του φυσικού επίπεδου. Το στρώμα MAC υποστηρίζει δυο υπηρεσίες δεδομένων: Την υπηρεσία δεδομένων MAC, η οποία είναι υπεύθυνη για την μετάδοση και την λήψη δεδομένων του πρωτόκολλου MAC μέσω της υπηρεσίας δεδομένων PHY και την υπηρεσία διαχείρισης MAC, η όποια διασυνδέεται με το σημείο προσβασης[36] .

Γ) Το επίπεδο δικτύου είναι υπεύθυνο για την δρομολόγηση. Η λειτουργία της δρομολόγησης είναι η διαδικασία επιλογής της διαδρομής για την αναμετάδοση των δεδομένων από τους κόμβους. Το επίπεδο δικτύου παρέχει ασφάλεια σε όλο το δίκτυο και βοήθα τις τελικές συσκευές να μεγιστοποιήσουν την διάρκεια ζωής της μπαταρίας τους . Το πρότυπο IEEE 802.15.4 υποστηρίζει τρεις τοπολογίες, αστέρα, δέντρο και πλέγμα [36] .

Δ) Το επίπεδο εφαρμογής είναι υπεύθυνο για τον έλεγχο και την διαχείριση των πρωτοκόλλων στις συσκευές ZigBee. Μια εφαρμογή ZigBee μπορεί να έχει έως 240 αντικείμενα εφαρμογής όπου κάθε προφίλ ορίζει τις διάφορες μορφές των δεδομένων, των πρωτοκόλλων και τις αλληλεπιδράσεις μεταξύ των αντικειμένων εφαρμογής [36].

4.3 Z-Wave

Εικόνα 17 Λογότυπο Z-Wave [56]

Το Z-Wave είναι ένα πρωτόκολλο ασύρματου δικτυού για επικοινωνίες RF χαμηλής ισχύος που δημιουργήθηκε από την ZenSys και προωθείται από την Z-Wave Alliance για οικιακούς αυτοματισμούς ή για εφαρμογές αυτοματισμού σε εμπορικά κέντρα στα οποία οι απαιτήσεις είναι πολύ χαμηλές.

Στόχος του Z-Wave είναι να στέλνει αξιόπιστα πακέτα από μια μονάδα σε έναν ή περισσότερους κόμβους. Η ζώνη συχνοτήτων του για την Ευρώπη, είναι τα 868 MHz με ρυθμό μετάδοσης δεδομένων 9,6 kb/s, ενώ για τις Ηνωμένες πολιτείες είναι 908 MHz με ρυθμό μετάδοσης δεδομένων 40 kb/s χρησιμοποιώντας διαμόρφωση BFSK (binary frequency shift keying) και έχει εμβέλεια έως και 30 μέτρα. Ακόμη η σειρά Z-Wave 400 υποστηρίζει την ζώνη συχνοτήτων 2,4GHz με ρυθμό μετάδοσης δεδομένων έως 200 kb/s [38].

Το Z-Wave υποστηρίζει την τοπολογία πλέγματος και περιλαμβάνει δυο τύπους συσκευών: τους controllers και τους slaves. Οι controllers στέλνουν εντολές στους slaves και εκτελούν εντολές ή απαντούν στους ελεγκτές ενώ οι slaves λειτουργούν ως δρομολογητές και αποθηκεύουν στατικές διαδρομές και μπορούν να στέλνουν μηνύματα σε άλλους κόμβους. Οι slaves είναι ιδανικοί για αισθητήρες παρακολούθησης ή για ενεργοποιητές που δεν έχουν υψηλές απατήσεις απόκρισης. Η αρχιτεκτονική του Z-Wave αποτελείται από πέντε επίπεδα : α) Το επίπεδο PHY β) το επίπεδο MAC γ) το επίπεδο μεταφοράς δ) το επίπεδο δρομολόγησης και ε) το επίπεδο εφαρμογής. Το επίπεδο MAC περιλαμβάνει έναν μηχανισμό αποφυγής συγκρούσεων και επιτρέπει την μετάδοση ενός πλαισίου όταν το κανάλι είναι διαθέσιμο. Το επίπεδο μεταφοράς χωρίζει την επικοινωνία σε δυο κόμβους και περιλαμβάνει έναν μηχανισμό αναμετάδοσης που βασίζεται σε ACKs. Το επίπεδο δρομολόγησης εκτελεί την δρομολόγηση, όπου όταν ένας ελεγκτής μεταδίδει ένα πακέτο περιλαμβάνει την διαδρομή που πρέπει να ακολουθήσει το πακέτο [38].

ΚΕΦΑΛΑΙΟ 5: Ασύρματες τεχνολογίες Μεγάλης εμβέλειας χαμηλής ισχύος (Low Power Wide Area Network, LPWAN)

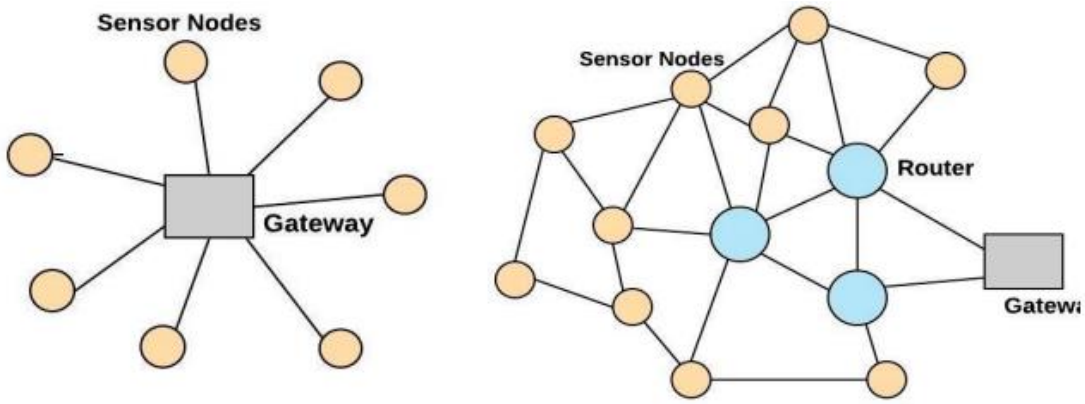
Εικόνα 18 Λογότυπο LPWAN [57]

Ένα πολύ μεγάλο μέρος των συσκευών IoT που χρησιμοποιούμε σήμερα έχουν σχεδιαστεί με παρωχημένες τηλεπικοινωνιακές τεχνολογίες στις οποίες υπάρχει μεγάλη κατανάλωση ενεργείας και μικρή εμβέλεια μετάδοσης δεδομένων[2]. Η μεγάλη κατανάλωση ενεργείας σε συνδυασμό με την μικρή εμβέλεια των πρωτοκόλλων όπως bluetooth ,Wi-Fi , zigbee καθίστανται ακατάλληλες τεχνολογίες για τις εφαρμογές που θέλουμε να έχουμε απομακρυσμένο έλεγχο και παρακολούθηση αισθητήρων. Οι τεχνολογίες LPWAN θεωρούνται μια πολύ καλή λύση στον τομέα του << βιομηχανικού IoT>> καθώς στοχεύουν στην κάλυψη εφαρμογών, όπου οι απαιτήσεις εμβελείας είναι πολύ μεγάλες και η κατανάλωση ισχύος τους πρέπει να είναι πολύ μικρή [1]. Η χαμηλή κατανάλωση ενέργειας, επιτυγχάνεται με την αποστολή μικρών πακέτων δεδομένων με πολύ χαμηλούς ρυθμούς, ενώ παράλληλα η εξοικονόμηση ενέργειας επιτυγχάνεται με μηχανισμούς όπως το να τίθενται οι συσκευές σε κατάσταση ύπνου (sleep mode)[2]. Ο σχεδιασμός των LPWAN δικτύων στηρίζεται σε τρία βασικά χαρακτηριστικά: α) την χαμηλή κατανάλωση ενεργείας β) την μεγάλη ασύρματη κάλυψη και γ) το χαμηλό κόστος σχεδίασης και κατασκευής.

5.1.1 Τοπολογίες LPWAN

Το δίκτυο LPWAN διαθέτει τρεις τοπολογίες δικτύων. Η απλούστερη μορφή τοπολογίας ενός ασύρματου δικτύου είναι το **point-to-point** όπου οι κόμβοι επικοινωνούν απευθείας με την κεντρική πύλη. Αυτή η τοπολογία χρησιμοποιείται για εφαρμογές απομακρυσμένης παρακολούθησης όπου δεν είναι εφικτή η σύνδεση των κόμβων ενσύρματα [21]. Η τοπολογία **αστέρα** (star topology) χρησιμοποιεί μια κεντρική πύλη όπου συνδέονται όλοι οι κόμβοι [26]. Οι κόμβοι μπορούν να επικοινωνήσουν με τους υπόλοιπους κόμβους μόνο μέσω της πύλης και τα μηνύματα των κόμβων αναμεταδίδονται από τις πύλες προς τους κεντρικούς διακομιστές. Πλεονέκτημα αυτής της κατηγορίας είναι η ταχύτητα και η αξιοπιστία των κόμβων λόγο της σχεδίασης single hop, διότι οι ελαττωματικοί κόμβοι μπορούν να εντοπιστούν πολύ εύκολα αφού κάθε κόμβος δεν συνδέεται με άλλον και μπορούν να απομονωθούν. Σε περίπτωση βλάβης της πύλης όλοι οι κόμβοι που είναι συνδεδεμένοι σε εκείνον τον κόμβο καθίστανται μη προσβάσιμοι [21].

Στην τοπολογία του **πλέγματος,** υπάρχουν δυο επιμέρους τοπολογίες για την σύνδεση των κόμβων, η τοπολογία πλήρους πλέγματος (full mesh topology) και η τοπολογία μερικού πλέγματος (partial mesh topology). Στην τοπολογία πλήρους πλέγματος οι κόμβοι μπορούν να συνδεθούν μεταξύ τους αλλά και με κόμβους που βρίσκονται σε τοπολογία πλήρους πλέγματος ενώ σε μια τοπολογία μερικού πλέγματος οι κόμβοι δεν συνδέονται όλοι μεταξύ τους αλλά μόνο με εκείνους που ανταλλάσουν περισσότερα μηνύματα μεταξύ τους . Τα δίκτυα αυτής της κατηγορίας έχουν αρκετά **πλεονεκτήματα**, όπως οι ταυτόχρονες ανοδικές και καθοδικές μεταδόσεις λόγο του σχεδιασμού τους, η διαθεσιμότητα πολλαπλών διαδρομών, η μεγάλη επεκτασιμότητα αλλά και η αυτό-προσαρμογή σε περίπτωση που κάποιος κόμβος δεν λειτούργει σωστά. Η αυτό-προσαρμογή παρολ'αυτά, αποτελεί και **μειονέκτημα**, αφού δεν μπορεί να βρεθεί εύκολα ο ελαττωματικός κόμβος. Τέλος ένα ακόμη μειονέκτημα είναι η μεγάλη καθυστέρηση επικοινωνίας, που οφείλεται στην αναμετάδοση της πληροφορίας. [21].



Εικόνα 19 Τοπολογία αστέρα και τοπολογία πλέγματος

Η τοπολογία αστέρα φαίνεται να είναι πιο ικανή έναντι της τοπολογίας πλέγματος για τα δίκτυα LPWAN, λόγο της μικρότερης κατανάλωσης ισχύος της μπαταρίας και της αυξημένης εμβέλειας [21] .

5.2 LoRa

Η τεχνολογία Lora είναι ένα πρωτόκολλο επικοινωνίας της εταιρίας Semtech που επιτρέπει την ασύρματη επικοινωνία σε μεγάλες αποστάσεις με χαμηλή ισχύ. Με τον ορό **LoRa** ορίζουμε την επικοινωνία σε φυσικό επίπεδο (**PHY**).

Εικόνα 20 Λογότυπο LoRa [58]

Βασίζεται σε μια τεχνική διαμόρφωσης σήματος που ονομάζεται Chirp Spread Spectrum (CSS). Η τεχνική διαμόρφωσης σε συνδυασμό με την δυνατότητα διόρθωσης σφαλμάτων (forward error correcting, FEC) επιτρέπει την μετάδοση των δεδομένων με ισχύ σήματος μικρότερη από το επίπεδο θορύβου στο περιβάλλον (noise floor), επιτυγχάνοντας μεταδόσεις σε πολύ μεγάλες αποστάσεις. Ένα ακόμη χαρακτηριστικό της τεχνολογίας LoRa είναι η αμφίδρομη λειτουργικότητα. Οι τελικές συσκευές (end points) μπορούν να μεταδίδουν πακέτα προς τους σταθμούς βάσης αλλά και αντίστροφα πράγμα που βρίσκει εφαρμογή στον απομακρυσμένο έλεγχο [1][68].

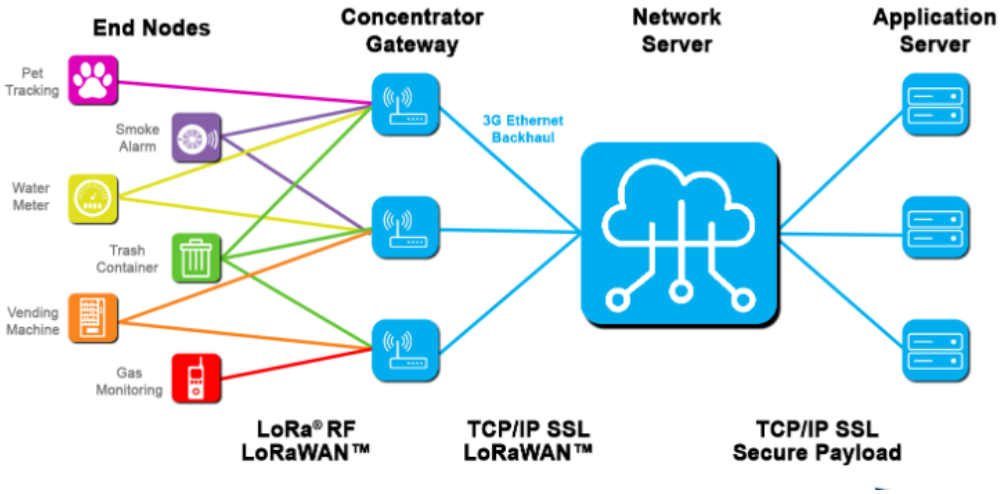
Το LoRa πρόκειται για μια τεχνολογία φυσικού επίπεδου όπου τα σήματα που μεταδίδει είναι στην ζώνη ISM sub-1GHz, χρησιμοποιώντας μια ιδιόκτητη τεχνική διασποράς φάσματος (spread spectrum) λειτουργώντας σε μη αδειοδοτημένες ζώνες . Στην Ευρώπη λειτούργει στις συχνότητες ISM 863-870 MHz , στη Βόρεια Αμερική στις ζώνες 902-928 MHz, στην κινά στις ζώνες 779-787 MHz & 470-510 MHz και στην Αυστραλία στις ζώνες 915-928 MHz[1] .

5.2.1 LoRaWAN

Με τον ορό **LoRaWAN** αναφερόμαστε στο πρωτόκολλο επικοινωνίας και στην αρχιτεκτονική συστήματος του δικτύου σε αντίθεση με το LoRa που αναφερόμαστε στην σύνδεση της επικοινωνίας . Η αρχιτεκτονική του LoRaWAN έχει επικεντρωθεί στις προδιαγραφές των LPWAN δικτύων όπως η μεγίστη διάρκεια ζωής της μπαταρίας , η χωρητικότητα δικτύου , η κάλυψη και το κόστος [1][68].

5.2.2 Αρχιτεκτονική

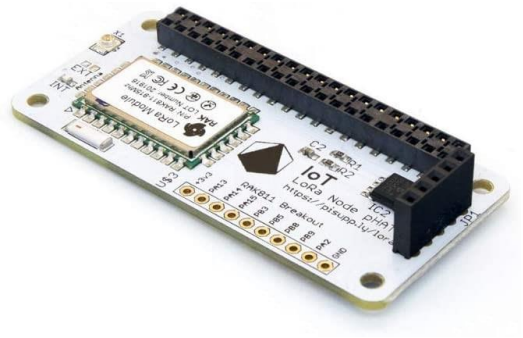
Τα δίκτυα LoRaWAN χρησιμοποιούν την τοπολογία αστέρα (star topology) . Οι πύλες εκτελούν αναμετάδοση των πακέτων μεταξύ των συσκευών και του κεντρικού διακομιστή δικτύου. Οι κόμβοι EDs δεν συνδέονται σε μια συγκεκριμένη πύλη, αλλά τα δεδομένα που μεταδίδουν λαμβάνονται από πολλές πύλες GWs. Η επικοινωνία των τερματικών συσκευών με τις πύλες GWs γίνεται μέσω της επικοινωνίας LoRa μονού άλματος (single-hop) ενώ η σύνδεση του κεντρικού διακομιστή δικτύου με τις πύλες GWs γίνεται με μια τυπική διεύθυνση IP. Ο ρυθμός μετάδοσης δεδομένων κυμαίνεται από 0,3 έως 50 kbps καθώς ένας χαμηλός ρυθμός έχει μεγαλύτερη εμβέλεια, μικρότερη κατανάλωση ενέργειας, αλλά και κάποια καθυστέρηση στα πακέτα (latency). Έτσι μια υποδομή του δικτύου LoRaWAN καθορίζει αυτόματα το κανάλι και τον ρυθμό μετάδοσης των δεδομένων, χρησιμοποιώντας ένα προσαρμοστικό σχήμα μετάδοσης δεδομένων (Adaptive Data Rate, ADR)[68].



Εικόνα 21 Αρχιτεκτονική δικτύου LoRa [63]

Η αρχιτεκτονική ενός δικτύου LoRaWAN περιγράφεται από τα παρακάτω τμήματα :

1) **End Device ,ED** : είναι μια συσκευή που συνήθως τροφοδοτείται από μπαταρία και είναι εξοπλισμένη με ένα chip LoRa για να μπορεί να στέλνει ή να λαμβάνει πληροφορίες. Ακόμη διαθέτει αισθητήρες (sensors) , ανιχνευτές (detectors) ή ενεργοποιητέ.ς (actuators)



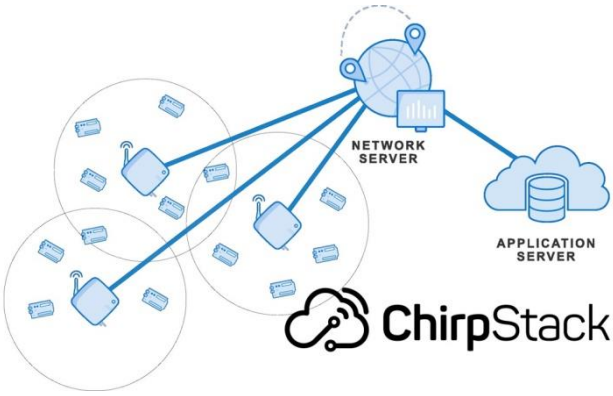
Εικόνα 22 Κόμβος LoRa [64]

2) **GateWay ,GW** : είναι μια συσκευή μόντεμ (modem) ή ένα σημείο πρόσβασης (access point), που είναι υπεύθυνο για την προώθηση μηνυμάτων από και προς μια ED και το Διακομιστή Δικτύου (Network Server, NS). Ένα σύστημα LoRaWAN περιλαμβάνει συνήθως περισσότερες από μια πύλες GW.

Εικόνα 23 Πύλη LoRa [65]

Ένα Gateway διαθέτει έναν μικροεπεξεργαστή για την επεξεργασία δεδομένων , μια θύρα Ethernet για την πρόσβαση των πυλών στο διαδίκτυο και ένα ολοκληρωμένο που είναι υπεύθυνο για την ραδιοσυχνότητες του LoRa.

3) Διακομιστής δικτύου Network Server NS



Εικόνα 24 Διακομιστής δικτύου LoRa Chirpstack [66]

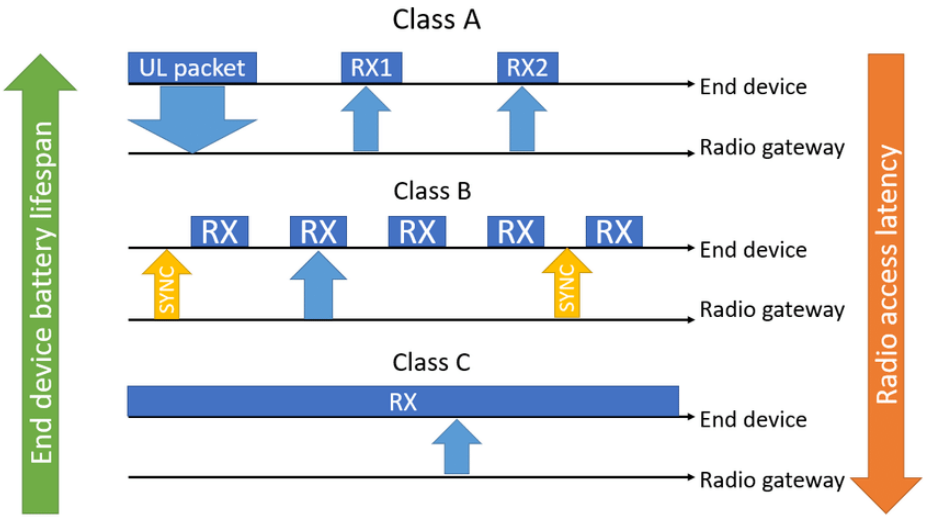
Ο διακομιστής ενός δικτύου LoRa είναι υπεύθυνος για την διαχείριση και την παρακολούθηση των GWs και EDs. Είναι μια πλατφόρμα cloud κατάλληλη για LoRaWAN και περιέχει ένα λογισμικό που προσφέρει ασφάλεια κάνοντας ταυτοποίηση των EDs . Έργο του είναι α) η δρομολόγηση και η προώθηση στον διακομιστή εφαρμογών (Application Server, AS), των ληφθέντων δεδομένων, β) η επεξεργασία των πακέτων, αφαιρώντας τα διπλότυπα δεδομένα που πρόεκυψαν από δεδομένα που στάλθηκαν από ένα ED μέσω πολλαπλών GWs. Τέλος επιλέγει μια πύλη GW με βάση την υψηλότερη αντοχή λήψης σήματος (Received Signal Strength, RSS)

4) Διακομιστής εφαρμογών (Application Server, AS)

Στον διακομιστή εφαρμογών LoRa γίνεται η ανάλυση των δεδομένων που λαμβάνονται από όλα τα EDs. Για παράδειγμα σε ένα σύστημα που είναι εγκατεστημένο σε ένα θερμοκήπιο αν η υγρασία των φυτών πέσει κάτω από ένα όριο, να αποφασίσει να ενεργοποιήσει το αυτόματο πότισμα .

5.2.3 LoRaWAN κλάσεις συσκευών end points

Οι τελικές συσκευές EDs μπορούν να εξυπηρετήσουν διαφορετικές εφαρμογές και να έχουν διαφορετικές απαιτήσεις. Με βάση τις απαιτήσεις κάθε εφαρμογής το LoRaWAN διαχωρίζει τα EDs σε κλάσεις. Τα EDs χωρίζονται σε τρεις κλάσεις A,B και C, ο διαχωρισμός των οποίων γίνεται με βάση την καθυστέρηση επικοινωνίας μεταξύ ED και GW και την διάρκεια ζωής της μπαταρίας[1] .



Εικόνα 25 Κλάσεις συσκευών end points LoRaWAN

Αμφίδρομες τελικές συσκευές (Κλάση Α) : Οι κόμβοι που ανήκουν στην κλάση Α λειτουργούν με αμφίδρομη επικοινωνία, κατά την μετάδοση των οποίων υπάρχουν δυο μικρές λήψεις. Οι συσκευές EDs αυτής της κλάσης καταναλώνουν την χαμηλότερη ισχύ σε σχέση με τους κόμβους των υπολοίπων κλάσεων αλλά περιορίζονται στην downlink επικοινωνία. Κατά την λειτουργία του κόμβου, το πρώτο παράθυρο λήψης (Receive Window) Rx1 ενεργοποιείται μετά από την καθυστέρηση λήψης (Receive Delay), 1 sec αφού τελειώσει η διαμόρφωση ανερχόμενης ζεύξης (uplink modulation). Στην περίπτωση που η πύλη δεν μπορεί να στείλει μήνυμα κατερχόμενης ζεύξης ο κόμβος ανοίγει ένα δεύτερο παράθυρο λήψης Rx2 (2sec).

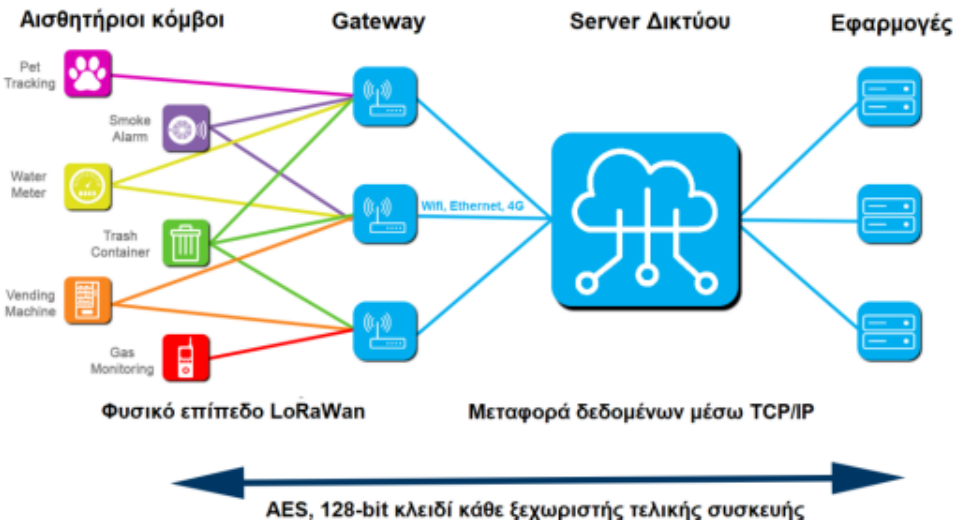
Αμφίδρομες συσκευές με προγραμματισμένες υποδοχές λήψης (κλάση Β) : Οι κόμβοι που ανήκουν στην κλάση Β διαθέτουν τα χαρακτηριστικά της κλάσης Α αλλά επιτρέπουν και την λήψη σε προγραμματισμένες στιγμές αφού λάβουν ένα σήμα συγχρονισμού από το gateway. Με αυτό τον τρόπο ο NS μπορεί να γνωρίζει σε ποιες χρονικές στιγμές ο κόμβος μπορεί να δεχτεί κάποιο σήμα . Η ισχύς που καταναλώνει είναι περισσότερη σε σχέση με την κλάση Α.

Αμφίδρομες συσκευές με μέγιστες υποδοχές λήψης (κλάση Γ) : Οι κόμβοι που ανήκουν στην κλάση Γ έχουν την μεγαλύτερη κατανάλωση ισχύς σε σχέση με τις προηγούμενες κλάσεις, αλλά μπορούν να δέχονται μηνύματα ανά πάσα στιγμή έκτος από την στιγμή της μετάδοσης.

5.2.4 Ασφάλεια LoRaWAN

Η **ασφάλεια** αποτελεί ένα από τα **σημαντικότερα κριτήρια** όλων των **IoT εφαρμογών**, έτσι κατά την σχεδίαση του LoRaWAN εκτός από τα γενικά κριτήρια σχεδιασμού του, όπως η χαμηλή κατανάλωση ενέργειας, η υψηλή επεκτασιμότητα, το χαμηλό κόστος κατασκευής και η χαμηλή πολυπλοκότητα υλοποίησης, χρησιμοποιήθηκαν δυο ακόμα επίπεδα ασφάλειας α) για το δίκτυο και β) για την εφαρμογή .

Στο επίπεδο ασφάλειας του δικτύου έχουμε την διασφάλιση της αυθεντικότητας του κάθε κόμβου στο δίκτυο ενώ στην ασφάλεια της εφαρμογής έχουμε την διασφάλιση ότι τα δεδομένα μπορεί να τα δει μόνο ο τελικός χρήστης. Επιπλέον το LoRaWAN διαθέτει αλλά δυο επίπεδα κρυπτογράφησης. Αρχικά διαθέτει ένα κλειδί συνεδρίας δικτύου (Network Session Key, NwkSKey) 128 –bit το οποίο είναι κοινόχρηστο, αναγνωρίζεται από τους κόμβους του δικτύου, και χρησιμοποιείται για την υπογραφή του πακέτου. Ο Network server κάνει την επαλήθευση της ταυτότητας του αποστολέα ενώ υπάρχει και το Application session key 128-bit το οποίο είναι κρυφό κλειδί. Ο application server με την χρήση του Application session key κάνει την αποκρυπτογράφηση των δεδομένων. Τέλος κάθε συσκευή LoRaWAN διαθέτει ακόμα ένα παγκοσμίως μοναδικό αναγνωριστικό (DevEUI με βάση το EUI-64) που χρησιμοποιείται για την διαδικασία της ταυτοποίησης κάθε κόμβου[1][68].



Εικόνα 26 Ασφάλεια LoRaWAN

5.2.5 Ενεργοποίηση End points

Για να γίνει η προσθήκη μιας νέας συσκευής στο δίκτυο του LoRa πρέπει να γίνει μια από τις παρακάτω τεχνικές επαλήθευσης : Η ενεργοποίηση Personalizaton (ABP) ή η ενεργοποίηση Over-The-Air (OTAA). Αφού ολοκληρωθεί αυτή η διαδικασία το κλειδί συνεδρίας δικτύου και το κλειδί συνεδρίας εφαρμογής θα υπάρχει μέσα στην συσκευή και θα μπορεί να λειτουργήσει σαν ED [1].

5.2.6 Over-The-Air-Activation (OTAA)

Η μέθοδος ενεργοποίησης OTAA αποτελεί την πιο ασφαλή ενεργοποίηση μιας τελικής συσκευής ED αφού πρέπει πρώτα να εκχωρηθεί μια δυναμική διεύθυνση στο δίκτυο και στην συσκευή [1].

5.2.7 Ενεργοποίηση Με εξατομίκευση (ABP)

Η μέθοδος ενεργοποίησης ABP κάνει κωδικοποίηση στα κλειδιά ασφάλειας της συσκευής, είναι πιο ευάλωτη σε σχέση με την μέθοδο OTAA και με κάθε αλλαγή στο δίκτυο θα πρέπει να γίνεται χειροκίνητη αλλαγή των κλειδιών στην τελική συσκευή ED [1].

Πλεονεκτήματα χρήσης LoRaWAN

- Χρησιμοποιεί τις ελεύθερες ζώνες ISM 868 MHz/ 915 MHz, οι οποίες είναι διαθέσιμες παγκοσμίως.
- Μεγάλη διάρκεια ζωής μπαταριάς με μέσο χρόνο ζωής τα 10 χρόνια
- Μεγάλη εμβέλεια της τάξης των 15 km σε βιομηχανικές περιοχές ενώ 5 km σε αστικές
- Χαμηλό κόστος κόμβου
- Λειτουργιά τριών τάξεων για εξυπηρέτηση διαφόρων εφαρμογών
- Δεν απαιτείται κάποια μηναία συνδρομή

Μειονεκτήματα χρήσης LoRaWAN

- Η πύλη Gateway δεν μπορεί να εξυπηρέτησει πολλούς κόμβους
- Υψηλό κόστος gateway

- Οι εφαρμογές που μπορεί να εξυπηρέτησει πρέπει να έχουν πολύ χαμηλό ρυθμό δεδομένων έως 27 kbps
- Χρησιμοποιεί μη αδειοδοτημένες ζώνες συχνοτήτων και τους περιορισμούς που αυτές περιλαμβάνουν (duty cycle, crowded bands, περιορισμένη ισχύς).

Πινάκας 1 Χαρακτηριστικά LoRaWAN

LoRaWAN	
Ανάπτυξη	LoRaWAN EDs ,GateWays
Συχνότητα	868 MHz, 433 MHz
Εμβέλεια	15 χιλιόμετρα
Ρυθμός δεδομένων	0.3 Kbps -50 Kbps
Uplink	14dBm
Διάρκεια ζωής μπαταριάς	10 χρόνια
Κλάσεις	Κλάση A, Κλάση B, Κλάση C
Διαμόρφωση	CSS
Κόστος	300 ευρώ/χρόνο
Εύρος ζώνης	125 kHz
MAC layer	Aloha based

5.3 Weightless

Εικόνα 27 Λογότυπο Weightless [60]

Το weightless είναι μια τεχνολογία που κυκλοφόρησε στα τέλη του 2015 από την ομάδα Weightless-SIG (Special Interest Group). Χρησιμοποιεί μη αδειοδοτημένες ζώνες συχνοτήτων όπως τα πρωτοκόλλα LoRa και Sigfox και διαθέτει χαρακτηριστικά όπως, μεγάλη εμβέλεια δικτύου, χαμηλή κατανάλωση ενεργείας και μεγάλη επεκτασιμότητα. Το Weightless υποστηρίζει το Firmware-Over-The-Air (FOTA) και είναι ικανό να εξυπηρέτησει εφαρμογές εξαιρετικά χαμηλής ισχύος χρησιμοποιώντας κόμβου με μπαταρία αλλά και συσκευές που τροφοδοτούνται με ρεύμα [1].

Υποστηρίζει τρία διαφορετικά πρότυπα : α) το Weightless-N (nWave) όπου χρησιμοποιεί το πρότυπο ALOHA σε μη αδειοδοτημένες ζώνες με μονόδρομη επικοινωνία των κόμβων όπου επιτυγχάνεται εμβέλεια επικοινωνίας έως και 3 km με ρυθμό δεδομένων έως και 100kbps, με εξαιρετικά χαμηλό κόστος. Β) το Weightless-W όπου χρησιμοποιεί ένα μέρος φάσματος που καταλάμβανε παλιά η τηλεόραση (TV whitespace spectrum) στην ζώνη συχνοτήτων 470-790 MHz. Η μετάδοση του είναι καλύτερη σε σύγκριση με το Weightless-N και P και το μέγεθος του κάθε πακέτου μπορεί να είναι έως και 10 bytes με ρυθμό μετάδοσης από 1 kbps έως 10 Mbps. Γ) το Weightless-P επικεντρώνεται στον σχεδιασμό για την υψηλή απόδοση . Χρησιμοποίει Gaussian minimum shift keying (GMSK) και quadrature phase-shift keying (QPSK) και δίνει την δυνατότητα αμφίδρομης επικοινωνίας. Ο ρυθμός δεδομένων είναι από 200bps έως 100kbps και προσεγγίζει τις ζώνες ISM sub-1Ghz έχοντας μικρότερη εμβέλεια από το Weightless-N 2km. Χρησιμοποιεί AES-128/256 bit κρυπτογράφηση στις πληροφορίες κατά την μετάδοση[1][34].

Η αποδοτικότητα του φάσματος, η καθυστέρηση, η αξιοπιστία της μετάδοσης, η κατανάλωση ισχύος και η αμφίδρομη επικοινωνία είναι κάποιες βασικές απαιτήσεις του QoS. Το Weightless φαίνεται να μπορεί να υποστηρίζει αυτές τις απαιτήσεις σε μεγαλύτερο βαθμό από ότι το LoRaWAN διότι οι μεταδόσεις μεταξύ των EDs με τις DCU είναι προγραμματισμένες, και έτσι εγγυάται ότι δεν θα υπάρχουν αποτυχημένες

αποστολές στο δίκτυο, υποστηρίζοντας την πλήρη επιβεβαίωση της αξιοπιστίας κάθε μετάδοσης.

5.4 Ingenu

Εικόνα 28 Λογότυπο Ingenu [59]

Η Ingenu, είναι μια τεχνολογία LPWAN όπου ιδρύθηκε το 2008 και αρχικά στράφηκε σε εφαρμογές βιομηχανίας για την μέτρηση του πετρελαίου και το φυσικού αερίου. Ωστόσο τα επόμενα χρόνια άρχισε να επεκτείνεται και σε εφαρμογές IoT . Η τεχνολογία Ingenu αποτελεί μια ιδιοκτήτη λύση και βασίζεται στην τεχνική πολλαπλής πρόσβασης τυχαίας φάσης (Random Phase Multiple Access, RPMA) κάνοντάς την να έχει πολύ υψηλή απόδοση και χωρητικότητα [1]. Η τεχνική αυτή είναι ιδιοκτήτη αφού η εταιρία είναι ο μοναδικός προγραμματιστής και κατασκευαστής. Χρησιμοποιεί την τεχνική άμεσης ακολουθίας spread spectrum και έχει μέγιστο ρυθμό μετάδοσης έως 80 kbps. Η ζώνη συχνοτήτων του είναι τα 2.4GHz πράγμα που περιορίζει την εμβέλεια του σε σχέση με τα υπόλοιπα πρωτόκολλα όπως το LoRa και το NB-IoT. Ακόμη η ζώνη συχνοτήτων 2.4GHz επειδή χρησιμοποιείται ευρέως από πολλά αλλά πρωτοκόλλα επικοινωνίας όπως το Wi-Fi συναντά αρκετές παρεμβολές .Το Ingenu έχει χαμηλό κόστος κατασκευής, χαμηλή κατανάλωση ισχύος, παρέχοντας αμφίδρομη επικοινωνία. Τέλος η τεχνολογία Ingenu συνίσταται για εφαρμογές που χρειάζονται ακριβή παρακολούθηση της τοποθεσίας αφού έχει ενσωματωμένο το Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης GNSS [1][35].

5.5 Sigfox

Εικόνα 29 Λογότυπο Sigfox [55]

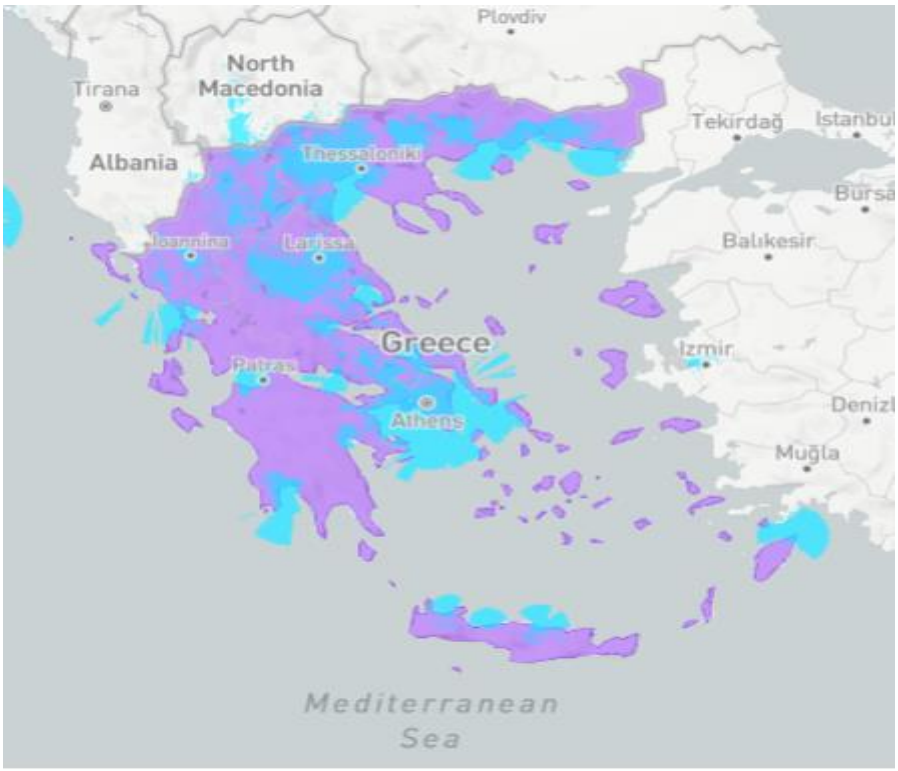
Η sigfox είναι μια γαλλική εταιρία που ιδρύθηκε το 2010 η όποια κατασκευάζει ασύρματα δίκτυα ιδιωτικής χρήσης (proprietary technology) με στόχο την χαμηλή κατανάλωση ισχύος και end-to-end συνδεσιμότητα. Το sigfox χρησιμοποιεί μη αδειοδοτημένες ζώνες συχνοτήτων και η μετάδοση των δεδομένων γίνεται σε μια πολύ στενή ζώνη (Ultra Narrow Band – UNB) συχνοτήτων χρησιμοποιώντας όλο το εύρος συχνοτήτων, κάνοντας το ευαίσθητο στον θόρυβο.

Το κόστος κατασκευής της κεραίας είναι χαμηλό αφού η ταχύτητα μετάδοσης των δεδομένων περιορίζεται στα 100 bps. Το sigfox χρησιμοποιεί την τοπολογία αστέρα (star network) όπου κάθε ένα σήμα που στέλνει ένας τελικός κόμβο ED πηγαίνει σε έναν σταθμό βάσης και στην συνεχεία προωθείται στο cloud του sigfox. Είναι ένα δίκτυο αμφίδρομης επικοινωνίας δηλαδή επιτρέπει και την uplink επικοινωνία αλλά και την downlink[1] . Για να γίνει μια επικοινωνία από τον σταθμό βάσης προς τις τελικές συσκευές πρέπει πρώτα να ακολουθηθεί μια uplinlk επικοινωνία, δηλαδή η τελική συσκευή να ανοίξει μια επικοινωνία προς τους σταθμούς βάσης και στην συνεχεία να γίνει η επικοινωνία από τον σταθμό βάσης . Ο μέγιστος αριθμός bytes ενός μηνύματος είναι 12 ενώ ο συνολικός αριθμός μηνυμάτων uplink την ημέρα περιορίζεται στα 140 ενώ για την καθοδική ζεύξη είναι μόνο 4 για κάθε τελική συσκευή πράγμα που καθιστά αδύνατη την επιβεβαίωση άφιξης κάθε μηνύματος ανοδικής ζεύξης από τον σταθμό βάσης προς τις τελικές συσκευές ενώ το μήκος των μηνυμάτων δεν πρέπει να ξεπερνά τα 8 bytes.

Παρόλα αυτά το sigfox χρησιμοποιεί έναν άλλο μηχανισμό κάνοντας επαλήθευση χρησιμοποιώντας μετάδοση σε πλήθος χρονικών στιγμών και συχνοτήτων κάνοντας πολλαπλές αποστολές του ιδίου μηνύματος σε διαφορετικά κανάλια συχνοτήτων. Στην Ευρώπη η ζώνη συχνοτήτων είναι μεταξύ 868.10 MHz και 868.220 MHz και διαχωρίζεται σε 400 κανάλια των 100 Hz εκ των οποίων τα 40 είναι δεσμευμένα και δεν χρησιμοποιούνται. Οι τελικές συσκευές μπορούν να επιλέξουν αυτόματα ένα κανάλι συχνότητας για την μετάδοση των μηνυμάτων αφού όλοι οι σταθμοί βάσης μπορούν να κάνουν σάρωση σε όλα τα κανάλια και

αποκωδικοποίηση των μηνυμάτων. Έτσι για να αυξηθεί η πιθανότητα επιτυχής λήψης από τους σταθμούς βάσης οι κόμβοι ρυθμίζονται να μεταδίδουν τα μηνύματα τουλάχιστον 3 φορές[1] .

Το δίκτυο sigfox ξεκίνησε από την Γαλλία το 2014 με συνολικά 1300 σταθμούς βάσης ενώ μέχρι σήμερα το δίκτυο έχει επεκταθεί και καλύπτει έκταση 6 εκατομμυρίων km2 παγκοσμίως, σε 75 χώρες, με πληθυσμιακή κάλυψη 1.4 δισεκατομμυρίου ανθρώπων. Στην παρακάτω εικόνα βλέπουμε την κάλυψη του δικτύου sigfox στην Ελλάδα το 2022 . (με μωβ χρώμα είναι Country under roll-out ενώ με μπλε χρώμα είναι Live Coverage)



Εικόνα 30 Κάλυψη δικτύου Sigfox στην Ελλάδα [55]

Πινάκας 2 Χαρακτηριστικά SigFox

SigFox	
Εύρος ζώνης	100Hz
Διαμόρφωση	BPSK
Συχνότητες	Ευρώπη 868 MHz
MCL	160db
Ρυθμός μετάδοσης δεδομένων	100bps
Εμβέλεια	40 χιλιόμετρα
Διάρκεια ζωής μπαταριάς	10 χρόνια
MAC Layer	Aloha based

5.6 MIOTY

Εικόνα 31 Λογότυπο MIOTY [52]

Το MIOTY είναι μια τεχνολογία LPWAN που προορίζεται για ιδιωτικά δίκτυα IoT και έχει δημιουργηθεί από μια γερμανική εταιρία την Fraunhofer IIS (Erlangen, Germany) το 2016 . Το MIOTY είναι εξοπλισμένο με μια τεχνολογία βάση του προτύπου ETSI TS 103 357 που εκτελεί πολλαπλή πρόσβαση στην διαίρεση τηλεγραφήματος (TSMA), το οποίο είναι ένα τυχαίο MAC πλαίσιο στο οποίο η μετάδοση ενός πακέτου διαχωρίζεται σε επτά πακέτα που μεταδίδονται με τυχαίο τρόπο σε διαφορετικούς χρόνους και σε διαφορετικά κανάλια . Ακόμη

βασίζεται στην τεχνολογία UNB και έχει πολύ στενό εύρος ζώνης της τάξης των 2kHz ώστε να μπορέσει να επιτύχει την επικοινωνία σε μεγάλες αποστάσεις μεταξύ χιλιάδων συσκευών IoT και ενός σταθμού βάσης . Ακόμη, χρησιμοποιεί στενό εύρος ζώνης για να μπορέσει να ελαχιστοποιήσει το επίπεδο του θορύβου, και η πολυπλοκότητα του πομποδέκτη να είναι χαμηλή [39]. Η τεχνική διαμόρφωσης που χρησιμοποιεί είναι GMSK. Το MIOTY προσφέρει εμβέλεια επικοινωνίας έως και 5 χιλιόμετρα σε αστικές περιοχές και έως 15 χιλιόμετρα σε ανοιχτούς χώρους. Ο ρυθμός μετάδοσης των δεδομένων είναι 512bps και χρησιμοποιεί μη αδειοδοτημένες ζώνες συχνοτήτων. Για την Ευρώπη χρησιμοποιεί τις συχνότητες 433 MHz και 868 MHz ενώ για τις Ηνωμένες πολιτείες 915 MHz. Το μέγεθος των πακέτων που μπορεί να στείλει κυμαίνεται από 10 έως 192 bytes και η καθυστέρηση μετάδοσης ενός πακέτου είναι 10 δευτερόλεπτα. Τέλος το MIOTY χρησιμοποιεί την τοπολογία αστέρα όπου υπάρχει ένας κεντρικός GW και συνδέονται όλα τα EDs όπου χρησιμοποιείται κρυπτογράφηση δικτύου εφαρμόζοντας το πρωτόκολλο ασφάλειας AES128 [39].

5.7 LTE-M

Εικόνα 32 Λογότυπο LTE-M [53]

Το Long Term Evolution—Machine Type Communications είναι μια τεχνολογία βασισμένη σε πρότυπα δικτύων ευρείας ζώνης χαμηλής ισχύος (LPWAN) που λειτουργεί σε αδειοδοτημένες ζώνες συχνοτήτων . Το LTE-M όπως και το NB-IoT αποτελούν δυο αλληλένδετες και συμπληρωματικές λύσεις αφού και τα δυο βασίζονται στο 4G LTE [1].

Η τεχνολογία LTE-M μπορεί να υποστηρίξει ένα ευρύ φάσμα εφαρμογών IoT και είναι φτιαγμένη για εφαρμογές που χρειάζονται υψηλούς ρυθμούς μετάδοσης δεδομένων με πολύ χαμηλή κατανάλωση ισχύος, πολύ χαμηλή καθυστέρηση και ευρεία κάλυψη. Ακόμη, αυτή η τεχνολογία μπορεί να υποστηρίξει την δυνατότητα

φωνής μέσω LTE(VoLTE). Ένα ακόμα προνόμιο αυτής της τεχνολογίας είναι ότι διαθέτει όλα τα χαρακτηριστικά ασφάλειας του ομίλου τηλεπικοινωνιακών οργανισμών 3GPP. Το LTE-M μπορεί να υποστηρίξει ένα πολύ μεγάλο αριθμό συσκευών με 100.000 ή και περισσότερες συσκευές ανά σταθμό βάσης. Ο κάθε κόμβος είναι σχεδιασμένος να λειτουργεί με μπαταριές και να έχει πολύ χαμηλή κατανάλωση ισχύος ώστε να μπορεί να εξυπηρετήσει εφαρμογές σε δυσπρόσιτα μέρη. Η κάλυψη του δικτύου είναι πολύ μεγάλη καθώς είναι συμβατό με τα δίκτυα LTE της κινητής τηλεφωνίας[1][7] .

5.7.1 Αρχιτεκτονική LTE-M

Το LTE είναι μια τεχνολογία, βασισμένη στο πρωτόκολλο δικτύου IP για την βελτίωση του 3G . Το LTE-M με βάση το 3GPP 12 περιλαμβάνει μια λειτουργία για εξοικονόμηση ισχύος κατά την όποια η συσκευή απενεργοποιείται για μικρά χρονικά διαστήματα, όταν όμως χρειαστεί να ξανά στείλει ένα πακέτο θα πρέπει να κάνει επανασύνδεση με το δίκτυο γεγονός που καταναλώνει περισσότερη ενεργεία. Ακόμα ένα μειονέκτημα του 3GPP 12 είναι ότι στην κατάσταση απενεργοποίησης η συσκευή δεν μπορεί να ελέγχεται. Έτσι με βάση το νέο 3GPP release 12 υποστηρίζονται 2 λειτουργίες εξοικονόμησης ενεργείας .

1) Στην λειτουργία PSM η συσκευή μπαίνει σε κατάσταση αδράνειας, αλλά διατηρεί την σύνδεση με το δίκτυο και μπορεί να δέχεται εντολές σε περίπτωση που κριθεί απαραίτητο [6][1]. Για παράδειγμα σε ένα σύστημα μετεωρολογικού σταθμού που στέλνει δεδομένα όπως θερμοκρασία, υγρασία και ταχύτητα του άνεμου, δεν έχει νόημα να στέλνει συνεχώς δεδομένα μετρήσεων διότι υπάρχει μεγάλη κατανάλωση ενεργείας . Επομένως μπαίνει σε κατάσταση αδρανείας και στέλνει δεδομένα ανά μια ώρα .

2) Στην λειτουργιά eDRX ο τελικός χρήστης μπορεί να ρυθμίσει την κατάσταση αδράνειας της συσκευής με λεπτομέρειες[6] . Η συσκευή όταν βρίσκεται σε αδράνεια αποσυνδέεται από το δίκτυα και δεν μπορεί να ελεχθεί.[7][1]

Πινάκας 3 Χαρακτηριστικά LTE-M

LTE-M	
Εύρος ζώνης	1.4MHz
Διαμόρφωση	16QAM
Συχνότητες	B20 (800 MHz), B8 (900 MHz), B3 (1800MHz)
MCL	156db
Ρυθμός μετάδοσης δεδομένων	1Mbps
Εμβέλεια	5 χιλιόμετρα
Διάρκεια ζωής μπαταριάς	10 χρόνια
MAC Layer	LTE

5.8 Narrow band Internet of Things

Εικόνα 33 Λογότυπο NB-IoT [54]

Το NB-IoT είναι μια τεχνολογία LPWAN που μπορεί να εξυπηρετεί την σύνδεση μιας μεγάλης γκάμας συσκευών και υπηρεσιών. Η κατασκευή του έχει βασιστεί σε μια ήδη υπάρχουσα τεχνολογία 4G LTE [5] που χρησιμοποιείται εδώ και πολλά χρόνια για την ασύρματη δικτύωση συσκευών και παρέχει πολύ υψηλές ταχύτητες δεδομένων χρησιμοποιώντας αδειοδοτημένες ζώνες συχνοτήτων. Η τεχνολογία αυτή θα συνεχίσει να συνυπάρχει και με τα νεότερα δίκτυα 5GNR ως μέρος του υποδικτύου mIoT (massive Internet of Things).

Όπως και στο LoRaWan έτσι και στο NB-IoT οι συσκευές αναμένονται να διαρκούν 10 χρόνια με μια μπαταρία και η εμβέλεια τους να είναι της τάξης των 10 km. Το εύρος ζώνης χαμηλής συχνότητας είναι 180 KHz, προσφέροντας κάλυψη δικτύου άνω των 160db με καθυστέρηση περίπου 10 δευτερόλεπτα. Το narrow band Internet of Things αναπτύχτηκε από τον τηλεπικοινωνιακό οργανισμό 3GPP (3rd Generation Partnership Project) το 2016[1] . Είναι μια τεχνολογία που σχεδιάστηκε για να έχει μεγάλη διάρκεια ζωής η μπαταρία της κάθε συσκευής με χαμηλό κόστος, γι'αυτό και κατά τον σχεδιασμό του αφαιρέθηκαν πολλές δυνατότητες από το LTE. Το κόστος τον NB-IoT modules ανέρχεται στα 20 ευρώ περίπου, ενώ η σύνδεση για την SIM εξαρτάται από τον πάροχο κινητής τηλεφωνίας. Η μετάδοση των δεδομένων γίνεται με χαμηλό ρυθμό και έχει ως αποτέλεσμα την μείωση της κατανάλωσης ισχύος[1][13]. Για την υλοποίηση του ασύρματου κόμβου θα χρησιμοποιήσουμε την τεχνολογία **NB-IoT** όπου θα αναλυθεί περεταίρω στο επόμενο κεφάλαιο .

ΚΕΦΑΛΑΙΟ 6: Narrow band Internet of Things

6.1 Αρχιτεκτονική

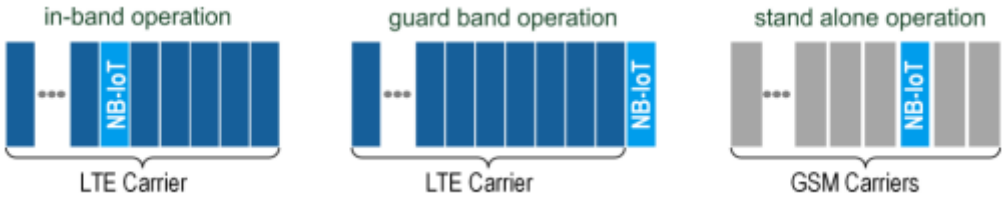
Το δίκτυα NB IoT βασίζονται στο σύστημα πακέτων EPS όπου περιέχει δυο βελτιστοποιημένα επίπεδα για το κυψελοειδές διαδίκτυο των πραγμάτων CIoT : α) το επίπεδο CIoT EPS Plane User και β) το επίπεδο CIoT EPS Plane Control. Και τα δυο επίπεδα βρίσκουν την καλύτερη διαδρομή για πακέτα των δεδομένων για uplink και downlink ζεύξης. Ακόμη, στο NB-IoT υπάρχουν δυο μηχανισμοί που χρησιμοποιούνται για την χαμηλή κατανάλωση ισχύος, την Power Saving Mode (PSM) και την extended Discontinuous Reception (eDRx) . Στην λειτουργία PSM η συσκευή μπαίνει σε λειτουργία ύπνου έως 413 ημέρες και μπορεί να δέχεται εντολές από τον σταθμό βάσης, ενώ στην λειτουργία eDRx η συσκευή μπαίνει σε κατάσταση ύπνου για μερικά λεπτά[13] .

6.2 Τρόπος λειτουργίας

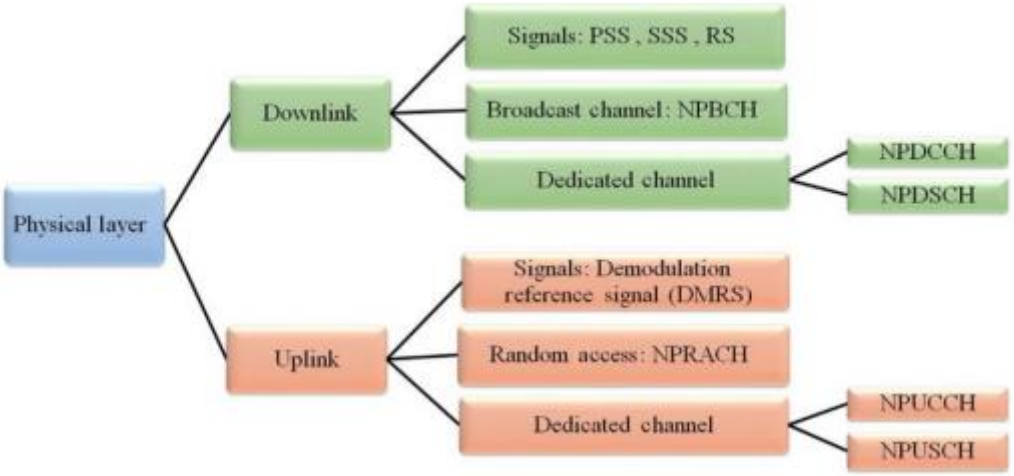
Το Narrow band Internet of Things υποστηρίζει τρεις διαφορετικούς τρόπους λειτουργίας : **in-band** ,**guard-band** και **standalone**[8] .

Στην **λειτουργία in-band**, το NB-IoT χρησιμοποιεί μια ζώνη συχνοτήτων 180 kHz ή οποία είναι μέρος ενός κανονικού φορέα LTE .

Στην λειτουργία **guard-band** το NB-IoT χρησιμοποιεί μια μπάντα συχνοτήτων 180 kHz στην πλαϊνή ζώνη συχνοτήτων ενός φορέα LTE ενώ στην λειτουργιά **standalone** χρησιμοποιείται μία ζώνη συχνοτήτων 180 kHz στην μπάντα GSM [8][1]. Το NB-IoT χρησιμοποίει ένα μηχανισμό τυχαίας προσπέλασης (NPRACH) για να αυξήσει την φασματική απόδοση και να μειώσει την πιθανότητα σύγκρουσης όταν θέλει να στείλει δεδομένα ακόμα για uplink . Για την ανοδική ζεύξη (uplink) υπάρχουν δυο φυσικά κανάλια το Narrowband Physical Upink Shared Channel (NPUSCH) και το Narrowband Physical Random-Accesss Channel (NPRAC) όπου χρησιμοποιούν QPSK ή BPSK διαμόρφωση με Single-Carrier Frequency Division Multiple Access (SC-FDMA), ενώ για την καθοδική ζεύξη (downlink) χρησιμοποιούνται τρία φυσικά κανάλια το Narrowband Physical Broadcast Channel (NPBCH) , το Narrowband Physical Downlink Control Channel (NPDCCH) και το Narrowband Physical Downlink Shared Channel (NPDSCH) όπου είναι διαμορφωμένα με QPSK και με Orthogonal Frequency Division Multiplexing (OFDM) όπως οι τυπικοί φορείς κινητής τηλεφωνίας στο LTE[1].



Εικόνα 34 Τρόποι λειτουργίας NB-IoT in-band , quard band , stand alone [62]



Εικόνα 35 Μηχανισμός τυχαίας προσπέλασης NB-IoT

6.2.1 Device to device

Το NB-IoT από την έκδοση 15 της 3GPP διαθέτει και την επικοινωνία Device to device, μια δυνατότητα όπου οι συσκευές μπορούν να συνδέονται μεταξύ τους χωρίς να υπάρχει κάποια άμεση σύνδεση με έναν κεντρικό σταθμό [12],[13]. Έτσι στο NB-IoT όταν κάποιος κόμβος δεν είναι συνδεδεμένος σε κάποιο δίκτυο , η D2D επικοινωνία βοήθα εκείνους τους κόμβους όπου γίνεται επαναπροώθηση των δεδομένων στον κεντρικό σταθμό, δηλαδή μια multi-hop δρομολόγηση πακέτων . Με αυτόν τρόπο μπορεί να γίνει δρομολόγηση δεδομένων από κόμβους που είναι τοποθετημένοι σε σημεία που δεν υπάρχει μεγάλη κάλυψη δικτύου, χρησιμοποιώντας ενδιάμεσους κόμβους όπου η επικοινωνία D2D βοηθά στην κάλυψή τους. Ακόμη η τοποθέτηση ενδιάμεσων κόμβων βοηθά το σήμα να διανύει μικρότερες αποστάσεις με στόχο την εξοικονόμηση ενεργείας . Παράλληλα οι κόμβοι NB-IoT μπορούν να χρησιμοποιούν και τα δίκτυα κινητής τηλεφωνίας που είναι συνδεδεμένα στην LTE ζώνη για την D2D επικοινωνία και όχι μόνο άλλους NB-IoT κόμβους ώστε να γίνεται

η αναμετάδοση [13][14]. Τέλος η D2D επικοινωνία δεν αναπτύσσεται μόνο σε συχνότητες που ανήκουν στην κινητή τηλεφωνία αλλά αναπτύσσονται και για ISM συχνότητες [15] .

6.3 Πλεονεκτήματα χρήσης NB-IoT

- Χαμηλό κόστος κόμβου
- Χρησιμοποιεί αδειοδοτημένες ζώνες χωρίς περιορισμούς
- Υποστηρίξει δυο μηχανισμών PSM και eDRx για μεγαλύτερη εξοικονόμηση ενέργειας
- Κάλυψη εφαρμογών σε δυσπρόσιτα σημεία λόγο της μεγάλης εμβελείας
- Σχετικά χαμηλή καθυστέρηση (latency) λόγο ικανού ρυθμού δεδομένων (data rate)
- QoS
- Επικοινωνία Device to device
- Μετάδοση δεδομένων σε χαμηλό ρυθμό για αύξηση εμβελείας
- Ανοιχτή τεχνολογία (non-proprietary)

6.4 Μειονεκτήματα χρήσης NB-IoT

- Απαιτείται συνδρομή
- Υψηλό κόστος σχεδίασης
- Μικρότερη διάρκεια ζωής της μπαταριάς σε σχέση με το LoRaWAN

Πινάκας 4 Χαρακτηριστικά NB-IoT

Ανάπτυξη	Κάρτα SIM, Plug n' Play
Συχνότητα	B20 (800 MHz), B8 (900 MHz), B3 (1800MHz)
Εμβέλεια	10 χιλιόμετρα
Ρυθμός δεδομένων	20 Kbps ,100 Kbps
Uplink	In-band, Guard-band, Stand-alone
Downlink	OFDMA
Διάρκεια ζωής μπαταριάς	10 χρόνια
MAC layer	LTE Based
Διαμόρφωση	QPSK, BPSK
Κόστος	Συνδρομή κινητής τηλεφωνίας
Εύρος ζώνης	180 KHz-200 KHz
Ισχύς στο Uplink	23 dBm, 20 dBm, 14 dBm
SC-FDMA σχήματα	Single-tone, Multi-tone
Διαχείριση ενέργειας	eDRx, PSM
Αριθμολογία	SC-FDMA3, OFDMA4

ΚΕΦΑΛΑΙΟ 7: Σύγκριση NB-IoT και LoRaWan

Και τα δυο πρωτόκολλα ανήκουν στην κατηγορία LPWAN τεχνολογιών . Το LoRaWAN φαίνεται να υπερτερεί σε εφαρμογές που βρίσκονται στον ελεύθερο χώρο ενώ το NB-IoT φαίνεται να είναι καλύτερη τεχνολογία για να αφομοιωθεί σε ένα βιομηχανικό περιβάλλον .

- **Physical features:** το LoRa είναι ένα πρωτόκολλο που χρησιμοποιεί μη αδειοδοτημένες ζώνες (ISM) με εύρος ζώνης 500 Hz – 1,25 KHz. Για να επιτευχθεί το δίκτυο LoRaWAN εφαρμόζει την τεχνική προσαρμοστική διαμόρφωση (adaptive modulation technique) ενώ αντίθετα το NB-IoT χρησιμοποιεί αδειοδοτημένες ζώνες συχνοτήτων όπως στο LTE με εύρος ζώνης 180kHz και χρησιμοποιεί 3 τρόπους λειτουργίας stand-alone, Guard-band, In-band [18], το οποίο εξυπηρετεί πιο ασφαλείς διαδικασίες όπως αυτές σε ένα βιομηχανικό περιβάλλον.

- **Network Architecture:** το LoRaWAN χρησιμοποιεί την αρχιτεκτονική Long range star όπου χρησιμοποιούνται GWs για την αναμετάδοση μηνυμάτων, ενώ το NB-IoT χρησιμοποιεί το δίκτυο LTE με Stand alone κόμβους [18].

- **Ποιότητα κάλυψης Quality of Service (QoS) και επεκτασιμότητα:** Το LoRa χρησιμοποιεί την διαμόρφωση CSS σε συνδυασμό με το gateway ενώ το NB-IoT χρησιμοποίει το πρωτόκολλο TCP στο δίκτυο LTE όπου φαίνεται να υπερτερεί σε σχέση με το LoRaWAN διότι μπορεί να εγγυηθεί την αποστολή των πακέτων [16]. Ακόμη το NB-IoT υπερτερεί στην επεκτασιμότητα των κόμβων αφού βάση κάποιων προσομοιώσεων στην λειτουργία 12 τόνων, μπορεί να στείλει 25000 μηνύματα έναντι των 2000 μηνυμάτων του LoRaWan το λεπτό [17].

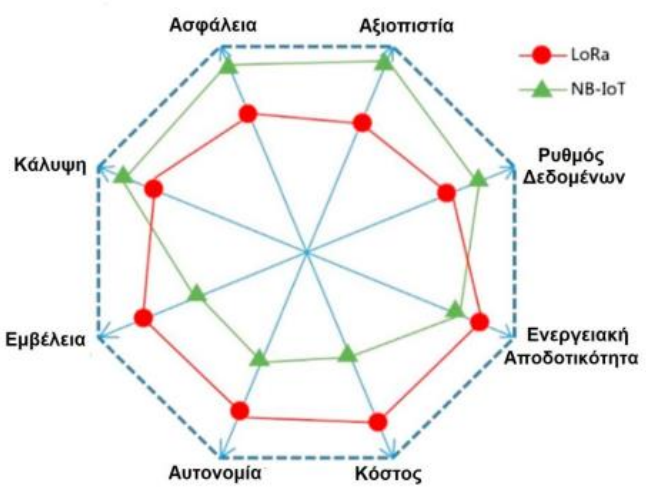
- **Κατανάλωση ενεργείας:** οι κόμβοι NB-IoT καταναλώνουν περισσότερη ενεργεία σε σχέση με τους κόμβους LoRaWan διότι το NB-IoT χρειάζεται να κάνει τακτικό συγχρονισμό με το δίκτυο LTE με αποτέλεσμα να καταναλώνεται περισσότερο η ενέργεια της μπαταρίας και ο μηχανισμός OFDM απαιτεί περισσότερη ενεργεία σε αντίθεση με το LoRaWan που βασίζεται στο ασύγχρονο πρωτόκολλο ALOHA [18].

- **Κόστος:** το LoRa φαίνεται να έχει ένα πλεονέκτημα χαμηλού κόστους αφού για το NB-IoT πρέπει να λάβουμε υπόψη ότι χρειαζόμαστε συνδρομή από πάροχο κινητής τηλεφωνίας και υπάρχει κόστος εγκατάστασης[18] .

- **Ασφάλεια** Το LoRaWan φαίνεται να υστερεί σε σχέση με το NB-IoT αφού εκτός από το πρωτόκολλο TCP χρησιμοποίει και την εξελιγμένη ασφάλεια του LTE σε αντίθεση με του LoRaWAN όπου ο κάθε κόμβος χρησιμοποιεί απλά ένα κλειδί 128 bit για την επικοινωνία του με τον server .

- **Κάλυψη εφαρμογών** με βάση κάποιες προσομοιώσεις, το LoRaWan φαίνεται να έχει μεγαλύτερη εμβέλεια στον εξωτερικό χώρο σε αντίθεση με τους κόμβους του NB-IoT οι οποίοι υπερτερούν σε ένα εσωτερικό χώρο, όπως μία βιομηχανία.

Με βάση όσα αναφέρθηκαν μεταξύ των δυο τεχνολογιών, το **NB-IoT** φαίνεται να είναι ένα <u>πιο ασφαλές πρωτόκολλο</u> που μπορεί να εγκατασταθεί στην βιομηχανία λόγο της μεγάλης κάλυψης σε εσωτερικούς χώρους, των μεγαλύτερων πακέτων με μικρότερη καθυστέρηση, καθώς σε θέμα ασφάλειας και δρομολόγησης των κόμβων του. Από την άλλη, φαίνεται το LoRaWAN να έχει λίγο μεγαλύτερη αυτονομία στην μπαταρία και μεγαλύτερη κάλυψη σε εξωτερικούς χώρους πράγμα που το κάνει ιδανικό για απομακρυσμένες εφαρμογές.



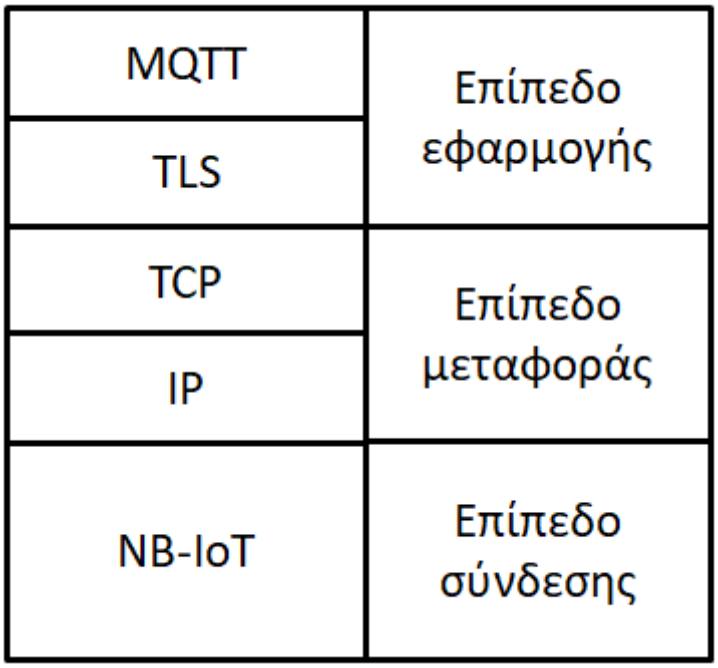
Εικόνα 36 Σύγκριση LoRa με NB-IoT

ΚΕΦΑΛΑΙΟ 8: Ασφάλεια κόμβου

Η ασφάλεια και η ακεραιότητα των δεδομένων είναι ένα από τα σημαντικότερα ζητήματα στις ασύρματες επικοινωνίες ιδίως στο διαδίκτυο των πραγμάτων (IoT)[9]. Έτσι μια ασφαλής επικοινωνία προϋποθέτει ότι οι απεσταλμένες πληροφορίες θα φθάσουν με ασφάλεια και ακεραιότητα δίχως να έχουν υποστεί κάποια υποκλοπή δεδομένων. Για την επίτευξη του στόχου της ασφάλειας υπάρχουν τρεις κύριες πτυχές, η εχεμύθεια, η ακεραιότητα και η πιστοποίηση, τις οποίες για να επιτύχουμε, χρησιμοποιούμε διάφορα πρωτόκολλα και τεχνικές κρυπτογράφησης.

Οι τεχνικές κρυπτογραφήσης όμως, χρειάζονται μεγάλη υπολογιστική ισχύ για να μπορέσουν να λειτουργήσουν, πράγμα που έρχεται σε αντιπαράθεση με τους κόμβους του IoT όπου οι πόροι (μνήμη και υπολογιστική ισχύς) των συσκευών είναι περιορισμένοι [9]. Για αυτόν τον λόγο χρησιμοποιούμε κάποια χαρακτηριστικά ασφάλειας που να μπορούν να χρησιμοποιηθούν στους κόμβους. Έτσι κατά την σχεδίαση του κόμβου, μπορεί να χρησιμοποιηθεί υλικό που να εκτελεί τις εργασίες της ασφάλειας και της κρυπτογράφησης απαλλάσσοντας τον μικροελεγκτή από τις διαδικασίες προγραμματισμού, παρατείνοντας με αυτό το τρόπο σημαντικά την διάρκεια ζωής της μπαταρίας. Ένα τέτοιο παράδειγμα, είναι τα sercure elements. Τέλος η χρήση της μνήμης για την αποθήκευση κλειδιών είναι ένας ακόμη τρόπος για να ασφαλίσεις τον κόμβο [9].

Στην εργασία χρησιμοποιήθηκε ο τρόπος της εισαγωγής κλειδιών μέσα στην μνήμη του μικροελεγκτή. Για την επίτευξη της ασφάλειας του κόμβου χρησιμοποιούνται τα παρακάτω πρωτόκολλα μετάδοσης και ασφάλειας[9]. Α) Το TCP (transmission Control Protocol) είναι ένα πρωτόκολλο μετάδοσης το οποίο παρέχει μια αξιόπιστη μεταφορά δεδομένων διαχωρίζοντας τα πακέτα ώστε να φτάσουν οργανωμένα, αναμένοντας επιβεβαίωση λήψης. Σε περίπτωση που τα δεδομένα δεν φτάσουν, ο κόμβος μπορεί να τα ξαναστείλει. Β) Το TLS/SSL (Transport Layer Security) είναι ένα πρωτόκολλο, που προσφέρει μια ασφαλή επικοινωνία. Βρίσκεται πάνω από το πρωτόκολλο μεταφοράς TCP όπου όταν γίνεται μια επικοινωνία, το TLS βοήθα στο τρόπο που θα γίνει αναγνώριση της συσκευής μέσω του αλγόριθμου cipher κατά την διάρκεια της σύνδεσης[10]. Τέλος γ) το πρωτόκολλο εφαρμογών MQTT είναι στο επίπεδο εφαρμογής βασιζόμενο σε ζεύγη εντολών public- subscribe[9][10].



Σχήμα 1 : Ταξινόμηση πρωτοκόλλων που χρησιμοποιήθηκαν

8.1 TCP/IP

Το πρωτόκολλο TCP (Transmission Control Protocol) αποτελεί ένα από τα σημαντικότερα πρωτόκολλα του δικτύου και χρησιμοποιείται στις περισσότερες περιπτώσεις που υπάρχει ανάγκη αμφίδρομης επικοινωνίας [71] . Είναι ένα πρωτόκολλο που προσφέρει αξιοπιστία στην επικοινωνία και χρειάζεται την χειραψία τριών σταδίων για την δημιουργία μιας σύνδεσης , πράγμα που έχει επίπτωση στην ταχύτητα σύνδεσης και παράλληλα στο κόστος των δεδομένων. Αφού πραγματοποιηθεί μια σύνδεση, τα δεδομένα του χρηστή στέλνονται μέσω αμφίδρομης σύνδεσης. Το TCP διαχωρίζει τα πακέτα που λαμβάνει ώστε να φτάσουν οργανωμένα στον αποστολέα περιμένοντας την αναγνώριση τους . Η παράδοση των πακέτων καθώς και η σειρά τους είναι εγγυημένη αφού , σε περίπτωση που χαθούν κάποια δεδομένα, στην πορεία θα αποσταλούν εκ νέου έως ότου τα δεδομένα φτάσουν ακέραια και με την σωστή σειρά .

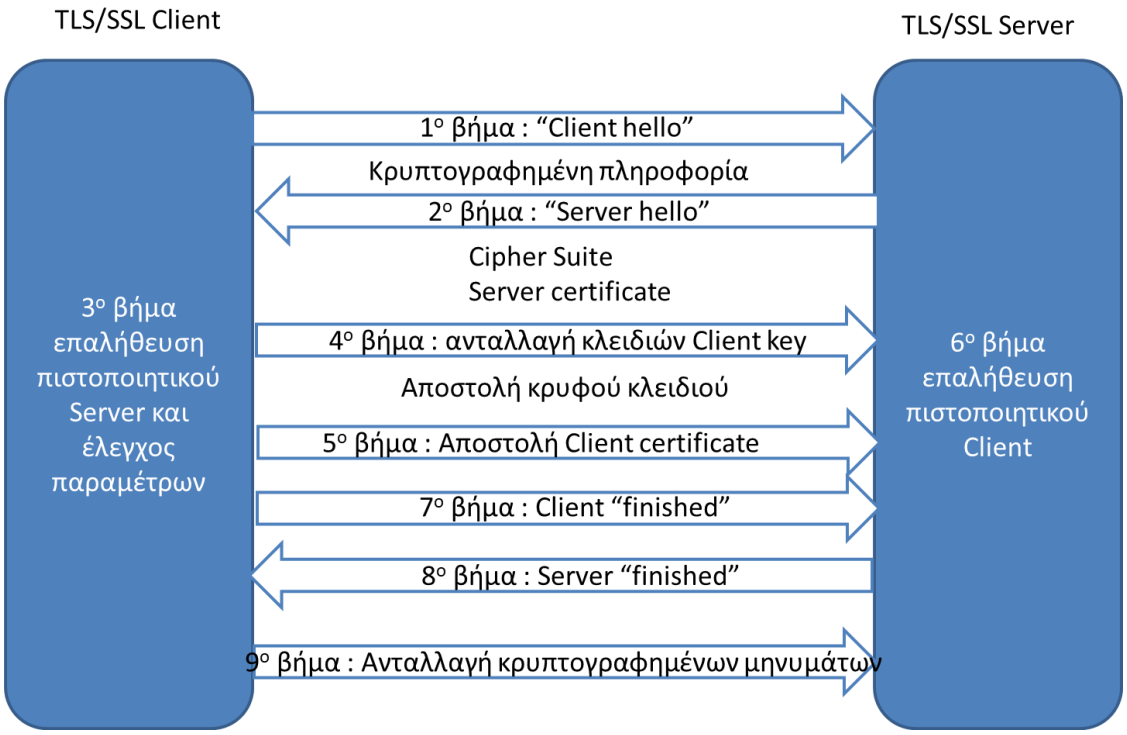
Τέλος σε περίπτωση που μια σύνδεση υπερβεί το χρονικό όριο της σύνδεσης τερματίζεται και εμφάνιζεται σφάλμα. Το πρωτόκολλο IP (Internet Protocol) βοήθα στην επικοινωνία μεταξύ των χρηστών όπου οι χρηστές αναγνωρίζονται με βάση την καθορισμένη τους IP διεύθυνση. Το IP πρωτόκολλο δεν μπορεί να προσφέρει από μόνο του αξιοπιστία για αυτό και συμπληρώνεται από το πρωτόκολλο TCP, οι επικοινωνίες TCP/IP ξεκίνησαν από την δεκαετία του 1970[71].

8.2 TLS/SSL

Το Transport Layer Security TLS είναι ένα πρωτόκολλο ασφάλειας που βασίζεται σε συγχρόνους αλγόριθμους κρυπτογραφίας και επιτρέπει την ασφαλή επικοινωνία από άκρο σε άκρο μεταξύ δυο μηχανών. Προκάτοχός του είναι, το Secure Sockets Layer SSL . Το TLS/SSL περιλαμβάνει τρία βασικά στοιχεία, όπως την κρυπτογράφηση , την πιστοποίηση και την ακεραιότητα των δεδομένων [43]. Το TLS είναι ένα πρωτόκολλο που βρίσκεται πάνω από το TCP/IP και κατά την σύνδεση μεταξύ δυο μηχανών το πρωτόκολλο αυτό ορίζει τον τρόπο με τον όποιο οι μηχανές θα αναγνωριστούν [43]. Ακόμη το TLS για την καλύτερη ασφάλεια, χρησιμοποιεί αλγορίθμους cipher και παρέχει αμοιβαία πιστοποίηση της ταυτότητας χρησιμοποιώντας πιστοποιητικά Certificate authority [43]. Το TLS παράλληλα περιλαμβάνει τον μηχανισμό Datagram Transport Layer Securiy (DTLS) που εξυπηρετεί εφαρμογές με περιορισμένους πόρους που χρησιμοποιούν το UDP .

8.2.1 Περιγραφή λειτουργίας πρωτόκολλου TLS/SSL

Κατά την διαδικασία της επικοινωνίας του πρωτόκολλου TLS/SSL παρέχεται αμοιβαία πιστοποίηση ταυτότητας με την χρήση των πιστοποιητικών για να γίνει η αυθεντικοποίηση των οντοτήτων. Η διαδικασία της επικοινωνίας αποτελείται από δυο μέρη. Το πρώτο μέρος είναι το πρωτόκολλο χειραψίας όπου γίνεται ο έλεγχος της ταυτότητας για την δημιουργία ενός ασφαλούς καναλιού επικοινωνίας. Μόλις ολοκληρωθεί το πρώτο μέρος ανταλλάσσεται το κλειδί συνεδρίας (sessionkey) και στην συνεχεία εκκινεί το δεύτερο μέρος της επικοινωνίας, που είναι το πρωτόκολλο εγγραφής και μεταφέρεται ο τύπος του περιεχομένου, η έκδοση, το μήκος και το περιεχομένου χρησιμοποιώντας κρυπτογραφία . Το παρακάτω σχήμα περιγράφει την διαδικασία χειραψίας του πρωτόκολλου TLS/SSL μεταξύ του client και του Server.



Σχήμα 2 Διαδικασία χειραψίας του πρωτόκολλου TLS/SSL

8.3 MQTT

Το Message queuing Telemetry Transport (MQTT) είναι ένα πρωτόκολλο εφαρμογής που αναπτύχτηκε αρχικά από την εταιρία IBM [40]. Είναι ένα πρωτόκολλο ασφάλειας που βρίσκεται πάνω από το πρωτόκολλο TCP όπου εγγυάται την επικοινωνία του κόμβου με τον server . Έτσι θεωρείται ιδανικό για εφαρμογές IoT κόμβων, αφού βασίζεται στην ανταλλαγή μηνυμάτων με ένα σημαντικό όμως μειονέκτημα το ότι παρέχει περιορισμένες δυνατότητες και πόρους [40][41] .

Το MQTT είναι βασισμένο στην λειτουργία publish-subscribe και διαθέτει την λειτουργία δυο χρηστών : α) τους MQTT **clients** και β) τους MQTT subscribers μέσω του MQTT **broker**. Οι MQTT clients κατατάσσονται σε δυο κατηγορίες : α) **publishers** και β) **subscribers**. Στην πρώτη κατηγορία οι clients μπορούν να στέλνουν μηνύματα στον broker ενώ στην δεύτερη κατηγορία μπορούν να λαμβάνουν μηνύματα . Η λειτουργία του broker βοήθα στην συλλογή, στην οργάνωση και την σωστή επαναπροώθηση των μηνυμάτων που έχει δεχτεί. Η διεύθυνση των μηνυμάτων δεν χρειάζεται να είναι γνωστή από τους publishers και τους subscribers αφού η

διαχείριση των μηνυμάτων γίνεται από τον broker με βάση το QoS που έχει καταχωρηθεί . Έτσι ο κάθε client μπορεί να στέλνει ή να λάβει κάποιο μήνυμα από τον broker όπου περιέχει την ονομασία του topic σε μορφή string [40][41]. Ακόμη το MQTT διαθέτει το QoS όπου προσφέρει μια εγγυημένη αποστολή πακέτων μεταξύ του broker και του client και μπορεί να καθορίσει εάν το μήνυμα θα σταλεί το πολύ μια φορά (QoS 0) ή θα σταλθεί τουλάχιστον μία φορά (QoS 1) ή ακριβώς μία φορά (QoS 2) [41].

Τέλος μεγάλο ενδιαφέρον έχουν οι λειτουργίες, **retain** και **last will** τις οποίες χρειάζεται το MQTT. Τα retained messages, είναι μηνύματα ενός topic όπου ο broker τα αποθηκεύει και τα στέλνει σε κάθε έναν νέο subscriber ενώ το last will είναι ένα καθορισμένο μήνυμα όπου μπορεί να σταλθεί σε ένα ή και σε περισσότερα topics σε περίπτωση που κάποιος χρήστης αποσυνδεθεί, πράγμα που το καθιστά πολύ χρήσιμο σε περιπτώσεις έκτακτης ανάγκης [42]. Έτσι αυτές οι λειτουργίες είναι πολύ σημαντικές για τις εφαρμογές του IoT καθώς μπορούμε να έχουμε έλεγχο των συσκευών, όπως για παράδειγμα σε ένα δίκτυο μιας βιομηχανίας με αισθητήρες, τα retained messages μπορούν να στείλουν κάποιο update στις νέες εγκαταστάσεις ή το last will να στείλει κάποιο μήνυμα στο σύστημα με τους αισθητήρες σε περίπτωση που υπάρχει κάποια βλάβη .

8.3.1 Χαρακτηρίστηκα MQTT

- Ο MQTT broker είναι εγκατεστημένος στον server όπου λαμβάνει αλλά και διαχειρίζεται όλα τα δεδομένα . Ένας MQTT Broker που είναι γνωστός είναι ο EMQX .
- Ο MQTT publishers είναι αυτοί που ενημερώνουν τον server όπως ένας αισθητήρας που στέλνει μετρήσεις .
- Ο MQTT subscriber συνδέεται στον Server και αντλεί δεδομένα .

8.3.2 Ωφέλει χρήσης πρωτόκολλου εφαρμογής MQTT

- Χρήση του πρωτόκολλου TCP (Transmission Control Protocol) όπου εγγυάται ότι όλα τα πακέτα θα σταλθούν με σωστή σειρά και διόρθωση σφαλμάτων .
- Εξασφάλιση παράδοσης μηνυμάτων .
- Πολύ ελαφρύ πρωτόκολλο επικοινωνίας.
- Είναι μια τεχνολογία που είναι σχεδιασμένη κατάλληλα για επικοινωνία M2M (MACHINE TO MACHINE).
- Αποστολή μηνυμάτων σε πολλαπλούς χρηστές με την αρχιτεκτονική publish-subscribe.
- Σύνδεση μεταξύ MQTT Client και Broker χωρίς την αποστολή μηνύματος από τον client .

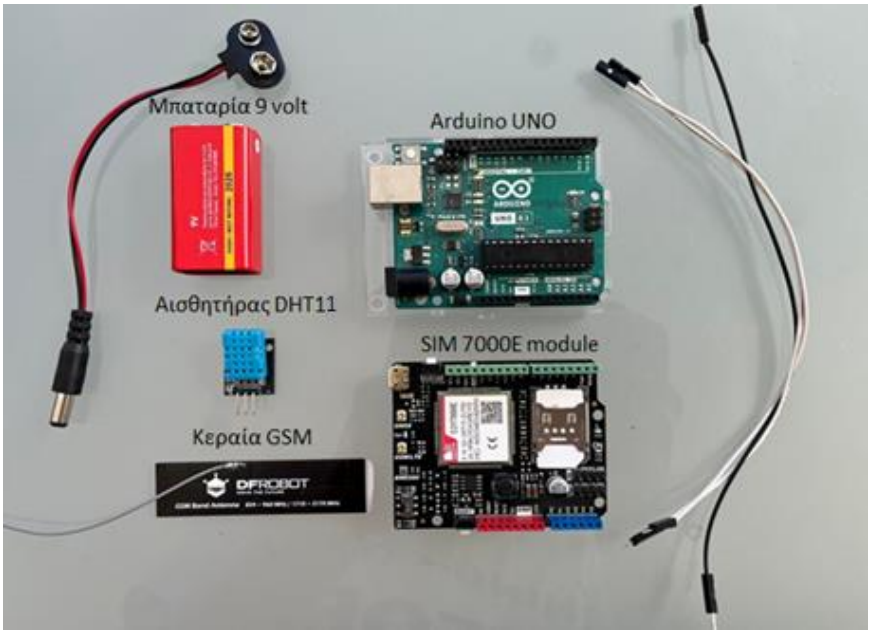
ΚΕΦΑΛΑΙΟ 9: Υλοποίηση Κατασκευής

Υλικά και Εξαρτήματα που χρησιμοποιήθηκαν

Για την υλοποίηση της κατασκευής χρησιμοποιηθήκαν τα παρακάτω εξαρτήματα και modules.

Πίνακας 5 Εξαρτήματα που χρησιμοποιήθηκαν

Εξάρτημα	Τιμή
Arduino Uno R3	20
Arduino NB-IoT module SIM7000	45
Αισθητήρας DHT11	3,5
Μπαταρία 9 volt	4,5
Κεραία για GSM συχνότητες	2



Εικόνα 37 Εξαρτήματα που χρησιμοποιήθηκαν για την κατασκευή του κόμβου

Arduino Uno

Εικόνα 38 Arduino Uno [67]

Το Arduino Uno είναι ένας προγραμματιζόμενος μικροελεγκτής που μπορεί να χρησιμοποιηθεί για διαφορές εφαρμογές. Είναι μια πλατφόρμα ανοιχτού λογισμικού και πρωτότυπων ηλεκτρονικών συσκευών που προσφέρουν ευκολία στην χρήση του υλικού και του λογισμικού. Ο μικροελεγκτής έχει ενσωματωμένο ένα μικροεπεξεργαστή της οικογενείας Atmega όπου είναι το <<μυαλό>> του και μπορεί να ελέγχει ψηφιακές αλλά και αναλογικές εισόδους και εξόδους . Ακόμη υπάρχει μια θύρα USB όπου μέσω αυτής γίνεται ο προγραμματισμός του και η μεταφορά δεδομένων. Όλα αυτά, βρίσκονται πάνω σε μια πλακέτα που γίνονται και οι συνδέσεις με τους αισθητήρες ,κινητήρες, LEDs, κ.α.[67]

Πλεονεκτήματα χρήσης Arduino

- Προγραμματιστικό περιβάλλον : το λογισμικό με το όποιο προγραμματίζουμε το arduino είναι φιλικό, απλό και πολύ εύκολο στην χρήση του αφού μπορεί εύκολα να το προγραμματίσει και ένας αρχάριος . Παρόλα αυτά είναι και ευέλικτο ώστε να μπορεί να χρησιμοποιηθεί και από πιο προχωρημένους χρήστες .
- Χαμηλό κόστος : Το arduino αποτελεί μια πολύ οικονομική λύση για την ανάπτυξη ενός project, αφού είναι η φθηνότερη πλατφόρμα που μπορεί να

αγοραστεί. Ακόμη, μπορούμε να την βρούμε και μη συναρμολογημένη, ώστε να είναι ακόμα φτηνότερη.

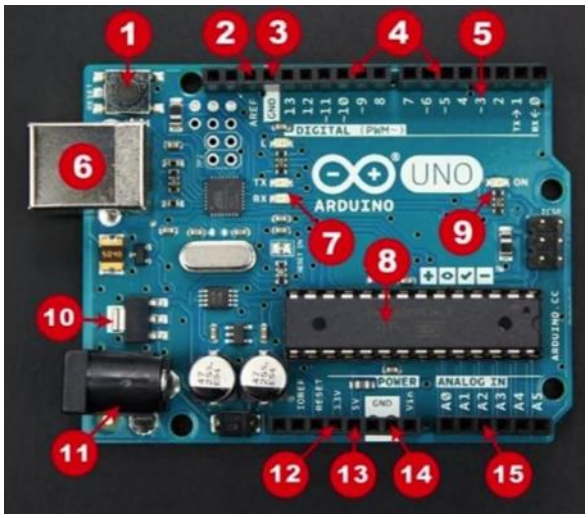
Επεκτάσιμη : Το λογισμικό και το υλικό της πλατφόρμας είναι ελεύθερο και ανοιχτό όπου μπορεί κάθε προγραμματιστής μπορεί να την φτιάξει μόνος του, δημιουργώντας νέες βιβλιοθήκες για την υποστήριξη της πλατφόρμας.

Τεχνικά χαρακτηριστικά

Το arduino βασίζεται στον μικροελεγκτή Atmega 328 ο οποίος είναι χρονισμένος στα 16 MHZ και είναι 8-bit Risc σύστημα. Ακόμη διαθέτει ενσωματωμένη μνήμη τύπου flash 32 KB , μνήμη SRAM 2KB και EEPROM 1 KB . Η σύνδεση του arduino με τον υπολογιστή πραγματοποιείται μέσω μια θύρας usb τύπου b όπου γίνεται η επικοινωνία του υπολογιστή με το arduino για τον προγραμματισμό και την μεταφορά αρχείων . Η τροφοδοσία του μπορεί να γίνει είτε με το καλώδιο usb είτε μέσω μιας εξωτερικής τροφοδοσίας που βρίσκεται στο κάτω αριστερά μέρος [67] .

Πίνακας 6 Χαρακτηρίστηκα Arduino [67]

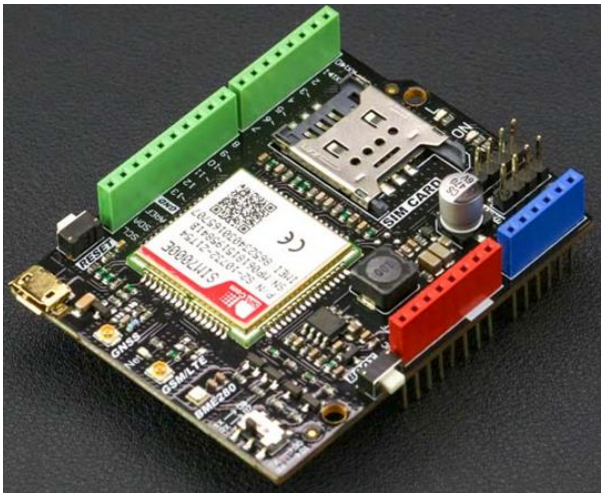
Μικροεπεξεργαστής	ATmega328
Analog inputs	6
Digital inputs/outputs	8 + 6(PWM εξόδοι)
Τάση λειτουργιάς	5V
Τάση εισόδου	7-12V
Ρεύμα εισόδων/εξόδων	40mA (max)
SRAM	2KB
EEPROM	1KB
Flash Memory	32KB
Clock Speed	16 Mhz



Εικόνα 39 Arduino Uno περιγραφή [67]

1) Κουμπί Reset: χρησιμοποιείται για επανεκκίνηση του κώδικα
2) AREF: ρυθμίζει μια τάση εξωτερικής αναφοράς .
3) GND : pin γείωσης
4) Digital input/output : ψηφιακές είσοδοι και έξοδοι
5) PWM : τα pins (11,10,9,6,5,3) που έχουν (~) χρησιμοποιούνται και ως PWM έξοδοι.
6) USB : θύρα για την σύνδεση με τον υπολογιστή για προγραμματισμό.
7) RX/TX : ένδειξη led για τους καταχωρητές .
8) Μικροελεγκτής : ATMEGA 328P
9) LED : ενεργοποίηση συσκευής
10) Mosfet : για σταθεροποίηση τάσης στα 5v
11) Pin για 3.3 V
12) Pin για 5V
13) PIN γείωσης
14) Analogue inputs : χρησιμοποιούνται για την υποδοχή αναλογικού σήματος .

Arduino NB-IoT module SIM7000



Εικόνα 40 Arduino NB-IoT module SIM7000 [31]

Η παρακάτω πλακέτα Arduino NB-IoT/LTE/GPRS είναι μια ασύρματη μονάδα επικοινωνίας που παράγεται από την εταιρία DFRobot και η σχεδίαση του βασίζεται στην SIMCom . Το παραπάνω chip υποστηρίζει την σύνδεση του δικτύου της κινητής τηλεφωνίας με δίκτυα συχνοτήτων LTE-FDD , GPRS/EDGE καθώς και NB-IoT. Ακόμη διαθέτει ενσωματωμένο το σύστημα GNSS (Παγκόσμιο Δορυφορικό Σύστημα Πλοήγησης) , το ευρωπαϊκό σύστημα Galileo , το GPS που υποστηρίζεται στην Αμερική , το GLONASS που υποστηρίζεται στην Ρωσία και το QZSS που υποστηρίζεται στην Ιαπωνία.

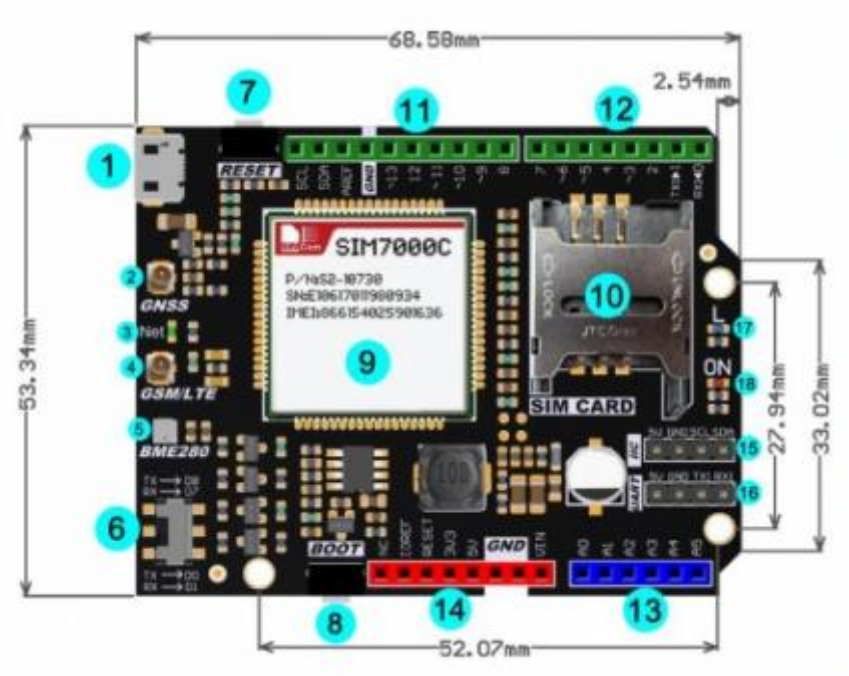
Για την σύνδεση σε έναν πάροχο κινητής τηλεφωνίας είναι υποχρεωτική η τοποθέτηση μιας κάρτας SIM. Η σύνδεση του NB-IoT γίνεται σε ένα συγκεκριμένο φάσμα συχνοτήτων όπου συνυπάρχει με τις μπάντες GSM , UMTS και LTE με εύρος ζώνης είναι 180KHZ χωρίς να υπάρχουν παρεμβολές μεταξύ των δικτύων. Ακόμη το συγκεκριμένο module διαθέτει έναν ενσωματωμένο αισθητήρα BME 280 όπου μπορεί να δώσει διάφορες μετρήσεις όπως θερμοκρασία , υγρασία και βαρομετρική πίεση.

Τέλος ο προγραμματισμός του για την σύνδεση με τον πάροχο κινητής τηλεφωνίας γίνεται με κάποια AT Commands (Attention Commands) τα όποια ορίζει ο κάθε κατασκευαστής. Έτσι το συγκεκριμένο module μπορεί να εξυπηρετήσει εφαρμογές IoT και IIoT, όπως τον απομακρυσμένο έλεγχο σε μεγάλες αποστάσεις, τον έλεγχο σε κάποιο κινούμενο μέσω (πχ αυτοκίνητο για παρακολούθηση τοποθεσίας) , σε έξυπνους μετρητές (πχ μετρητής ηλεκτρικού ρεύματος , νερού)

αλλά και σε έξυπνα δάση (πχ παρακολούθηση θερμοκρασίας και υγρασίας) όπου η πρόσβαση μπορεί να είναι δυσπρόσιτη ή να υπάρχουν προβλήματα εμβελείας [31].

Πίνακας 7 Χαρακτηρίστηκα Arduino SIM7000E

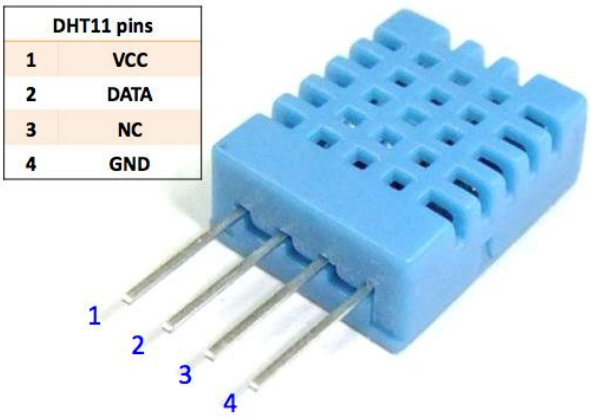
Τάση εισόδου	7-12V
Διαστάσεις	53,4 x 68,6 mm/2,1 x 2,7 in
Βάρος	46 γραμμάρια
Συχνότητα	900/1800Mhz
Ισχύς σε ύπνο	1mA
Ισχύς σε αδράνεια	11mA
Ισχύς σε PSM	9uA
Uplink	66
Downlink	34
Πρωτόκολλα	TCP/UDP/TLS/HTTP/DTLS



Εικόνα 41 Arduino NB-IoT module SIM7000 περιγραφή [31]

1) USB Firmware Update Interface
2) GNSS Antenna
3) Network Indicator
4) GSM/LTE Antenna
5) BME280 sensor
6) Software/Hardware Serial Port Switch
7) RESET Button
8) SIM7000 Control Button
9) SIM700 Module
10) SIM Socket
11) Arduino Digital Interface
12) Arduino Digital Interface
13) Arduino Analog Interface
14) Arduino Power Supply Interface
15) Arduino IIC Interface
16) Arduino UART Interface
17) Arduino Blink indicator
18) Power Supply Indicator

Αισθητήρας DHT11



Εικόνα 42 Αισθητήρας DHT11 [44]

Ο παραπάνω αισθητήρας χρησιμεύει στην μέτρηση της θερμοκρασίας και της υγρασίας και διαθέτει βαθμονομημένο ψηφιακό σήμα στην έξοδο . Χρησιμοποιώντας την τεχνική του ψηφιακού σήματος μπορεί να εξασφαλίσει αξιοπιστία και μεγάλη σταθερότητα μακροπρόθεσμα ,παρόλο που είναι ένας αισθητήρας πολύ χαμηλού κόστους. Για την μέτρηση της θερμοκρασίας χρησιμοποιεί ένα θερμίστορ ενώ για την μέτρηση της υγρασίας χρησιμοποιεί έναν πυκνωτή. Ακόμη έχει αρκετά χαμηλή κατανάλωση ισχύος κατά την χρήση πράγμα που τον κάνει ικανό να ενσωματωθεί σε εφαρμογές που λειτουργούν με μπαταρίες. Τέλος ο αισθητήρας έχει 4 ακροδέκτες, εκ των οποίων, ο πρώτος είναι για την τροφοδοσία , ο δεύτερος στέλνει τα δεδομένα του αισθητήρα , (ο τρίτος δεν χρειάζεται να συνδεθεί) και ο τελευταίος είναι για την γείωση [44].

Πίνακας 8 Χαρακτηρίστηκα αισθητήρα DHT11

Τάση λειτουργίας	3,3-5V
Διαστάσεις	18,03 mm * 29,21mm
Εύρος μέτρησης υγρασίας	20% ~ 90%
Σφάλμα μέτρησης υγρασίας	±5%
Εύρος μέτρησης θερμοκρασίας	0℃~50℃
Σφάλμα μέτρησης θερμοκρασίας	±2 ℃
Τύπος εξόδου	Ψηφιακή
Ρεύμα λειτουργιάς	0,3mA

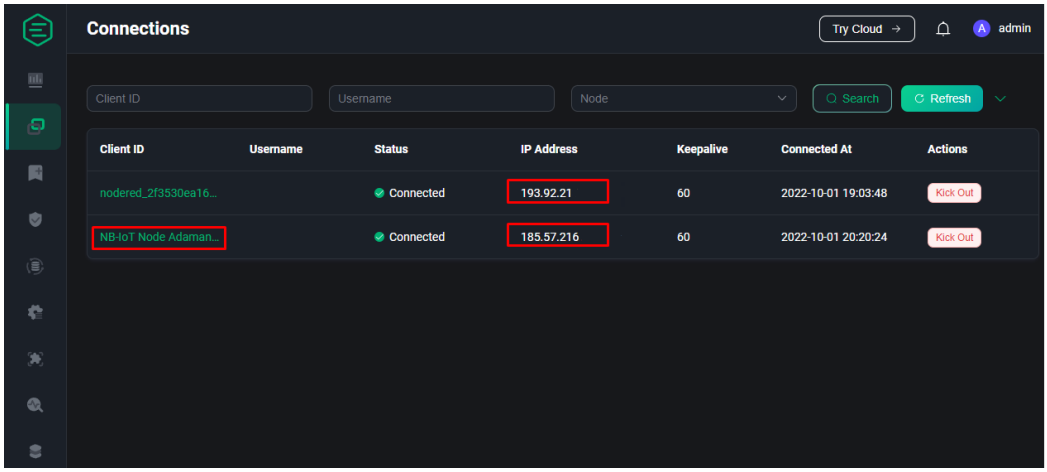
Ρεύμα αναμονής	60uA
Ακρίβεια μετρήσεων	±1°C και ±1%

Arduino IDE

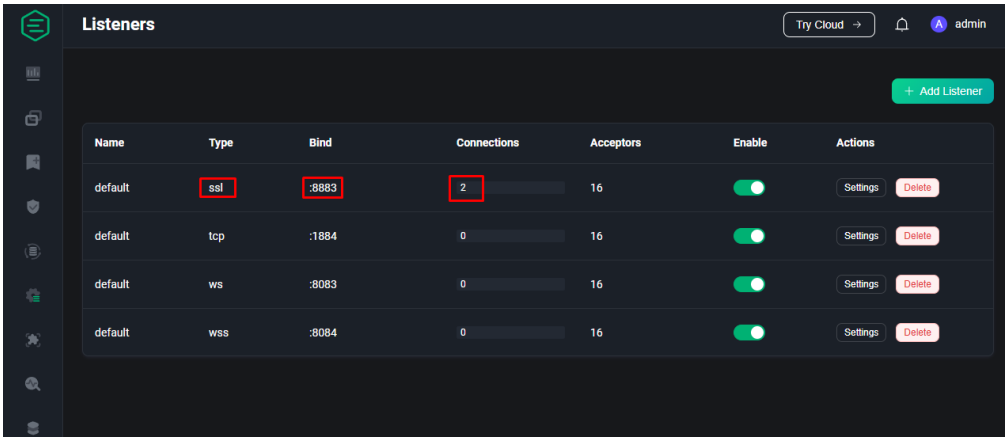
Το Arduino IDE (Integrated Development Environment) είναι ένα open-source λογισμικό το όποιο έχει δημιουργηθεί από την εταιρία Arduino [12] . Το λογισμικό αυτό χρησιμοποιείται για την σύνταξη και την επεξεργασία του κώδικα για τις πλατφόρμες της Arduino. Υποστηρίζεται σε λειτουργικά συστήματα όπως Windows ,MAC , Linux και εκτελείται στην πλατφόρμα Java όπου περιέχει κάποιες επιπρόσθετες λειτουργίες και εντολές όπως ο εντοπισμός σφαλμάτων στον κώδικα και για την σύνταξη αλλά και την επεξεργασία [70]. Το Arduino IDE υποστηρίζει τις γλώσσες προγραμματισμού C και C++ ενώ ο κώδικας που μεταφέρεται στην πλακέτα είναι σε δεκαεξαδική μορφή [70]. Ακόμη το Arduino IDE διαθέτει κάποιες ενσωματωμένες βιβλιοθήκες όπου περιέχουν κάποιες συγκεκριμένες συναρτήσεις για τον εύκολο έλεγχο των ενσωματωμένων συσκευών. Τέλος το Arduino IDE διαθέτει ένα πολύ βοηθητικό εργαλείο το Serial Monitor που δίνει την δυνατότητα στον χρηστή να βλέπει την σειριακή επικοινωνίας με τον ελεγκτή ώστε να μπορεί να ελέγξει τυχόν σφάλματα ή ακόμη και να δίνει εντολές στην σειριακή επικοινωνία κατά την λειτουργία του μικροελεγκτή για να ορίσει κάποιες παραμέτρους [70].

EMQX

Ο EMQX είναι ένας open-source MQTT broker, ο οποίος καταφέρνει να έχει πολύ γρήγορη απόκριση και να διαχειρίζεται πάνω από 20000 μηνύματα το δευτερόλεπτο. Ακόμη διαθέτει παρά πολύ φιλικό περιβάλλον προς τον χρηστή. Παράλληλα διαθέτει alarms που ενημερώνουν τους κόμβους σε περίπτωση που ο server βρίσκεται σε κρίσιμη κατάσταση [69]. Ο EMQX διαχειρίζεται τις TCP συνδέσεις των συνδεδεμένων χρηστών και επιβλέπει μία λίστα από συνδεδεμένους subscribers μαζί με το topic το οποίο περιμένει ο κάθε subscriber. Εισάγει τον κάθε νέο subscriber στην λίστα subscription και το μήνυμα μαζί με το topic στο message que. Σε περίπτωση που ενας client κάνει publish, εκτελείται μια σύγκριση στο topic του μηνύματος στο message que με topics που υπάρχουν διαθέσιμα στην λίστα των subscribers. Αν τα δύο topics ταιριάζουν γίνεται η σύνδεση και η μετάδοση του μηνύματος σε κάθε subscriber ανάλογα με την προτεραιότητά του [69].



Εικόνα 43 EMQX interface φαίνεται ο NB-IoT στον broker



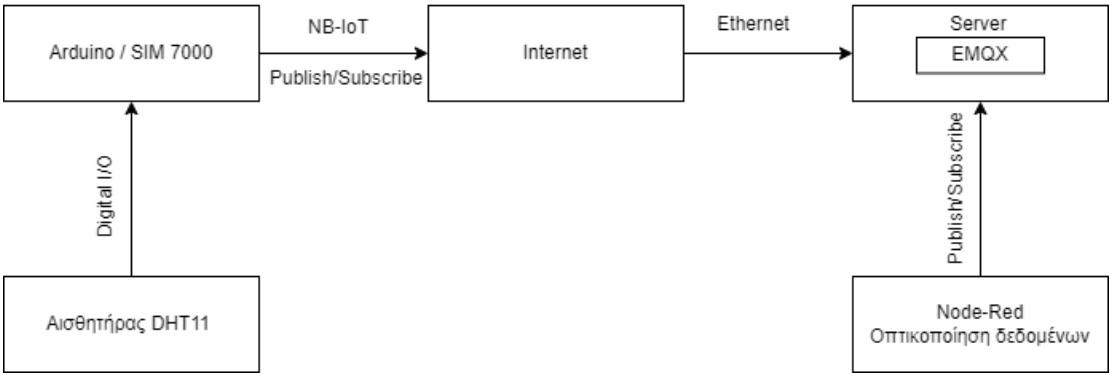
Εικόνα 44 EMQX interface η κρυπτογραφημένη θύρα όπως φαίνεται από τον broker

Περιγραφή υλοποίησης

Στο πειραματικό κομμάτι της συγκεκριμένης διπλωματικής εργασίας θα γίνει μια υλοποίηση ενός ασύρματου κόμβου για την αποστολή μετρήσεων από έναν αισθητήρα υγρασίας και θερμοκρασίας με κύριο στόχο την ασφαλή μετάδοση των δεδομένων. Η διαδικασία έχει ως έξης : οι μετρήσεις που παράγει ο αισθητήρας DHT11 στέλνονται μέσω της ψηφιακής θύρας εισόδου 2 του μικροελεγκτή Arduino, ο όποιος διαθέτει το module SIM 7000E . Το module στέλνει στο διαδίκτυο τα δεδομένα μέσω του NB-IoT δικτύου και φτάνουν στον Server που έχει εγκατεστημένο των EMQX broker με πιστοποίηση TLS 1.3 . Στην συνεχεία έχουμε επιλέξει την πλατφόρμα Node-Red όπου με την χρήση dashboard panels έχουμε φτιάξει ένα interface για τα δεδομένα που λαμβάνουμε από τον αισθητήρα μας που

είναι συνδεδεμένος με τον μικροελεγκτή Arduino . Το Node-Red χρησιμοποιεί τον μηχανισμό public-subscribe για να λάβει και να στείλει τα δεδομένα .

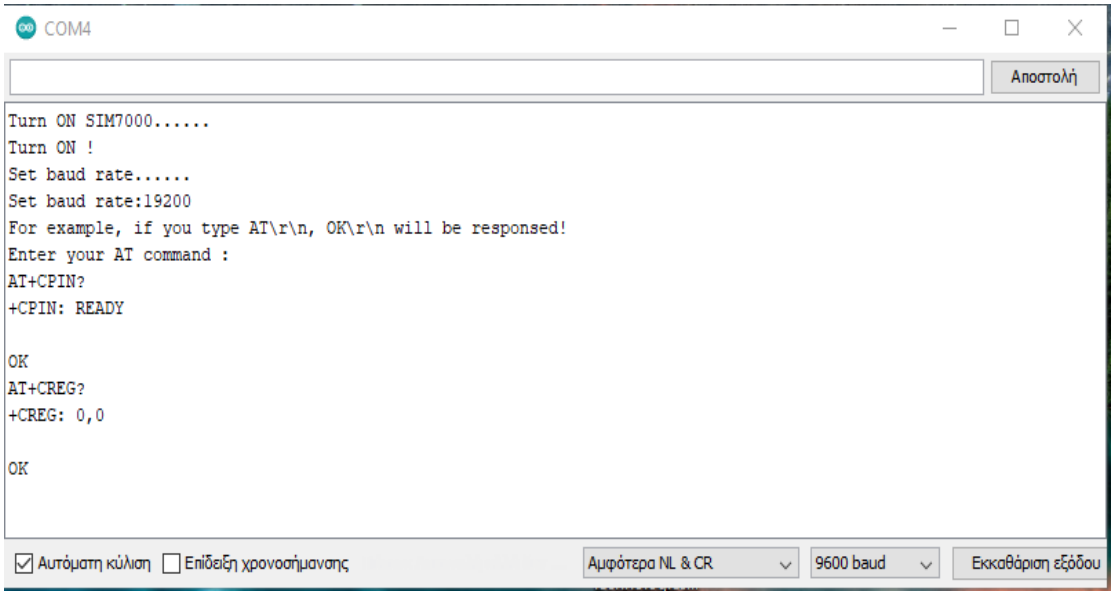
Το πιο βασικό γεγονός είναι ότι τα δεδομένα θα φθάσουν με ασφάλεια και ακεραιότητα στον server μας δίχως να έχουν υποστεί κάποια υποκλοπή κατά την μετάδοση τους. Αυτό επιτυγχάνεται με την χρήση, του TCP/IP πρωτόκολλου δικτύου, του πρωτόκολλου ασφάλειας TLS/SSL και του πρωτοκόλλου εφαρμογής MQTT. Το πρωτόκολλο ασφάλειας TLS/SSL χρησιμοποιεί τα certificates authority που είναι περασμένα μέσα στην μνήμη του chip ενώ το MQTT διαθέτει τον μηχανισμό publish-subscribe.



Σχήμα 3 Περιγραφή λειτουργιάς

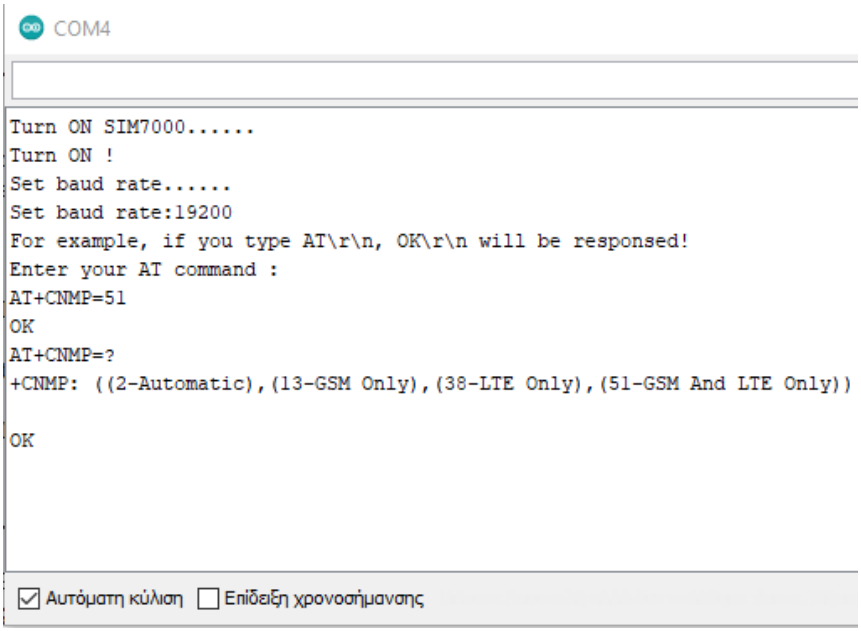
Σύνδεση του Arduino SIM7000E σε δίκτυο κινητής τηλεφωνίας

Ο προγραμματισμός του SIM7000E γίνεται με την χρήση At commands που πληκτρολογούμε μέσα από την σειριακή του Arduino IDE . Για να δούμε εάν υπάρχει κάποιο PIN στην SIM κάρτα που έχουμε τοποθέτηση στο SIM7000E module και αν έχει συνδεθεί σε κάποιο δίκτυο πληκτρολογούμε την εντολή AT+CPIN? Και αν μας επιστρέψει +CPIN:<code> θα πρέπει να πληκτρολογήσουμε τον κωδικό της κάρτας . Στην περίπτωση μας δεν έχουμε θέσει κάποιο PIN όποτε μας επιστρέφει την εντολή +CPIN: READY . Για να δούμε αν έχει συνδεθεί σε κάποιο δίκτυο πληκτρολογούμε την εντολή AT+CREG? και μας επιστρέφει +CREG: 0,0 που σημαίνει ότι δεν είναι συνδεδεμένο σε κάποιο παροχή κινητής τηλεφωνίας .



Εικόνα 45 Σειριακή Arduino IDE

Αρχικά πρέπει να ρυθμίσουμε το chip ώστε να μπορεί να συνδεθεί σε δίκτυα NB-IoT και GSM πληκτρολογώντας την εντολή AT+CNMP=51 και στην συνέχεια με το AT+CNMP=? βλέπουμε αν την έχει πάρει . Για να μας εμφανίσει τα διαθέσιμα δίκτυα κινητής τηλεφωνίας GSM αλλά και NB-IoT όπου μπορούμε να συνδεθούμε πληκτρολογούμε την εντολή AT+COPS=? . Για την σύνδεση σε ένα δίκτυο που μας εμφάνισε στην σειριακή πληκτρολογούμε την εντολή AT+COPS=1,2,"κωδικός δικτύου", τύπος δικτύου .



Εικόνα 46 Σειριακή Arduino IDE επιλογή δικτύων για σύνδεση

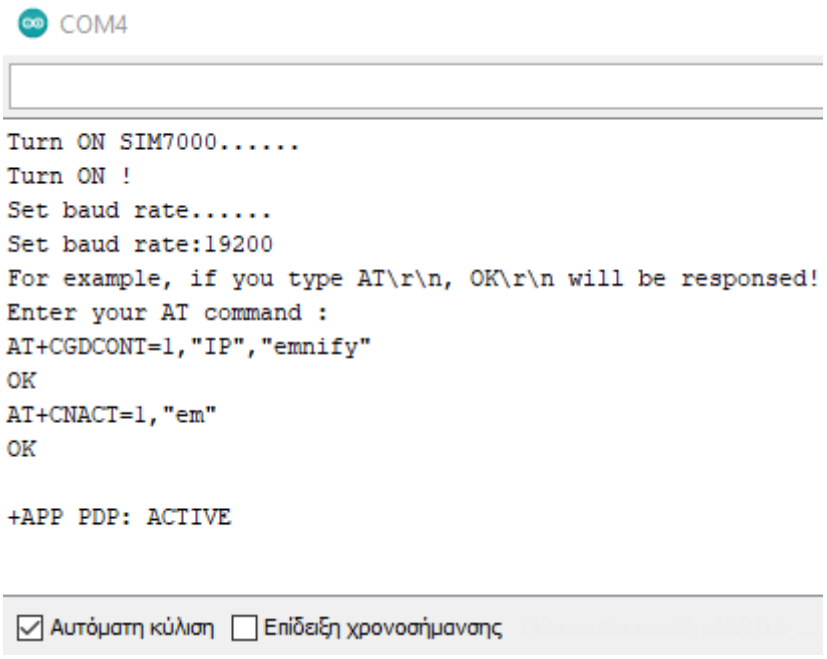
```
Turn ON SIM7000......
Turn ON !
Set baud rate......
Set baud rate:19200
For example, if you type AT\r\n, OK\r\n will be responsed!
Enter your AT command :
AT
OK
AT+CPIN?
+CPIN: READY

OK
AT+COPS=?
+COPS: (2,"202 05","202 05","20205",0),(1,"202 01","202 01","20201",0),(1,"202 10","202 10","20210",0),(1,"202 01","202 01","20201",9),(1,"202 05","202 05","20205",9),

OK
AT+COPS=1,2,"20205",9
OK
```

Εικόνα 47 Σειριακή Arduino IDE σύνδεση σε δίκτυο NB-IoT

Πίνακας 9 Πάροχοι κινητής τηλεφωνίας

Πάροχος κινητής τηλεφωνίας	**Κωδικός(0 GSM ,9 NB-IoT)**
Vodafone NB-IoT	"20205",9
Cosmote NB-IoT	"20201",9
Cosmote 2G	"20201",0
Vodafone 2G	"20205",0
Wind 2G	"20210",0

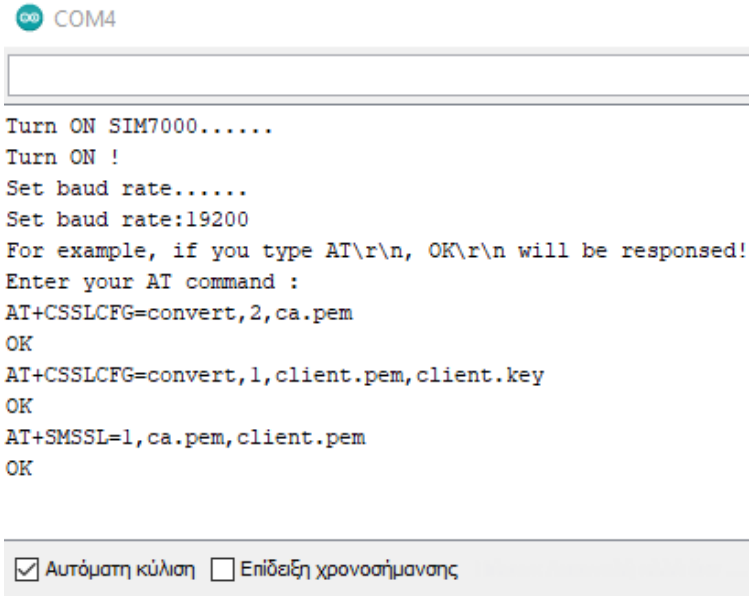
Εμείς επειδή θέλουμε να συνδεθούμε σε δίκτυο NB-IoT της Vodafone πληκτρολογούμε την εντολή AT+COPS=1,2,"20205",9 και στην συνέχεια πρέπει να του δώσουμε το APN(access point name) πληκτρολογώντας AT+CGDCONT=1,"IP","emnify". Ακόμη πληκτρολογούμε την εντολή AT+CNACT=1,"em" για να πάρουμε IP μέσω του PDP (packet data protocol).



Εικόνα 48 Σειριακή Adruino IDE σύνδεση σε δίκτυο NB-IoT

Αφού έχει ολοκληρωθεί η σύνδεση του Arduino SIM7000E module με το δίκτυο της Vodafone NB-IoT πρέπει να δώσουμε κάποιες εντολές για να διαβάσει τα Certificates Authority που περάσαμε στο module στο παράρτημα 2 της εργασίας ώστε να μπορέσουμε να στείλουμε δεδομένα στην πόρτα 8883. Πληκτρολογούμε τις παρακάτω εντολές στην σειριακή του Arduino IDE.

1) AT+CSSLCFG=convert,2,ca.pem
2) AT+CSSLCFG=convert,1,client.pem,client.key
3) AT+SMSSL=1,ca.pem,client.pem



Εικόνα 49 Σειριακή Adruino IDE εισαγωγή certificates

Για να μπορέσουμε να στείλουμε από τον αισθητήρα τις μετρήσεις , πρέπει να δηλώσουμε την βιβλιοθήκη του καθώς και να δηλώσουμε την ψηφιακή είσοδο που είναι συνδεδεμένος ο αισθητήρας στο Arduino .

```
#define DHTPIN 2     // Σύνδεση στην ψηφιακή είσοδο 2
#define DHTTYPE DHT11   // Τύπος αισθητήρα DHT11
DHT dht(DHTPIN, DHTTYPE);
```

Εικόνα 50 Σειριακή Arduino IDE δήλωση βιβλιοθηκών

Ακόμη για να μπορέσουμε να διαβάσουμε την θερμοκρασία και την υγρασία του αισθητήρα χρησιμοποιούμε τις εντολές float temp = dht.readTemperature(); Και float humi = dht.readHumidity(); Που υπάρχουν μέσα στην βιβλιοθήκη DHT dht(DHTPIN, DHTTYPE) Και την εντολή Serial.print() για να μπορέσουμε να το εμφανίσουμε στην σειριακή του arduino .

```
float temp = dht.readTemperature();
 Serial.print(F("%  Temperature: "));
  Serial.print(temp);
   Serial.print(F("°C "));

float humi = dht.readHumidity();
  Serial.print(F("Humidity: "));
   Serial.print(humi);
```

Εικόνα 51 Εμφάνιση μετρήσεων στην σειριακή

Για να μπορέσουμε να στείλουμε τις μετρήσεις στον server μας χρησιμοποιούμε την εντολή AT+SMPUB=”topic”,5,1,1 όπου το topic είναι το θέμα που στέλνουμε τα δεδομένα και το 5 είναι οι χαρακτήρες του μηνύματος που θέλουμε να στείλουμε . Μόλις πληκτρολογήσουμε την εντολή αυτή στην σειριακή του arduino περιμένει να στείλουμε ένα μήνυμα .

```
AT+SMPUB="topic","5",1,1
> 24,56

OK
```

Εικόνα 52 Σειριακή arduino αποστολή πακέτου

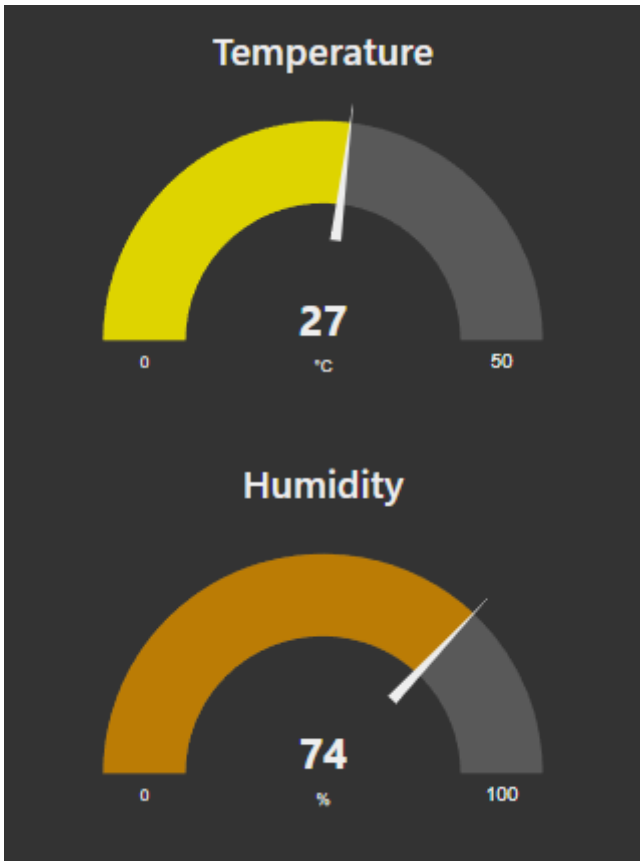
Επειδή θέλουμε το πρόγραμμα να τρέχει αυτόματα και οι μετρήσεις από τον αισθητήρα, να στέλνονται αυτόματα χωρίς να ανοίξουμε την σειριακή του Arduino, δημιουργήσαμε δυο συναρτήσεις με ονόματα sendATcommand και sendATcommand1 ώστε το Arduino να στέλνει στο CHIP SIM7000 χωρίς να στέλνουμε εμείς τις εντολές AT Commands μέσω της σειριακής θύρας και να διαβάζει αυτόματα την μέτρηση του αισθητήρα . Τέλος τοποθετήσαμε ένα delay(60000) μέσα στο loop του προγράμματος για να στέλνουμε μετρήσεις κάθε ένα λεπτό .

```
void loop() {

float temp;
float humi;
  dht.begin();
sendATcommand("AT+SMPUB=uniwa,5,1,1",2000);
sendATcommand1(dht.readTemperature(),2000);
temp = dht.readTemperature();
Serial.println(temp);

sendATcommand("AT+SMPUB=uniwa1,5,1,1",2000);
sendATcommand1(dht.readHumidity(),2000);
humi = dht.readHumidity();
Serial.println(humi);

delay(60000);

}
```

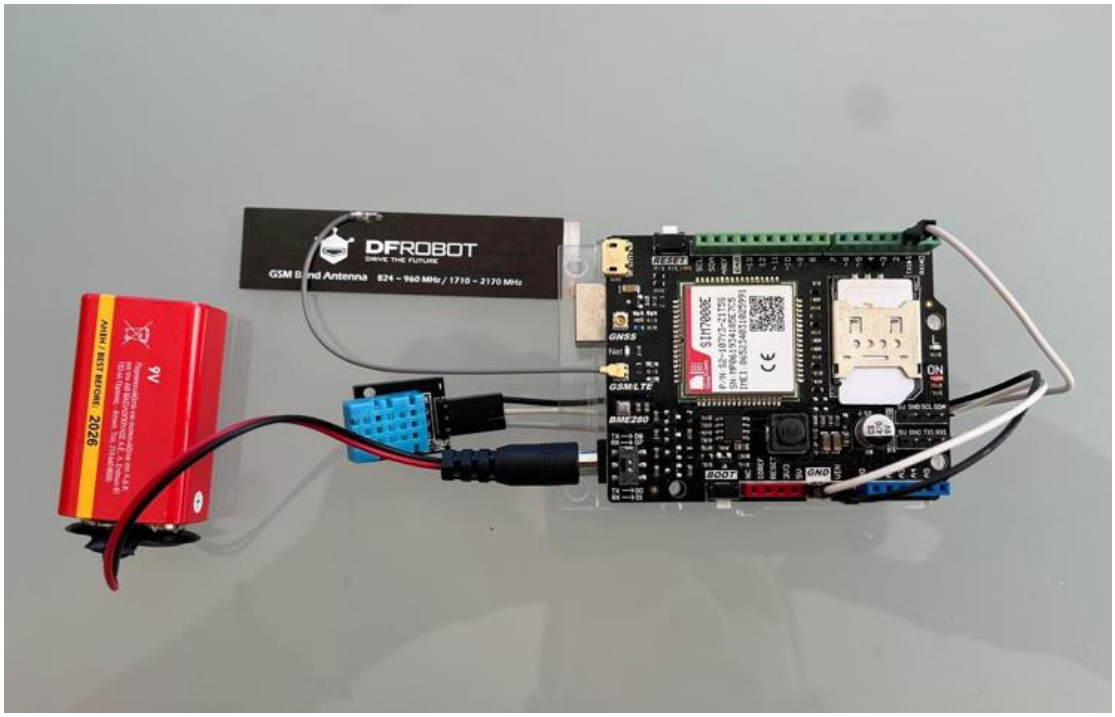
Εικόνα 53 Προγραμματισμός Arduino

Παρακολούθηση δεδομένων σε πραγματικό χρόνο

Για την παρακολούθηση των δεδομένων που μας στέλνει ο αισθητήρας κάθε ένα λεπτό , έχουμε δημιουργήσει στο παράρτημα 4 της εργασίας ένα dashboard το όποιο κάθε φορά που στέλνεται μια νέα μέτρηση ενημερώνεται αυτόματα . Έτσι μπορούμε να παρατηρούμε τα δεδομένα σε πραγματικό χρόνο παρότι ο αισθητήρας μας μπορεί να βρίσκεται σε έναν απομακρυσμένο χώρο, όπως μια βιομηχανία. Το παραπάνω interface μπορεί να διαμοιραστεί μέσω internet για την συνεχή παρακολούθηση του ασύρματου κόμβου . Το συγκεκριμένο interface τρέχει τοπικά στον υπολογιστή μας αλλά θα μπορούσε να διαμοιραστεί και μέσω internet μέσω της τεχνικής portforwarding. Ένας άλλος τρόπος που θα μπορούσε να διαμοιραστεί το παραπάνω interface θα μπορούσε να είναι ένας κεντρικός ιδιωτικός server μιας βιομηχανίας .



Εικόνα 54 dashboard θερμοκρασίας και υγρασίας



Εικόνα 55 Ασύρματος Κόμβος

Λόγοι για τους οποίους επιλέχθηκε το δίκτυο NB-IoT

Για την υλοποίηση ενός ασύρματου ασφαλούς κόμβου που να στέλνει δεδομένα από ένα βιομηχανικό περιβάλλον χρειάζεται να υπάρχει μέγιστη ασφάλεια κατά την μετάδοση των δεδομένων γιατί υπάρχουν πολλοί κίνδυνοι που μπορούν είτε να παραβιάσουν είτε να τροποποιήσουν τα δεδομένα του κόμβου με αποτέλεσμα να μην υπάρχει σωστή αντιμετώπιση. Στην παρούσα εργασία επιλέξαμε το δίκτυο LPWAN NB-IoT για την υλοποίηση του κόμβου αφού φαίνεται να υπερτερεί στην ασφάλεια έναντι τον άλλων τεχνολογιών . Παρακάτω θα παρουσιάσουμε τους πιο σημαντικούς λογούς που καταλήξαμε στην επιλογή του :

- Το NB-IoT χρησιμοποιεί αδειοδοτημένες ζώνες συχνοτήτων αυτό συνεπάγεται στην ευρεία κάλυψη του δικτύου αφού ο κάθε κόμβος μπορεί να τοποθετηθεί ακόμα και στο δυσπρόσιτο σημείο μιας βιομηχανίας και να μπορέσει να στέλνει τα δεδομένα χωρίς παράσιτα .

- Η κατανάλωση ισχύος του ασύρματου κόμβου είναι πολύ χαμηλή, πράγμα που διευκολύνει την απομακρυσμένη κάλυψη μίας ευρείας περιοχής χωρίς την ανάγκη συνεχούς συντήρησης, ενώ ταυτόχρονα αποτελεί μία αρκετά οικονομική λύση .

- Η ασφάλεια είναι ένα από τα σημαντικότερα πλεονεκτήματα αυτής της τεχνολογίας, αφού χρησιμοποιεί το πρωτόκολλο δικτύου TCP/IP που προσφέρει εγγυημένη παράδοση των δεδομένων, το πρωτόκολλο ασφάλειας

TLS/SSL που προσφέρει ακεραιότητα και κρυπτογράφηση στα δεδομένα και το πρωτόκολλο εφαρμογής MQTT το οποίο διαχειρίζεται ευέλικτα πολλούς κόμβους.

Έτσι η διάταξη του ασύρματου κόμβου μας προσφέρει αρκετά μεγάλη ευελιξία καθώς μπορεί να εφαρμοστεί σε πάρα πολλές εφαρμογές της βιομηχανίας ανεξάρτητα από την απόσταση που έχει ο κάθε κόμβος καθώς το NB-IoT χρησιμοποιεί SIM κάρτα και μπορεί να λειτουργήσει όπου υπάρχει σήμα κινητής τηλεφωνίας.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα διπλωματική εργασία, αναπτύξαμε την υλοποίηση μιας διάταξης ενός ασφαλούς ασύρματου κόμβου που είναι βασισμένος σε τεχνολογίες LPWAN, όπου σε συνάρτηση με το IIoT και με την τέταρτη βιομηχανική επανάσταση βλέπουμε ότι ο τομέας παραγωγής, περνάει πλέον από τον ανθρώπινο παράγοντα στις αυτοματοποιημένες διαδικασίες και τον έλεγχο εξ αποστάσεως.

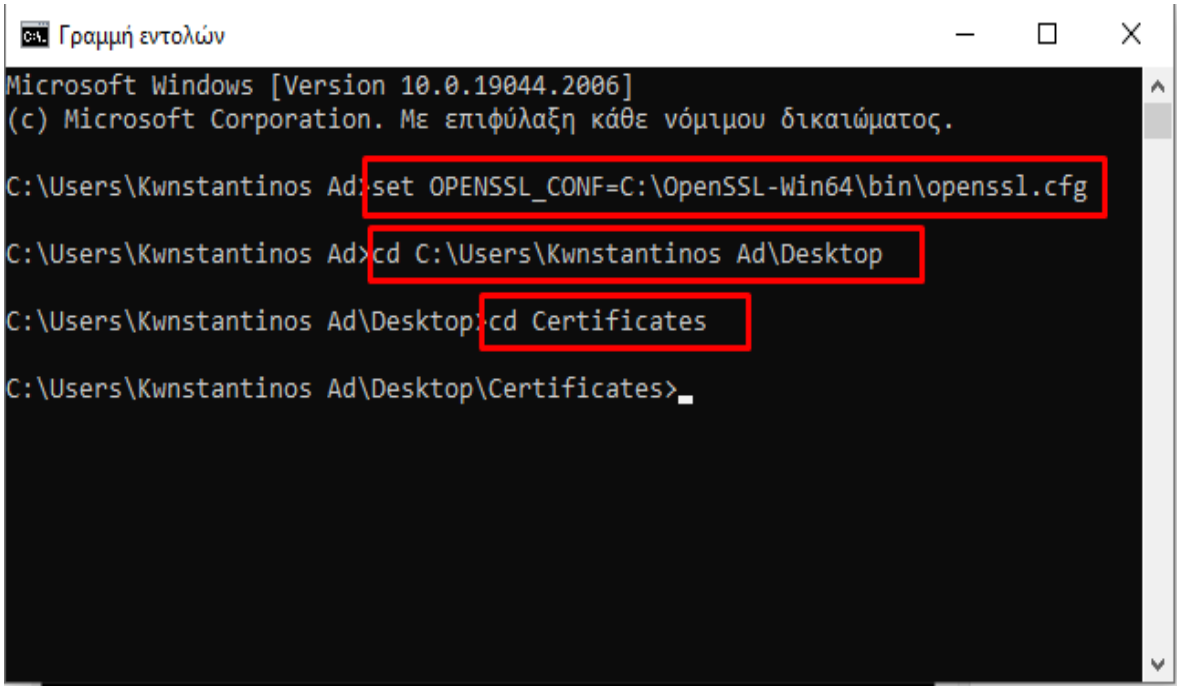
Το μεγάλο ζήτημα επομένως που εξετάσαμε στην ασύρματη ασφαλή επικοινωνία του κόμβου με το διαδίκτυο είναι, η ασφάλεια και η ακεραιότητα των δεδομένων που αποστέλλονται, χωρίς να υπάρξει υποκλοπή ή αλλοίωσή τους. Αυτό το καταφέραμε χρησιμοποιώντας τα διάφορα πρωτόκολλα ασφάλειας, επικοινωνίας και δικτύου που περιγράψαμε στα προηγούμενα κεφάλαια, καθώς και με εισαγωγή certificates authority στην μνήμη του chip. Η κατασκευή όσον αφορά το επίπεδο εξαρτημάτων (Hardware) διαθέτει το Arduino Uno, το SIM7000E module, τον αισθητήρα DHT11 όπου μας δίνει μετρήσεις θερμοκρασίας και υγρασίας και μια μπαταρία 9(volt) ώστε ο κόμβος να είναι αυτόνομος .

Τέλος, καταλήγουμε στο συμπέρασμα ότι το δίκτυο NB-IoT με βάση την υλοποίηση που κάναμε φάνηκε να είναι το πιο επαρκές δίκτυο για την ασφαλή ασύρματη επικοινωνία ενός κόμβου στο τομέα της βιομηχανίας λόγω α) ότι υπερτερεί έναντι άλλων δικτύων σε ασφάλεια και β) χρησιμοποιεί αδειοδοτημένες ζώνες συχνοτήτων.

ΠΑΡΑΡΤΗΜΑ 1 Δημιουργία πιστοποιητικών TLS/SSL

Με το πρόγραμμα OpenSSL δημιουργούμε τα πιστοποιητικά που θα χρησιμοποιήσει το TLS για να υπάρχει η ταυτοποίηση μεταξύ του EMQX broker και των clients. Για την ταυτοποίηση θα χρειαστούμε την δημιουργία πιστοποιητικών CA (Certfiicate Authority), Server και Client. Έτσι αφού και ο server και ο client μοιράζονται τα CA , η μεταξύ τους επικοινωνία γίνεται με την χρήση επιμέρους πιστοποιητικών και κλειδιών τα όποια είναι το ca.pem , client.pem και το client.key. Τα πιστοποιητικά θα τα περάσουμε στην μνήμη του Arduino NB-IoT module SIM7000 και στον server .

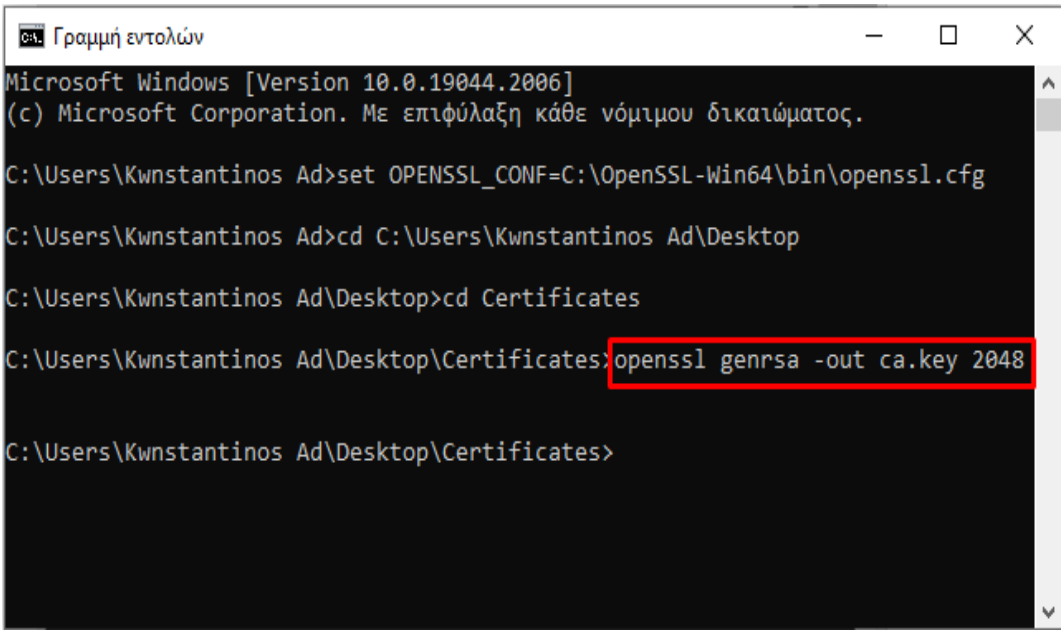
Αφού ανοίξαμε το comand line και εκτελέσαμε το πρόγραμμα OpenSSL πληκτρολογώντας την εντολή C:\Users\Kwnstantinos Ad>openssl μας εμφανίζει της εντολές .



Εικόνα 56 Εγκατάσταση OpenSSL και επιλογή φάκελου στην γραμμή εντολών

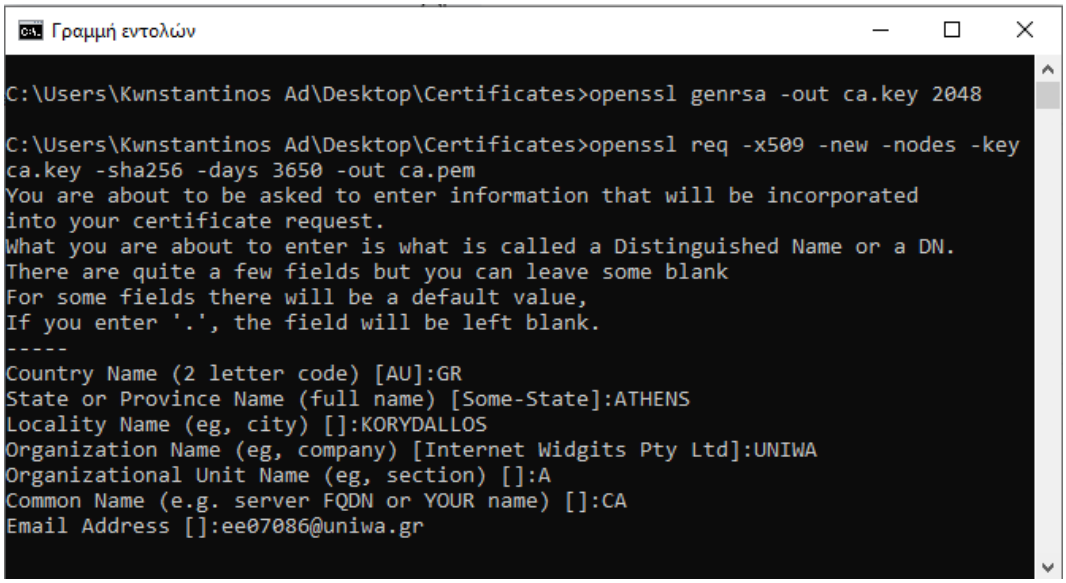
Πληκτρολογώντας την εντολή cd C:\Users\Kwnstantinos Ad\Desktop\ Certfiicates δείχνουμε στο command line τον φάκελο που θέλουμε να αποθηκευτούν τα certificates.

Για την δημιουργία του κλειδιού ca.key πληκτρολογούμε την εντολή openssl genrsa -out ca.key 2048



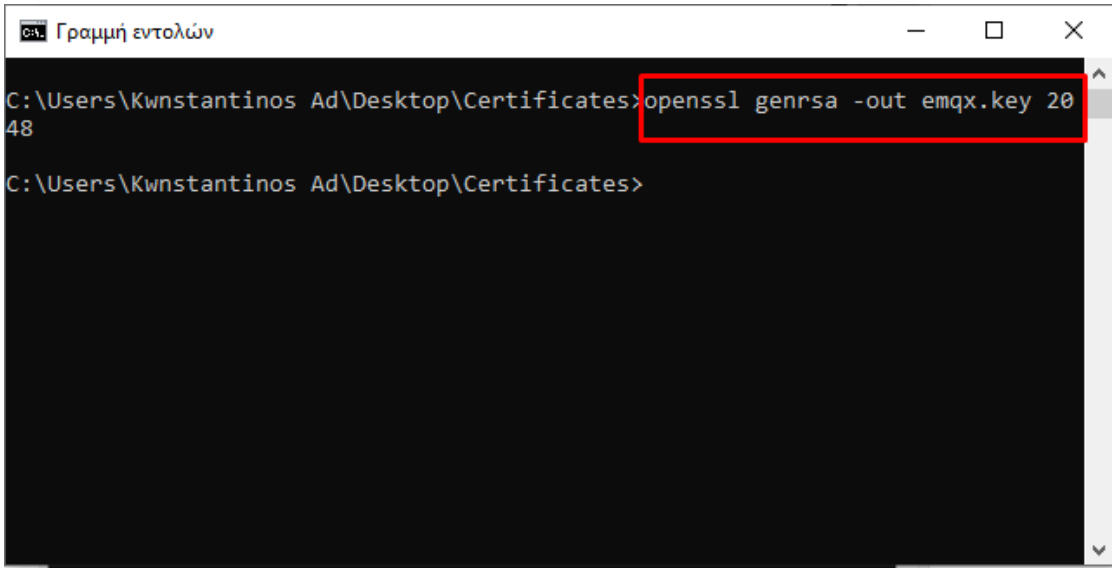
Εικόνα 57 Δημιουργία του κλειδιού ca.key

Και στην συνεχεία φτιάχνουμε το πιστοποιητικό ca με το κλειδί που δημιουργήσαμε με την προηγούμενη εντολή πληκτρολογώντας την εντολή : openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.pem . Για να δημιουργηθεί το πιστοποιητικό ca (certificate authority) συμπληρώνουμε τα στοιχεία όπως : Country Name , State or Province Name , Locality Name ,Organization Name, Organizational Unit Name , Common Name , Email Address.



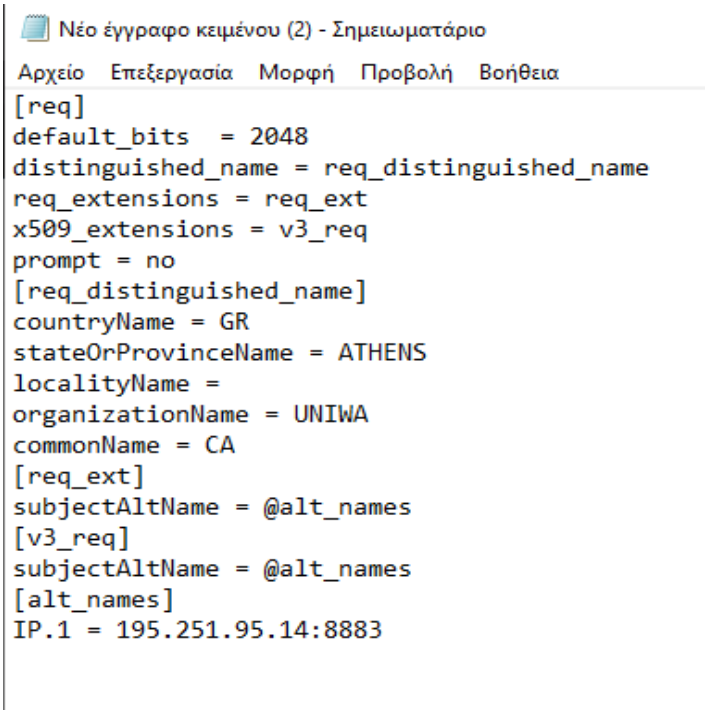
Εικόνα 58 Δημιουργία πιστοποιητικού ca.pem

Στην συνεχεία για να δημιουργήσουμε το πιστοποιητικό για τον server μας EMQX πληκτρολογούμε openssl genrsa -out emqx.key 2048



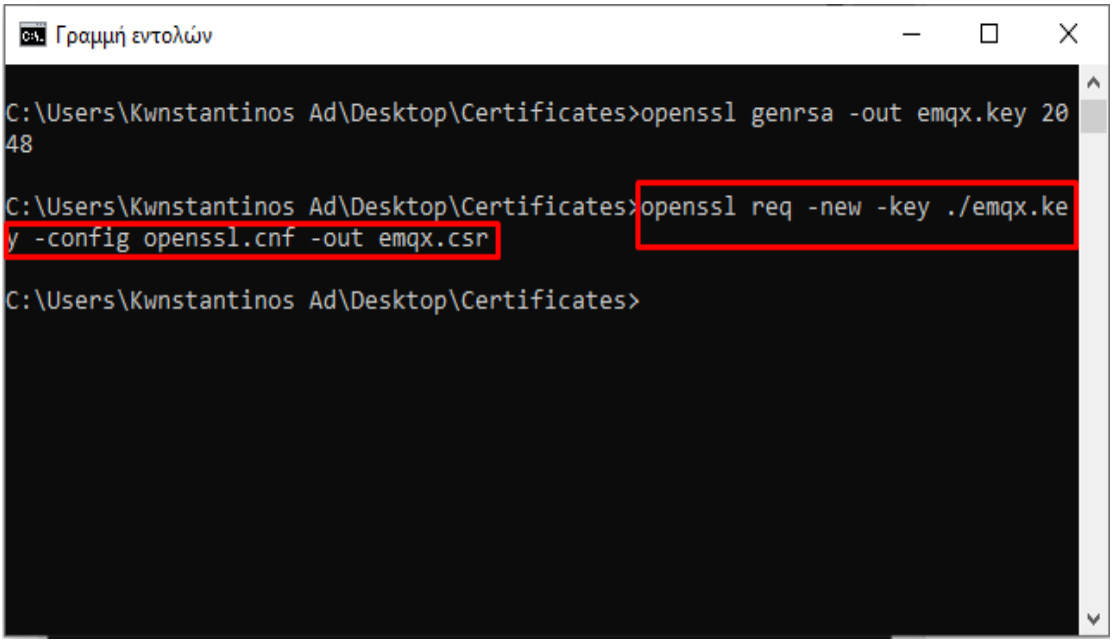
Εικόνα 59 Προετοιμασία για δημιουργία πιστοποιητικού για τον server emqx

Στην συνέχεια δημιουργούμε ένα αρχείο στο WordPad με όνομα openssl.cnf και συμπληρώνουμε τις μεταβλητές που είχαμε βάλει για την δημιουργία του πιστοποιητικού ca ώστε να γίνει επαλήθευση.



Εικόνα 60 Δημιουργία αρχείου openssl.cnf στο WordPad

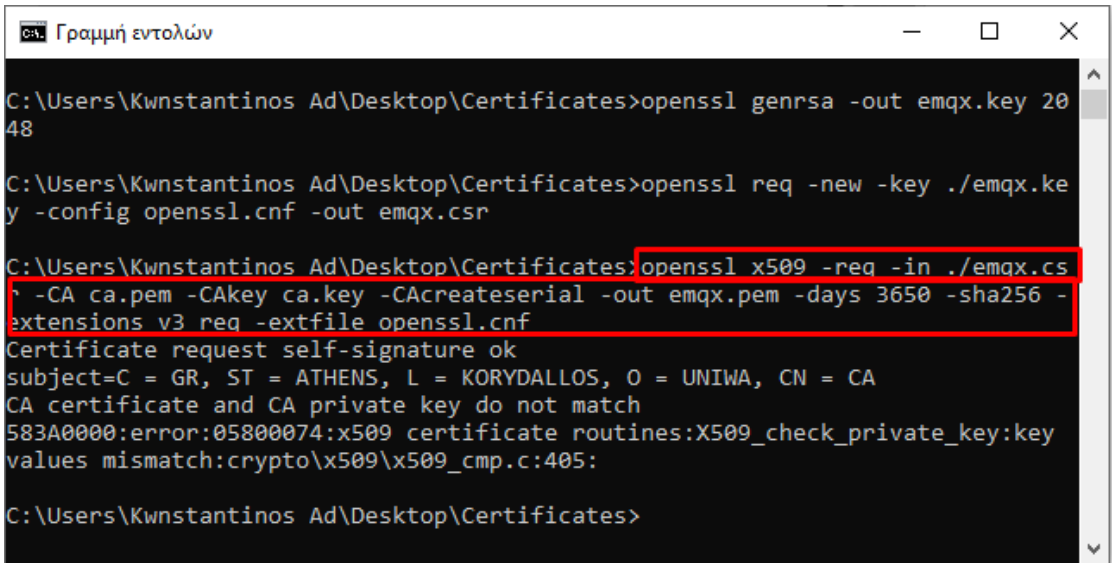
Και δημιουργούμε ένα πιστοποιητικό για τον broker με την εντολή openssl req -new -key ./emqx.key -config openssl.cnf -out emqx.csr όπου καλούμε το αρχείο που φτιάξαμε openssl.cnf



Εικόνα 61 Δημιουργία πιστοποιητικού για τον server emqx

Στην συνεχεία παίρνει το αρχείο openssl.cnf που καλέσαμε στην προηγούμενη εντολή και φτιάχνουμε το certificate για τον broker πληκτρολογώντας openssl x509 -

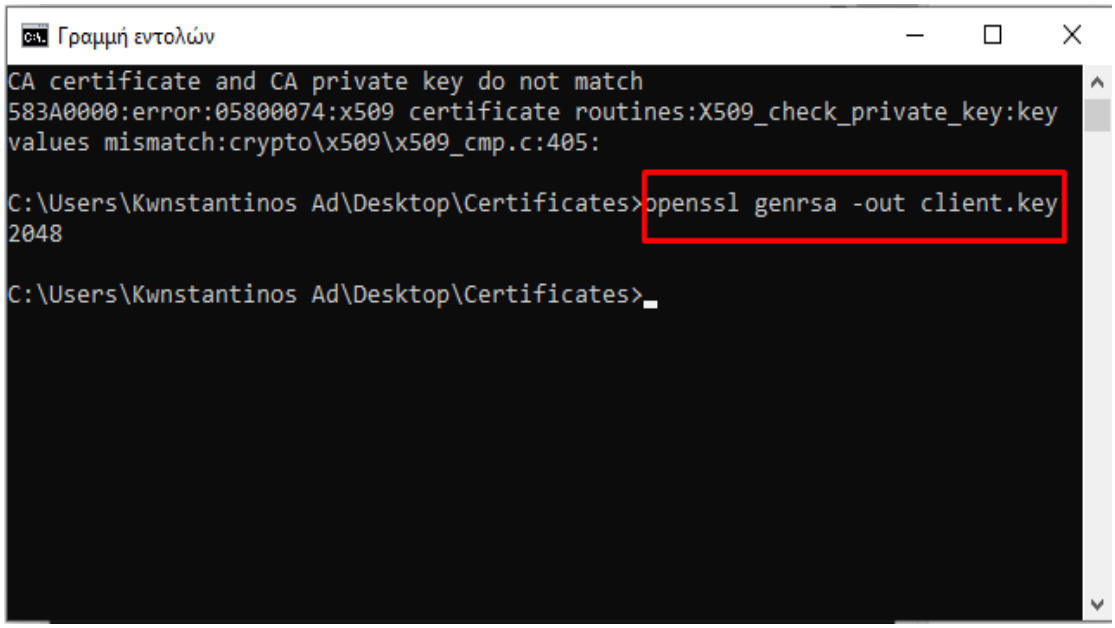
req -in ./emqx.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out emqx.pem -days 3650 -sha256 -extensions v3_req -extfile openssl.cnf .



Εικόνα 62 Δημιουργία certificate για τον server emqx

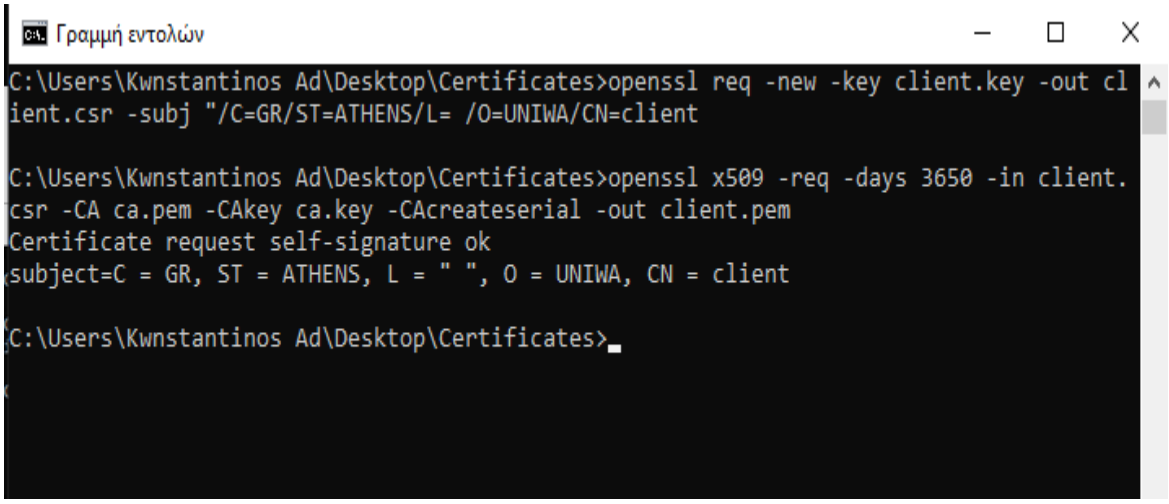
Το κλειδί και το πιστοποιητικό που δημιουργήθηκε το εγκαθιστούμε στον broker EMQX του server .

Για την δημιουργία του client.key πληκτρολογούμαι : openssl genrsa -out client.key 2048



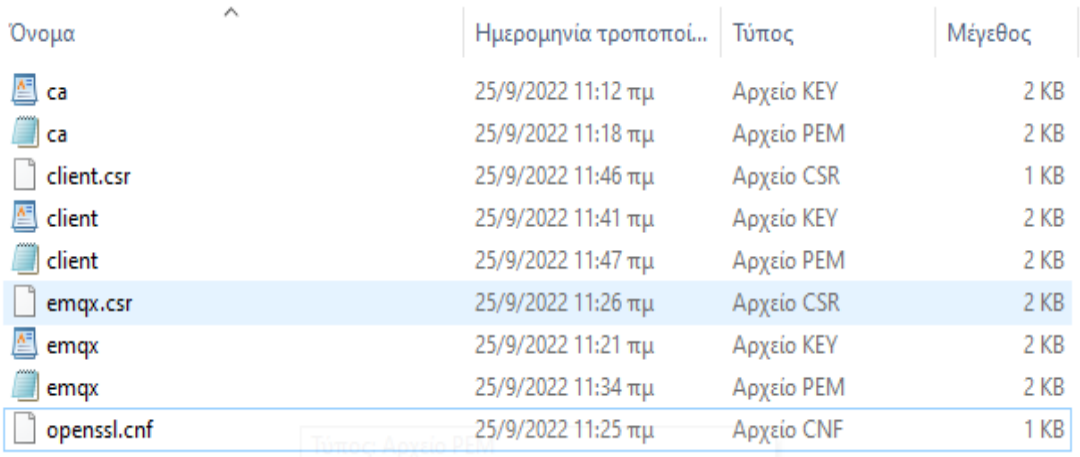
Εικόνα 63 Δημιουργία του πιστοποιητικού client.key

Τέλος για να δημιουργήσουμε το client.pem χρησιμοποιούμε το πιστοποιητικό CA που δημιουργήσαμε προηγούμενως. Πληκτρολογώντας την εντολή openssl req -new -key client.key -out client.csr -subj "/C=GR/ST=ATHENS/L= /O=UNIWA/CN=client" και συμπληρώνουμε τις μεταβλητές που είχαμε ορίσει παραπάνω .



Εικόνα 64 Δημιουργία του πιστοποιητικού client.pem

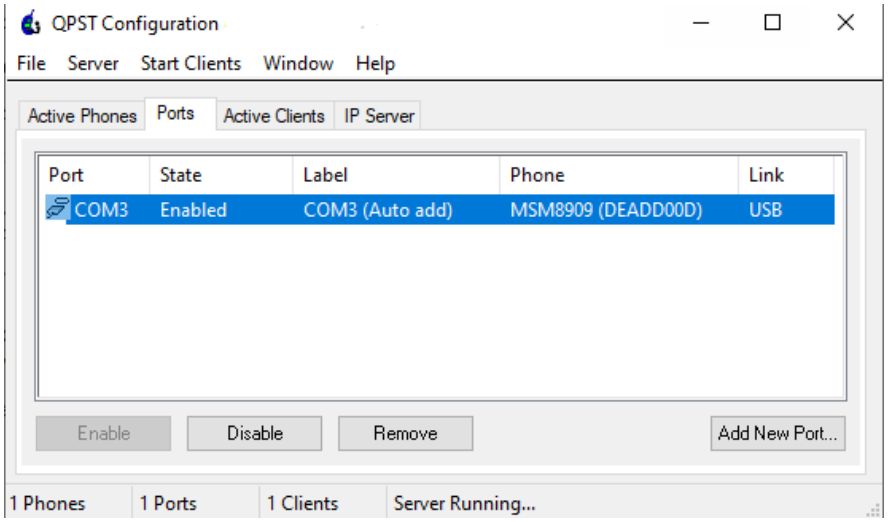
Τέλος έχουμε δημιουργήσει όλα τα πιστοποιητικά στον φάκελο Certificates .



Εικόνα 65 Πιστοποιητικά

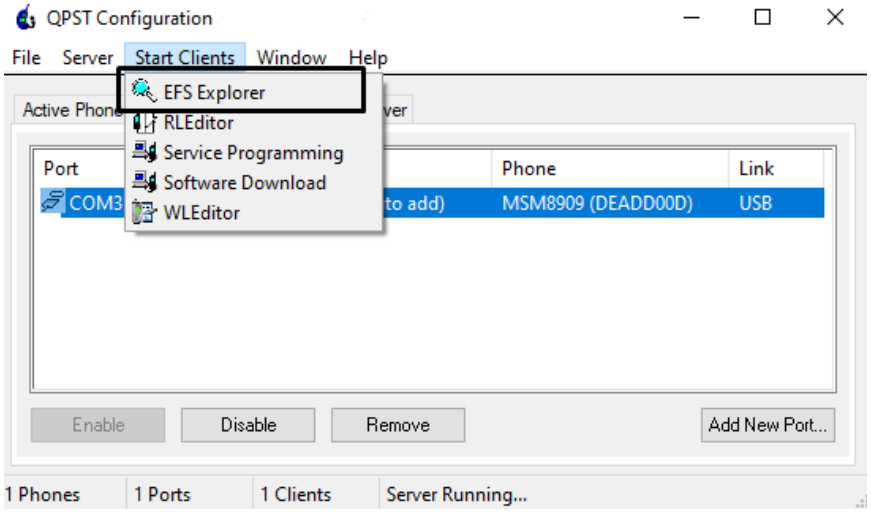
ΠΑΡΑΡΤΗΜΑ 2 Εισαγωγή πιστοποιητικών στο SIM7000

Αφού δημιουργήσαμε τα πιστοποιητικά με το πρόγραμμα OpenSSL στο παράρτημα 1 της εργασίας πρέπει να εγκαταστήσουμε το πρόγραμμα QPST Configuration για να μπορέσουμε να περάσουμε στην εσωτερική μνήμη ROM του Arduino NB-IoT module SIM7000 τα πιστοποιητικά. Έτσι μόλις το συνδέσουμε στον υπολογιστή και ανοίξουμε το πρόγραμμα μας το εμφανίζει στο COM3.



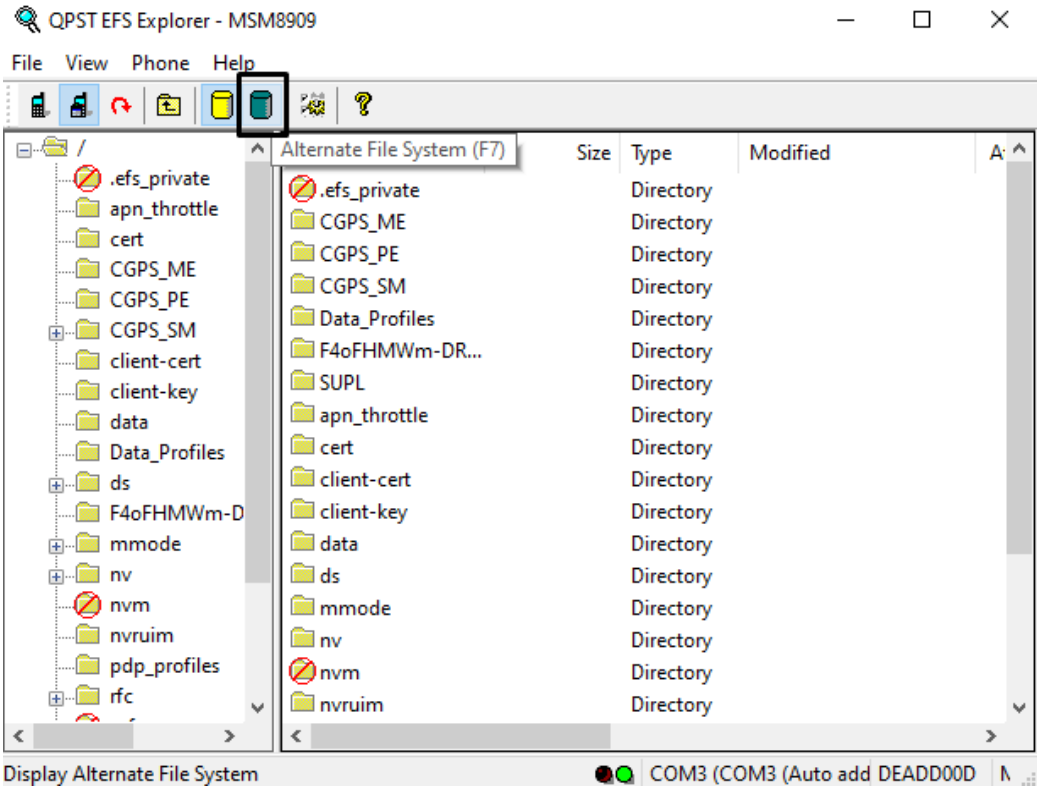
Εικόνα 66 Πρόγραμμα QPST Configuration

Στην συνεχεία επιλεγούμε την εντολή Start Clients και επιλεγούμε το EFS Explorer.

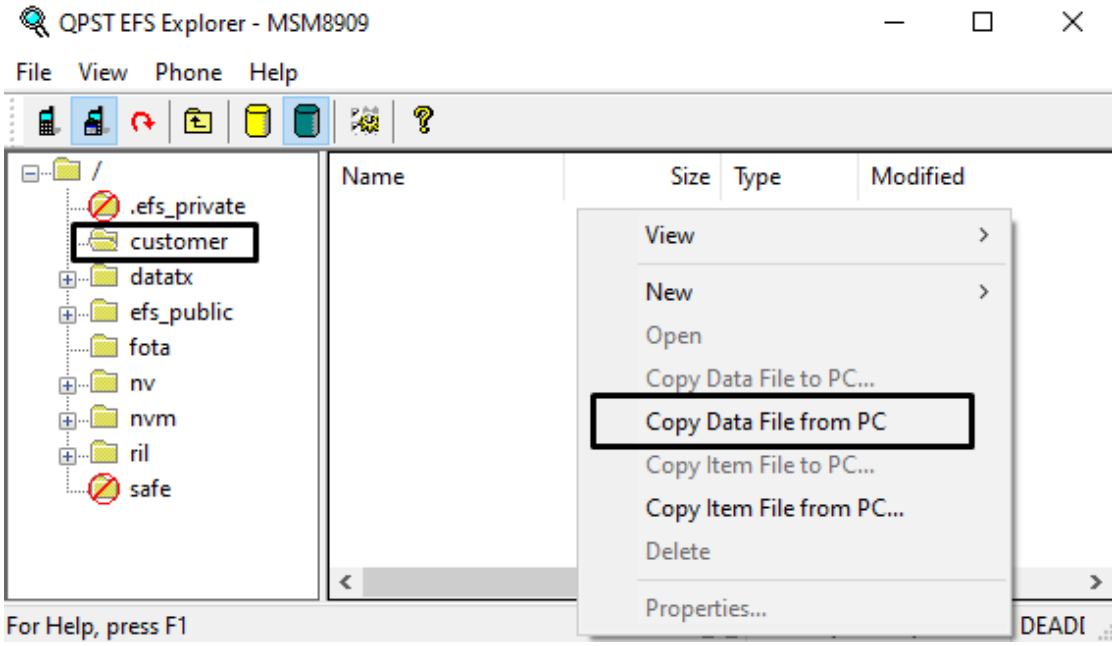


Εικόνα 67 Πρόγραμμα QPST Configuration EFS Explorer

Στην συνεχεία αφού ανοίξει το QPST EFS Explorer επιλεγούμε το Alternate File System και μας ανοίγει ένα νέο παράθυρο.

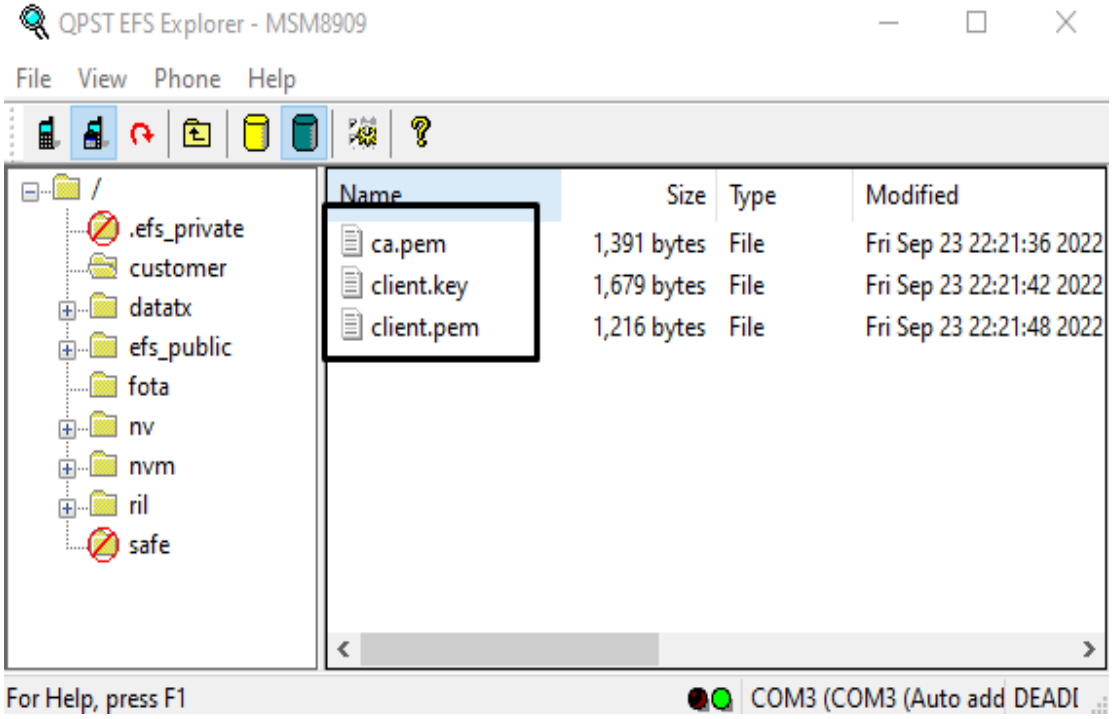


Εικόνα 68 EFS Explorer Alternate File System



Εικόνα 69 EFS Explorer copy data file from PC

Και επιλεγούμε από τον υπολογιστή τα πιστοποιητικά και τα αντιγράφουμε .



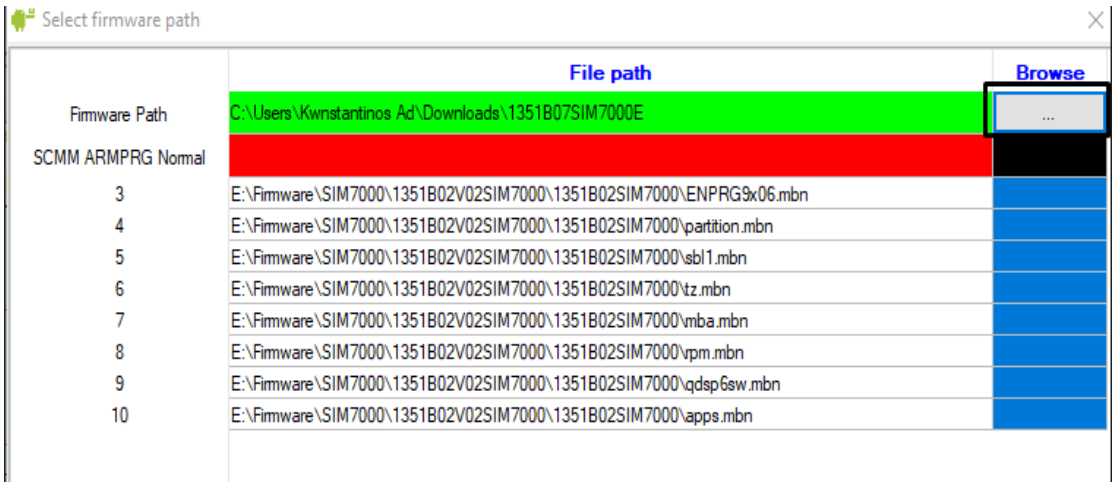
Εικόνα 70 EFS Explorer εισαγωγή πιστοποιητικών

ΠΑΡΑΡΤΗΜΑ 3 Αναβάθμιση firmware SIM7000

Για την εισαγωγή πιστοποιητικών TLS/SSL πρέπει να γίνει αναβάθμιση στο firmware του SIM7000. Για την διαδικασία της αναβάθμισης θα εγκαταστήσουμε το πρόγραμμα SIM7000 QDL και θα κατεβάσουμε το νέο Firmware από την SimCom. Αφού εκτελέσαμε το πρόγραμμα SIM7000 QDL μας εμφανίζει :

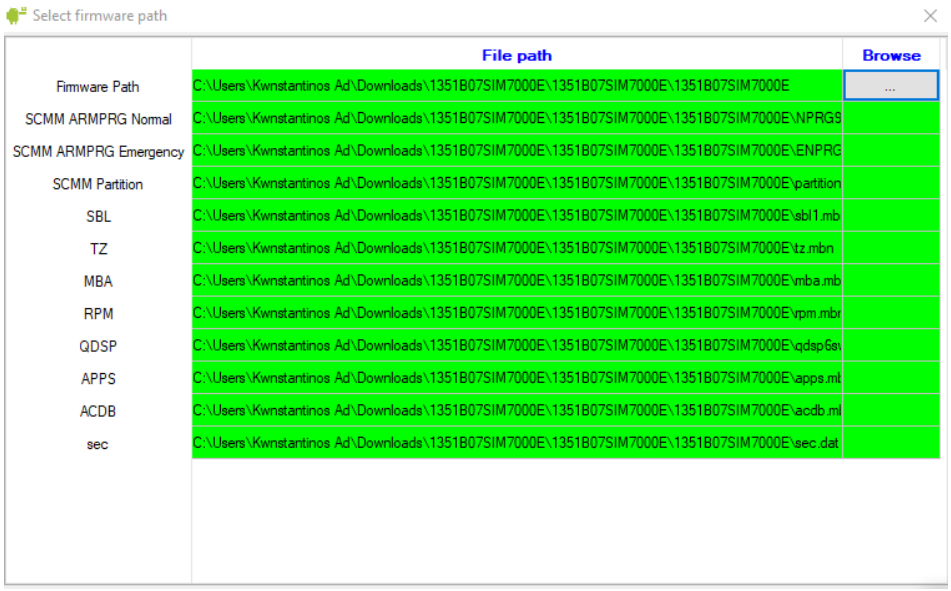
Εικόνα 71 Προγράμματος SIM7000 QDL

Στην συνεχεία πατάμε την εντολή Platform και μας εμφανίζει την επιλογή Select firmware path και πατάμε την εντολή browse επιλέγοντας τον firmware που θέλουμε να περάσουμε .



Εικόνα 72 Προγράμματος SIM7000 QDL επιλογή firmware

Στην συνεχεία αφού φορτώσει το firmware μας εμφανίζει :

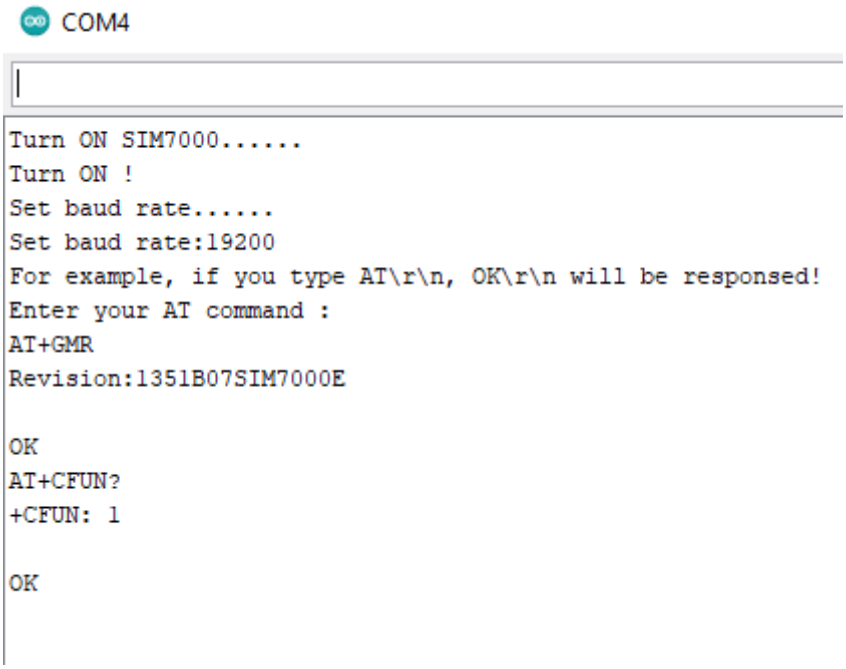


Εικόνα 73 Προγράμματος SIM7000 QDL εισαγωγή firmware

Και πατάμε το start για να ξεκινήσει η διαδικασία της αναβάθμισης το πρόγραμμα εντοπίζει αυτόματα την θύρα που είναι συνδεδεμένο το SIM7000 και θα ξεκινήσει την διαδικασία αναβάθμισης. Όταν ολοκληρωθεί η διαδικασία θα εμφανίσει το μήνυμα Update Success

Εικόνα 74 Προγράμματος SIM7000 QDL ολοκλήρωση εγκατάστασης firmware

Τέλος για να ελέγξουμε την έκδοση του Firmware εάν έγινε σωστά η αναβάθμιση, πληκτρολογούμε στην σειριακή του Arduino IDE την εντολή AT+GMR και μας επιστρέφει την έκδοση του Firmware και με την εντολή AT+CFUN? Μας επιστρέφει εάν το module λειτουργεί κανονικά .

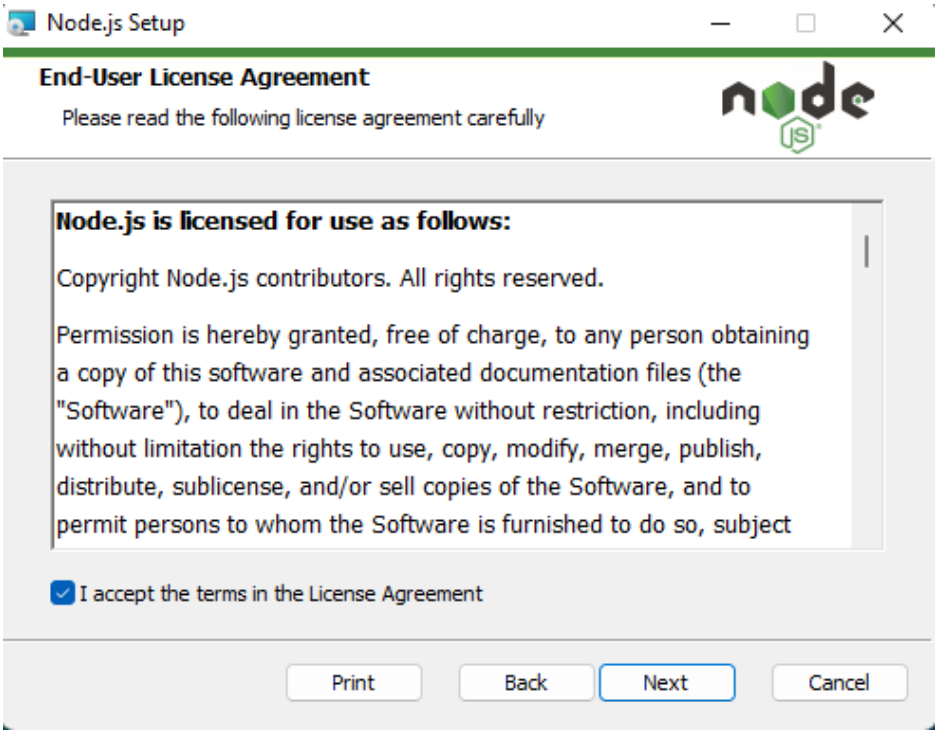


Εικόνα 75 Σειριακής επικοινωνίας με το Arduino

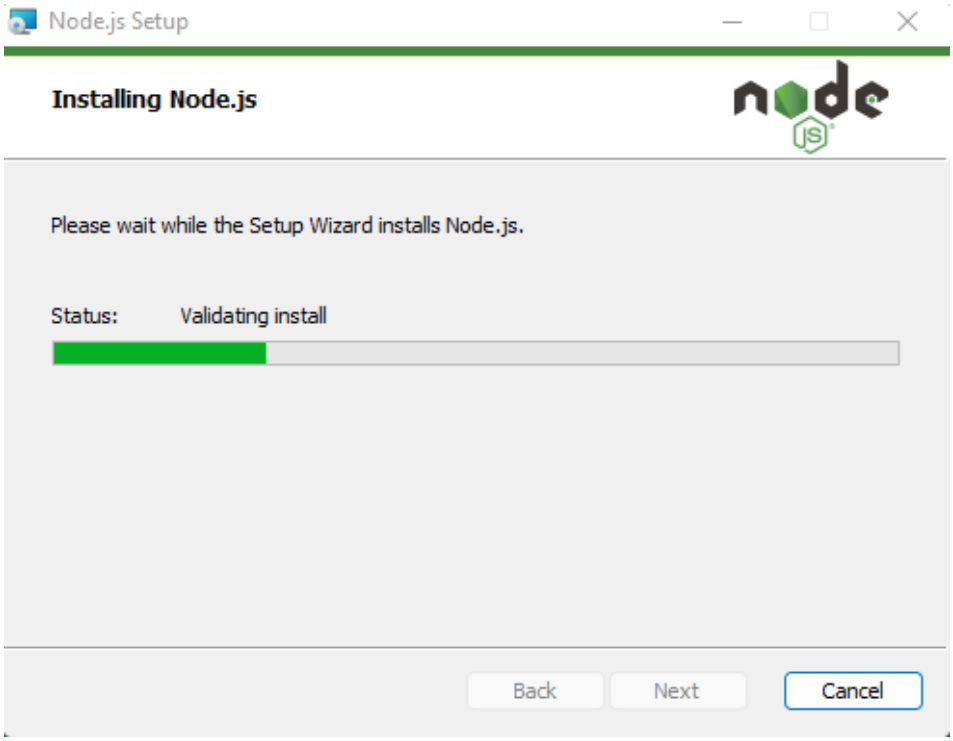
ΠΑΡΑΡΤΗΜΑ 4 Εγκατάσταση Node-Red

Το node-red είναι ένα εργαλείο ανάπτυξης λογισμικού που εξυπηρετεί εφαρμογές IoT και είναι βασισμένο στο Node.js. Η κυκλοφορία του έγινε για πρώτη φορά το 2013 από την εταιρία IBM και αργότερα μετατράπηκε σε εργαλείο ανοιχτού κώδικα . Το Node-RED διαθέτει ένα οπτικό περιβάλλον προγραμματισμού που βασίζεται σε ροές και σε μοντέλα προγραμματισμού που δίνει έτοιμα nodes στον χρηστή ώστε να μπορεί να φτιάξει την δική του εφαρμογή συνδέοντας τα nodes μεταξύ τους . Η αποθήκευση των ροών που δημιουργούνται από το Node-RED και αποθηκεύονται σε μορφή JSON. Το Node-RED φτιάχτηκε για να εξυπηρετεί εφαρμογές του IoT διευκολύνοντας την διασύνδεση των συσκευών , των υπηρεσιών και τον APIs.

Για την εγκατάσταση του Node-RED εκτελούμε το αρχείο εγκατάστασης Node.js που μπορούμε να το βρούμε στο ανάλογο site εγκαθιστώντας την local έκδοση του Node-RED σε Windows 10.

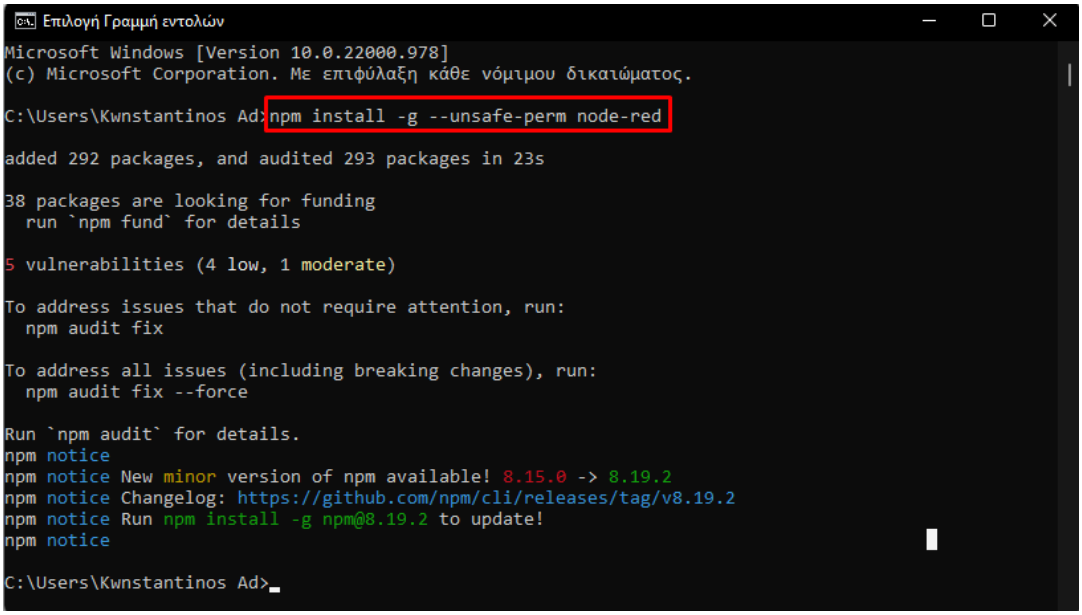


Εικόνα 76 Εγκατάσταση node.js



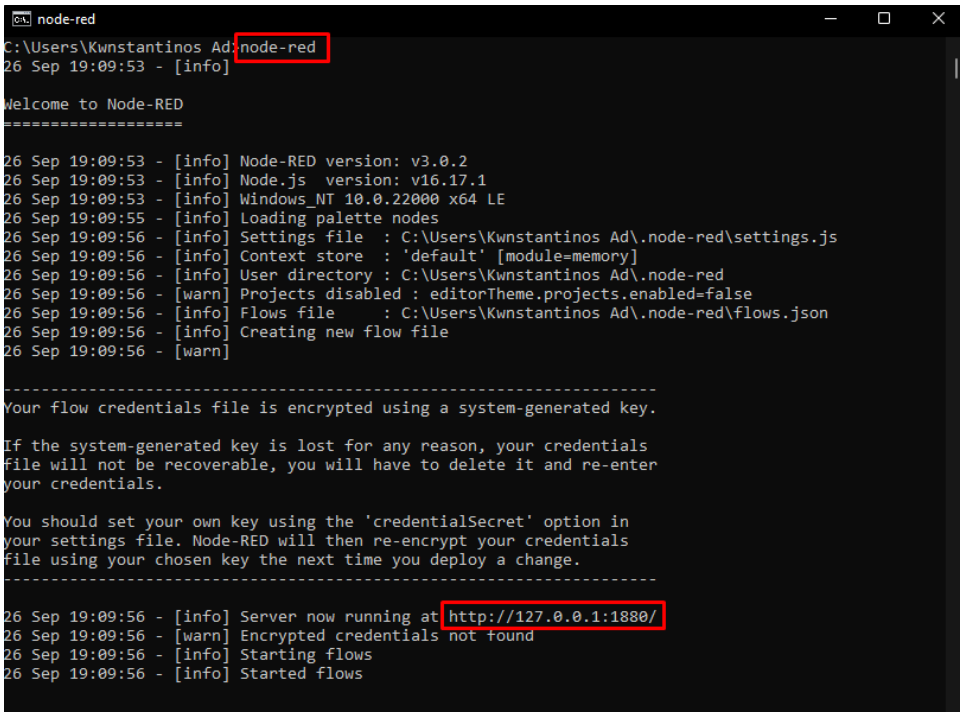
Εικόνα 77 Εγκατάσταση node.js

Αφού ολοκληρωθεί η εγκατάσταση του πρώτου μέρους ανοίγουμε την γραμμή εντολών των Windows και πληκτρολογούμε την εντολή npm install -g --unsafe-perm node-red.



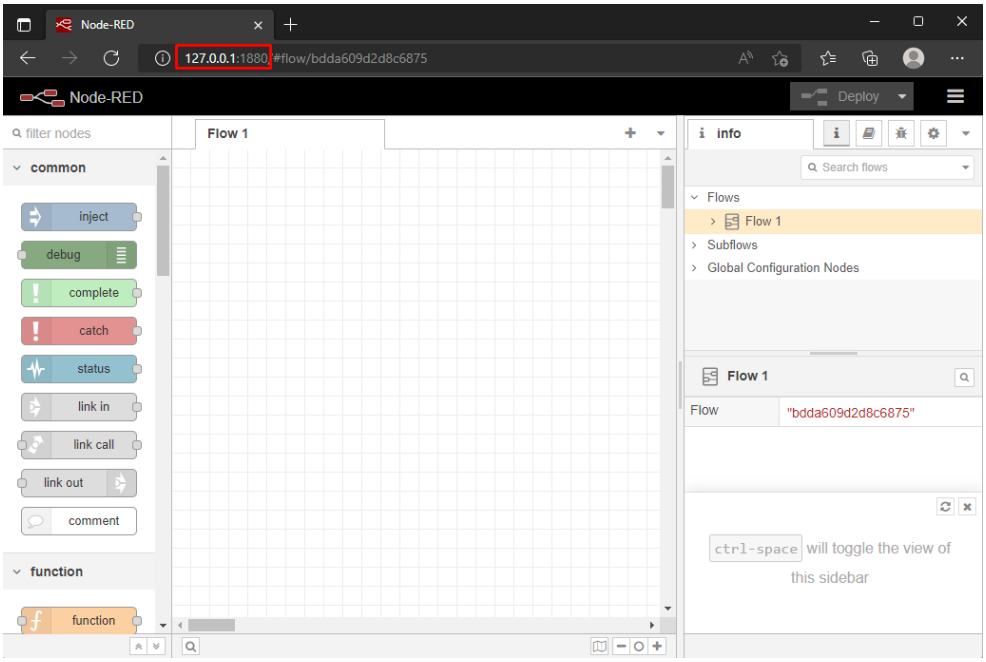
Εικόνα 78 Εγκατάσταση node-red

Στην συνεχεία αφού ολοκληρωθεί το δεύτερο μέρος της εγκατάστασης πληκτρολογούμε την εντολή node-red και μας εμφανίζει την IP διεύθυνση που τρέχει τοπικά το node-red 127.0.0.1 (localhost) στην πόρτα 1880



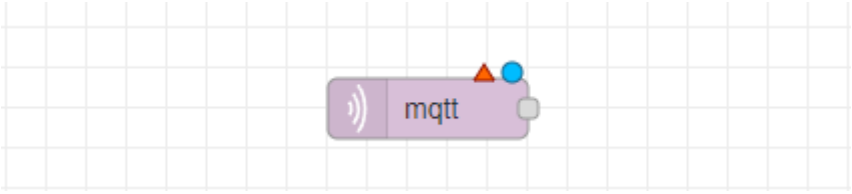
Εικόνα 79 Εκκίνηση προγράμματος node-red

Τέλος βλέπουμε ότι η εφαρμογή τρέχει στην διεύθυνση http://127.0.0.1:1880/ και ανοίγοντας ένα πρόγραμμα περιήγησης πληκτρολογώντας την διεύθυνση μπορούμε να περιηγηθούμε στην εφαρμογή.



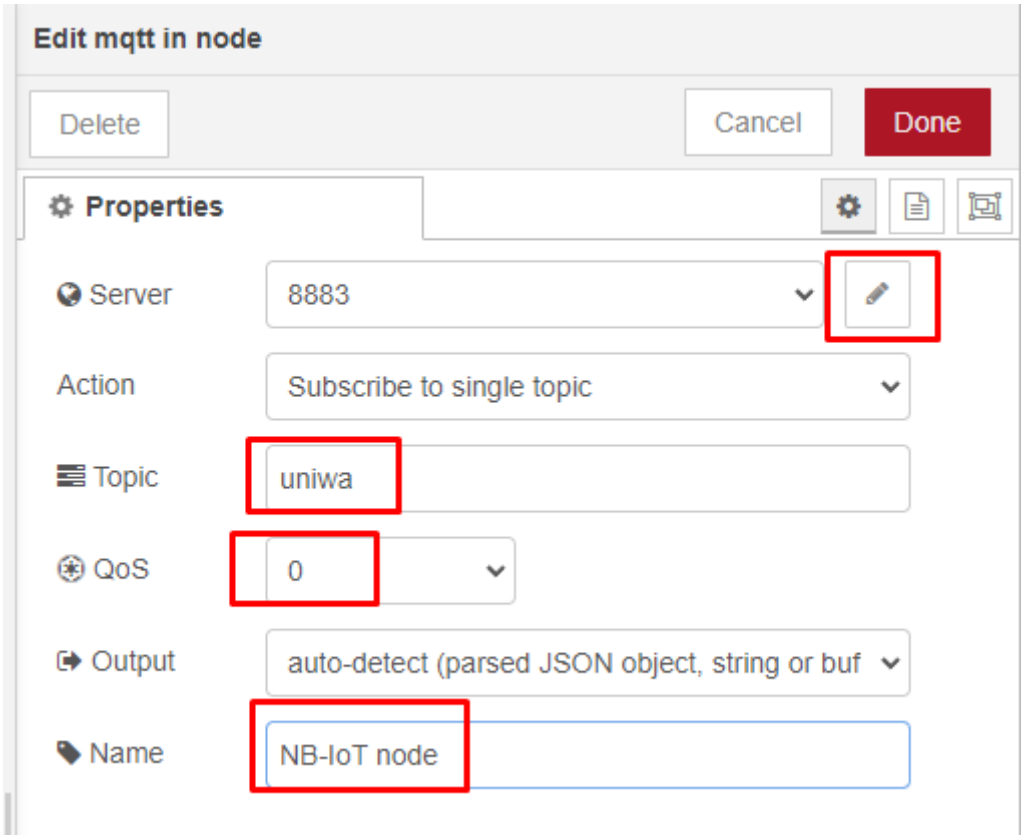
Εικόνα 80 Περιβάλλον node-red

Για να λάβουμε τα αποτελέσματα του αισθητήρα από τον κόμβο μας, χρησιμοποιούμε από το μενού με τα nodes του network το MQTT in που λειτουργεί σαν subscriber στον MQTT broker και κάνει επαναπροώθηση στα δεδομένα τα όποια δέχεται .



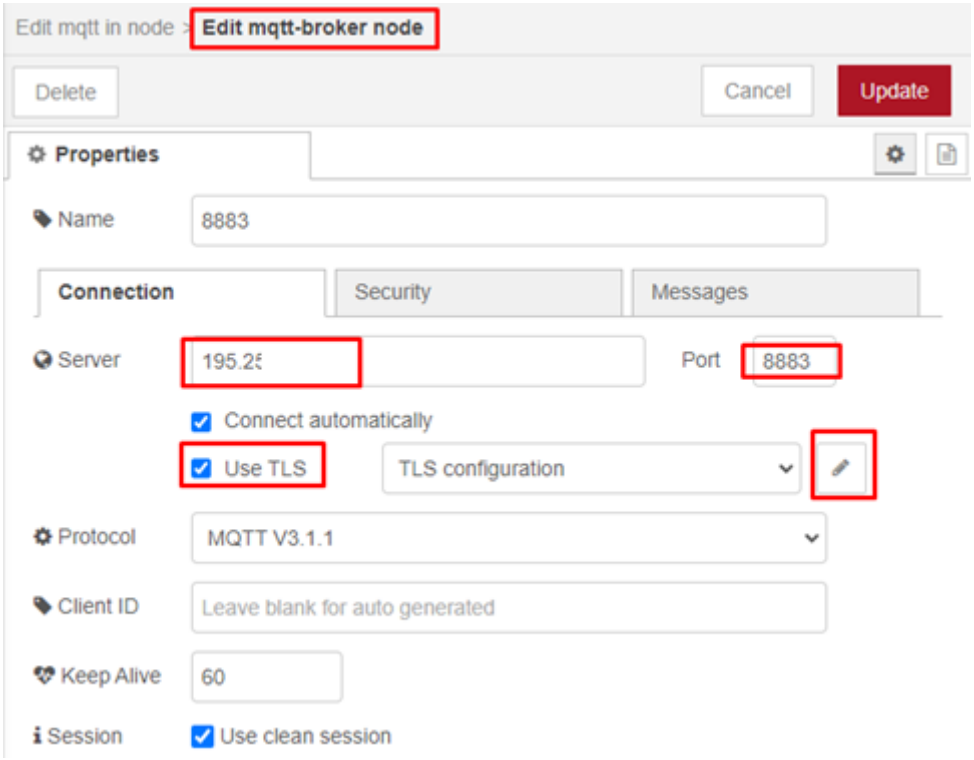
Εικόνα 81 MQTT node

Στην συνεχεία ανοίγουμε το node MQTT για να τροποποιήσουμε τα στοιχειά με την IP του server το Topic , το QoS και το Output.



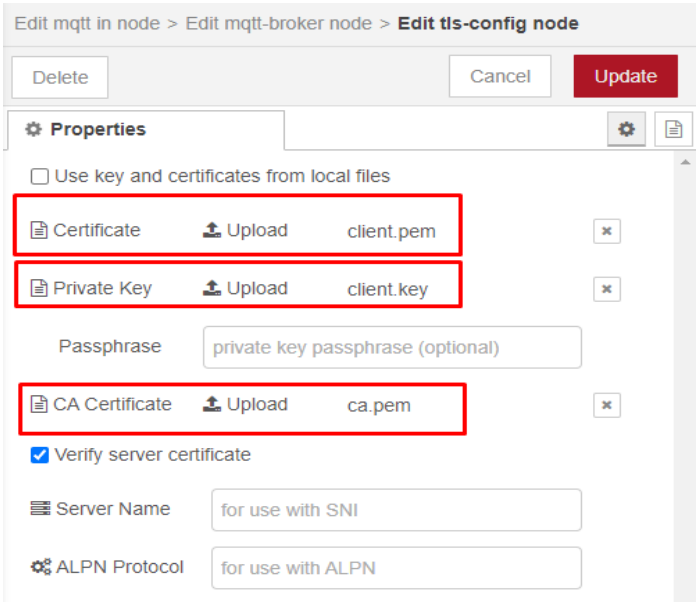
Εικόνα 82 Ρύθμιση MQTT node

Πατώντας την εντολή Edit MQTT-broker node πληκτρολογούμε την IP του server μας και στο port βάζουμε την κωδικοποιημένη πόρτα 8883. Ακόμη ενεργοποιούμε την εντολή TLS και πατάμε την εντολή Edit MQTT-broker node.



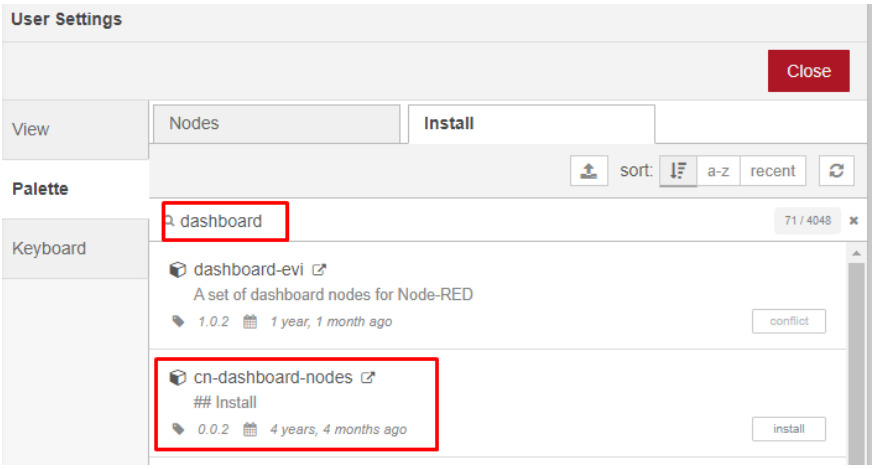
Εικόνα 83 Ρύθμιση mqtt-broker node

Πατώντας την εντολή Edit tls-config node μας εμφανίζει το παρακάτω παράθυρο και ανεβάζουμε από τον υπολογιστή τα πιστοποιητικά client.pem ,client.key ,ca.pem που δημιουργήσαμε στο παράρτημα 1 της εργασίας.



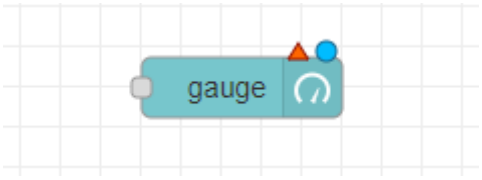
Εικόνα 84 Ρύθμιση tls-config node

Ακόμη, για την εργασία μας θα χρειαστούμε να εγκαταστήσουμε dashboard panels ώστε να βλέπουμε τις μετρήσεις μας από τον αισθητήρα . Για την εγκατάσταση πρέπει να μεταβούμε στο παράθυρο «Manage palette» και να πληκτρολογήσουμε στην αναζήτηση dashboard ώστε να κάνουμε εγκατάσταση της βιβλιοθήκης .

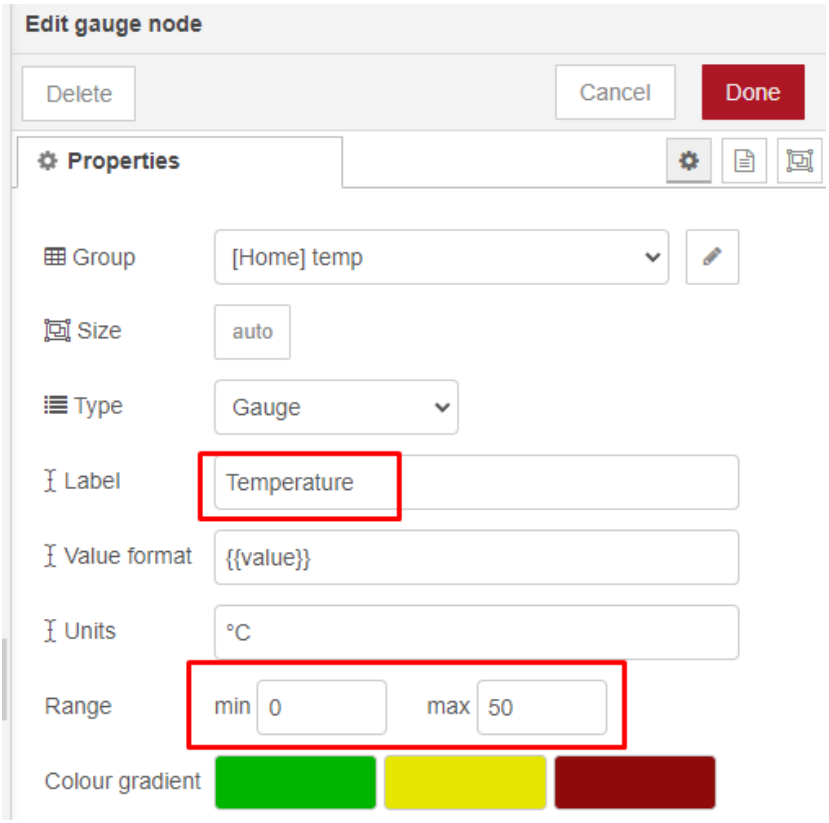


Εικόνα 85 Εγκατάσταση βιβλιοθήκης dashboard

Αφού ολοκληρώσαμε την εγκατάσταση από το μενού με τα nodes παίρνουμε δυο gauge ένα για την θερμοκρασία και ένα για την υγρασία και πατάμε πάνω τους για να τα ρυθμίσουμε θέτοντας σαν Label το Temperature και σαν Range 0 έως 50. Το ίδιο επαναλαμβάνουμε στο gauge για το γράφημα της υγρασίας .

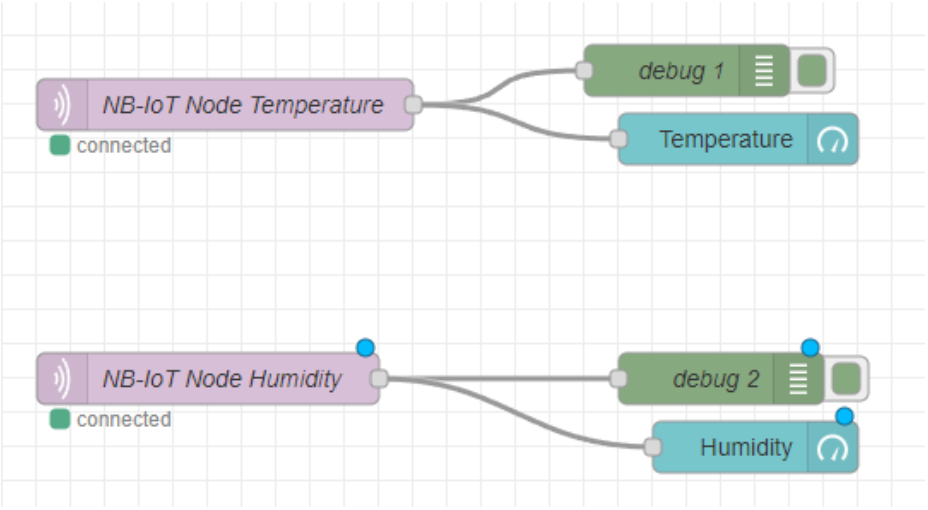


Εικόνα 86 Node gauge node-red



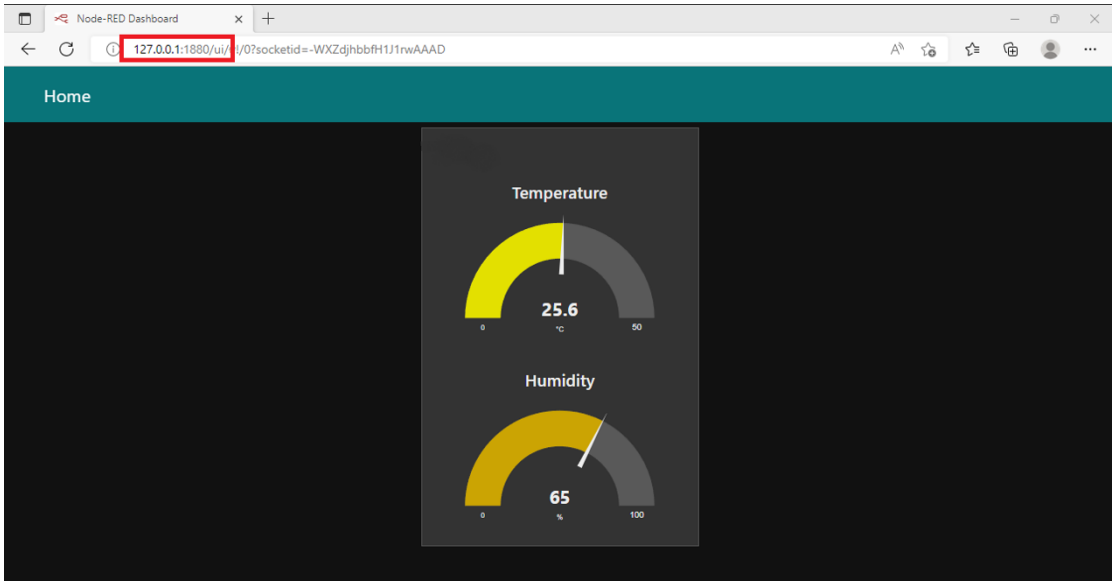
Εικόνα 87 Ρύθμιση gauge node-red

Αφού ολοκληρώσαμε την ρύθμιση και του gauge και του MQTT in τα συνδέουμε μεταξύ τους για να μπορέσουμε να βλέπουμε τα αποτελέσματα .



Εικόνα 88 Σχέδιο node-red

Τέλος εάν ανοίξουμε ένα νέο πρόγραμμα περιήγησης πληκτρολογώντας την διεύθυνση http://127.0.0.1:1880/ui/ μπορούμε να δούμε τα dashboards της θερμοκρασίας και της υγρασίας .



Εικόνα 89 Dashboards

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Chaudhari, B. S., & Zennaro, M. (2020). *LPWAN Technologies for IoT and M2M Applications* (1st ed.). Academic Press.

[2] Naik, N. (2018). LPWAN Technologies for IoT Systems: Choice Between Ultra Narrow Band and Spread Spectrum. 2018 IEEE International Systems Engineering Symposium (ISSE). doi:10.1109/syseng.2018.8544414

[3] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The Internet Society (ISOC)

[4] Xu, L. D., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243. https://doi.org/10.1109/tii.2014.2300753

[5]: Li, Y., Cheng, X., Cao, Y., Wang, D., & Yang, L. (2018). Smart Choice for the Smart Grid: Narrowband Internet of Things (NB-IoT). IEEE Internet Of Things Journal, 5(3), 1505-1515. doi: 10.1109/jiot.2017.2781251

[6]: PSM and eDRX: Power saving in cellular LPWAN - possibilities and limitations. (2022). Retrieved 6 August 2022, from https://1nce.com/en/blog/psm-and-edrx/?fbclid=IwAR3ZSyLR6Y-Kj7SRiyg62S6oT-Xum0muWRXML_BJxfikeRHX1TW6fE0HVzE

[7]: PSM and eDRX: LTE eDRX and PSM Explained for LTE-M1. Retrieved 22 May 2016, from LTE eDRX and PSM Technology Explained for LTE-M1 | Link Labs

[8] ¨ Díaz Zayas, A., Rivas Tocado, F. J., & Rodríguez, P. (2020). Evolution and Testing of NB-IoT Solutions. Applied Sciences, 10(21), 7903. https://doi.org/10.3390/app10217903

[9] Secured by hardware client-server communication based on NB-IoT technology Retrieved 02 August 2021 https://doi.org/10.1109/ZINC52049.2021.9499263

[10] W. Stevens, TCP/IP Illustrated, Volume 1, 1st ed. 1994.

[11] C. Lesjak et al., "Securing smart maintenance services: Hardware-security and TLS forMQTT," 2015 IEEE 13th International Conference on Industrial Informatics (INDIN),Cambridge,2015, pp. 1243-1250.

[12] Díaz Zayas, A., Rivas Tocado, F. J., & Rodríguez, P. (2020). Evolution and Testing of NB-IoT Solutions. Applied Sciences, 10(21), 7903. https://doi.org/10.3390/app10217903

[13] Nauman, A., Jamshed, M. A., Ahmad, Y., Ali, R., Zikria, Y. B., & Won Kim, S. (2019, June). An Intelligent Deterministic D2D Communication in Narrow-band Internet of Things. 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC). 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC). https://doi.org/10.1109/iwcmc.2019.8766786

[14] Althobaiti, O. S., & Dohler, M. (2021). Narrowband-Internet of Things Device-to-Device Simulation: An Open-Sourced Framework. Sensors, 21(5), 1824. https://doi.org/10.3390/s21051824

[15] Wu, F., Zhang, H., Di, B., Wu, J., & Song, L. (2019, May). Network Controlled D2D Communications: Licensed or Unlicensed Spectrum? ICC 2019 - 2019 IEEE International Conference on Communications (ICC). ICC 2019 - 2019 IEEE International Conference on Communications (ICC). https://doi.org/10.1109/icc.2019.8761477A.

[16] W. Ayoub, A. E. Samhat, F. Nouvel, M. Mroue and J. Pr´evotet, ”Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs Standards and Supported Mobility,” in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp.

[17] H. Mroue, A. Nasser, S. Hamrioui, B. Parrein, E. Motta-Cruz and G. Rouyer, ”MAC layer-based evaluation of IoT technologies: LoRa, SigFox and NB-IoT,” 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, 2018, pp. 1-5, doi: 10.1109/MENACOMM.2018.8371016

[18] Sinha, R.S., Wei, Y. & Hwang, S.-H., 2017. A survey on LPWA technology: Lora and Nb-IOT. ICT Express, 3(1), pp.14–21.

[19] Migabo, E., Djouani, K., & Kurien, A. (2020). A Novel Spread Spectrum and Clustering Mixed Approach with Network Coding for Enhanced Narrowband IoT (NB-IoT) Scalability. *Sensors*, *20*(18), 5219. https://doi.org/10.3390/s20185219

[20] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” Journal of Electrical and Computer Engineering, vol. 2017, p. 25, 2017. Article ID 9324035, doi:10.1155/2017/9324035.

[21] Chaudhari, B. S., Zennaro, M., & Borkar, S. (2020). LPWAN Technologies: Emerging Application Characteristics, Requirements, and Design Considerations. Future Internet, 12(3), 46. https://doi.org/10.3390/fi12030046

[22] K. Rose, S. Eldridge and L. Chapin, The Internet Of Things: An Overview Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC), 2015, pp. 9, 18-22.

[23] "What is an IoT Gateway? Open Automation Software",Open Automation Software, 2021. [Online]. Available: https://openautomationsoftware.com/open-automation-systems-blog/what-is-an-iot-gateway/

[23] https://www.plm.automation.siemens.com/global/en/our-story/glossary/industrial-internet-of-things/57242

[24] https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT

[25] https://www.rockwellautomation.com/en-fi/company/news/blogs/industry-4-0--the-challenges-and-risks.html

[26 Industry 4.0 Design Principles. (2022, August 29). RMIT University. https://www.rmit.edu.au/news/c4de/industry-4-0-design-principles

[27] Dikhanbayeva, D., Shaikholla, S., Suleiman, Z., & Turkyilmaz, A. (2020). Assessment of Industry 4.0 Maturity Models by Design Principles. *Sustainability*, *12*(23), 9927. https://doi.org/10.3390/su12239927

[28] Lele, A. (2018). Industry 4.0. *Disruptive Technologies for the Militaries and Security*, 205–215. https://doi.org/10.1007/978-981-13-3384-2_13

[29] Κακόγιαννος, Γ. (2020, May 26). *Τί είναι το Industry 4.0; Όλα όσα χρειάζεται να γνωρίζουμε.* industry4.gr. Retrieved September 1, 2022, from https://industry4.gr/what-is-industry-4-0/

[30] Telukdarie, A., & Sishi, M. N. (2018). Enterprise Definition for Industry 4.0. *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. https://doi.org/10.1109/ieem.2018.8607642

[31] SIM7000E Arduino NB-IoT/LTE/GPRS/GPS Expansion Shield - DFRobot. (2022, September 2). SIM7000E Arduino NB-IoT/LTE/GPRS/GPS Expansion Shield. https://www.dfrobot.com/product-1732.html

[32] Weinstein, R. (2005). RFID: a technical overview and its application to the enterprise. IT Professional, 7(3), 27–33. https://doi.org/10.1109/mitp.2005.69

[33] Khajenasiri, I., Estebsari, A., Verhelst, M., & Gielen, G. (2017). A Review on Internet of Things Solutions for Intelligent Energy Control in Buildings for Smart City Applications. Energy Procedia, 111, 770–779. https://doi.org/10.1016/j.egypro.2017.03.239

[34] Petitgrand, F., Peng, T. H., Wey, J., Sabihuddin, S., & Balijepalli, V. M. (2021). LPWAN Technologies: Design and Implementation of WEIGHTLESS Enabled AMI

in Tai-Power. 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT). https://doi.org/10.1109/isgt49243.2021.9372253

[35] M. Madhumitha et al.(2019); International Journal of Advance Research, Ideas and Innovations in Technology https://www.researchgate.net/publication/330840657_A_survey_on_LPWAN_technologies_in_content_to_IoT_applications

[36] Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011). Study on ZigBee technology. 2011 3rd International Conference on Electronics Computer Technology. https://doi.org/10.1109/icectech.2011.5942102

[37] Ondrej, S., Zdenek, B., Petr, F., & Ondrej, H. (2006). ZigBee Technology and Device Design. International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06). https://doi.org/10.1109/icniconsmcl.2006.233

[38] Gomez, C., & Paradells, J. (2010). Wireless home automation networks: A survey of architectures and technologies. *IEEE Communications Magazine*, *48*(6), 92–101. https://doi.org/10.1109/mcom.2010.5473869

[39] E, J. S., Sikora, A., Schappacher, M., & Amjad, Z. (2019, July). Test and Measurement of LPWAN and Cellular IoT Networks in a Unified Testbed. 2019 IEEE 17th International Conference on Industrial Informatics (INDIN). https://doi.org/10.1109/indin41052.2019.8972256

[40] R. K. Kodali and S. Soratkal, "MQTT based home automation system using ESP8266," 2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), Agra, 2016, pp. 1-5.

[41] K. Hwang, J. M. Lee, I. H. Jung and D. Lee, "Modification of Mosquitto Broker for Delivery of Urgent MQTT Message," 2019 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE), Yunlin, Taiwan, 2019, pp. 166-167.

[42] Soni, Dipa, and Ashwin Makwana. "A survey on mqtt: a protocol of internet of things (iot)." In International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017). 2017.

[43] C. Lesjak et al., "Securing smart maintenance services: Hardware-security and TLS for MQTT," 2015 IEEE 13th International Conference on Industrial Informatics (INDIN), Cambridge, 2015, pp. 1243-1250.

[43] F. Leens, "An introduction to I2C and SPI protocols", IEEE Instrumentation & Measurement Magazine, vol. 12, no. 1, pp. 8-13, 2009.

[44] https://www.mouser.com/datasheet/2/758/DHT11-Technical-Data-Sheet-Translated-Version-1143054.pdf

[45] https://www.offlinepost.gr/2022/05/20/h-prwth-biomhxanikh-epanastash-kai-oi-allages-pou-epefere/

[46] https://www.maxmag.gr/politismos/istoria/viomichaniki-epanastasi-i-archi-mias-neas-epochis/

[47] https://ewood.gr/4%CE%B7-%CE%B2%CE%B9%CE%BF%CE%BC%CE%B7%CF%87%CE%B1%CE%BD%CE%B9%CE%BA%CE%AE-%CE%B5%CF%80%CE%B1%CE%BD%CE%AC%CF%83%CF%84%CE%B1%CF%83%CE%B7-02/

[48] https://texnologia.net/h-tetarth-viomhxanikh-epanastash-kai-to-provlhma-ths-paragogikothtas/2017/09

[49] https://www.technologyrecord.com/Article/how-to-implement-an-industrial-internet-of-things-automation-plan-61582

[50] https://www.androidauthority.com/what-is-rfid-975910

[51] https://www.neothingsiot.com/portfolio/zigbee/

[52] https://www.weptech.de/en/technology/mioty.html

[53] https://intelilight.eu/connected-street-lighting/intelilight-lte-m-compatible-streetlighting-remote-management/

[54] https://thethings.io/nb-iot-narrowband-iot-platform/

[55] https://www.sigfox.gr/

[56] https://en.wikipedia.org/wiki/Z-Wave

[57] https://iotlab.tertiumcloud.com/2017/11/08/which-lpwan-is-right-for-you/

[58] https://es.farnell.com/lorawan-101

[59] https://en.wikipedia.org/wiki/Ingenu

[60] https://www.cnx-software.com/2015/08/10/weightless-p-standard-is-designed-for-high-performance-low-power-2-way-communications-for-iot/

[61] https://dat4zero.eu/what-is-industry-4-0/

[62] https://enterpriseiotinsights.com/20190718/channels/fundamentals/three-nb-iot-deployment-models

[63] https://cicicom.gr/pages/lora-wan/

[64] https://www.thethingsnetwork.org/marketplace/product/lora-node-phat-for-raspberry-pi-868-mhz-915-mhz

[65] https://topelectronics.gr/iot/dragino-lg01-p-lora-gateway-868-mhz/

[66] https://medium.com/@hendraputra/how-to-access-chirpstack-api-d9643a282c07

[67] https://docs.arduino.cc/hardware/uno-rev3

[68]"A technical overview of LoRa® and LoRaWAN™" LoRa Alliance November 2015. https://lora-alliance.org/wp-content/uploads/2020/11/what-is-lorawan.pdf

[69] Mishra, B., Mishra, B., & Kertesz, A. (2021, September 14). Stress-Testing MQTT Brokers: A Comparative Analysis of Performance Measurements. *Energies*, *14*(18), 5817. https://doi.org/10.3390/en14185817

[70] M. Fezari and A. Al Dahoud, "Integrated Development Environment "IDE," 2018, pp. 1–12

[71] W. Stevens, TCP/IP Illustrated, Volume 1, 1st ed. 1994.