ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Απειλές και προκλήσεις ασφάλειας του "Πράσινου" Διαδικτύου των Πραγμάτων (IoT).

Μελέτη περίπτωσης με χρήση έξυπνων συσκευών IoT.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

Πάντογλου Νικόλας

(ΑΕΜ: 2709)

Επιβλέπων : Σπυρίδων Νικολάου

Λέκτορας

Καστοριά, Σεπτέμβριος 2022

Η παρούσα σελίδα σκοπίμως παραμένει λευκή

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Απειλές και προκλήσεις ασφάλειας του "Πράσινου" Διαδικτύου των Πραγμάτων (IoT). Μελέτη περίπτωσης με χρήση έξυπνων συσκευών IoT.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

Πάντογλου Νικόλας

(ΑΕΜ: 2709)

Επιβλέπων : Σπυρίδων Νικολάου

Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ημερομηνία εξέτασης

.....	.....	.....
Ον/μο Μέλους	Ον/μο Μέλους	Ον/μο Μέλους
Ιδίοτητα Μέλους	Ιδίοτητα Μέλους	Ιδίοτητα Μέλους

Καστοριά, Σεπτέμβριος 2022

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά, τον επιβλέποντα καθηγητή της παρούσας πτυχιακής εργασίας, κύριο Σπυρίδωνα Νικολάου, για τη συστηματική καθοδήγηση και τις πολύτιμες συμβουλές που μου παρείχε, καθ' όλη τη διάρκεια εκπόνησης της εργασίας.

Περίληψη

Το Πράσινο Διαδίκτυο των Πραγμάτων έχει ως στόχο να συνδέσει δισεκατομμύρια έξυπνα πράγματα με το Διαδίκτυο, με κύριο γνώμονα την εξοικονόμηση ενέργειας και τη μεγιστοποίηση της αποδοτικότητας των συστημάτων IoT, μέσω της συνολικής και διαρκούς παρακολούθησής τους, με αποτέλεσμα να γίνεται πιο εύκολη η συλλογή και καταγραφή δεδομένων από πληθώρα αισθητήρων, καθώς και η επικοινωνία και μετάδοσή τους σε όλα τα επίπεδα, η απομακρυσμένη αποθήκευση και επεξεργασία των δεδομένων αυτών και η λήψη αποφάσεων για το συνολικό έλεγχο της βιωσιμότητας τους, σε ποικίλες περιπτώσεις της καθημερινής ζωής (έξυπνες πόλεις, έξυπνες μεταφορές, έξυπνη υγεία, έξυπνη βιομηχανία, έξυπνη γεωργία, κ.ά.). Το Πράσινο Διαδίκτυο των Πραγμάτων, βασίζεται σε καινοτόμες τεχνολογικές επενδύσεις, που έχουν σκοπό να παρέχουν πολύτιμες υπηρεσίες τόσο στα άκρα του δικτύου, όσο και συνολικά σε ολόκληρο το οικοσύστημα IoT, έτσι ώστε να είναι δυνατή η ανάπτυξη των αυτοματοποιημένων υπηρεσιών και εφαρμογών που να ενισχύουν την αποτελεσματικότητα και αποδοτικότητα τους.

Σε αυτή την εργασία παρουσιάζονται και αναλύονται οι πιο σημαντικές απειλές και προκλήσεις ασφαλείας που αντιμετωπίζει το Πράσινο Διαδίκτυο των Πραγμάτων. Επίσης, δίνεται έμφαση σε μελέτη περίπτωσης για το οικοσύστημα «πράσινου» IoT την έξυπνης γεωργίας, με ανάλυση των βασικών απειλών και προκλήσεων σε θέματα ασφάλειας που αντιμετωπίζει, καθώς και τους κύριους μηχανισμούς για την προστασία της ασφάλειας του, όπως είναι ο έλεγχος πιστοποίησης ταυτότητας των οντοτήτων που εμπλέκονται σε αυτό το οικοσύστημα IoT, καθώς και η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των δεδομένων του, με λύσεις που βασίζονται σε τεχνολογία blockchain για να μπορέσει κάποιος να διατηρήσει το απόρρητο με τη χρήση αλγορίθμων συναίνεσης για εφαρμογές που βασίζονται σε IoT.

Λέξεις Κλειδιά: ***Green Internet of Things, Cloud, αισθητήρες, τεχνολογίες επικοινωνιών, Έξυπνη Γεωργία,***

Abstract

The Green Internet of Things (Green IoT) aims to connect billions of smart things to the Internet, with the main target of saving energy and maximizing the efficiency of the IoT systems, through their comprehensive and continuous monitoring, thus making it easier to collect and record data from a variety of sensors, as well as to communicate and transmit them at all levels of the IoT ecosystem, the remote data storage and data processing and the decision-making support systems, for the overall control of their viability, in various cases of everyday life (smart cities, smart transport, smart health, smart industry, smart agriculture, etc.). The Green Internet of Things is based on innovative technology investments, designed to provide valuable services both at the edge of the network and throughout the IoT ecosystem as a whole, in order to develop automated services and applications that enhance their effectiveness and efficiency.

This thesis presents and analyzes the most important security threats and challenges of the Green Internet of Things. Emphasis is placed on a case study analysis of the key security threats and challenges of "green" IoT ecosystem of smart agriculture, as well as the main security mechanisms applies for protecting, such as the authentication of the entities involved in this IoT ecosystem, as well as data integrity, confidentiality and availability, with solutions based on blockchain technologies, to enable one to maintain privacy by using consent algorithms for IoT-based applications.

Key-Words: ***Green Internet of Things, Cloud, sensors, communication technologies, smart agriculture,***

Πίνακας Περιεχομένων

Λίστα Εικόνων

Εισαγωγή

Στην παρούσα πτυχιακή εργασία παρουσιάζονται και αναλύονται οι πιο σημαντικές απειλές και προκλήσεις ασφαλείας που αντιμετωπίζει το Πράσινο Διαδίκτυο των Πραγμάτων. Επίσης, δίνεται έμφαση σε μελέτη περίπτωσης για το οικοσύστημα «πράσινου» IoT την έξυπνης γεωργίας, με ανάλυση των βασικών απειλών και προκλήσεων σε θέματα ασφάλειας που αντιμετωπίζει, καθώς και τους κύριους μηχανισμούς για την προστασία της ασφάλειας του.

Στο πρώτο κεφάλαιο γίνεται αναφορά στο Διαδίκτυο των Πραγμάτων (IoT), στα χαρακτηριστικά του, στις εφαρμογές, στην αρχιτεκτονική του.

Στο δεύτερο κεφάλαιο αναλύεται η έννοια του Πράσινου Διαδικτύου των Πραγμάτων (Green IoT) και γίνεται αναφορά στις εφαρμογές και στην αρχιτεκτονική του

Στο τρίτο κεφάλαιο παρουσιάζονται οι προκλήσεις ασφαλείας του Πράσινου Διαδικτύου των Πραγμάτων σε κάθε επιμέρους επίπεδο της αρχιτεκτονικής του και για κάθε εφαρμογή του και αναφέρονται οι βασικές κατηγορίες των επιθέσεων ανά επίπεδο.

Στο τέταρτο κεφάλαιο παρουσιάζονται ενδεικτικά παραδείγματα για τις προκλήσεις ασφαλείας που αντιμετωπίζει το Πράσινο Διαδίκτυο των Πραγμάτων σε εφαρμογές για έξυπνες πόλεις και αναλύονται διάφορες προσεγγίσεις της αρχιτεκτονικής ενός οικοσυστήματος πράσινου IoT για μία έξυπνη πόλη, καθώς και οι λειτουργικές του απαιτήσεις του.

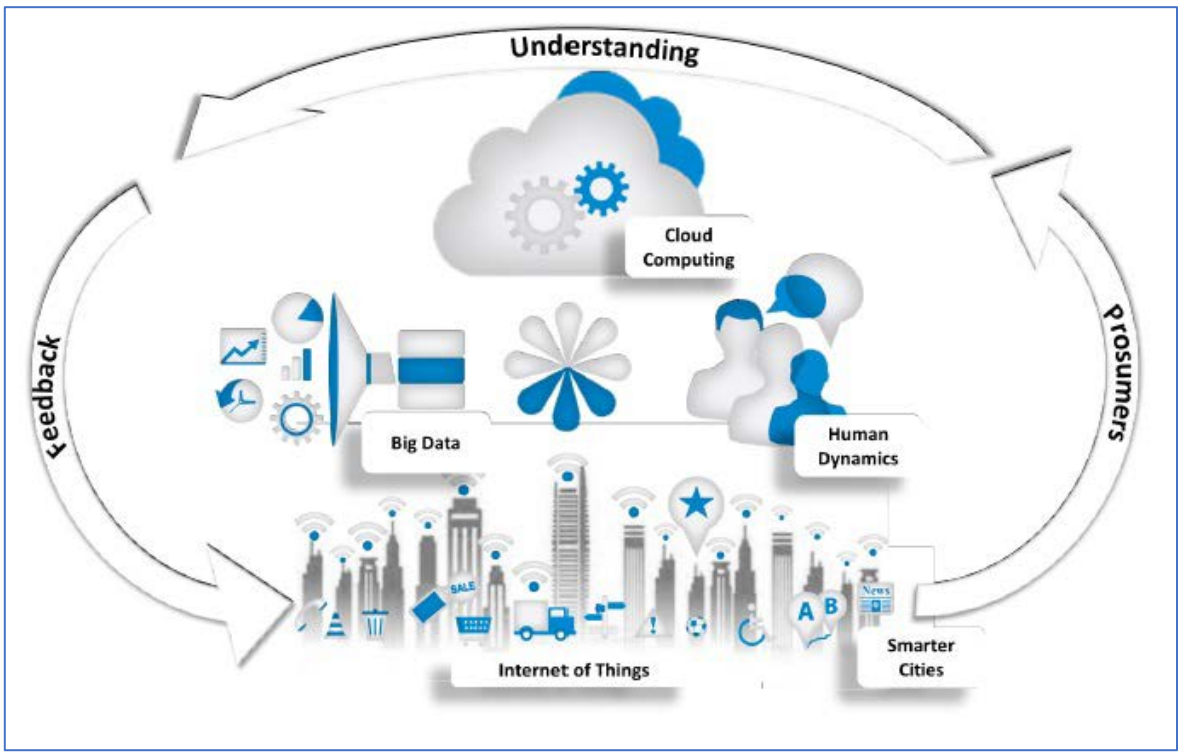
Στο πέμπτο κεφάλαιο παρουσιάζονται ορισμένοι από τους κυριότερους μηχανισμούς ασφαλείας του πράσινου Διαδικτύου των Πραγμάτων και προτείνονται λύσεις στις σημαντικότερες προκλήσεις που αφορούν την ασφάλεια του.

Στο έκτο κεφάλαιο αναλύεται μια μελέτη περίπτωσης όπου παρουσιάζονται οι ερευνητικές προκλήσεις σε θέματα ασφάλειας και απορρήτου στην περιοχή της έξυπνης γεωργίας (smart agriculture) που βασίζεται στο Πράσινο Διαδίκτυο των Πραγμάτων. Δίνεται έμφαση στους βασικούς μηχανισμούς ασφάλειας όπως είναι ο έλεγχος πιστοποίησης ταυτότητας των οντοτήτων που εμπλέκονται σε αυτό το οικοσύστημα IoT, καθώς και η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των δεδομένων του, με λύσεις που βασίζονται σε τεχνολογία blockchain.

Τέλος για μελλοντική επέκταση της εργασίας αναφέρονται προκλήσεις οι οποίες στο μακρινό μέλλον θα εξεταστούν από ερευνητές όσον αφορά το Πράσινο Διαδίκτυο των Πραγμάτων.

1. Διαδίκτυο των Πραγμάτων (Internet of Things – Iota)

Το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) αποτελεί το δρόμο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Με λίγα λόγια η Διεθνής Ένωση Τηλεπικοινωνιών θέτει το IoT ως μία παγκόσμια υποδομή για την κοινωνία της πληροφορίας επιτρέποντας στις προηγμένες υπηρεσίες είτε φυσικές είτε εικονικές τη διασύνδεση πραγμάτων με κριτήριο τις τωρινές τεχνολογίες επικοινωνίας και το πως εξελίσσονται οι διαλειτουργικές πληροφορίες. Η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό).



Εικόνα 1. Το Οικοσύστημα του Διαδικτύου των Πραγμάτων (IoT Ecosystem)

Το IoT είναι μία από τις τρείς κορυφαίες τεχνολογικές εξελίξεις της επόμενης δεκαετίας και αποτελεί το επόμενο μεγάλο βήμα στο χώρο της τεχνολογίας. Ο όρος IoT έγινε γνωστός στα τέλη της δεκαετίας του 1990 από τον επιχειρηματία Kevin Ashton [1].Ο Ashton είναι ένας από τους ιδρυτές του Auto-ID center στο MIT, ήταν μέλος μίας ομάδας που ανακάλυψε τον τρόπο να συνδέσει τα αντικείμενα με το διαδίκτυο μέσω μίας ετικέτας αναγνώρισης ραδιοσυχνοτήτων (Radio Frequency Identification -RFID tag). Το σύστημα αναγνώρισης ραδιοσυχνοτήτων (RFID) είναι στην ουσία μία μικρή ηλεκτρονική συσκευή που περιλαμβάνει πολλές ετικέτες RFID ή/και πολύ μικρούς αισθητήρες ανάγνωσης ετικετών. Οι ετικέτες RFID μπορούν να αποθηκεύσουν πληροφορίες σχετικά με τα αντικείμενα με τα οποία συνδέονται. Γενικά, το εύρος μετάδοσης του συστήματος RFID είναι λίγα μέτρα. Υπάρχουν δύο είδη ετικετών RFID που ονομάζονται ενεργές και παθητικές

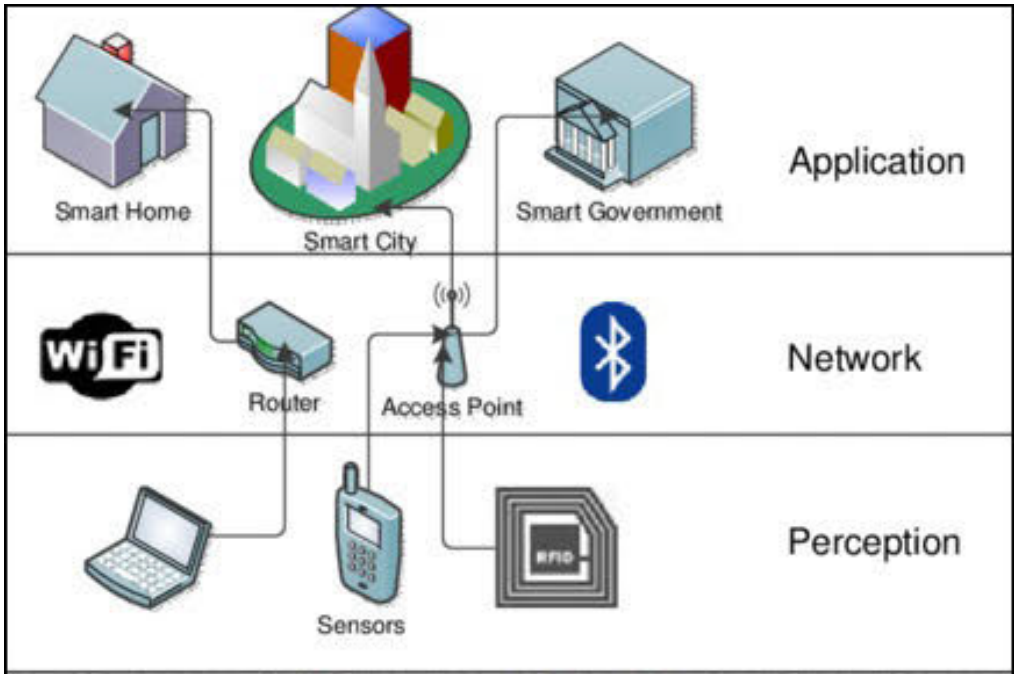
ετικέτες. Οι ενεργές ετικέτες διαθέτουν μπαταρίες για να μεταδίδουν συνεχώς το δικό τους σήμα, ενώ οι παθητικές ετικέτες δεν έχουν ενσωματωμένη μπαταρία και χρειάζονται να συλλέξουν ενέργεια συγκομιδής μέσα από τα σήματα που λαμβάνουν από τους αισθητήρες ανάγνωσης ετικετών.

1.1. Αρχιτεκτονική Διαδικτύου των Πραγμάτων

Το 1999 ο Kevin Ashton εισήγαγε την έννοια του IoT σχετικά με τη διαχείριση της αλυσίδας εφοδιασμού. Το IoT είναι μία βασισμένη με ένα ευφυές δίκτυο υποδομής στο οποίο πολλά αντικείμενα, συμπεριλαμβανομένου και των αισθητήρων, των ενεργοποιητών, των ασύρματων συσκευών που έχουν μοναδική αναγνώριση διασυνδέονται για να εκπληρωθούν πολύπλοκες εργασίες.

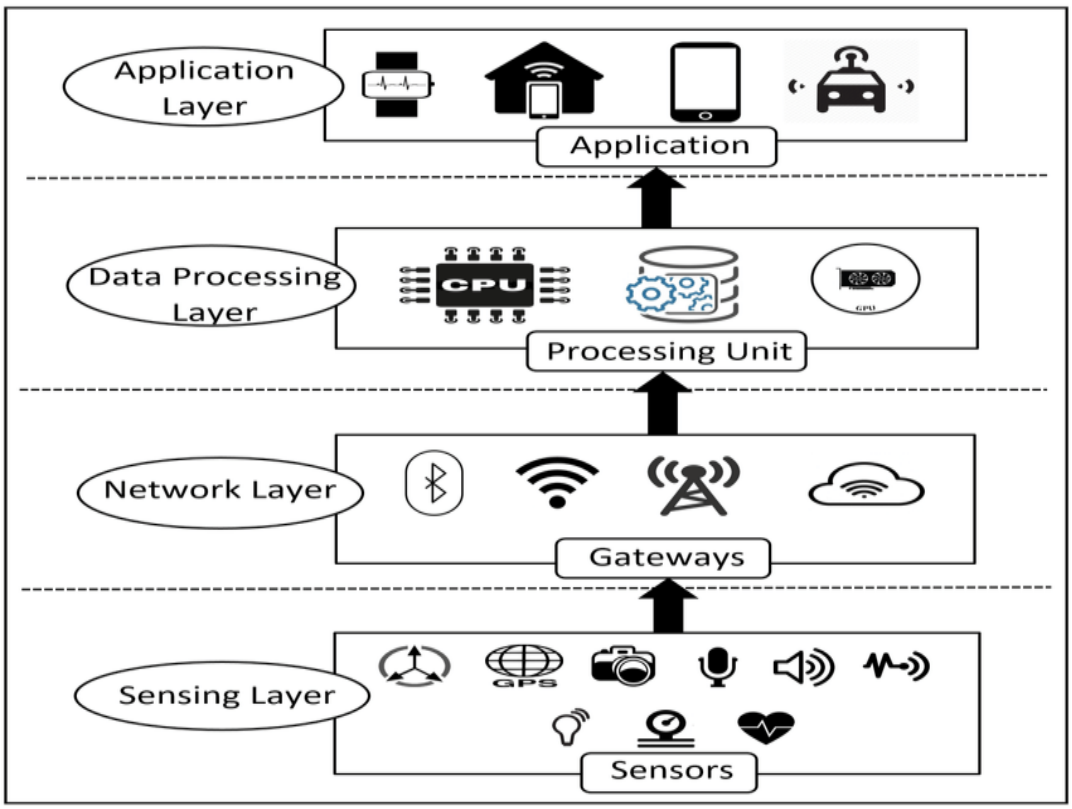
Στη βιβλιογραφία προτείνονται διάφορα μοντέλα αναφοράς για την αρχιτεκτονική του IoT που αποτελούνται από τρία ή τέσσερα ή πέντε διακριτά επίπεδα.

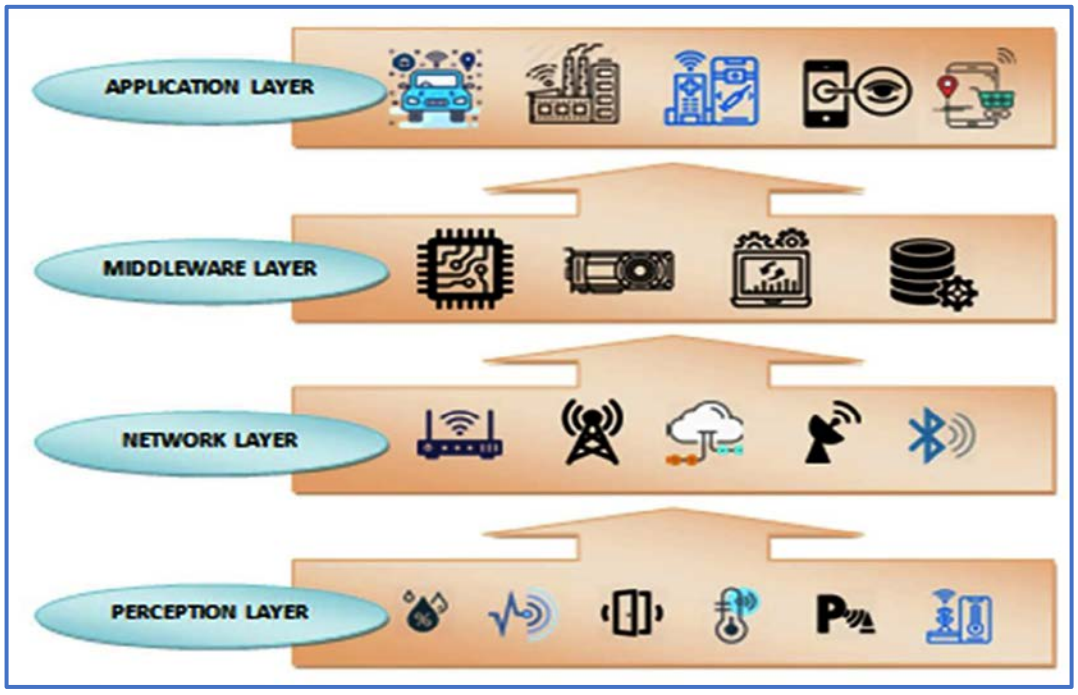
- Στην περίπτωση της αρχιτεκτονικής IoT τριών επιπέδων, έχουμε το επίπεδο αντίληψης (Perception Layer) για συλλογή δεδομένων, το επίπεδο πρόσβασης στο δίκτυο (Network Layer), ή ενδιάμεσο επίπεδο (Middleware Layer) και το επίπεδο εφαρμογής (Application Layer) για τη συλλογή, αποθήκευση, επεξεργασία και διαχείρισης των δεδομένων IoT.



Εικόνα 2. Αρχιτεκτονική IoT τριών επιπέδων

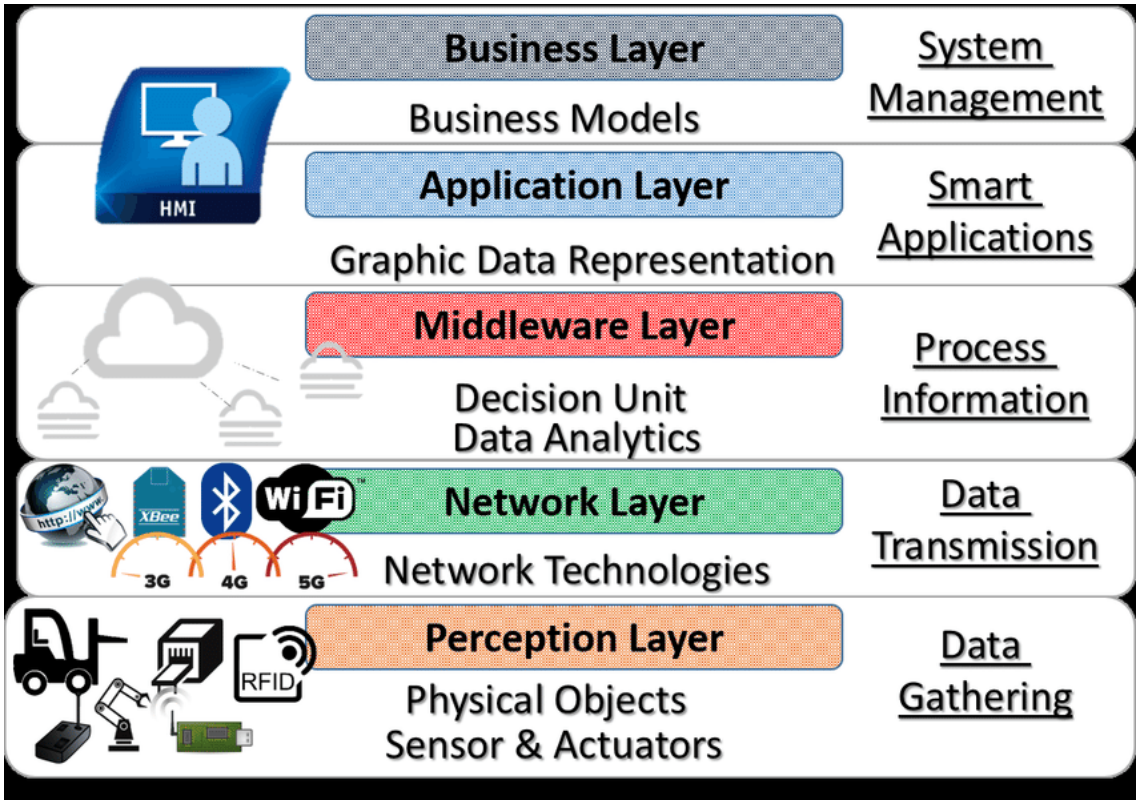
- Στην περίπτωση της αρχιτεκτονικής IoT τεσσάρων επιπέδων, έχουμε το επίπεδο αντίληψης (Perception or Sensing Layer), το επίπεδο δικτύου (Network Layer), το ενδιάμεσο επίπεδο (Middleware Layer) ή επίπεδο επεξεργασίας δεδομένων (Data Processing Layer) και το επίπεδο εφαρμογής (Application Layer).





Εικόνα 3. Αρχιτεκτονική IoT τεσσάρων επιπέδων [2]

- Στην περίπτωση της αρχιτεκτονικής IoT πέντε επιπέδων, από το επίπεδο αντίληψης, από το επίπεδο δικτύου, από το ενδιάμεσο επίπεδο, από το επίπεδο εφαρμογής και από το επιχειρηματικό επίπεδο.



Εικόνα 4. Αρχιτεκτονική IoT πέντε επιπέδων [3]

1.1.1. Επίπεδο Αντίληψης (Perception Layer)

Αυτό το επίπεδο ασχολείται με την αναγνώριση και τη συλλογή συγκεκριμένων πληροφοριών από τα φυσικά αντικείμενα και τις συσκευές αισθητήρων. Ανάλογα με τη μέθοδο ταυτοποίησης των αντικειμένων υπάρχουν διάφορες συσκευές αισθητήρων όπως, οι ηλεκτρονικές διεπαφές δεδομένων, οι ασύρματοι αισθητήρες δικτύων, τα συστήματα RFID, οι αισθητήρες υπερύθρων, τα συστήματα εντοπισμού θέσης, κ.ά. Τα δεδομένα που συλλέγονται από αυτά τα φυσικά αντικείμενα και τις συσκευές αισθητήρων διαβιβάζονται στο αμέσως επόμενο επίπεδο δικτύου για την ασφαλή μετάδοση τους προς επεξεργασία, αποθήκευση και ταυτοποίηση, αλλά και τον απομακρυσμένο έλεγχο και τη λήψη αποφάσεων.

1.1.2. Επίπεδο Δικτύου (Network Layer)

Θεωρείται γνωστό ως επίπεδο μεταφοράς ή επίπεδο πρόσβασης σε πύλη και ο κύριος σκοπός αυτού του επιπέδου είναι η διαχείριση και η ασφαλής μεταφορά των δεδομένων από τις συσκευές αισθητήρων στο σύστημα επεξεργασίας πληροφοριών. Περιλαμβάνει την εγκαθίδρυση και διαχείριση συνόδων, τη δρομολόγηση και τη μετάδοση δεδομένων, κ.λπ. Τα δεδομένα που συλλέγονται από το κατώτερο επίπεδο αντίληψης μπορούν να μεταφερθούν μέσω των διαφορετικών καναλιών επικοινωνίας, ενσύρματα ή ασύρματα, όπως για παράδειγμα GSM, UMTS, 4G, 5G, Wi-Fi, Bluetooth, ZigBee, Lora Wan, Ethernet, κ.λπ. ανάλογα με τις συσκευές αισθητήρων και αποστέλλονται στο ενδιάμεσο επίπεδο.

1.1.3. Ενδιάμεσο Επίπεδο (Middleware Layer)

Οι συσκευές μέσω του Α εφαρμόζουν διαφορετικούς τύπους υπηρεσιών. Κάθε συσκευή συνδέει και επικοινωνεί μόνο με τις άλλες συσκευές που εφαρμόζουν τον ίδιο τύπο υπηρεσίας. Αυτό το επίπεδο είναι υπεύθυνο για τη διαχείριση υπηρεσιών και έχει σύνδεση με τη βάση δεδομένων. Λαμβάνει τις πληροφορίες από το Επίπεδο Δικτύου και τις αποθηκεύει στη βάση δεδομένων. Εκτελεί παρακολούθηση και έλεγχο πρόσβαση της συσκευής, φιλτράρισμα και επεξεργασία των δεδομένων, ανάλυση σημασιολογικών δεδομένων, αλλά και υπολογισμούς και λαμβάνει αυτόματα απόφαση με βάση τα αποτελέσματα.

1.1.4. Επίπεδο Εφαρμογής (Application Layer)

Ο ρόλος αυτού του επιπέδου είναι να προσφέρει διαφορετικές εφαρμογές στους χρήστες του οικοσυστήματος IoT. Χωρίζεται σε δύο υπό-επίπεδα:

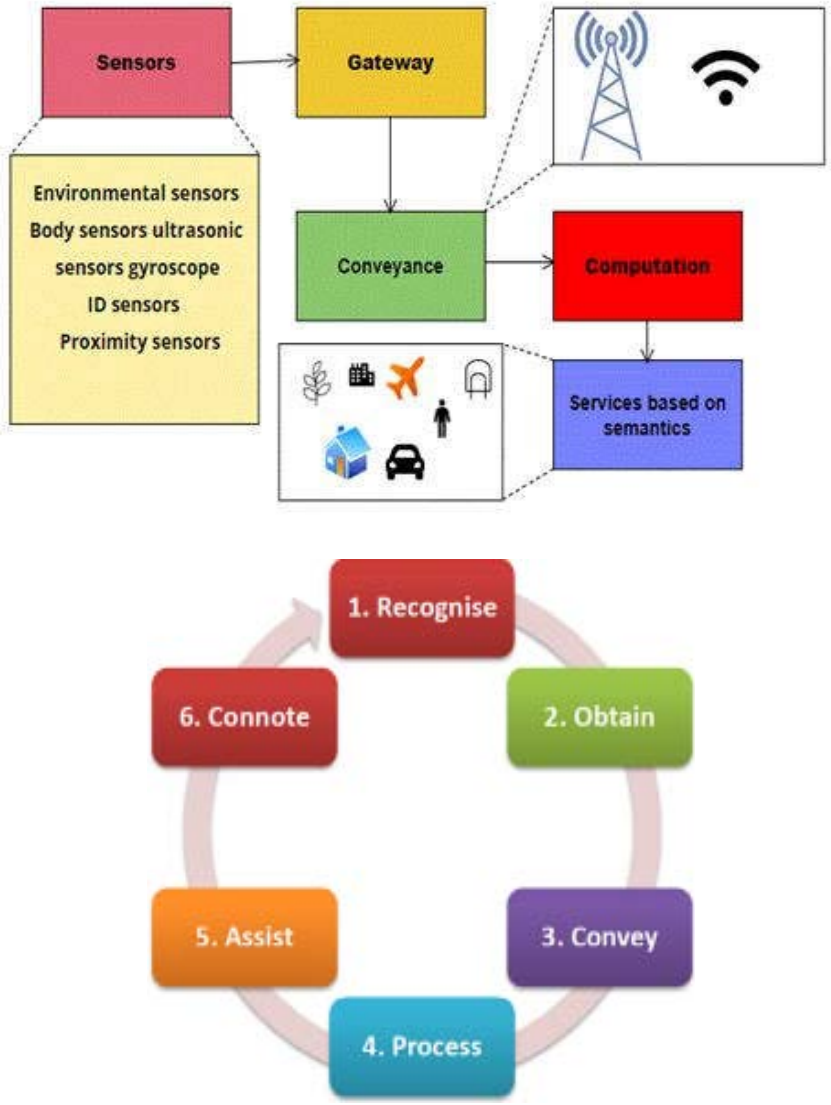
1) **Υπό επίπεδο διαχείρισης δεδομένων**: Περιλαμβάνει διεργασίες όπως cloud computing, Quality of Service (QoS), υπηρεσίες επεξεργασίας δεδομένων και καταλόγου, αλλά και υπηρεσίες από μηχανή σε μηχανή(M2M).
2) **Υπό-επίπεδο υπηρεσίας εφαρμογής**: Ενώ εκτελείται αυτό το υποεπίπεδο οι λειτουργίες μιας διασύνδεσης μεταξύ εφαρμογών και τελικών χρηστών βρίσκονται στο αμέσως ανώτερο επίπεδο από το Επίπεδο Εφαρμογής του Α.

1.1.5. Επιχειρησιακό Επίπεδο (Business Layer)

Αυτό το επίπεδο είναι υπεύθυνο για τη διαχείριση του συνολικού οικοσυστήματος IoT, συμπεριλαμβανομένων των εφαρμογών και των υπηρεσιών με βάση τα δεδομένα που λαμβάνονται από το Επίπεδο Εφαρμογής. Περιλαμβάνει επιχειρηματικά μοντέλα, γραφήματα, διαγράμματα ροής κλπ. Με βάση την ανάλυση των αποτελεσμάτων, το επίπεδο αυτό συμβάλλει στον προσδιορισμό των μελλοντικών ενεργειών και των στρατηγικών.

1.2. Δομικά Συστατικά Διαδικτύου των Πραγμάτων

Τα βασικά δομικά στοιχεία στο IoT μπορούν να ταξινομηθούν σε έξι φάσεις όπως η αναγνώριση, η ανίχνευση και συλλογή δεδομένων, οι τεχνολογίες επικοινωνιών και μετάδοσης, η υπολογιστική επεξεργασία, οι υπηρεσίες και η σημασιολογία [4].



Εικόνα 5. Δομικά συστατικά Διαδικτύου των Πραγμάτων [2]

1.2.1.Αναγνώριση (Identification) - Recognise

Όλα τα αντικείμενα που υπάρχουν σε ένα δίκτυο πρέπει να είναι μοναδικά αναγνωρισμένα. Κάτι τέτοιο σημαίνει ότι κάθε οντότητα θα πρέπει να έχει μη αναγνωριστική ταυτότητα. Αυτό μπορεί να επιτευχθεί χρησιμοποιώντας την έννοια της διεύθυνσης και της ονοματοδοσίας που είναι τα δύο μέρη της αναγνώρισης. Το θέμα είναι πως μπορεί να είναι ίδια τα ονόματα αλλά οι διευθύνσεις πάντα ενιαίες. Το έργο της κατανομής των δικτύων σε κάθε αντικείμενο γίνεται χρησιμοποιώντας διευθύνσεις Ip6 που υπάρχει το σχήμα αριθμού 128 bits και τα ονόματα μπορούν να δεχθούν χρησιμοποιώντας διάφορες μεθόδους όπως κώδικες και κωδικοί που βασίζονται σε IP και κωδικοί ηλεκτρονικών προϊόντων.

1.2.2.Ανίχνευση (Sensing) - Συλλογή Δεδομένων (Obtain)

Το IoT χρησιμοποιεί διάφορες συσκευές για ανίχνευση και συλλογή δεδομένων, όπως ετικέτες RFID, συσκευές με δυνατότητα φθοράς και ενεργοποιητές για να λάβει και να

συλλέξει δεδομένα από διαφορετικές συσκευές. Τα συγκεκριμένα δεδομένα κοινοποιούνται μέσω των πυλών στους χώρους αποθήκευσης όπως τα σύννεφα.

1.2.3. Επικοινωνία (Communication) - Μετάδοση (Conveyance)

Είναι ένας από τους σημαντικούς λόγους που αφορούν την ομαλή λειτουργία του IoT αναθέτοντας την ευθύνη της μεταφοράς πληροφοριών από το ένα σημείο στο άλλο. Όλα αυτά τα μηνύματα, οι συνομιλίες, τα αρχεία και τα άλλα δεδομένα μεταφέρονται μέσω αυτού του στοιχείου χρησιμοποιώντας ορισμένα πρωτόκολλα όπως ασύρματα πράσινα δίκτυα χαμηλής ισχύος, Zigbee κ.λπ.

1.2.4. Υπολογιστική (Computation) - Επεξεργασία Δεδομένων (Processing)

Αφού συλλέχθηκαν τα δεδομένα μέσω των αισθητήρων υποβάλλονται σε επεξεργασία χρησιμοποιώντας μία ποικιλία λειτουργικών συστημάτων στο μέτωπο του λογισμικού όπως Android, Tiny OS και διαφορετικές πλατφόρμες υλικού όπως το Arduino και το Intel Galileo.

1.2.5. Υπηρεσίες (Services) - Εξυπηρέτηση (Assistance)

Όταν αναφερόμαστε στην εξυπηρέτηση που προσφέρουν οι εφαρμογές IoT παρέχονται τέσσερις κύριοι τύποι:

1) Η πιο σπουδαία εξυπηρέτηση αφορά στον καθορισμό της ταυτότητας των δεδομένων.
2) Κατόπιν, η εξυπηρέτηση που σχετίζεται με τη συγκέντρωση των δεδομένων και πληροφοριών, η οποία μπορεί να εφαρμοστεί χωρίς τη χρήση οποιουδήποτε τύπου επικοινωνίας και μπορεί να ενσωματώνει διαφορετικές τεχνολογίες σε μία μόνο εφαρμογή.
3) Η επόμενη εξυπηρέτηση χρησιμοποιεί τα συγκεντρωμένα δεδομένα και τις πληροφορίες για την εκτέλεση των απαιτούμενων διεργασιών και τη λήψη αποφάσεων και δράσεων.
4) Η τελευταία εξυπηρέτηση αφορά τη διαρκή παροχή υπηρεσιών χωρίς περιορισμούς ως προς τη χρονικότητα και την τοποθεσία.

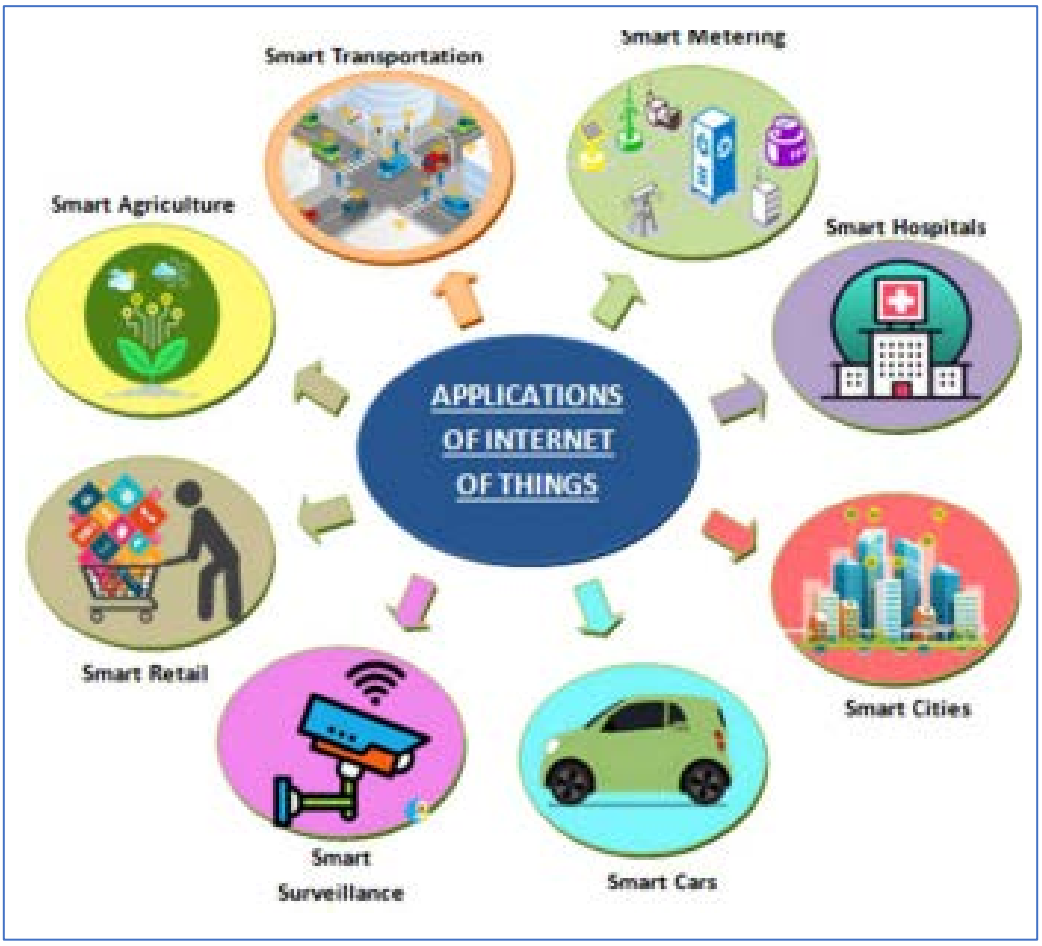
1.2.6. Νοηματοδοσία (Connotation) - Σημασιολογία (Semantics)

Τα πάντα εκπληρώνονται μέσα από αυτό το στοιχείο που λειτουργεί και στον εγκέφαλο του IoT. Οι συσκευές λαμβάνουν την ακριβή απάντηση επειδή οι αποκλειστικές αποφάσεις υπονοούνται εδώ.

1.3. Εφαρμογές IoT

Το IoT μπορεί να συλλέγει, να αποθηκεύει πληροφορίες που λαμβάνονται, από αντικείμενα εξοπλισμένα με ετικέτα ή αισθητήρα. Η τεχνολογία μπορεί να χρησιμοποιηθεί σε εφαρμογές όπως ο βιομηχανικός αυτοματισμός, η υγειονομική περίθαλψη, η μεταφορά και η αντιμετώπιση έκτακτης ανάγκης όπου ο άνθρωπος δεν δύναται να λάβει αποφάσεις. Μία από τις βασικότερες απαιτήσεις για κάθε εφαρμογή IoT είναι να εξασφαλίζει την επιτυχία στο περιβάλλον και να βεβαιωθεί ότι εφαρμόζονται οι κατάλληλοι μηχανισμοί ασφαλείας. Οι προοπτικές ασφαλείας περιλαμβάνουν κάποιες παραμέτρους που πρέπει να

διασφαλιστούν όπως η εμπιστευτικότητα, η ιδιωτικότητα, η ευρωστία, η αυθεντικότητα, η ακεραιότητα, η εξουσιοδότηση. Πολλές συσκευές και συσκευές IoT είναι ήδη πετυχημένες όταν είναι ενσωματωμένες και αναπτύσσονται σε διάφορες περιοχές από όλο τον κόσμο με πρόθεση τη διασφάλιση της ασφάλειας ως ένα βαθμό. Πολλές δημοφιλείς χρήσεις του Internet of Things αναφέρονται παρακάτω:



Εικόνα 6. Εφαρμογές Διαδικτύου των Πραγμάτων [2]

Παραδείγματα όπως η δικτύωση που καθορίζεται από λογισμικό (Software Defined Networking – SDN), η πληροφοριοκεντρική δικτύωση (InfoCentric Networking - ICN), η εικονικοποίηση λειτουργιών δικτύου (Network Function Virtualization - NFN), η επικοινωνία κοντινού πεδίου (Near-Field Communication - NFC) και το Wi-Fi επιταχύνουν τη χρήση της τεχνολογίας IoT. Επιπλέον, τα δίκτυα υπολογιστικής ομίχλης (Fog Computing) και τα εργαλεία ανάλυσης μεγάλου όγκου δεδομένων (Big-Data Analytics) διευκολύνουν στο να προσαρμοστεί αυτή η τεχνολογία με τα υφιστάμενα λειτουργικά δίκτυα. Το IoT μπορεί να συλλέξει δεδομένα από συσκευές και από το περιβάλλον για να ελέγχει τον κόσμο και παρέχεται για να υπάρξει ένας έξυπνος βιότοπος. Επομένως, λοιπόν εφαρμόζονται τα εργαλεία πρόβλεψης και βελτιστοποίησης σε πραγματικό χρόνο για την ανάλυση δεδομένων και την εξαγωγή γνώσεων απαραίτητο για την επίτευξη ενός αυτοματοποιημένου σύμπαντος είναι ο συμπληρωματικός στόχος του IoT.

1.3.1.Έξυπνες Μετρήσεις (Smart Metering)

Όλες οι εργασίες όπως η παρακολούθηση και η βελτιστοποίηση της ηλεκτρικής ενέργειας, του νερού και του αέρα χρησιμοποιούν ορισμένα gadget και αισθητήρες που μαζί με το Διαδίκτυο ανήκουν στη κατηγορία της έξυπνης μέτρησης. ΄Ενα από τα χαρακτηριστικά παραδείγματα αφορά τη παρακολούθηση εργοστασίου με ηλιακή ενέργεια που μπορούμε να συλλέξουμε στο έπακρο την ένεργεια του ήλιου τροποποιώντας τις γωνίες δυναμικά των ηλιακών συστημάτων.Σε σύγκριση με τους παραδοσιακούς μετρητές που μπορούν να επιτεθούν μόνο σωματικά, οι έξυπνοι μετρητές έχουν απευθείας σύνδεση στο διαδίκτυο, άρα είναι πιο επιρρεπείς σε επιθέσεις τόσο σε φυσικό χώρο όσο και σε κυβερνοχώρο. Μία από τις επιθέσεις είναι η σκόπιμη διείσδυση όπου ένας αντίπαλος έχει το δικαίωμα να συλλέγει και να τροποποιεί τα δεδομένα που συγκεντρώνονται μέσω του εξοπλισμού που έχει σχέση με τους έξυπνους μετρητές και μπορεί να οδηγήσει σε απώλειες και τους προμηθευτές αλλά και τους τελικούς χρήστες.
Οι έξυπνες μετρήσεις που αφορούν το νερό αποτελούνται από δύο κατηγορίες:

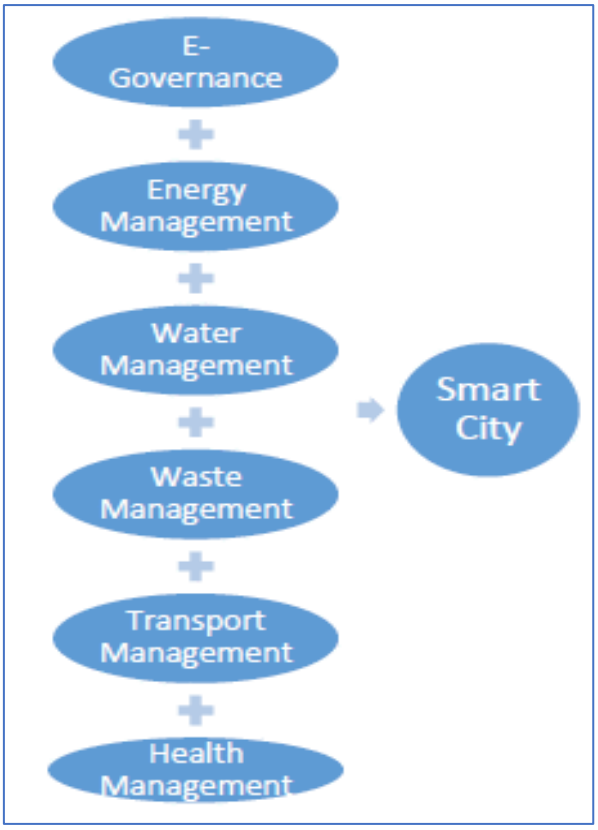
1) **Ανίχνευση και πρόληψη διαρροών**: Έχοντας τη χρήση υπέρηχων αισθητήρων αυτό βοηθά στο να μετράται η στάθμη της δεξαμενής του νερού. Ο αισθητήρας ροής επίσης βοηθά στο να μετράται ο όγκος που έχει το νερό στον σωλήνα με συνέπεια την ανίχνευση των διαρροών. Μέσα από τη χρήση αυτών των υπέρηχων ο αισθητήρας παίρνει πίσω τα σήματα του ήχου που μετρούν τη διαδρομή στο χρόνο που είναι απαραίτητο για να αποσταλούν και να ληφθούν τα σήματα.
2) **Έλεγχος ποιότητας νερού**: Ο αισθητήρας PH έχει τον ρόλο στο να μετρά τη τιμή του νερού. Αυτοί οι αισθητήρες στέλνουν τα δεδομένα ηλεκτρονικά στη πλατφόρμα IoT που έχει τη δυνατότητα να αλλάζει τα δεδομένα σε μορφή που θα είναι σαφή και κατανοητά για να αναλυθούν περαιτέρω. Με τον ίδιο τρόπο ο αισθητήρας θολότητας Arduino χρησιμοποιείται για να μετρά τα σωματίδια που αιωρούνται πάνω στο νερό. Όσο περισσότερα είναι τα σωματίδια τόσο μεγαλύτερη θα είναι η θολότητα. Οι αισθητήρες θολότητας χρησιμοποιούνται για να μετρηθεί η στάθμη του νερού σε ποτάμια, λίμνες, ρυάκια κ.λπ.

Οι έξυπνες μετρήσεις που αφορούν τη διαχείριση ενέργειας αποτελούνται από μετρητές ενέργειας που στέλνουν τα δεδομένα χρησιμοποιώντας τις τεχνολογίες IoT σε κεντρικό γραφείο. Τα δεδομένα οργανώνονται σε μία μορφή που θα μπορεί να παρουσιάζονται σε ειδικά άτομα για να αναλυθούν περαιτέρω.

Οι τεχνολογίες του IoT όπως Sigfox, RPMA, Ingenu, LoRa, κλπ., είναι αρμόδιες για τη δημιουργία μίας σύνδεσης μετρητών που θα αφορά τη συλλογή δεδομένων.

1.3.2.Έξυπνες πόλεις (Smart Cities)

Από το ίδιο το όνομα εξηγεί μία ολόκληρη πόλη που είναι έξυπνη. Αναφέρει με απλά λόγια το συμφέρον που παρέχεται στη ποιοτική ζωή σε όλους τους λαούς της πόλης, περιλαμβάνει τα στοιχεία που αφορούν μία πόλη, συμπεριλαμβανομένου των σχολείων, της κυκλοφορίας οχημάτων, τη διαχείριση νερού, των λυμάτων, της ισχύος, των σπιτιών, των δρόμων και τη διαχείριση των καταστροφών που λειτουργούν μέσω του Διαδικτύου.



Εικόνα 7. Παραδείγματα εφαρμογών IoT σε μια Έξυπνη Πόλη [5]

Η μεγαλύτερη απειλή σε ένα τέτοιο σενάριο είναι η ασφάλεια της προσωπικής ζωής των ανθρώπων που ζούνε σε αυτή τη πόλη και μπορούν να χρησιμοποιούν εφαρμογές για τα κινητά και τη παρακολούθηση στη τοποθεσία ενός ατόμου καθώς και των παιδιών, η πρόσβαση στις υπηρεσίες των έξυπνων καρτών σε στοιχεία της πιστωτικής κάρτας αλλά και των οικονομικών στοιχείων του ατόμου. Κάθε πληροφορία και κάθε στοιχείο πρέπει να λαμβάνεται μόνο επισκέπτοντας τα τμήματα. Το ίδιο ισχύει και όσον αφορά τις συναντήσεις σε γραφεία κυβερνητικών στελεχών.

Επιπλέον, είναι δύσκολο για κάποιον που έχει αναλάβει τη διαχείριση της πόλης και της παρακολούθησης όσον αφορά τη κυκλοφορία και την εγκληματικότητα χωρίς αυτές τις τεχνολογίες. Ακριβώς τα ίδια ισχύουν και για τους αρμόδιους ανθρώπους που έχουν αναλάβει τη λειτουργία του νερού, τον έλεγχο για την ποιότητα παροχής του, τη μετατροπή των απόβλητων σε ενέργεια και την επεξεργασία τους για να μπορέσουν να ξαναχρησιμοποιηθούν μέσα στην πόλη.

Οι παραπάνω λόγοι για το αυτόματο σύστημα υγείας θα βοηθήσουν σταδιακά στο να μειωθεί ο χρόνος. Με σκοπό να κάνουμε πιο εύκολη τη ζωή του κάθε πολίτη, ή του διαχειριστή, αυτές οι τεχνολογίες IoT μπορούν να αξιοποιούνται για να κάνουν μία πολύ έξυπνη σχετικά με την υγεία, τις μεταφορές, τη διαχείριση νερού, τη διαχείριση απορριμμάτων και την ηλεκτρονική διακυβέρνηση. Η ηλεκτρονική διακυβέρνηση περιλαμβάνει τρεις κατηγορίες:

1) **Δημόσια πληροφορία**: Το City Admiration έχει τη δυνατότητα να δίνει τη διαθέσιμη πληροφορία σε πύλη χρησιμοποιώντας τις πληροφορίες που εξαρτώνται από SMS. Οι άνθρωποι μίας πόλης μπορούν να αποκτήσουν τις συγκεκριμένες πληροφορίες

ηλεκτρονικά μέσα από τα κυβερνητικά γραφεία. Η οποιαδήποτε πρόβλεψη που γίνεται όσον αφορά το σεισμό, το νερό κ.λπ. αποτελείται από χρήση αισθητήρων που χρησιμοποιούν IoT που αφορά τη θερμοκρασία, τη πίεση, το σεισμό κ.λπ. Το ότι αυτές οι πληροφορίες είναι διαθέσιμες στο διαδίκτυο θα βοηθήσουν το πολίτη για να κερδίσει χρόνο και να προγραμματίσει καλύτερα τις επόμενες ανάλογες περιπτώσεις.

2) **Συμμετοχή του πολίτη**: Κάθε συνάντηση μεταξύ του κράτους και του πολίτη έχει τη δυνατότητα να γίνεται διαδικτυακά. Άρα λοιπόν, η φυσική επαφή μπορεί να μειωθεί πολύ σημαντικά. Συνεπώς για το περιβάλλον θα μειωθεί ο χρόνος που θα χρειάζονται οχήματα για τις μετακινήσεις.
3) **Παρακολούθηση του Εγκλήματος**: Θα έχει τη δυνατότητα ο διαχειριστής μίας πόλης να παρακολουθεί και να ελέγχει το έγκλημα μέσα από τους αισθητήρες ή τις συσκευές που χρησιμοποιούν IoT, οι οποίες τελικά θα στείλουν τις πληροφορίες στο κεντρικό γραφείο. Αυτό με τη σειρά του θα βοηθήσει στο να ληφθούν οι γρήγορες αποφάσεις για την αποφυγή του εγκλήματος.

1.3.3.Έξυπνη Υγειονομική Περίθαλψη (Smart Health – Smart Hospitals)

Οι τρεις βασικοί παράγοντες που απαιτούνται για να λειτουργεί πετυχημένα ένας τομέας υγειονομικής περίθαλψης είναι η διοίκηση του νοσοκομείου, τα κλινικά ευρήματα και η εργαστηριακή παρακολούθηση. Για να υπάρχει ένα έξυπνο τμήμα υγειονομικής περίθαλψης όλες οι προαναφερθείσες βασικές παράμετροι πρέπει να έχουν ενσωματωθεί με ενεργοποιητές, συσκευές και αισθητήρες με σκοπό να μπορούν να έχουν έξυπνη πρόσβαση μέσω του Διαδικτύου. Αυτό σημαίνει ότι είναι απαραίτητο να εξασφαλιστεί μία ενιαία επικοινωνία μεταξύ των στοιχειών του ασθενούς, του τρόπου που προχωρούν οι εργασίες των επιχειρηματικών διαδικασιών , των συνολικών συσκευών αλλά και των εξοπλισμών που χρησιμοποιούνται στην αποτελεσματικότητα των στοιχειών του ασθενούς και του γιατρού. Η διαχείριση της υγείας αποτελείται από δύο κατηγορίες

1) **Παρακολούθηση Προσωπικής Υγείας**: Η πλατφόρμα που εξαρτάται από το IoT είναι για να παρακολουθείται η προσωπική υγεία. Οι έξυπνες συσκευές χρησιμοποιούνται για να ανιχνευθεί ο καρδιακός παλμός, η θερμοκρασία του σώματος κ.λπ. Τα δεδομένα από αυτές τις συσκευές μπορούν να αξιοποιηθούν για να παρακολουθείται η υγεία χρησιμοποιώντας τις εφαρμογές που βασίζονται σε κινητά.
2) **Αυτοματοποιημένη Αποστολή Ιατρικών Δεδομένων**: Τα δεδομένα σε πραγματικό χρόνο που παράγονται με τη χρήση των έξυπνων συσκευών που αφορούν την υγεία όπως ο σφυγμός, ο καρδιακός ρυθμός, θερμοκρασία κ.λπ. Τα δεδομένα από αυτές τις συσκευές μπορούν να σταλούν μέσω των έξυπνων συσκευών στον εκάστοτε γιατρό που ενδιαφέρεται. Έχει τη δυνατότητα να αναλάβει τα δεδομένα και να προτείνει το κατάλληλο φάρμακο. Εφόσον επιλεχθεί το φάρμακο οι κατάλληλοι χημικοί που είναι συνδεδεμένοι στο δίκτυο θα στείλουν το φάρμακο άμεσα στο σπίτι των ασθενειών. Συνεπώς όλος ο αυτοματισμός που αφορά την επίλυση για προβλήματα υγείας και την εξέταση αλλά και την αποστολή των φαρμάκων μπορεί να γίνει αυτόματα.

1.3.4.Έξυπνα Οχήματα (Smart Cars)

Μπορεί τα αυτοκίνητα προς το παρόν να είναι εγκατεστημένα με GPS και με μέτρο που ελέγχει την επιτάχυνση, ωστόσο απαιτείται μία πιο ασφαλή και υψηλού επιπέδου υποδομή για τη συστηματική διαχείριση κυκλοφορίας και οχημάτων για το προσδιορισμό της ταχύτητας και τη θέση των αυτοκινήτων σε πραγματικό χρόνο. Θα μπορούσε μία τέτοια συνθήκη να συνδυαστεί με την υπάρχουσα τεχνολογία με το IoT γιατί όταν τα αυτοκίνητα εγκαθίστανται με gadget και λογισμικά IoT στη συνέχεια γίνονται πλήρως έξυπνα. Μερικά από τα κοινά χαρακτηριστικά που προσφέρονται είναι:

- Εγκατάσταση ενός τσιπ οχήματος που θα περιλαμβάνει πληροφορίες που αφορούν το όνομα του ιδιοκτήτη, τα στοιχεία επικοινωνίας, τα στοιχεία οικογένειας και βασικά δεδομένα για το ιατρικό του ιστορικό.
- Τακτικός έλεγχος και ενημέρωση λογισμικού.
- Εγκατάσταση αισθητήρων σύγκρουσης που θα ειδοποιούν το κοντινότερο νοσοκομείο και αστυνομικό τμήμα.
- Έλεγχος ορίου ταχύτητας στους δρόμους με την εγκατάσταση αισθητήρων ταχύτητας.

1.3.5.Έξυπνες Μεταφορές (IoT Transportation)

Η συνεργασία των οντοτήτων σε ένα σύστημα μεταφοράς όπως τα αντικείμενα και τα άτομα με το IoT έχουν οδηγήσει στο όφελος τους ολόκληρο το τμήμα με διάφορους τρόπους όπως:

- Βελτίωση και διατήρηση της ροής της κυκλοφορίας
- Αποφάσεις όπως τον καλύτερο χρόνο για ταξίδια, το επίδομα της καλύτερης διαδρομής επιλέγοντας τον κατάλληλο τρόπο επικοινωνίας που θα μπορεί να αποφασίζεται εύκολα από τους ταξιδιώτες.
- Ο ναύλος μπορεί να συλλεχθεί αυτόματα
- Οι αισθητήρες θα μπορούν να βοηθήσουν στον εντοπισμό των ατυχημάτων εκ των προτέρων.

Η διαχείριση μεταφοράς περιλαμβάνει τρεις κατηγορίες.

1) **Έξυπνος έλεγχος κυκλοφορίας**: Το Fasting με τη χρήση του RFID έχει στόχο την είσπραξη χρημάτων από τα διόδια μέσα από το Διαδίκτυο που φυσικά θα έχει ως συνέπεια το να μην υπάρχει κίνηση στους δρόμους αλλά και τη μείωση καυσίμων που ρυπαίνουν το περιβάλλον. Οι αισθητήρες που θα μπουν στα φανάρια θα βοηθήσουν στην ανάλογη λειτουργία του σήματος με κριτήριο την συγκέντρωση οχημάτων και ανάλογα με το πόσα υπάρχουν κάθε φορά θα τα στέλνουν σε έναν κεντρικό διαχειριστή που θα ελέγχει την παρακολούθηση της κυκλοφορίας.
2) **Έξυπνο παρκινγκ**: Θα υπάρχουν σε αυτή τη περίπτωση αισθητήρες εγγύτητας για να σταθμεύονται τα οχήματα χωρίς βοήθεια. Οι αισθητήρες που υπάρχουν θα εντοπίζουν το υλικό και τη κάμερα θα βλέπουν τις λεπτομέρειες κάθε πινακίδας. Οι συγκεκριμένες πληροφορίες θα βοηθούν στο αν μία θέση στάθμευσης για όχημα είναι διαθέσιμη ή πλήρης. Όσο για τη πόλη τα δεδομένα για τη στάθμευση θα χρησιμοποιούνται από εφαρμογές του χρήστη.

3) **Έξυπνη παρακολούθηση στόλου οχημάτων**: Η συγκεκριμένη κατηγορία γίνονται χρησιμοποιώντας λύσεις με δυνατότητα που περιλαμβάνει IoT. Αυτοί οι αισθητήρες εξαρτώνται από στοιχεία που στέλνουν πληροφορίες σε πραγματικό χρόνο για να παρακολουθούν τα στοιχεία σε πραγματικό χρόνο στα οχήματα.

1.3.6.Έξυπνα Συστήματα Επιτήρησης (IoT Surveillance)

Ξεκάθαρα το πιο συνηθισμένο εργαλείο ή αντικείμενο που χρησιμοποιείται για την εγγραφή και παρακολούθηση οποιουδήποτε είναι η τηλεόραση κλειστού κυκλώματος(CCTV).Η συγκεκριμένη χρησιμοποιεί τη δύναμη της παρατήρησης.

Όταν όμως αφορά τη σύζευξη του έργου της συλλογής πληροφοριών και της επεξεργασίας μέσω των διακομιστών και των cloud γίνεται μία πιο ακριβής επιτήρηση. Ο συνδυασμός κλειστού κυκλώματος με IoT μπορεί να λάβει βοήθεια με διάφορους τρόπους, όπως με αισθητήρες που θα είναι ενσωματωμένοι σε περιουσίες πολιτών για να χτυπά ο συναγερμός σε περίπτωση που υπάρχει μία απόπειρα κλοπής, η λήψη ειδοποίησης push για ύποπτες κινήσεις ή προειδοποίηση για την εξέλιξη της θερμοκρασίας ή της διαρροής αερίων.

1.3.7.Έξυπνο Λιανικό Εμπόριο (Smart Retail)

Εδώ και πολύ καιρό χρησιμοποιούν τα σημεία πώλησης τη δύναμη του IoT.Οι υπηρεσίες που έχουν εξελιχθεί με τη τεχνολογία περιλαμβάνουν κατανόηση και δράση στη συμπεριφορικές δραστηριότητες όπως οι ανάγκες, οι συνήθειες και οι προτιμήσεις των καταναλωτών στα έξυπνα προϊόντα.

1.3.8.Έξυπνη Γεωργία (Smart Agriculture)

Κάποιες από τις δουλειές που σχετίζονται με τη γεωργία περιλαμβάνουν κατανόηση των συνθηκών θερμοκρασίας και υγρασίας αλλά και υγρασίας στο έδαφος. Αυτές οι καταστάσεις μπορούν να αντιμετωπιστούν έξυπνα και μόνο με την ενσωμάτωση αισθητήρων και συσκευών στη γεωγραφική σφαίρα μαζί με την αποφυγή πάντα οικονομικών ελλειμμάτων. Ταυτόχρονα αρκετές καλλιέργειες δεν τυγχάνουν τον κίνδυνο της μόλυνσης, είτε από μικρόβιο, είτε από μύκητες. Επιπλέον η ενσωμάτωση αισθητήρων στη ζωή μπορεί να βοηθήσει τη διασφάλιση της υγείας τους σε μεγάλο βαθμό.

1.3.9.Έξυπνα Σπίτια (IoT IoT)

Ο στόχος τους είναι για να αυξάνουν την ποιότητα της ζωής των ανθρώπων. Αυτός ο τομέας ενώνει διάφορους τομείς όπως ο οικιακός αυτοματισμός, η παρακολούθηση στη ποιότητα του αέρα, η υγειονομική περίθαλψη, η επιτήρηση και η έξυπνη κηπουρική:

- **Οικιακός αυτοματισμός**: Σε αυτή την περίπτωση επιτρέπει στους κατοίκους να παρακολουθούν από μακρινή απόσταση τις οικιακές τους συσκευές, όπως smartphone,προσωπικούς υπολογιστές, ψυγεία, πλυντήρια ρούχων, κλιματιστικά κ.λπ.
- **Παρακολούθηση της ποιότητας του αέρα σε εσωτερικό χώρο**: Εφόσον υπάρχουν άνθρωποι που αφιερώνουν τον πιο πολύ χρόνο της ημέρας τους στο σπίτι ή στο γραφείο είναι σημαντικό να παρακολουθείται η ποιότητα του αέρα. Ο εσωτερικός αέρας είναι πιο βλαβερός από τον εξωτερικό αέρα. Με βάση μία έρευνα που έγινε

όταν χρησιμοποιούμε καπνό στα σπίτια και απορρυπαντικά αυξάνεται το διοξείδιο του άνθρακα(CO2), το μονοξείδιο(NO) και το διοξείδιο του αζώτου(NO2). Οι επιστήμονες έχουν προσέξει ότι τα παιδιά επηρεάζονται πολύ στη ψυχική τους διάθεση λόγω αυτών των χημικών ουσιών. Επομένως το IoT μας κάνει πιο εύκολη τη ζωή με παρακολούθηση της ποιότητας του αέρα, ειδοποιώντας τους κατοίκους.

- **Έξυπνη κηπουρική**: Οι περισσότεροι άνθρωποι λόγω των πολλών υποχρεώσεων τους αδυνατούν να φροντίσουν όσοι έχουν τον δικό τους κήπο που φτιάχνει τη ψυχική υγεία των κατοίκων της γειτονιάς και βελτιώνει τη ποιότητα του αέρα πρωτίστως γύρω από το σπίτι που βρίσκεται. Η χρήση του IoT σε αυτή τη κατηγορία δίνει στον άνθρωπο τη δυνατότητα να παρακολουθεί τα φυτά και να προσφέρει τροφή και νερό κάθε φορά που χρειάζεται από απόσταση.
- **Σύστημα Επιτήρησης**: Τα συστήματα επιτήρησης που υποστηρίζει το IoT έχουν σκοπό να παρέχουν το αίσθημα της ασφάλειας στους ανθρώπους που μένουν στα έξυπνα σπίτια. Από τη στιγμή που βάλαμε αισθητήρες για να βελτιώσουμε τις τεχνικές της όρασης των ανθρώπων και των υπολογιστών η τεχνολογία IoT βρίσκει τις ανωμαλίες και τους εισβολείς οι οποίοι δίνουν τις ειδοποιήσεις αμέσως στους κατοίκους της εκάστοτε περιοχής.
- **Παρακολούθηση Ηλικιωμένων**: Με βάση έρευνα που έγινε ο πληθυσμός των ηλικιωμένων αναμένεται να αυξηθεί κατά 16,7% το έτος 2050. Αυτοί οι άνθρωποι έχουν προβλήματα υγείας όπως η αρτηριακή πίεση, ο διαβήτης, οι καρδιακές παθήσεις και ο καρκίνος. Με την εξέλιξη των βιοχαρτικών αισθητήρων το IoT έχει τη δυνατότητα να παρακολουθεί την υγεία των συγκεκριμένων ευπαθών ομάδων από απόσταση. Το αποτέλεσμα αυτό θα ήταν να ανέβει ο μέσος προσδόκιμος όρος ζωής.

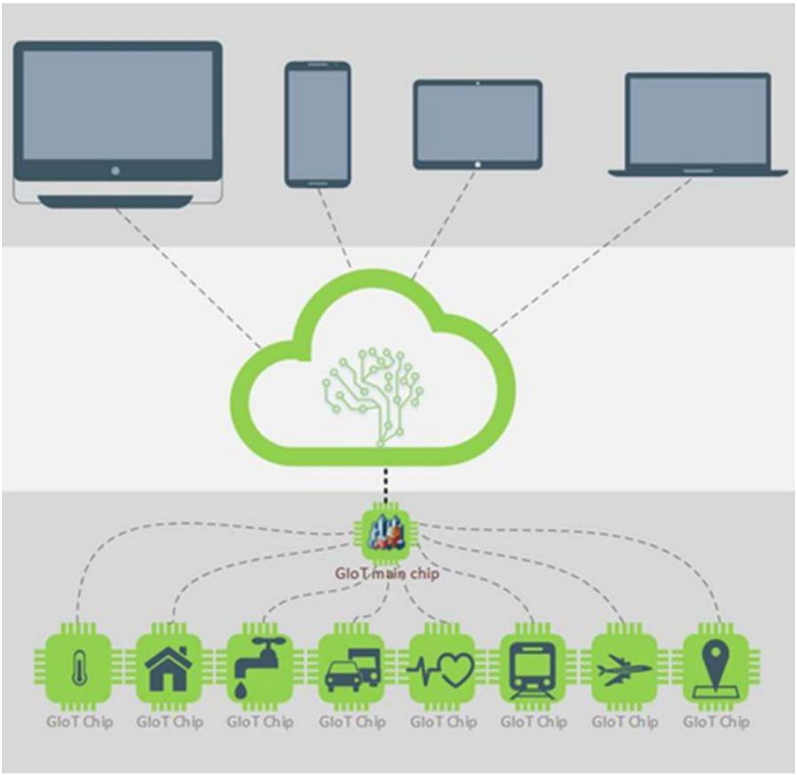
Για να αναλυθεί το βίντεο σε πραγματικό χρόνο που αφορά τους ηλικιωμένους πρέπει να υπάρχει η εγκυρότητα των στοιχείων τους για να μπορέσουν να τακτοποιηθούν πολλά θέματα όπως ο τρόπος που περπατούν, η έκφραση του προσώπου, ο κύκλος του ύπνου κ.λπ.

Ταυτόχρονα είναι βασικό να βελτιώσουμε και τις τεχνικές που αξιολογούν την υγεία των συγκεκριμένων ανθρώπων. Εφόσον, έχουν ένα έξυπνο σπίτι αυτό περιλαμβάνει διάφορους αισθητήρες και ενεργοποιητές όπως για παράδειγμα το Alexi, το Fitbit, τα ασύρματα ηχεία, η βοήθεια μέσω του Google, οι φορητοί υπολογιστές κ.λπ. Οι πιο πολλές από τις συσκευές είναι φορητές και έχουν τη δυνατότητα να αξιοποιούνται για να παρακολουθούνται για πολύ καιρό. Άρα λοιπόν οι αλγόριθμοι της επικοινωνίας και του υπολογιστή πρέπει να είναι ενεργά αποδοτικοί. Οι συσκευές που υπάρχουν στα έξυπνα σπίτια είναι πάρα πολλές στον αριθμό και σε μεγάλο βαθμό ανομοιόμορφες. Το να διατηρείται η διαλειτουργικότητα μεταξύ τους αποτελεί σημαντικό κριτήριο αλλά και η παρακολούθηση των συγκεκριμένων συσκευών και ο χειρισμός των δεδομένων που δημιουργούνται από αυτές είναι ακόμη και σήμερα η μεγαλύτερη πρόκληση.

2. Πράσινο Διαδίκτυο των Πραγμάτων (Green Internet of Things)

Το πράσινο Διαδίκτυο των Πραγμάτων (Green Internet of Things – GIoT) είναι ένα ενεργειακά αποδοτικό IoT που επιδιώκει να δημιουργήσει μία σύνδεση μεταξύ οποιουδήποτε, οποτεδήποτε και οπουδήποτε με κύριο χαρακτηριστικό ότι οι ενεργειακές του απαιτήσεις πρέπει να έχουν προτεραιότητα. Το πράσινο Διαδίκτυο των Πραγμάτων σχετίζεται με τη χρήση έξυπνων συσκευών ανανεώσιμων πηγών ενέργειας, κτιρίων κ.λπ. Χρησιμοποιούνται αισθητήρες για τη λήψη ζωντανών δεδομένων από το περιβάλλον και γίνεται επεξεργασία σε αυτά. Ανάλογα με αυτά λαμβάνονται αποφάσεις και εφαρμόζεται αποτελεσματική χρήση της ενέργειας. Άρα, συνολικά αποτελείται από ανανεώσιμες πηγές ενέργειας, αισθητήρες, μικροελεγκτές, ελεγχόμενες έξυπνες συσκευές, υπολογιστικά νέφη, κ.λπ. Το Green IoT είναι μία εντυπωσιακή τεχνολογία διότι τα στοιχεία του είναι αναγνωρίσιμα, έξυπνα και αυτόνομα που μοιράζονται τα δεδομένα τους με άλλους και έχουν πρόσβαση σε δεδομένα άλλων πραγμάτων. Τα δεδομένα του Green IoT συλλέγονται από ενεργειακά αποδοτικά αντικείμενα και αισθητήρες που είναι ενσωματωμένα σε συσκευές. Επομένως είναι απαραίτητο να χρησιμοποιούμε κατάλληλους αισθητήρες για να βελτιώσουμε τη διάρκεια ζωής των συσκευών και να πετύχουμε την απαραίτητη μείωση ως προς την κατανάλωση ενέργειας.

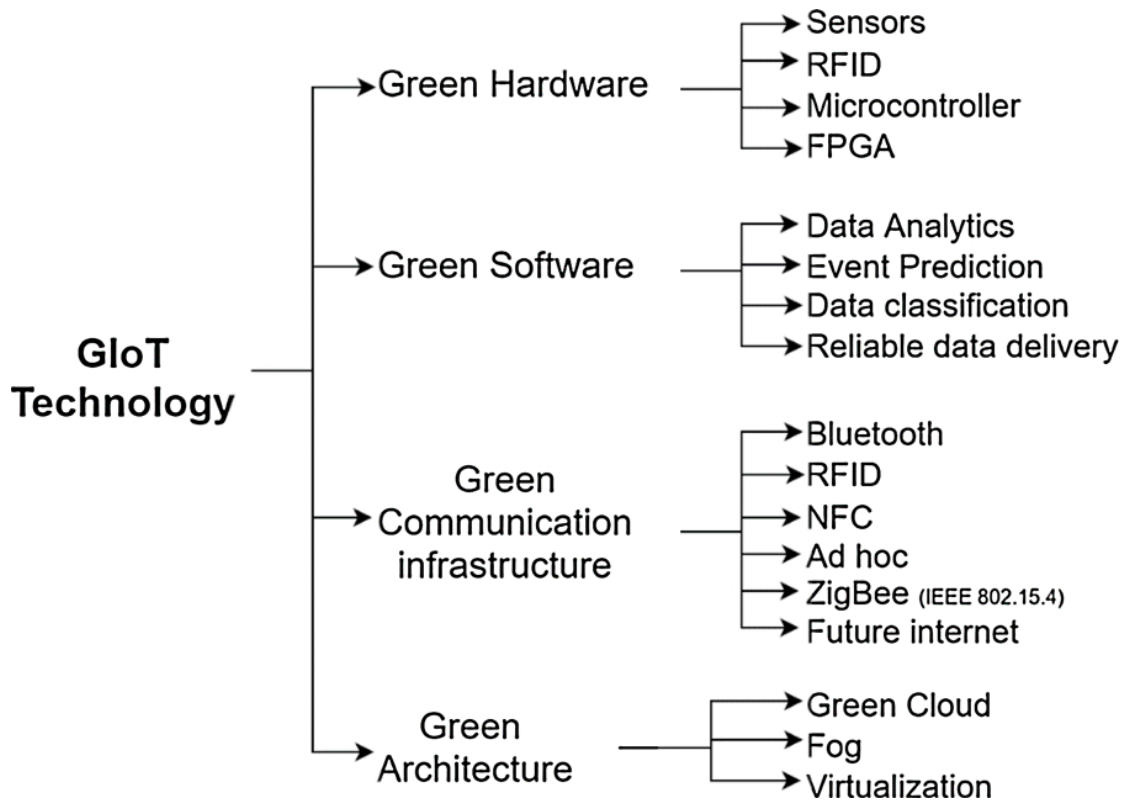
Ωστόσο, πρέπει να επισημανθεί ότι εξακολουθούν να υπάρχουν αρκετές προκλήσεις και προβλήματα στην καθιέρωση ενός πράσινου έξυπνου δικτύου. Συνεπώς, όταν ξεπεραστούν αυτές οι προκλήσεις της τεχνολογίας, η διαχείριση της ενέργειας, οι μεταφορές, οι πόλεις και η παρακολούθηση της υγείας θα γίνουν πιο έξυπνα. Για να επιτευχθεί η πράσινη τεχνολογία η ενεργειακή απόδοση πρέπει να είναι ενσωματωμένη με όλα τα επίπεδα IoT.



Εικόνα 8. Σχηματική αναπαράσταση των τεχνολογιών του Πράσινου Διαδικτύου των Πραγμάτων [6]

2.1 Δομικά Στοιχεία του Πράσινου Διαδικτύου των Πραγμάτων

Για να επιτευχθεί ένα Πράσινο Διαδίκτυο των Πραγμάτων αντιμετωπίζουμε τις βασικές απαιτήσεις σε τέσσερα δομικά στοιχεία του, δηλαδή στο πράσινο υλικό, στο πράσινο λογισμικό, στην πράσινη επικοινωνία και στην πράσινη αρχιτεκτονική.



Εικόνα 9. Δομικά Στοιχεία Πράσινου Διαδικτύου των Πραγμάτων [6]

2.1.1 Πράσινο Υλικό (Green Hardware)

Χωρίς αμφιβολία, τα στοιχεία υλικού (συσκευές αισθητήρων και τα φυσικά αντικείμενα) παίζουν σημαντικό ρόλο την επίτευξη της τεχνολογίας Green IoT. Δεδομένου ότι τα στοιχεία υλικού καταναλώνουν ένα σημαντικό ποσοστό της ενέργειας του δικτύου, δίνοντας προσοχή στην ενεργειακή αποδοτικότητα κατά το σχεδιασμό και την κατασκευή των συσκευών αισθητήρων και των φυσικών αντικειμένων με αβλαβή και φιλικά προς το περιβάλλον υλικά, καθώς και στη χρήση ανανεώσιμων πηγών ενέργειας, συμβάλλουμε στην επίτευξη ενός συστήματος Green IoT, όπου η χρήση του θα ελαχιστοποιεί τον αντίκτυπό του στο περιβάλλον.

Αν θεωρήσουμε ως δεδομένο ότι οι συσκευές αισθητήρων και τα φυσικά αντικείμενα διασυνδέονται μέσω των ασύρματων καναλιών, ο βέλτιστος σχεδιασμός της κεραίας σύμφωνα με τα πράσινα πρότυπα αποτελεί βασική απαίτηση για την επίτευξη του Green IoT. Το επιστημονικό άρθρο Guerchouce έχει προτείνει πως η κεραία με βάση το αγωγικό πολυμερές είναι για εφαρμογές ασύρματων πράσινων αισθητήρων. Ισχυρίζεται ότι η σχεδιασμένη ακτίνα κεραίας είναι στα 75 cm που είναι κατάλληλη για την παρακολούθηση και τον εντοπισμό συμβάντων. Αυτή η κεραία μπορεί να χρησιμοποιηθεί ως σημεία πρόσβασης Wi-Fi σε γυάλινα παράθυρα, πάνελ σπιτιών και γραφεία. Οι διαφανείς και

ανακυκλώσιμοι αισθητήρες μπορούν να χρησιμοποιηθούν ευρέως σε πράσινες ασύρματες εφαρμογές και σε Green IoT. Να επισημανθεί ότι το Green IoT είναι συνήθως εγκατεστημένο με μεγάλο αριθμό στοιχείων υλικού που εξοικονομεί σημαντική ενέργεια απενεργοποιώντας περιττά στοιχεία. Ωστόσο η διαρροή της ισχύς εξακολουθεί να υπάρχει αν και υπάρχουν ορισμένα στοιχεία που είναι απενεργοποιημένα. Το ρεύμα διαρροής έχει ανεπιθύμητη επίδραση στο χρόνο λειτουργίας της μπαταρίας. Κατά συνέπεια είναι ένας σημαντικός παράγοντας για κατασκευαστές φορητών συσκευών και παρόχους Green IoT. Ωστόσο, το να βελτιωθεί ο σχεδιασμός των περιττών στοιχείων υλικού και η απενεργοποίηση είναι μια απαίτηση για Green IoT που ελαχιστοποιεί το πρόβλημα της διαρροής ρεύματος. Ένας καινούριος επεξεργαστής που θεωρείται διπύρηνος ενεργειακά αποδοτικός ετερογενής για το IoT εισήχθη από το επιστημονικό άρθρο Wany et al. στον οποίο ένας ενεργειακά αποδοτικός πυρήνας L είναι κοντά στο κατώφλι και ο κανονικός υψηλής απόδοσης τάσης H είναι ενσωματωμένοι δημιουργώντας έναν πυρήνα LH. Αυτός ο πυρήνας είναι μία σωστή επιλογή για εφαρμογές Green IoT με σκοπό ο πυρήνας L να είναι κατάλληλος για ελαφριές διαδικασίες και ο πυρήνας H για βαριές διαδικασίες που θα πρέπει να ολοκληρώνονται άμεσα. Σύμφωνα με τους συγγραφείς αυτό αποτυπώνεται από τα αποτελέσματα της σύγκρισης των διπύρηνων επεξεργαστών με σχέδια τομέων εναντίον ισχύων με την αρχιτεκτονική να μπορεί να πετύχει τη μέγιστη ενεργειακή απόδοση.

Το επιστημονικό άρθρο Muzaffar έχει προτείνει μία πλατφόρμα Prototype Iot(PIoT) ως FPGA υλικό που είναι εξαιρετικά χαμηλής ισχύος και είναι η κατάλληλη επιλογή για αισθητήρες Green IoT. Όπως φαίνεται στην παρακάτω εικόνα η πλατφόρμα περιλαμβάνει πυρήνες μικροελεγκτή MSP430 με εξαιρετικά χαμηλή ισχύ οι οποίοι λειτουργούν ως κόμβοι αισθητήρων και Pulsh-Index Communication(PIC) δηλαδή ως ενιαίο πρωτόκολλο επικοινωνίας. Λόγω του ότι το PIC δεν απαιτεί ανάκτηση CDR (Clock and Data) σπαταλά πιο λίγη ενέργεια και μπορεί να αποτελέσει μία κατάλληλη πλατφόρμα για Green IoT. Επιπρόσθετα μία καινούρια μέθοδος έχει χρησιμοποιηθεί στη συγκεκριμένη κωδικοποίηση της πλατφόρμας η οποία έχει βέβαιη αποκωδικοποίηση χωρίς σφάλματα και διατηρεί υψηλούς ρυθμούς δεδομένων ακόμη και αν τα ρολόγια πομπού και δέκτη είναι ασύγχρονα. Σύμφωνα με τους συγγραφείς αυτή η πλατφόρμα είναι επεκτάσιμη και απαιτεί λίγους πόρους ανά κόμβο. Με ίδιο τρόπο χρησιμοποιηθεί μια μονάδα ελέγχου πολλαπλών πυρήνων εντοπισμού σφαλμάτων και ένας παράλληλος εντοπισμός σφαλμάτων πολλαπλών κόμβων και αισθητήρων. Το PIoT επιταχύνει αναδιαμόρφωση δικτύου που θεωρείται αποτελεσματικός τρόπος για να μειώσει την κατανάλωση ενέργειας σε συσκευές Green IoT.

Σε γενικές γραμμές οι κόμβοι ενός δικτύου περιορισμένου πόρου προσπαθούν να κερδίσουν ενέργεια εναλλάσσοντας ύπνο και ενεργείς λειτουργίες και διαφοροποιώντας τις λειτουργίες της κατάστασης. Ο Chung Nguygen έχει αξιολογήσει τον αντίκτυπο του χρόνου ύπνου σε πιο λειτουργικές ιδιότητες εφαρμογών για το IoT. Στην προσομοίωση της συγκεκριμένης προσέγγισης οι κόμβοι θα έπρεπε να αλλάξουν μεταξύ λειτουργίας ύπνου και ενεργής λειτουργίας σε προκαθορισμένο χρονικό διάστημα[0-60]. Σε 12 διαφορετικές περιπτώσεις οι συγγραφείς απέδειξαν ότι αυτή η νοοτροπία μπορεί να επεκτείνει τη διάρκεια ζωής των αισθητήρων. Έτσι λοιπόν, αυτή η ενεργειακή αποδοτική νοοτροπία μπορεί να εφαρμοστεί στη λειτουργία των στοιχείων Green IoT. Το Green SoC είναι ένα άλλο κατάλληλο υλικό για Green IoT που έχει αναπτυχθεί από το επιστημονικό άρθρο

Bolletul. Το πράσινο SoC έχει κατασκευαστεί με χρήση νανομέτρων υψηλής πυκνότητας σε συνδυασμό με την εξαιρετικά χαμηλή τάση Ultra-Low Voltage (ULV)(0,3-0,5 V) CMOS που έχει χαμηλή μέση ισχύ και βολική απόδοση ταχύτητας στο καθεστώς σχεδόν του κατωφλίου. Ένα αποτελεσματικό ULV SoC μπορεί να επιτευχθεί ξεπερνώντας πολλές προκλήσεις όπως η υψηλή ισχύς αναμονής δηλαδή να αποδίδεται σε ρεύματα διαρροής και στη μεγάλη ζώνη προστασίας του χρόνου κύκλου που ικανοποιεί τη λειτουργία χαμηλής θερμοκρασίας. Συνεπώς αυτό το υλικό λόγω των ξεχωριστών πλεονεκτημάτων του όπως το μικρό μέγεθος, η υψηλή συχνότητα και η χαμηλή κατανάλωση ενέργειας είναι η βέλτιστη πλατφόρμα για το Green IoT. Σε μία άλλη μελέτη το επιστημονικό άρθρο Xue et al. έχει προτείνει ιεραρχικό Network-on-Chip(NoC) μία αρχιτεκτονική για να βελτιώσει την απόδοση του συστήματος της μεγάλης κλίμακας (ex-scale) όσον αφορά την επεξεργασία δεδομένων. Αυτή η αρχιτεκτονική χρησιμοποιεί δίκτυο που είναι συνεργαζόμενο σε χρήστες με έννοιες κωδικοποίησης(NC) και βασίζεται σε ένα ελαφρύ υποδίκτυο δρομολογητών της μονάδας συνεργασίας(CUR) για κυκλοφορία πολλαπλών εκπομπών. Σύμφωνα με τα ιδιαίτερα χαρακτηριστικά αυτής της πλατφόρμας όπως η χαμηλή καθυστέρηση, η ελάχιστη επιβάρυνση και η υψηλή απόδοση μπορούν να θεωρηθούν κατάλληλα υλικά για το Green IoT. Ο Bogdan έχει προτείνει μία σύνθετη δυναμική προσέγγιση μοντελοποίησης που αποτυπώνει το ότι παρατηρήθηκαν χαρακτηριστικά πολλαπλών κλασμάτων του χρόνου μεταξύ συμβάντων και των διαδοχικών μεταβολών του φόρτου εργασίας και του μεγέθους των αυξήσεων σε φορτία εργασίας Data-Center-on-Chip(DCoC). Το συγκεκριμένο μαθηματικό πλαίσιο μπορεί να εφαρμοστεί για την μοντελοποίηση και την ανάλυση της τοπολογίας, της αναδιοργάνωσης του μεγέθους buffer, της χαρτογράφησης, του προγραμματισμού, της διαχείρισης πόρων και του ελέγχου συμφόρησης των πλατφόρμων Green IoT.

Η ενεργειακή συγκομιδή (Energy Harvesting-EH) είναι ένας άλλος χρήσιμος τρόπος για να επιτευχθεί ένα ενεργειακά αποδοτικό σύστημα. Αναφέρεται στην εξαγωγή ενέργειας από το περιβάλλον όπως η κινητική ενέργεια, οι μηχανικές δονήσεις και οι άνεμοι, η ηλιακή ενέργεια που αποτελείται από φωτοβολταϊκά PV η συμπυκνωμένη ηλιακή ενέργεια CSP και η ασύρματη μετάδοση ενέργειας. Η εξαγόμενη ενέργεια μπορεί εύκολα να μετατρέπεται σε ηλεκτρικό ρεύμα και να φορτίζει τις μπαταρίες των κόμβων ακόμα και αν είναι σε λειτουργία. Αυτή η τεχνική είναι ένας κατάλληλος μηχανισμός για δίκτυα περιορισμένης ενέργειας όπως τα ασύρματα δίκτυα αισθητήρων (WSN) και του πράσινου IoT λόγω της αύξησης της διάρκειας ζωής του δικτύου. Θα πρέπει να αναφερθεί ότι η αποτελεσματικότητα των μηχανισμών EH με βάση τον ήλιο και τον άνεμο εξαρτώνται εξολοκλήρου από τον καιρό, την εποχή, τη γεωγραφική θέση, την ημέρα και από τον κύκλο της νύχτας. Ωστόσο, οι τεχνολογίες EH που βασίζονται σε τραντάγματα είναι πιο αποτελεσματικές λόγω του ότι εμφανίζουν άγνοια με τα αναφερόμενα ζητήματα. Στο συγκεκριμένο μηχανισμό οι επιδράσεις των πιεζοηλεκτρικών, ηλεκτρομαγνητικών και ηλεκτροστατικών φαινομένων χρησιμοποιούνται για τη μετατροπή της μηχανικής ενέργειας σε ηλεκτρική. Οι μεταφορικές υποδομές όπως αυτοκίνητα και τρένα, οι οικιακές εφαρμογές, συμπεριλαμβανομένου των πλυντηρίων ρούχων και των κατασκευών όπως π.χ κτήρια, γέφυρες και ανθρώπινες κινήσεις μπορούν να θεωρηθούν ως πηγές των μηχανικών τρανταγμάτων. Από την άλλη πλευρά οι κινητικές πηγές μπορούν πιθανόν να παρέχουν απεριόριστη ισχύ με την πάροδο του χρόνου. Ωστόσο, η παραγόμενη ενέργεια της

ποσότητας από αυτές τις πηγές είναι περιορισμένη σε μία δεδομένη στιγμή καθώς και η ποσότητα που παράγεται η ισχύς εξαρτάται από την ποσότητα της κινητικής ενέργειας, την απόδοση της γεννήτριας και τον εξοπλισμό της μεταφοράς ισχύος. Σαν τελικό αποτέλεσμα είναι απαραίτητο για την ανάπτυξη ενός αποτελεσματικού ΕΗ για το Green IoT εξετάζοντας τις προκλήσεις από διάφορους μηχανισμούς ΕΗ.

2.1.2 Πράσινο Λογισμικό (Green Software)

Πέρα από το σχεδιασμό του βέλτιστου υλικού και την κατασκευή του από ανανεώσιμα υλικά, εφαρμόζοντας τεχνική ΕΗ για υλικό Green IoT, το λογισμικό Green IoT παίζει επίσης κρίσιμο ρόλο στην επίτευξη των πράσινων επικοινωνιών. Οι λειτουργίες του Green IoT όπως η ανάλυση δεδομένων, τα δεδομένα που ταξινομούνται και η πρόβλεψη συμβάντων που συνήθως εκτελείται από λογισμικό είναι απαραίτητα για κατάλληλη αντίδραση. Επομένως, είναι σημαντικό να δοθεί προσοχή στο πόση ενέργεια καταναλώνεται από το πράσινο λογισμικό από λογισμικό του Green IoT. Επιπλέον με τον σχεδιασμό ενός αξιόπιστου λογισμικού αποτρέπεται η επανάληψη των διαδικασιών και μειώνεται επίσης η κατανάλωση ενέργειας.

2.1.2.1 Ανάλυση δεδομένων

Εξαιτίας του ότι υπάρχει μεγάλος αριθμός αντικειμένων και μεγάλος χρόνος τη στιγμή που γίνεται η δραστηριότητα τους παράγονται τεράστια δεδομένα από το Green IoT που ονομάζονται μεγάλα δεδομένα. Με λίγα λόγια τα μεγάλα δεδομένα είναι μεγάλα και πολύπλοκα σύνολα δεδομένων τα οποία είναι παραδοσιακά λογισμικά τα οποία δεν μπορούμε να επεξεργαστούμε. Στις περισσότερες εφαρμογές Green IoT όπως οι έξυπνες πόλεις, η παρακολούθηση της υγείας απαιτούνται διάφορες οθόνες για τις καταστάσεις περιβάλλοντος όπως η θερμοκρασία, ο καπνός για ανίχνευση πυρκαγιάς, η κατανάλωση ενέργειας και νερού και οι κάμερες για τον έλεγχο των δραστηριοτήτων των ανθρώπων και στην έλεγχο της κυκλοφορίας. Τα δεδομένα που δημιουργούνται πρέπει να αναλυθούν και να αποσπαστούν οι γνώσεις που είναι απαραίτητες για την κατάλληλη αντίδραση σε περιπτώσεις έκτακτης ανάγκης. Για παράδειγμα η εξαγόμενη γνώση μπορεί να χρησιμοποιηθεί για να διαχειριστούν δημόσιοι πόροι όπως το νερό, το φυσικό αέριο και η ενέργεια. Άρα με την υψηλή απόδοση της εξαγόμενης γνώσης έχουμε αποτελεσματικές και αξιόπιστες διαχείρισης πόρων. Για να χρησιμοποιηθεί το Green IoT για έξυπνες σταθμεύσεις με σκοπό αυτό το σύστημα να ελέγχει τις ελεύθερες και κενές θέσεις για τη στάθμευση και να ενημερώνει για το ποιες είναι οι πιθανές στα οχήματα. Με αυτό τον τρόπο απαιτείται επεξεργασία σε πραγματικό χρόνο για να επιτευχθεί γρήγορη πλοήγηση και να προταθεί το πλησιέστερο πάρκο στη κενή θέση. Κατά συνέπεια η αποτελεσματική ανάλυση δεδομένων μειώνει τα περιττά ταξίδια εντός πόλης και αποτρέπει τη σπατάλη χρόνου των οδηγών. Σε εφαρμογές που το Green IoT χρησιμοποιείται για συστήματα παρακολούθησης του κλίματος αναλύονται διάφορες παράμετροι όπως η θερμοκρασία, η υγρασία, το χιόνι, η βροχή, η ταχύτητα ανέμου και η πίεση σχετικά με τη πρόβλεψη στο να μειωθούν οι ζημιές που προκλήθηκαν από τις φυσικές καταστροφές όπως οι πλημμύρες, οι καταιγίδες στην ανάλυση ρόλου έχουν κρίσιμη σημασία. Γίνεται προφανές πως η ακρίβεια στην ταχύτητα ανάλυσης των μεγάλων δεδομένων επηρεάζει τις αποφάσεις με το λογισμικό να έχει συμβάλλει σημαντικά στην απόδοση του Green IoT. Άρα λοιπόν η

διαχείριση στο να καταναλωθεί η ενέργεια και στην ανάλυση δεδομένων είναι απαραίτητα για την επίτευξη του Green IoT.

2.1.2.2 Πρόβλεψη γεγονότος

Στο Green IoT τα αντικείμενα είναι υπεύθυνα για την παρακολούθηση του περιβάλλοντος του εντοπισμού των συμβάντων αλλά και τη καταγραφή στη βάση δεδομένων συμβάντων. Το ίδιο ισχύει και για ένα άλλο αντικείμενο που μπορεί να εντοπίσει ένα άλλο συμβάν και η ειδοποίηση άλλων αντικειμένων γίνεται μέσω του πρωτοκόλλου M2M. Τα ηχογραφημένα γεγονότα θα πρέπει να ταξινομούνται σύμφωνα με τα πρότυπα πρόβλεψης. Από ιστορικά γεγονότα η εξαγόμενη γνώση στο Green IoT αφορά τη πρόβλεψη μελλοντικών γεγονότων. Θα πρέπει να αναλύσουν περιοδικά τις πιθανές εξαρτήσεις μεταξύ συμβάντων οι προγνωστικοί παράγοντες για να ενημερώσουν τη βάση δεδομένων συμβάντων. Το λογισμικό στατιστικής ανάλυσης και πρόβλεψης χρησιμοποιείται για να ληφθεί η ακριβής απόφαση. Για παράδειγμα σε μερικές αναλύσεις ο αριθμός των εμφανίσεων των συμβάντων μεγαλώνει στον εντοπισμό συμβάντων που ο αριθμός εμφανίσεων έχει ξεπεράσει ένα συγκεκριμένο όριο. Θεωρώντας δεδομένο ότι η βάση δεδομένων συμβάντων στο Green IoT, η διαχείριση, η ειδοποίηση συμβάντων σε άλλα αντικείμενα, η ταξινόμηση συμβάντων και τα μοντέλα πρόβλεψης πραγματοποιούνται από λογισμικό, το πράσινο λογισμικό έχει αξιόλογο ρόλο σε αυτές τις διαδικασίες. Στις εφαρμογές που χρησιμοποιούν Green IoT διάφοροι παράγοντες όπως η ακριβής συλλογή δεδομένων, η αποτελεσματική ανάλυση δεδομένων και η ανακοίνωση των αποτελεσμάτων σε πραγματικό χρόνο πρέπει να ληφθεί υπόψιν για την ακριβή πρόβλεψη των συμβάντων. Επιπρόσθετα το να υπάρχει βιώσιμος υπολογισμός με μεγάλα δεδομένα και ο υπολογισμός υψηλής απόδοσης (HPC) είναι επίσης βασικές απαιτήσεις για αυτό το πεδίο. Συνήθως η ακριβής λήψη αποφάσεων εξαρτάται εξολοκλήρου από τον πραγματικό χρόνο, την ανταλλαγή πληροφοριών η οποία επιτυγχάνεται με τη βελτίωση της αρχιτεκτονικής Green IoT σε επίπεδο υλικού και λογισμικού. Σαν αποτέλεσμα απαιτείται αποδοτικό λογισμικό που θα προβλέπει γεγονότα με ελάχιστο υπολογιστικό κόστος.

2.1.2.3 Ταξινόμηση δεδομένων

Με απλά λόγια οι απαιτήσεις μεταξύ των στοιχείων δικτύου, της ανίχνευσης συμβάντων, της συλλογής δεδομένων, της ανάλυσης δεδομένων και της ταξινόμησης δεδομένων έπρεπε ήδη να έχουν αντιμετωπιστεί. Το Green IoT και το M2M μπορούν να χρησιμοποιηθούν σε δύσκολα σενάρια. Επιπλέον ο όγκος και η ποικιλία των δεδομένων περιορίζουν το παραδοσιακό λογισμικό ανάλυσης και τη συμβατική αποθήκευση για πολύπλοκα σενάρια Green IoT/M2M. Ο υψηλός όγκος των δεδομένων Green IoT και η έλλειψη επίσημου προτύπου για δεδομένα Green IoT είναι ένας συνδυασμός μη δομημένων δεδομένων και μεγάλων μοντέλων δεδομένων. Η αποτελεσματικότητα του Green IoT καθορίζεται πλήρως από το ότι είναι γρήγορο σε αντιδράσεις γεγονότων σε πραγματικό χρόνο και οι ακριβείς αντιδράσεις αποτυπώνουν την αποτελεσματικότητα αυτής της τεχνολογίας. Με τον ίδιο τρόπο ένα αποτελεσματικό Green IoT επιτυγχάνεται εάν λειτουργούν σωστά η ανάλυση και η ταξινόμηση των δεδομένων. Θα πρέπει να σημειωθεί ότι η ακριβής ανάλυση και η ανακάλυψη σχετικών σχέσεων μεταξύ των δεδομένων στη βάση δεδομένων είναι βασική προϋπόθεση για τη σωστή ταξινόμηση. Οι εφαρμογές που βασίζονται σε Green IoT πολλά αναλυτικά τους εργαλεία εξαρτώνται από

τις προηγούμενες σχέσεις και την ανθρώπινη ανάλυση. Τα πιο πολλά εργαλεία ταξινόμησης όσον αφορά τα σωστά δεδομένα, η ταξινόμηση έχει σημαντικές προκλήσεις και σε ειδικές περιπτώσεις υπάρχει ο εξαναγκασμός να εφαρμοστεί η τεχνική αυτή, ενώ η εσφαλμένη μπορεί να είναι καταστροφική. Το Green IoT χρησιμοποιείται στην έξυπνη πόλη και στον έξυπνο αυτοκινητόδρομο από επικίνδυνους ελιγμούς και ύποπτες συμπεριφορές και σε αυτή τη περίπτωση τα δεδομένα που μαζεύονται θα ταξινομηθούν σε φυσιολογικές και μη φυσιολογικές συμπεριφορές με την ταξινόμηση δεδομένων να αποτελεί το πιο ευαίσθητο μέρος. Συνεπώς θα πρέπει να πούμε ότι ο ρόλος του λογισμικού στη ταξινόμηση δεδομένων Green IoT είναι καθοριστικός.

2.1.3 Πράσινη Τηλεπικοινωνιακή Υποδομή (Green Communications Infrastructure)

Είναι προφανές ότι σημαντικό μέρος της ενέργειας ενός τηλεπικοινωνιακού δικτύου (ενσύρματου ή ασύρματου) να καταναλώνεται για τη μετάδοση δεδομένων. Σαν συμπέρασμα μπορεί να τονιστεί ότι η πράσινη επικοινωνία παίζει σημαντικό ρόλο στο Green IoT. Συν τοις άλλοις οι υπολογιστικές συσκευές του δικτύου όπως τα κέντρα υπερυπολογιστών, οι αποθήκες δεδομένων και τα κέντρα δεδομένων ανταλλάσουν συνεχώς μεγάλες ποσότητες με το κάθε άλλο. Ωστόσο, έχουν πραγματοποιηθεί λίγες μελέτες σχετικά με τα πρωτόκολλα επικοινωνίας για να μειωθεί το αποτύπωμα του άνθρακα.

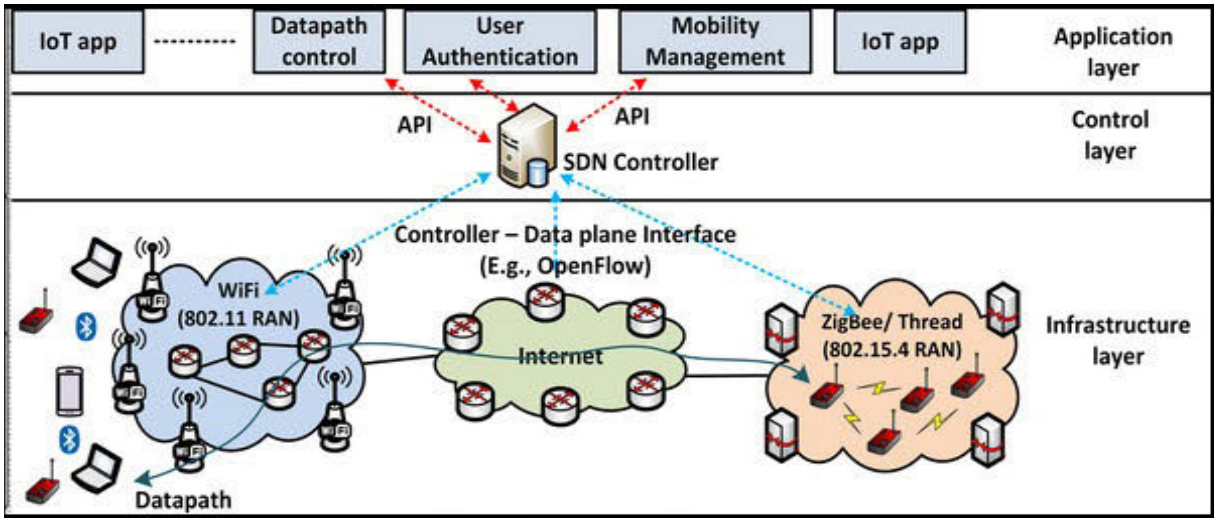
Στις διασυνδέσεις Device-to-Device (D2D) χρησιμοποιείται άμεση επικοινωνία μικρής πρόσβασης μεταξύ των συσκευών χωρίς να υπάρχουν υποδομές όπως οι σταθμοί βάσης και τα σημεία πρόσβασης όπου τα στοιχεία του δικτύου λειτουργούν ως δρομολογητές και τα πακέτα του δικτύου ανταλλάσσονται μεταξύ των στοιχείων του δικτύου μέσω μιας μετάδοσης multi-hop. Στις περισσότερες εφαρμογές Green IoT η επικοινωνία μεταξύ του αντικειμένου χαρακτηρίζεται από D2D και το Zigbee, BLE, PLC, RFID και NFC εφαρμόζονται για διασυνδέσεις. Συνδυάζοντας τις απαιτήσεις αξιοπιστίας όπως του υψηλού πακέτου και της αναγνώρισης του καθιστά τα πρωτόκολλα TCP/IP ασύμβατα με τις συσκευές επικοινωνίας στο Green IoT και οι μηχανισμοί επανεκπομπής αυξάνουν την κατανάλωση ενέργειας και αποφορτίζουν την ισχύ της μπαταρίας. Οι συμβατικές τεχνικές επικοινωνίας όπως το Ethernet, το ευρυζωνικό PLC και οι κυτταρικές τεχνικές όπως το UMT Sand LTE είναι ακατάλληλα για τεχνικές Green IoT λόγω του ότι διαθέτουν υψηλή αξιοπιστία, χαμηλή καθυστέρηση, μεγάλο ποσοστό μετάδοσης και είναι από τη φύση τους περίπλοκα καταναλώνοντας πολύ μεγάλη ενέργεια. Εν αντιθέσει με τις τεχνολογίες του πράσινου φυσικού επιπέδου και του πράσινου επιπέδου σύνδεσης δεδομένων καταναλώνουν λιγότερη ενέργεια και τοπικά χαρακτηρίζονται από μετάδοση με ρυθμούς μικρότερους από 1Mbit/sec, IEEE 802.15.4 Bluetooth με χαμηλή ενέργεια. Στο Bluetooth χαμηλής ενέργειας IEEE 802.11 το PLC, το NFC και το RFID μπορούν να είναι ξεχωριστά πρωτόκολλα για το Green IoT.

Τα τελευταία χρόνια έχει παρουσιαστεί σημαντική πρόοδο για τα πρότυπα IoT και Green IoT κάνοντας δημοφιλείς τις πράσινες ασύρματες συσκευές. Η χαμηλή ενέργεια Bluetooth είναι ένα προϊόν που αυτή την άποψη είναι μία μικρή, χαμηλού κόστους, χαμηλής κατανάλωσης και προσαρμόσιμης συσκευής. Το BLE βασίζεται σε Bluetooth 4.0 που δημιουργεί συνδέσεις με χαμηλή ισχύ μεταξύ των συσκεύων με δυνατότητα Bluetooth

και μπορούν επίσης να λειτουργούν για μήνες με μικρή μπαταρία. Το Bluetooth έχει νέες δυνατότητες αλλά δεν έχει κάνει σημαντικές βελτιώσεις σε σχέση με το Bluetooth 4.0, ενώ το Bluetooth 4.2 έχει ενισχύσει τις δυνατότητες του BLE κάνοντας το ευνοϊκή τεχνολογία για Green IoT. Αυτή τη στιγμή πρωτόκολλα επικοινωνίας όπως το Zigbee και το Z-Wave μπορούν να χρησιμοποιηθούν για εφαρμογές Green IoT που λειτουργούν στις ζώνες συχνοτήτων από μερικά MHz σε δεκάδες GHz, Wi-Fi, IEEE 802.15.4, Bluetooth, LTE-advanced και IrDA. Οι τοπικές και διεθνείς επίσημες ρυθμιστικές αρχές καθορίζουν τις εφαρμοζόμενες ζώνες συχνοτήτων για διάφορες εφαρμογές.

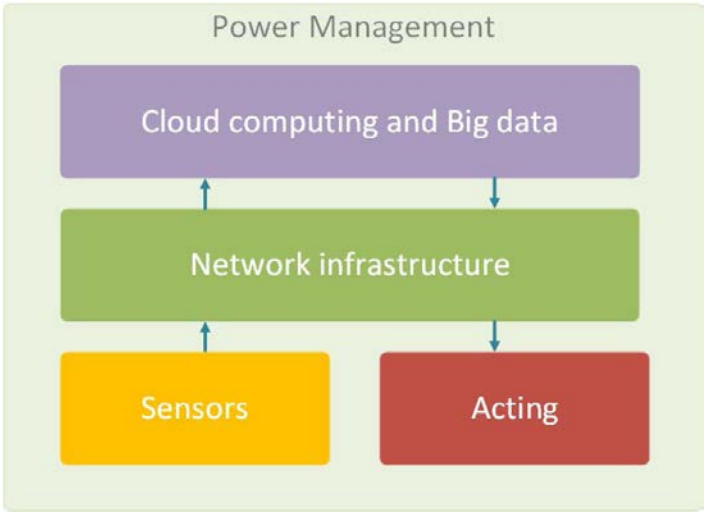
Στις στρατηγικές μετάδοσης υπάρχει ένας σοβαρός ανταγωνισμός μεταξύ των συστημάτων κατοχής του κοινόχρηστου καναλιού, έτσι ώστε σε περίπτωση που είναι αποτελεσματικό να μην χρησιμοποιείται η τεχνική ελέγχου πρόσβασης μέσω (MAC), οπότε οι συγκρούσεις στις μεταβιβάσεις θα είναι αναπόφευκτες. Οι συγκρούσεις μετάδοσης έχουν ως αποτέλεσμα οι αναμεταδόσεις και τα επιπλέον γενικά έξοδα και η υψηλή κατανάλωση ενέργειας να είναι ανησυχητικοί παράγοντες για την επίτευξη του Green IoT. Το επιστημονικό άρθρο Chen et.al έχει προτείνει ένα ασύμμετρο σύστημα πολλαπλής διαίρεσης της χρονικής αντιστροφής (TRDMA) για το IoT που είναι η κατάλληλη επιλογή για Green IoT λόγω του ότι υπάρχει υψηλή απόδοση ενέργειας. Το συγκεκριμένο σύστημα έχει συγκεκριμένες δυνατότητες όπως η υποστήριξη πολλαπλών ενεργειών πραγμάτων, του χειρισμού τερματικών συσκευών με χαμηλό κόστος, τη προσαρμογή ετερογενών τερματικών συσκευών, την επεκτασιμότητα και την περαιτέρω ασφάλεια φυσικού επιπέδου. Συμπερασματικά μπορεί να υποστηριχθεί το ασύμμετρο TRDMA που είναι καλό για ασύρματη λύση διότι το Green IoT έχει χαμηλή πολυπλοκότητα όσον αφορά την υψηλή ασφάλεια και την υψηλή επεκτασιμότητα.

Το Green IoT περιλαμβάνει διάφορα δίκτυα όπως Wireless Sensor Network (WSN), Wireless Personal Area Network (WPAN), Radio Frequency Identification (RFID), Home Area Network (HAN), Machine to Machine (M2M), Near area Network (NAN), Gateways. Οι συγκεκριμένες κατηγορίες δικτύων μπορούν να χρησιμοποιηθούν για μία συγκεκριμένη εφαρμογή λόγω του ότι έχουν από τη φύση τους ιδιαίτερα χαρακτηριστικά. Αν θεωρήσουμε ότι αυτά τα δίκτυα είναι υπεύθυνα για τη δημιουργία των συνδέσεων μεταξύ των διαφόρων στοιχείων του IoT είναι απαραίτητο να δοθεί η προσοχή στο ζήτημα της ενεργειακής απόδοσης σε αυτά τα δίκτυα για να επιτευχθεί το Πράσινο IoT.



2.1.4 Πράσινη Αρχιτεκτονική (Green Architecture)

Γίνεται προφανές πως για να επιτευχθεί ένα σύστημα Green IoT που πρέπει να είναι πράσινο θα χρειάζεται να αξιολογείται στην αρχιτεκτονική επικοινωνίας που συνδέει το Green IoT με άλλα δίκτυα και τελικούς χρήστες. Ο υπολογιστής του νέφους και ο υπολογιστής ομίχλης θεωρούνται ως οι δύο κορυφαίες αρχιτεκτονικές και για το λόγο αυτό πρέπει να είναι πράσινες. Ο υπολογιστής νέφους αναφέρεται στη χρήση πολλών υπηρεσιών όπως λογισμικό, διακομιστές, αποθήκευση και επεξεργασία μέσω του Διαδικτύου που είναι γνωστή ως σύννεφο. Το cloud computing επιτυγχάνει συνέπεια, συνοχή και επεκτασιμότητα με βάση την ικανότητα που έχει στη κοινή χρήση πόρων. Επιπροσθέτως, το cloud computing παρέχει επεκτασιμότητα και ευελιξία που απαιτείται για να καλυφθούν οι επιχειρηματικές αλλαγές, παρέχει ευκαιρία στους χρήστες για πρόσβαση σε ελεύθερους απαιτούμενους πόρους και διευκολύνεται η πρόσβαση στα δεδομένα. Συνεπώς, η έννοια του πράσινου νέφους πρέπει να ενισχυθεί για να επιτευχθεί το Green IoT. Τα δεδομένα που μαζεύτηκαν από πραγματικά πράγματα πρέπει να συνδυαστούν με άλλους πόρους που είναι διαθέσιμοι για να δημιουργηθεί πληροφορία προστιθέμενης αξίας για τους χρήστες. Το cloud computing συνήθως αναγνωρίζεται ως ένα μοντέλο προσανατολισμένο στην εξυπηρέτηση για συστηματική αποθήκευση και ανάλυση μεγάλων δεδομένων. Ο συνδυασμός του Green IoT με το cloud computing είναι ένα καινούριο παράδειγμα που επικρατεί παντού στη σημερινή πληροφορική και αναφέρεται ως πράσινο σύννεφο του πράγματος.



Εικόνα 10. Ιεραρχική Αρχιτεκτονική του Πράσινου Διαδικτύου των Πραγμάτων [6]

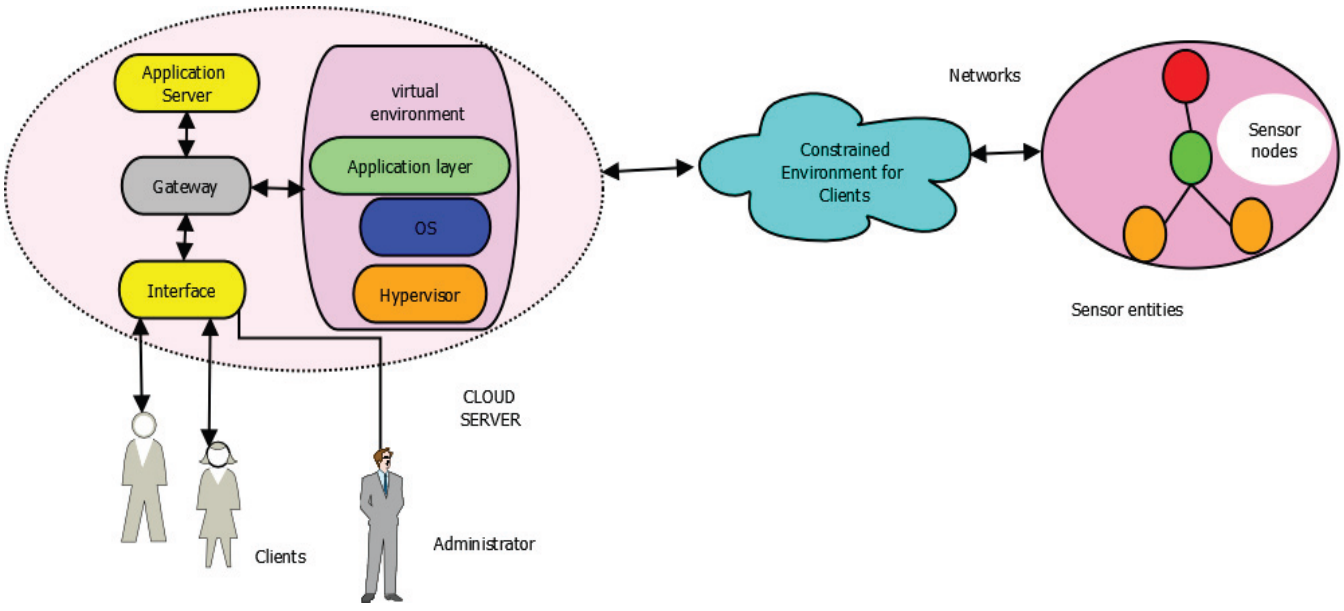
Το cloud computing χαρακτηρίζεται από υψηλή επεξεργασία και πυκνότητες αποθήκευσης. Για να δημιουργηθεί η επικοινωνία μεταξύ του cloud και των συσκευών Green IoT απαιτείται περισσότερη ενέργεια. Παρόλα αυτά η τοποθέτηση του cloud computing μεταξύ του Green IoT και των συσκευών cloud μειώνει την κατανάλωση ενέργειας. Ο Latif και ο Osborn έχουν προτείνει ένα σύστημα βάσεων δεδομένων για ανοιχτό κώδικα και αντικείμενα για παρακολούθηση, παραγωγή, διανομή και κατανάλωση ενέργειας για να γίνει η ενέργεια πιο αποδοτική. Οι συγγραφείς ισχυρίζονται ότι αυτή η βάση δεδομένων παρέχει δεδομένα, ακεραιότητα και αξιοπιστία στο σύστημα και ότι μπορεί να λειτουργεί με τα περισσότερα λειτουργικά συστήματα. Αφού αναφέρονται τα

παραπάνω χαρακτηριστικά η συγκεκριμένη βάση θα μπορούσε να είναι μία σωστή επιλογή για Green IoT. Το ίδιο ισχύει και για τη πλήρη συνεργασία όλων των στοιχείων του Green IoT και για ρη πρόληψη του εγωισμού των αντικειμένου θα αυξήσουν τη διάρκεια ζωής του δικτύου για να γίνει ένα αποτελεσματικό βήμα προκειμένου να φτάσουμε στην επίτευξη του Green IoT. Το επιστημονικό άρθρο Bogdan έχει ψάξει το ρόλο του ελέγχου σε πραγματικό χρόνο για τον διαδικτυακό έλεγχο για να επιτευχθεί ένα ενεργειακό αποδοτικό IoT. Οι συγγραφείς έχουν μιλήσει για την αρχιτεκτονική Wireless Control Networks (WSN) και τις προκλήσεις των αποφάσεων ελέγχου κλειστού βρόγχου σε πραγματικό χρόνο, όπως το να περιορισθεί η μνήμη, το να περιορισθεί το εύρος ζώνης και να υπάρχει η αναποτελεσματικότητα της ισχύος στους υπερυπολογιστές. Αυτοί οι τύποι ελέγχου μπορεί να είναι αποτελεσματικοί που είναι ένα βήμα για να επιτευχθεί το Green IoT μειώνοντας την κατανάλωση ενέργειας.

2.2 Αρχιτεκτονική Πράσινου Διαδικτύου των Πραγμάτων

Το Green IoT αποτελείται από τέσσερα επίπεδα:

1) Επίπεδο Αισθητήρων και Αντικειμένων: Είναι υπεύθυνο για τη λήψη δεδομένων μέσω των πράσινων αισθητήρων και τη σωστή αντίδραση από τους ηθοποιούς.
2) Επίπεδο Επικοινωνίας: Είναι υπεύθυνο για τη συνδεσιμότητα του δικτύου.
3) Επίπεδο Εφαρμογής: Είναι υπεύθυνο για την επεξεργασία δεδομένων και για την αποθήκευση μεγάλων δεδομένων αποθήκευσης
4) Επίπεδο Διαχείρισης Ενέργειας: Ως αφηρημένο επίπεδο είναι υπεύθυνο για να διαχειρίζεται την ενέργεια όλων των στρωμάτων.



Εικόνα 11. Παράδειγμα Αρχιτεκτονικής Πράσινου Διαδικτύου των Πραγμάτων

Οι εξελιγμένες τεχνολογίες και οι συσκευές που βασίζονται στο Διαδίκτυο αποτελούν αναπόσπαστο μέρος της ανθρώπινης ζωής σήμερα. Άρα, οι άνθρωποι πρέπει να πληρώσουν με προσοχή σε αυτές τις τεχνολογίες για να έχουμε πράσινη γη και φρέσκο

υγιεινό νερό. Η ενεργειακή απόδοση που χρησιμοποιεί πράσινες ανανεώσιμες πηγές είναι ζωτικής σημασίας λόγω της παροχής ευκαιρίας για εξοικονόμηση ενέργειας και χρημάτων για ανάπτυξη Green IoT και για δημιουργία βιώσιμου αποτυπώματος CO_2. Επιπλέον, η βελτιστοποίηση του IoT λειτουργεί με τη μείωση της κατανάλωσης ενέργειας όσο το δυνατόν είναι περισσότερο απαραίτητο για τη διατήρηση των φυσικών πόρων και τον καθαρισμό του φυσικού περιβάλλοντος.

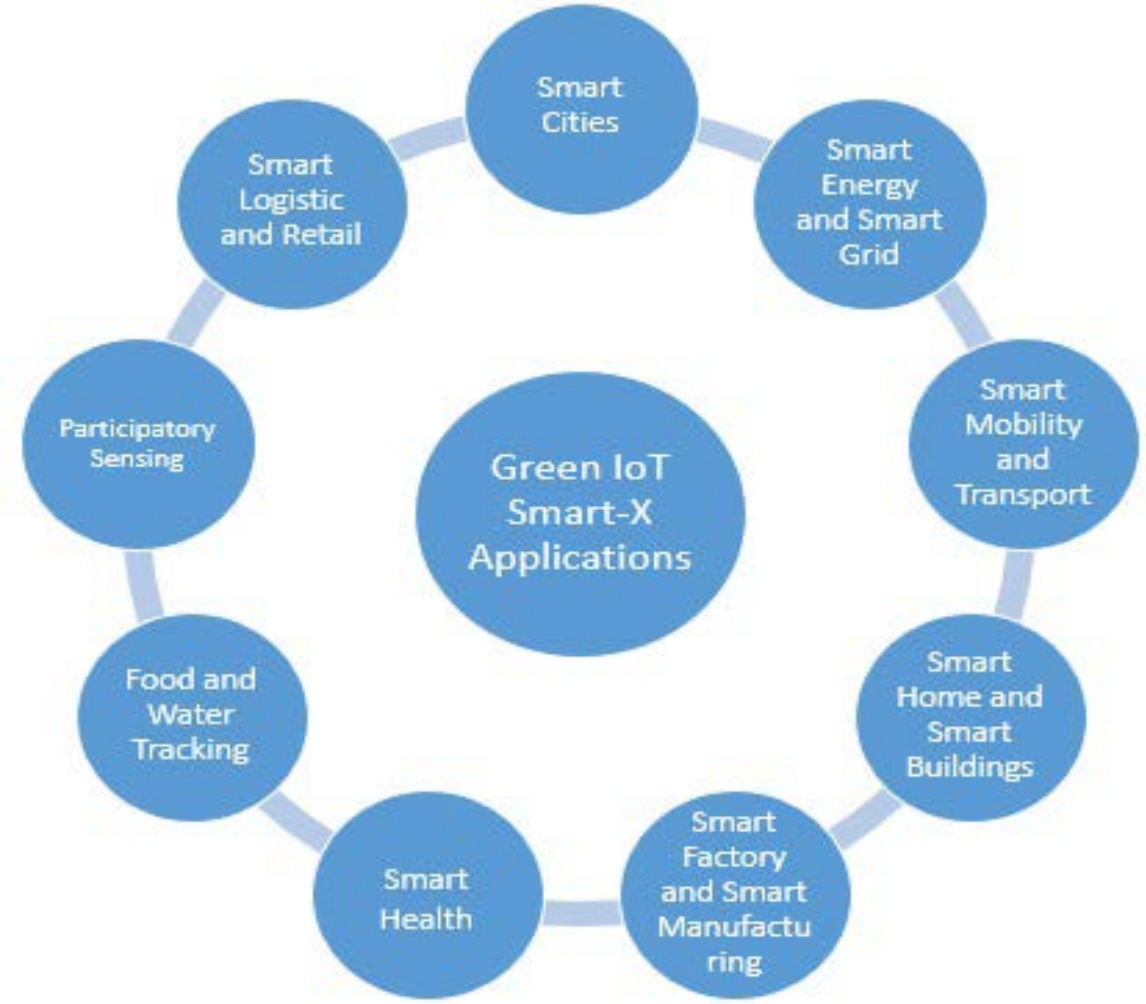
Πρέπει να σημειωθεί ότι εκτός από τη μείωση της ενέργειας και τη κατανάλωση όλων των συσκευών Green IoT θα πρέπει να είναι ένα ενεργειακά αποδοτικό σχέδιο που θα λαμβάνεται υπόψη καθ'όλη τη διάρκεια ζωής αυτής της τεχνολογίας συμπεριλαμβανομένης της παραγωγής, της λειτουργίας και της διάθεσης. Επιπλέον, είναι σημαντικό να αντιμετωπιστεί η κατανάλωση ενέργειας εξαρτημάτων και εξοπλισμού Green IoT που περιλαμβάνει πράγματα, υποδομές, πρωτόκολλα επικοινωνίας και συσκευές. Γενικά, η πρόοδος στις επιστήμες των ηλεκτρονικών και των επικοινωνιών και η καινοτομία στην παραγωγή έξυπνων αισθητήρων και βιώσιμων υλικών διευκολύνουν την επίτευξη του Green IoT. Το ίδιο ισχύει και με τις συσκευές του Green IoT που είναι συνήθως εξοπλισμένες με μικρές μπαταρίες και περιορισμένη τροφοδοσία, ενώ η διάρκεια ζωής του Green IoT είναι ένας κρίσιμος παράγοντας σε μακροπρόθεσμες εφαρμογές όπως η συνεχής περιβαλλοντική παρακολούθηση.

Ωστόσο, η χρήση επαναφορτιζόμενων μπαταριών και η παραγωγή βιώσιμης ενέργειας από ηλιακή και αιολική ενέργεια είναι οι κατάλληλες επιλογές για εξαιρετικές εφαρμογές. Παράλληλα, η αύξηση του κόστους παραγωγής της ενέργειας, η αύξηση του κόστους της ενέργειας και η κατανάλωση και η ευαισθητοποίηση σχετικά με τις οικολογικές πληροφορίες είναι θετικό πλεονέκτημα για τους ανθρώπους να οργανώσουν την κατανάλωση ενέργειας και να χρησιμοποιήσουν το Green IoT. Σε γενικές γραμμές οι περισσότερες υπαίθριες εφαρμογές Green IoT ακολουθούν ένα ίδιο πρότυπο σχετικά με τη λειτουργία τους με στόχο τα δεδομένα να λαμβάνονται από αισθητήρες και τα δεδομένα να υποβάλλονται για επεξεργασία σε μια μονάδα επεξεργασίας και στη συνέχεια, οι απαραίτητες πληροφορίες να μεταδίδονται μέσω των ασύρματων καναλιών.

Συμπερασματικά, η ενέργεια του Green IoT χρησιμοποιείται για τρεις σκοπούς, τη λήψη των δεδομένων από αισθητήρες, τον χειρισμό και την επεξεργασία δεδομένων και την επικοινωνία δεδομένων. Θα ήταν σημαντικό να αναφερθεί ότι η κατανάλωση ενέργειας για τη λειτουργία του λειτουργικού συστήματος αφύπνισης είναι ασήμαντη. Άρα η κατανάλωση όλων των βημάτων υψηλής κατανάλωσης και η μείωση του αριθμού αυτών των βημάτων όσο το δυνατόν περισσότερο είναι απαραίτητα για ένα ενεργειακά αποδοτικό Green IoT. Πέρα από τη μείωση στη κατανάλωση ενέργειας θα πρέπει να διερευνηθούν μέθοδοι παραγωγής ηλεκτρονικής ενέργειας από ηλιακό, αιολικό, γεωθερμικό τα οποία φυσικά επηρεάζονται από παράγοντες όπως η θερμοκρασία, η ταχύτητα του ανέμου και η ώρα της ημέρας.

2.3 Εφαρμογές Πράσινου Διαδικτύου των Πραγμάτων

Το Green IoT λόγω της χαμηλής κατανάλωσης ενέργειας και της υψηλής προσαρμοστικότητας με το περιβάλλον μπορεί να χρησιμοποιηθεί σε διαφορετικές εφαρμογές ως εξής:



Εικόνα 12. Εφαρμογές Green IoT

2.3.1 Green IoT για έξυπνες πόλεις

Το Green IoT στις έξυπνες πόλεις μπορεί να εφαρμοστεί για να βελτιώσει η διαχείριση ροών στις αστικές περιοχές και την ανταπόκριση των προβλημάτων σε πραγματικό χρόνο. Τα τελευταία χρόνια υπήρχαν διάφορα κριτήρια που έχουν αυξήσει την προσοχή στις έξυπνες πόλεις όπως οι τεχνολογικές, οικονομικές και περιβαλλοντικές εξελίξεις που αφορούν στην κλιματική αλλαγή, στον οικονομικό προϋπολογισμό, οι δυσκολίες σε οικονομικά θέματα και η γήρανση του πληθυσμού. Επίσης το Green IoT μπορεί να εφαρμοστεί και σε έξυπνους χώρους στάθμευσης για να ελέγξει τη δύναμη των κτηρίων, των γεφυρών και των μνημείων αλλά και στη κυκλοφορία, στη καλύτερη διαχείριση του δρόμου και στις διασταυρώσεις.

Με απλά λόγια μπορούμε να διασφαλίσουμε ότι το Green IoT μπορεί να χρησιμοποιηθεί σε περιπτώσεις όπως τα φανάρια, στις έξυπνες γέφυρες και στα οχήματα για να δημιουργηθεί μία οικονομικά έξυπνη πόλη. Συνεπώς, το πράσινο είναι βασική ανάγκη για διάφορες εφαρμογές της συγκεκριμένης τεχνολογίας που μειώνει τη συνολική κατανάλωση της ηλεκτρικής ενέργειας μειώνοντας ταυτόχρονα τη περιβαλλοντική καταστροφή

2.3.2 Green IoT για έξυπνα σπίτια

Το κοινοβούλιο της Ευρωπαϊκής Ένωσης ανακοίνωσε μία οδηγία το 2002 που υποχρέωνε τις χώρες της Ευρώπης να εφαρμόσουν συγκεκριμένες τεχνικές για να βελτιωθεί η ενεργειακή απόδοση σε σπίτια, κτίρια και γραφεία. Τα ερευνητικά έργα όπως το SEEMPubs, το DIMMER, το AIM, το IntUBE και το DEH EMS έχουν δρομολογηθεί προς αυτή την κατεύθυνση. Η τεχνολογία Green IoT συμπίπτει με την οδηγία της Ευρωπαϊκής Ένωσης που χρησιμοποιείται στη διαχείριση των έξυπνων συστημάτων και στη μείωση του ξοδέματος της ενέργειας σε πράσινα έξυπνα σπίτια. Σε ένα έξυπνο σπίτι, το Green IoT σβήνει αυτόματα τα φώτα όταν οι άνθρωποι εγκαταλείψουν το σπίτι στο οποίο ζούνε. Επίσης, τα κλιματιστικά μπορούν να προσαρμόσουν την εσωτερική θερμοκρασία σύμφωνα με τις συνθήκες που επικρατούν σπαταλώντας τη λιγότερη ενέργεια. Το Green IoT μπορεί να μειώσει την κατανάλωση ενέργειας ενός κτιρίου και σχετικού κόστους με την παρακολούθηση και τον έλεγχο των ενεργειακών παραγόντων. Το περιβάλλον διαβίωσης με το να είναι πράσινο γίνεται πιο υγιές.

2.3.3 Green IoT για έξυπνο περιβάλλον και βιομηχανικό έλεγχο

Η τεχνολογία Green IoT μπορεί να χρησιμοποιηθεί για να αποφευχθούν πυρκαγιές στο δάσος, για την ανάλυση της μόλυνσης του αέρα και του νερού της θάλασσας, για την παρακολούθηση στη κατανάλωση του πράσινου νερού, για τον έλεγχο της περιοχής που βρίσκεται σε κίνδυνο για το σύστημα αυτόματης διάγνωσης οχημάτων και για τη δημιουργία ενός έξυπνου πλέγματος. Επιπλέον, το Green IoT μπορεί να χρησιμοποιηθεί σε ευαίσθητες εφαρμογές όπως για την ανίχνευση υγρών σε κέντρα δεδομένων για τη μέτρηση της διάβρωσης και για την ακτινοβολία σε πυρηνικούς σταθμούς για να υπάρχει η δημιουργία προειδοποίησης της διαρροής και παρακολούθηση των ευαίσθητων κτηρίων για να αποφευχθεί η κατάρρευση. Εφόσον είσαι πράσινος εξασφαλίζεις ότι σε τέτοιες εφαρμογές όπου η τεχνολογία έχει άμεση σχέση με το περιβάλλον δεν προκαλείται σοβαρή ζημιά στη φύση.

2.3.4 Green IoT για έξυπνη γεωργία και κτηνοτροφία

Η τεχνολογία Green IoT μπορεί επίσης να αξιοποιηθεί στη γεωργία, την κτηνοτροφία και στη βιομηχανία για να αυξήσει την ποιότητα και την ποσότητα των καλλιεργειών. Από αυτή την άποψη, το Green IoT μπορούμε να το χρησιμοποιήσουμε για να παρακολουθήσουμε την υγρασία του εδάφους των παρασίτων του δέντρου, των έξυπνων μετεωρολογικών σταθμών για τη φροντίδα νεογέννητων ζώων και για την παρακολούθηση των ζωνών. Η τήρηση των πράσινων προτύπων σε όλα τα στάδια είναι απαραίτητα για την παραγωγή πράσινων καλλιεργειών και υγιεινών ζωτικών προϊόντων για τον άνθρωπο.

2.3.5 Green IoT για την ηλεκτρονική υγεία

Γενικώς, η βελτίωση της ευημερίας και της ανθρώπινης υγείας είναι κάτι κοινό και στόχος όλων των τεχνολογιών με σκοπό το Green IoT να εισαχθεί ευθυγραμμισμένα με αυτόν τον στόχο. Το Green IoT μπορεί να χρησιμοποιηθεί ιατρικών ψυγείων, για τη φροντίδα σε αθλητές, για την παρακολούθηση ασθενών και ηλικιωμένων και για τη μέτρηση της υπεριώδους ακτινοβολίας. Με απλά λόγια ένα σύστημα ηλεκτρονικής υγείας

που βασίζεται στο Green IoT αποτελείται από ένα αριθμό μικροσκοπικών αντικειμένων για την παρακολούθηση της θερμοκρασίας του σώματος και του αίματος και των αισθητήρων πίεσης Blood Pressure(BP) που ο εξοπλισμός της είναι με περιορισμένη ισχύ μπαταρίας. Σε αυτές τις εφαρμογές εάν ένα αντικείμενο δεν χρειάζεται να ενεργοποιηθεί σε μία συγκεκριμένη στιγμή, μεταβαίνει σε λειτουργία εξοικονόμησης ενέργειας για να την διατηρήσει. Επιπλέον, η ταχύτητα της CPU μειώνεται εάν δεν υπάρχουν εργασίες επεξεργασίας. Με δεδομένο ότι σε τέτοιες εφαρμογές το Green IoT είναι πολύ κοντά στον άνθρωπο, το να είναι κάποιος πράσινος είναι μία σημαντική προϋπόθεση για να επιβεβαιώσει ότι αυτή η τεχνολογία είναι ακίνδυνη και όχι επικίνδυνη. Επιπρόσθετα, πρέπει να σημειωθεί ότι η προσπάθεια μείωσης του αριθμού των χρησιμοποιούμενων αισθητήρων για την παρατήρηση των φυσιολογικών σημάτων είναι ευθυγραμμισμένα με στόχους Green IoT. Με τον ίδιο τρόπο παρέχοντας πράσινη επικοινωνία εγκεφάλου με μηχανή η σύνδεση παίζει σπουδαίο ρόλο σε εφαρμογές Green IoT που ελέγχονται από τον εγκέφαλο.

3. Προκλήσεις Ασφαλείας στο Πράσινο Διαδίκτυο των Πραγμάτων

Όπως έχει ήδη αναφερθεί, οι επιθέσεις που γίνονται κατά των συσκευών και συστημάτων IoT είναι πολλές φορές απλές και εύκολες στον τρόπο που πραγματοποιούνται. Ο στόχος τους είναι να καταρρίψουν το απόρρητο των χρηστών και να αποσπάσουν σημαντικές τους προσωπικές πληροφορίες. Όσα δεδομένα μαζεύονται μπορούν να αφορούν απλές μετρήσεις της θερμοκρασίας έως πιο σύνθετες πληροφορίες όπως το σήμα που υπάρχει στην καρδιά η ακόμη και τον τόπο διαμονής και τον τρόπο ζωής των χρηστών. Ένας άλλος τρόπος επίθεσης αφορά στο να παραβιαστεί μία συσκευή στο δίκτυο IoT και στη χρησιμοποίηση της ως αιχμή για την εκτέλεση παράξενων ενεργειών προς έναν άλλον κόμβο του δικτύου. Παρακάτω δίνεται μία αναλυτική επισκόπηση των απαιτήσεων για ασφάλεια του IoT και των σχετικών προκλήσεων

3.1 Απαιτήσεις ασφαλείας αρχιτεκτονικής IoT τριών επιπέδων

Στην περίπτωση της αρχιτεκτονικής IoT τριών επιπέδων, μία κατηγοριοποίηση για τις απαιτήσεις της ασφάλειας σε ένα σύστημα IoT σε σχέση με τα διαφορετικά λειτουργικά επίπεδα του, μπορεί να περιλαμβάνει τα εξής:

Στο **Επίπεδο Αντίληψης** για την ανίχνευση πληροφοριών και τη συλλογή δεδομένων, οι κυριότερες απαιτήσεις ασφάλειας σε ένα σύστημα IoT αφορούν τα εξής:

- **Εμπιστευτικότητα**: Τα δεδομένα δεν μπορούν να μεταφερθούν από τρίτους. Θα πρέπει να δημιουργηθεί μία αξιόπιστη σχέση μεταξύ των συσκευών IoT με στόχο να ανταλλάσσονται ελεγχόμενες πληροφορίες. Όσα μηνύματα έχουν τη δυνατότητα να αναπαράγονται πρέπει απαραίτητα να αναγνωρίζονται.
- **Ακεραιότητα**: Όσα δεδομένα λαμβάνονται πρέπει να είναι αδιάβλητα
- **Απόρρητο**: Κατά την ανταλλαγή των δεδομένων τα προσωπικά στοιχεία του πελάτη δεν πρέπει να αποκαλύπτονται σε κανέναν. Ταυτόχρονα χρειάζεται να είναι δυνατόν να μαζεύουν πληροφορίες που θα αναγνωρίζονται από όσους κάνουν απόπειρα να τα κλέψουν.
- **Ανωνυμία**: Τα δεδομένα πρέπει να παραμένουν κρυφά σε τρίτους.

Στο **Επίπεδο Πρόσβασης Δικτύου ή Ενδιάμεσο Επίπεδο**, οι κυριότερες απαιτήσεις ασφάλειας σε ένα σύστημα IoT, αφορούν τα εξής:

- **Έλεγχος πρόσβασης**: Εξασφαλίζει ότι μόνο οι νόμιμοι και εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις συσκευές IoT και στις δικτυακές υποδομές και υπηρεσίες που υποστηρίζουν το σύστημα IoT (π.χ. έλεγχος των συσκευών και του δικτύου IoT, απομακρυσμένος επαναπρογραμματισμός, κ.ά.)
- **Έλεγχος ταυτότητας**: Ελέγχει το δικαίωμα πρόσβασης που μπορεί να έχει μία συσκευή IoT σε ένα δίκτυο και παράλληλα εάν το δίκτυο έχει δικαίωμα διασύνδεσης των συσκευών IoT. Τις πιο πολλές φορές αυτή είναι η πρώτη λειτουργία που πραγματοποιείται από έναν κόμβο όταν υπάρχει σύνδεση σε νέο δίκτυο. Οι συσκευές IoT πρέπει να μπορούν να προσφέρουν δυνατές και αξιόπιστες διαδικασίες ως προς τον έλεγχο της ταυτότητας.

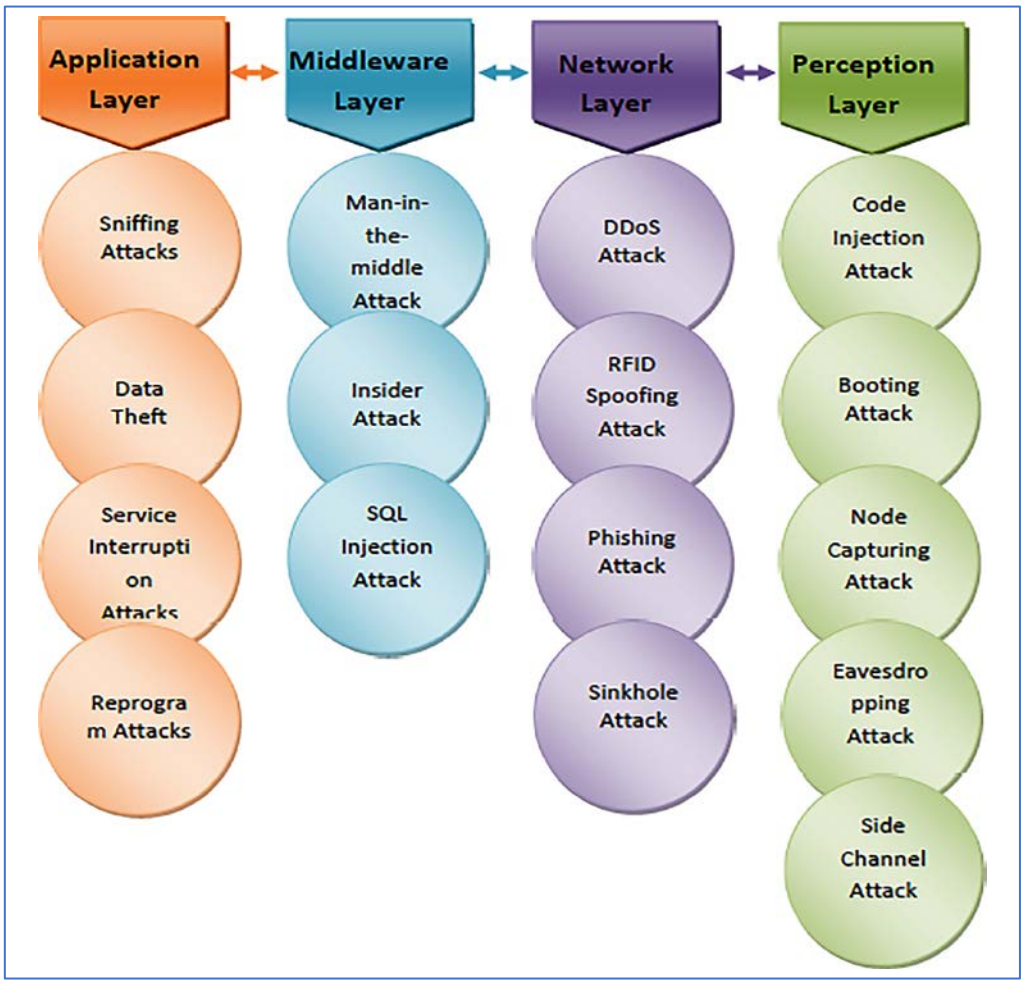
- **Εξουσιοδότηση**: Μόνο οι εξουσιοδοτημένες συσκευές IoT και οι εξουσιοδοτημένοι χρήστες θα πρέπει να έχουν πρόσβαση στις υπηρεσίες ή στους πόρους του δικτύου.

Στο **Επίπεδο Εφαρμογής**, οι κυριότερες απαιτήσεις ασφάλειας σε ένα σύστημα IoT, αφορούν τα εξής:

- **Ανθεκτικότητα και Διαθεσιμότητα**: Αφορά τη διατήρηση της διαθεσιμότητας των υπηρεσιών που συλλέγουν, επεξεργάζονται, αποθηκεύουν και διαχειρίζονται τα δεδομένα του συστήματος IoT, με στόχο να εξασφαλίζεται η αδιάλειπτη λειτουργία τους ακόμη και αν υπάρξει κάποια επίθεση ή/και αστοχία.
- **Αυτοοργάνωση**: Παρέχει την ικανότητα σε ένα σύστημα IoT να προσαρμόζεται με σκοπό να μπορεί να διατηρείται λειτουργικό, εφόσον υπάρξει αστοχία σε ορισμένα εξαρτήματα λόγω των δυσλειτουργιών που συμβαίνουν κάποιες φορές ή κακόβουλων επιθέσεων.

3.2 Απαιτήσεις ασφαλείας αρχιτεκτονικής IoT τεσσάρων επιπέδων

Στην περίπτωση της αρχιτεκτονικής IoT τεσσάρων επιπέδων, δηλαδή το επίπεδο εφαρμογής, το επίπεδο ενδιάμεσου λογισμικού, το επίπεδο δικτύου και το επίπεδο αντίληψης, μία κατηγοριοποίηση για τις απαιτήσεις της ασφάλειας σε ένα σύστημα IoT σε σχέση με τα διαφορετικά λειτουργικά επίπεδα του, μπορεί να περιλαμβάνει τα εξής:



Εικόνα 13. Απειλές και Προκλήσεις Ασφαλείας σε Εφαρμογές IoT [2]

3.2.1 Επίπεδο Αντίληψης (Perception Layer)

Μερικοί από τους δημοφιλείς αισθητήρες είναι αισθητήρες κάμερας, υγρασίας θερμοκρασίας, χημικών και ανίχνευσης. Στο συγκεκριμένο επίπεδο χρησιμοποιούνται τεχνολογίες όπως WSN,GPS και RFID. Το συγκεκριμένο επίπεδο είναι επιρρεπές στις επιθέσεις που περιλαμβάνει κόμβους στους αισθητήρες και στην υποκλοπή που αναφέρεται παρακάτω.

- **Επίθεση με έκχυση κώδικα (Code Injection Attack)**: Τα λογισμικά των κόμβων του IoT συνήθως ενημερώνονται μέσω ασύρματων δικτυακών υποδομών παρέχοντας με αυτό το τρόπο σε οποιονδήποτε δράστη την ευκαιρία να εισάγει ένα κακόβουλο κώδικα που μπορεί να οδηγήσει σε ανεπιθύμητες ενέργειες και σε πρόσβαση σε μη εξουσιοδοτημένα επίπεδα του συστήματος.
- **Επίθεση εκκίνησης (Booting Attack)**: Όλες οι υπηρεσίες ασφαλείας ενεργοποιούνται όταν μία συσκευή IoT είναι λειτουργική. Κατά την εκκίνηση ή τη διαδικασία της εκκίνησης υπάρχει ένα παράθυρο για τους χάκερς που μπορούν να επιτίθενται στις συσκευές-κόμβους του δικτύου IoT. Οι συσκευές IoT στα άκρα του δικτύου είναι χαμηλής ισχύος, έχουν έναν σταθερό κύκλο ύπνου-αφύπνισης που γίνεται όλο και περισσότερο ευάλωτη σε αυτές τις επιθέσεις.
- **Επίθεση σύλληψης κόμβου (Node Capturing Attack)**: Ένας επιτιθέμενος κυριεύει ένα νόμιμο κόμβο του συστήματος IoT και τον αντικαθιστά με το δικό του παράνομο (rogue) κόμβο, παρέχοντας πλέον πρόσβαση σε τμήμα ή σε ολόκληρο το σύστημα IoT μέσω του ψευδεπίγραφου παράνομου κόμβου.
- **Επίθεση Υποκλοπής (Eavesdropping Attack)**: Οι εισβολείς μπορούν να παρακολουθούν παθητικά το οικοσύστημα IoT με σκοπό να ακούσουν, να παρατηρήσουν, ή να υποκλέψουν τα δεδομένα όταν αυτά διαβιβάζονται μεταξύ διαφορετικών κόμβων στο δίκτυο IoT.
- **Επίθεση πλευρικών καναλιών (Side Channel Attack)**: Τα ευαίσθητα δεδομένα θα μπορούν να διαρρεύσουν από τα ενσωματωμένα ολοκληρωμένα κυκλώματα των επεξεργαστών των συσκευών IoT, μέσα από τις επιθέσεις των πλευρικών καναλιών, όπως η ηλεκτρομαγνητική επίθεση και οι επιθέσεις χρονισμού.

3.2.2 Επίπεδο Δικτύου (Network Layer)

Ο πιο σημαντικός ρόλος αυτού του επιπέδου είναι η μεταφορά δεδομένων από το επίπεδο αντίληψης στο ενδιάμεσο επίπεδο και κατά συνέπεια περιλαμβάνει μία ποικιλία σε επιθέσεις, που μπορεί να αντιμετωπιστούν.

- **Κατανεμημένη επίθεση άρνησης εξυπηρέτησης (DDoS Attack)**: Στη προκειμένη περίπτωση, ένας εισβολέας ή μια ομάδα από εισβολείς που έχουν υπό τον έλεγχό τους ένα δίκτυο (botnet) από εξ' αποστάσεως ελεγχόμενες μολυσμένες συσκευές (bots), ενεργοποιούν την ταυτόχρονη αποστολή από αυτές τις συσκευές (bots) ενός πολύ μεγάλου πλήθους από κακόβουλα αιτήματα εξυπηρέτησης προς τους διακομιστές υπηρεσίας που έχουν στο στόχαστρο, με σκοπό να εξαντλήσουν τους υπολογιστικούς πόρους τους και να τις καταστήσουν μη διαθέσιμες στους νόμιμους/εξουσιοδοτημένους χρήστες τους.
- **Επίθεση πλαστογράφησης RFID (RFID Spoofing Attack)**: Με το συγκεκριμένο τύπο

επίθεσης οι πληροφορίες που μεταδίδονται μέσω μιας ετικέτας RFID μπορεί να αλλάξουν με κακόβουλο τρόπο, καθώς ο επιτιθέμενος παραποιεί το σήμα RFID.

- **Επίθεση ηλεκτρονικού ψαρέματος (Phishing Attack)**: Ο εισβολέας στέλνει ένα παραπλανητικό μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail) σε πολλούς χρήστες του συστήματος IoT με την ελπίδα ότι κάποιοι από αυτούς, που έχουν πρόσβαση στο συγκεκριμένο e-mail, θα ενεργοποιήσουν την κακόβουλη σύνδεση (link) που εμπεριέχεται μέσα στο παραπλανητικό e-mail. Αμέσως μετά το άνοιγμα της παραπλανητικής κακόβουλης σύνδεσης (link) από το νόμιμο χρήστη-θύμα και την εισαγωγή των διαπιστευτηρίων (credentials) του, παρέχεται στον χάκερ πλήρη πρόσβαση στο συγκεκριμένο σύστημα IoT.
- **Επίθεση καταβόθρας (Sinkhole Attack)**: Η επίθεση δημιουργείται από το κόμβο που έχει παραβιαστεί από τον εισβολέα στο δίκτυο IoT. Στη συγκεκριμένη κατηγορία επίθεσης, προστίθενται από τον εισβολέα ψεύτικες λεπτομέρειες όσον αφορά τη δρομολόγηση μεταξύ διαδοχικών κόμβων του δικτύου IoT, δημιουργώντας έτσι ένα τεράστιο φόρτο στην κυκλοφορία του δικτύου IoT με στόχο, είτε την εξάντληση των διαθέσιμων πόρων του, είτε να χρησιμοποιηθεί και για την εκτέλεση άλλων επιθέσεων.

3.2.3 Ενδιάμεσο επίπεδο (Middleware Layer)

Το συγκεκριμένο επίπεδο λειτουργεί ως buffer για δύο βασικές εργασίες: Η μία είναι η επιβεβαίωση και η αυθεντικοποίηση του χρήστη και η άλλη η μεταφορά δεδομένων.

- **Επίθεση Man in the middle**: Σε αυτή τη περίπτωση ο εισβολέας παίζει το ρόλο του ανθρώπου που παριστάνει το νόμιμο χρήστη του συστήματος IoT, όπως όταν δύο πραγματικοί χρήστες επικοινωνούν μεταξύ τους, ενώ στην πραγματικότητα βρίσκονται σε άμεση συνομιλία με έναν χάκερ που μιλάει και στους δύο και έχει τη δύναμη να ελέγχει και να χειρίζεται την επικοινωνία.
- **Εσωτερική επίθεση (Insider Attack)**: Αυτή είναι μία από τις πολύ δύσκολες επιθέσεις στον εντοπισμό επειδή ο δράστης είναι ένας νόμιμος-εξουσιοδοτημένος χρήστης του συστήματος IoT. Ο δράστης μπορεί να είναι ένα προσωρινό μέλος (guest) ή ένας κανονικός χρήστης που έχει πρόσβαση στα στοιχεία και στα διαπιστευτήρια του συστήματος, έχοντας την ικανότητα εκτόξευσης διαφορετικών τύπων επιθέσεων.
- **Επίθεση με έκχυση κώδικα SQL (SQL injection Attack**: Είναι μία από τις πολύ σοβαρές απειλές για κάθε σύστημα που μπορεί να οδηγήσει σε απώλεια εμπιστευτικών δεδομένων, σε μη εξουσιοδοτημένη πρόσβαση και ακόμα να υπάρχει κίνδυνος παραβίασης ολόκληρου δικτύου ή μεμονωμένων συσκευών-κόμβων. Ένας επιτιθέμενος εισάγει ορισμένες κακόβουλες εντολές SQL στον ευάλωτο κώδικα ιστού και σε εφαρμογές στο προσκήνιο (front-end) που έχουν διεπαφές με τις βάσεις δεδομένων στο εσωτερικό μέρος του συστήματος (backend).

3.2.4 Επίπεδο Εφαρμογής (Application Layer)

Το συγκεκριμένο επίπεδο αφορά τόσο τους τελικούς χρήστες όσο και τους διακομιστές υπηρεσίας του συστήματος IoT που είναι υπεύθυνοι για την υποστήριξη των εφαρμογών IoT και παροχή των κατάλληλων υπηρεσιών. Επομένως εμπλέκονται πολλές απειλές όπως:

- **Επιθέσεις παρακολούθησης και καταγραφής (Sniffing Attacks)**: Τα πακέτα δεδομένων ενός συστήματος IoT μπορούν να καταγράφονται κατά τη μετάδοσή τους από κακόβουλους εισβολείς χρησιμοποιώντας ειδικά λογισμικά παρακολούθησης και σύλληψης (sniffers) κι εφόσον υπάρχει ελάχιστη ή καθόλου κρυπτογράφηση στα πακέτα δεδομένων που υποκλέπτονται, μπορούν να εξαχθούν από αυτά ευαίσθητα δεδομένα .
- **Υποκλοπή Δεδομένων (Data Theft)**: Τα δεδομένα ή οι πληροφορίες που συλλέγονται από τους αισθητήρες από συσκευές IoT είναι πιο ευάλωτα όταν βρίσκονται στο στάδιο ασύρματης μετάδοσής τους μέσω δικτύου και μπορούν να υποκλαπούν πιο εύκολα, εάν δεν τηρούνται τα πρωτόκολλα ασφαλείας και δεν έχουν ληφθεί τα κατάλληλα μέτρα προστασίας.
- **Επιθέσεις διακοπής παροχής υπηρεσίας (Service Interruption Attack)**: Καθιστά τους διακομιστές υπηρεσίες απασχολημένους από κακόβουλα αιτήματα εξυπηρέτηση, με στόχο την εξάντληση των υπολογιστικών πόρων τους και καθιστώντας τις υπηρεσίες/εφαρμογές τους μη διαθέσιμες στους νόμιμους χρήστες.
- **Επιθέσεις Επαναπρογραμματισμού (Reprogram Attacks)**: Εάν υπάρχει ελλιπής πρόβλεψη για μηχανισμούς ασφαλείας κατά τη διαδικασία του προγραμματισμού εφαρμογών και υπηρεσιών, ένας εισβολέας θα μπορεί πιο εύκολα να εκμεταλλευτεί κενά ασφαλείας των εφαρμογών και να επαναπρογραμματίσει από απόσταση οποιαδήποτε συσκευή IoT με κακόβουλες προθέσεις κώδικα.

3.3 Κατηγοριοποίηση Επιθέσεων Ασφαλείας

Πέρα από τις όποιες απαιτήσεις ασφαλείας υπάρχουν στα διάφορα μοντέλα αρχιτεκτονικής συστημάτων IoT, είναι σημαντικό να καταλάβουμε ποια είναι τα αδύναμα σημεία και ποιες επιθέσεις μπορούν να γίνουν στα διαφορετικά επίπεδα της στοίβας επικοινωνίας. Η αρχιτεκτονική της επικοινωνίας ενός συστήματος IoT χωρίζεται γενικά σε τρία επίπεδα: **Edge**, **Access** και **Application**. Στη συνέχεια θα παρουσιάσουμε μία ταξινόμηση των επιθέσεων που μπορούν να απειλούν τα συγκεκριμένα επίπεδα επικοινωνίας σε ένα σύστημα IoT.

3.3.1 Επιθέσεις στο Επίπεδο Άκρων (Edge Layer)

Μία από τις βασικές απειλές στο συγκεκριμένο επίπεδο αφορά στις επιθέσεις που γίνονται στα κανάλια επικοινωνίας μεταξύ των τερματικών συσκευών και αισθητήρων IoT και του οικοσυστήματος IoT. Ο στόχος που έχουν αυτές οι επιθέσεις είναι να γίνουν γνωστές πολλές πληροφορίες από την ανάλυση των μεταδιδόμενων σημάτων δεδομένων, όπως για παράδειγμα η κατανάλωση της ενέργειας, οι ηλεκτρομαγνητικές εκπομπές και ο συγχρονισμός της επικοινωνίας, ενώ οι κόμβοι ταυτόχρονα εκτελούν τις διαδικασίες της κρυπτογράφησης. Μεταξύ των παραπάνω που αναφέρθηκαν όταν καταναλώνεται ενέργεια στις συσκευές αυτή αξιοποιείται παντού για να προβλέψει και να ανακτήσει τα μυστικά στα κλειδιά κρυπτογράφησης. Για κάθε λειτουργία κρυπτογράφησης μπορεί να καταγραφεί και ένα ίχνος ισχύος. Σε αυτή τη περίπτωση τα δεδομένα της ισχύος υπολογίζονται από τη διαφορά της τάσης σε μία αντίσταση που έχει τοποθετηθεί σε σειρά με το τροφοδοτικό. Οι

απλές επιθέσεις ανάλυσης ισχύος επιδιώκουν να εξηγήσουν γρήγορα τα ίχνη ισχύος που διασυνδέονται με ένα μικρό αριθμό γύρων κρυπτογράφησης. Αντίθετα, όταν αναλύσουμε τη διαφορά ισχύος είναι μία αποτελεσματική και προηγμένη προσέγγιση. Εδώ πέρα ο μεγάλος αριθμός ιχνών αναλύεται στατιστικά έτσι ώστε να βγουν παραπάνω πληροφορίες που αφορούν την κρυπτογράφησης.

Στο επίπεδο των άκρων οι συσκευές IoT είναι επίσης ευαίσθητες όταν έχουμε επιθέσεις υλικού Trojan και Dos οι οποίες προσπαθούν να βάλουν μη διαθέσιμους πόρους στους νόμιμους χρήστες. Για παράδειγμα, αναγκάζουν μία συσκευή να μην συνεχίσει την κατάσταση αναστολής της λειτουργίας, δηλαδή τη χαμηλή κατανάλωση της ενέργειας της με στόχο να εξαντληθούν οι μπαταρίες τους ή για να παρεμποδίσουν τις ραδιοεπικοινωνίες. Επίσης ακόμη και το πακέτο της συσκευής μπορεί να παραβιαστεί έτσι ώστε να βγουν τα τροποποιητικά μυστικά της συσκευής τροποποιώντας το δικό της λογισμικό για να υπερασπιστεί έναν κακόβουλο κόμβο παλαιού τύπου, γνωστό και ως καμουφλάζ. Παράλληλα μπορεί να επιδιώξει την αντίστροφη μηχανική με σκοπό να κατανοήσει τις λεπτομέρειες των όσων πρωτοκόλλων επικοινωνίας έχουν ανακτηθεί και όσες πληροφορίες πιθανόν να έχουν δεσμευτεί(ως αλγόριθμοι που καλύπτονται από διπλώματα ευρεσιτεχνίας).

3.3.2 Επιθέσεις στο Επίπεδο Πρόσβασης (Access Layer)

Το επίπεδο πρόσβασης δίνει τη δυνατότητα για να υπάρξει σύνδεση με τον υπόλοιπο κόσμο που αυτό συνήθως γίνεται μέσω μίας συσκευής πύλης και ενός επιπέδου Middleware που λειτουργεί ως ενδιάμεσος μεταξύ του κόσμου του IoT και του κλασικού διαδικτύου. Στο συγκεκριμένο επίπεδο οι βασικές επιθέσεις είναι η υποκλοπή που ονομάζεται sniffing, η ένωση των δομών πακέτων και οι μη εξουσιοδοτημένες συνομιλίες. Ακόμη και οι επιθέσεις της δρομολόγησης πρέπει να έχουν τη δέουσα προσοχή. Ένας εισβολέας μπορεί να χρησιμοποιήσει το συγκεκριμένο είδος επίθεσης για να πλαστογραφεί, ανακατευθύνει, κατευθύνει λανθασμένα ή ακόμη και να απορρίψει τα πακέτα των δεδομένων.

3.3.3 Επιθέσεις στο Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογής έχει στις αρμοδιότητες του τις επικοινωνίες των δεδομένων και των υπηρεσιών του συστήματος IoT, οι επιθέσεις διαφέρουν αρκετά από τις προηγούμενες διότι σημαδεύουν απευθείας το λογισμικό που εκτελείται στις συσκευές και όχι την τεχνολογία της επικοινωνίας. Οι συγκεκριμένες επιθέσεις έχουν τη δυνατότητα να αντιμετωπίζουν την ακεραιότητα όπως για παράδειγμα στους αλγορίθμους μηχανικής μάθησης όπου ο εισβολέας έχει στην υπευθυνότητα του τη διαδικασία του να εκπαιδεύσει τον αλγόριθμο εκμάθησης για να προτείνει κακές συμπεριφορές. Την ίδια ώρα μπορεί να έχουμε και επιθέσεις στη φάση της σύνδεσης και του ελέγχου της ταυτότητας.

Ο Fremante και ο Scott και ο Mosenia και ο Jha έχουν παρουσιάσει μία εις βάθος ανάλυση όλων των συγκεκριμένων πτυχών όπου αναλύουν ορισμένες από τις βασικές ευπάθειες που αναλύθηκαν παραπάνω προτείνοντας λύσεις σε διαφορετικά επίπεδα από την πλευρά της συσκευής έως και τις υπηρεσίες του cloud. Βέβαια, οι πιθανές επιθέσεις εναντίον των συσκευών του IoT παρουσιάζονται από διαφορετική προσέγγιση δηλαδή εξετάζουμε το πως ένας εισβολέας μπορεί να αξιοποιήσει τη συσκευή του IoT για κακούς

και παράνομους σκοπούς. Παρακάτω, οι συγγραφείς θέτουν τέσσερις πιθανές προσεγγίσεις.

Παράβλεψη της λειτουργικότητας: Αυτός ο παράγοντας αφορά όλες τις επιθέσεις στις οποίες δεν είναι γνωστές οι συγκεκριμένες λειτουργίες της συσκευής IoT με αποτέλεσμα να γίνεται εκμετάλλευση μόνο της δυνατότητας της να συνδέεται στο τοπικό δίκτυο (LAN) ή στο Διαδίκτυο.

Μείωση της λειτουργικότητας: Εδώ πέρα ο εισβολέας επιδιώκει να σκοτώσει ή να μειώσει τις λειτουργίες που έχει η συσκευή για να απασχολήσει το θύμα ή ακόμη και να προκαλέσει σοβαρότερα προβλήματα σε ένα ευρύτερο σύστημα. Για παράδειγμα ο συγκεκριμένος τύπος επίθεσης ενδέχεται να αφορά συσκευές IoT, όπως τις έξυπνες τηλεοράσεις, ή τα έξυπνα ψυγεία με σκοπό να σταματήσει εντελώς ή να μειώσει τη λειτουργία τους έτσι ώστε να αποκτήσει χρήματα από το θύμα προκειμένου να αλλάξει την κακή του συμπεριφορά.

Κατάχρηση της λειτουργικότητας: Οι κανονικές λειτουργίες στις συσκευές IoT είναι για να προκαλέσουν προβλήματα σε αυτόν που τις κατέχει. Για παράδειγμα ένας εισβολέας μπορεί να προκαλέσει ζημιά σε μία μονάδα ελέγχου θέρμανσης, εξαερισμού και κλιματισμού (HVAC) και να τροποποιήσει ένα συγκεκριμένο περιβάλλον με δυσάρεστο τρόπο αυξάνοντας ή μειώνοντας υπερβολικά τις θερμοκρασίες. Με τον ίδιο τρόπο η επίθεση μπορεί να σημαδέψει ένα σύστημα έξυπνου φωτός με δυνατότητα ανακατεύθυνσης των φώτων στο δωμάτιο ή στο κτίριο, έτσι ώστε να αλλάξουν πλήρως οι εντολές των θυμάτων

Επέκταση της λειτουργικότητας: Η συσκευή του IoT χρησιμοποιείται για να επιτευχθούν εντελώς διαφορετικές λειτουργίες. Για παράδειγμα ένας αισθητήρας που έχει παρουσία σε ένα σύστημα του συναγερμού θα έχει τη δυνατότητα να αξιοποιηθεί για να επιβλέπεται η θέση των θυμάτων στο περιβάλλον που ζούνε ακόμη και όταν το συγκεκριμένο σύστημα είναι απενεργοποιημένο.

4. Παραδείγματα Προκλήσεων Ασφαλείας στο Πράσινο Διαδίκτυο των Πραγμάτων

4.1 Προκλήσεις ασφαλείας πράσινου IoT σε έξυπνες πόλεις

Το IoT έχει στόχο να πείσει τον κόσμο να πείσει τον κόσμο των μηχανών να ασχοληθεί πρωτίστως με την ευφυΐα μεταδίδοντας τις αισθήσεις αισθητήρων. Οι αισθήσεις και οι αισθητήρες μαζεύουν τα δεδομένα που αφορούν τις μηχανές ή τα συστήματα και η δουλειά τους είναι να τα μεταφράζουν ή να τα επεξεργάζονται. Όσα δεδομένα μαζεύονται μέσα από αυτούς τους αισθητήρες πρέπει να πηγαίνουν σε συγκεκριμένα κέντα επεξεργασίας και οι πληροφορίες που βγαίνουν έπειτα από την επεξεργασία θα πρέπει να επιστραφούν στις πληροφορίες του ενδιάμεσου λογισμικού. Η συνεχής ροή των δεδομένων που ξεκινά από τη παραγωγή μέχρι και το σημείο κατανάλωσης και αντίστροφα μπορεί να εξασφαλιστεί με έναν μηχανισμό ουράς και δρομολόγησης. Αυτή είναι μία κοινή πλατφόρμα που παρέχει έναν συγκεκριμένο μηχανισμό στη συγκέντρωση δεδομένων που είναι ένα από τα βασικότερα στοιχεία ενός ενδιάμεσου λογισμικού IoT όταν μιλάμε για τις έξυπνες πόλεις.

Στο ενδιάμεσο λογισμικό που έχει να κάνει με τις έξυπνες πόλεις είναι ένας κεντρικός κόμβος όπου τα συστήματα της κοινής ωφέλειας έχουν τη δυνατότητα να επικοινωνούν με τη δική τους παραγωγή, με κόμβους συλλογής δεδομένων και αισθητήρων μεταξύ τους για συγχρονισμένες λειτουργίες. Αυτό το ενδιάμεσο σύστημα συγκροτείται από συστήματα ανταλλαγής μηνυμάτων, από μία ουρά και από ένα σύστημα που δρομολογεί όλα τα δεδομένα σε μία ανάλυση πλατφόρμας και σε ένα σύστημα για να είναι ασφαλές. Από τα σημαντικά πλεονεκτήματα όταν χρησιμοποιούμε ενδιάμεσο λογισμικό που αφορά όλα τα συστήματα IoT σε μία έξυπνη πόλη είναι η χρησιμοποίηση υλικών για επικοινωνία και όσο μεγαλώνει το κόστος λειτουργιών και οι δημόσιες δαπάνες θα μειωθούν σε αντίθεση με τα πολλαπλά συστήματα end-to-end. Ο διαμοιρασμός των δεδομένων μεταξύ των συστημάτων είναι εύκολος, διαχειρίσιμος και καθοριστικός από την αρχή του ελέγχου με αυτή την πλατφόρμα.

4.2 Τι χρειάζεται μία έξυπνη πόλη από ένα οικοσύστημα πράσινου IoT;

- **Αυτονομία**: Μία πόλη μπορεί να γίνει έξυπνη στη περίπτωση που τα ετερογενή συστήματα κοινής ωφέλειας και τα υποσυστήματα της εντός μέσα στην έξυπνη πόλη έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους για μία ολοκληρωμένη λειτουργία. Για να γίνει αυτό χρειάζεται μία πλατφόρμα ενδιάμεσου λογισμικού.
- **Κεντρικός έλεγχος για τις Αρχές**: Οι Αρχές της έξυπνης πόλης θα πρέπει να ελέγχουν τα δεδομένα κεντρικά που περνούν μέσα από τα διάφορα βοηθητικά και τα υποσυστήματα. Θα πρέπει να έχουν τη δυνατότητα να παρακολουθούν τα δεδομένα που αποκτώνται και διαχειρίζονται τα συγκεκριμένα συστήματα. Επιπλέον, με βάση τις απαιτήσεις οι αρχές πρέπει να μπορούν να ταξινομούν τα δεδομένα όταν αυτά απαιτούνται από ένα σύστημα κοινής ωφέλειας σε ένα άλλο.

- **Μειωμένες Δαπάνες κεφαλαίου και λειτουργίες**: Ένα κοινό ενδιάμεσο λογισμικό που αφορά όλα τα συστήματα IoT σε μία έξυπνη πόλη θα μπορεί να μειώσει τις δαπάνες κεφαλαίου και τις λειτουργίες από τα μεμονωμένα αυτόνομα συστήματα. Η χρησιμοποίηση των υλικών και των πόρων από τους ανθρώπους μπορεί να μεγιστοποιηθεί με τη σύγκλιση όλων των συστημάτων σε ένα ενιαίο κεντρικό σημείο. Το συνολικό κόστος των αδειών για τη χρήση λογισμικού μπορεί πάλι να μειωθεί αν υπάρξει μία τέτοια καλή προοπτική.
- **Βιωσιμότητα και Διατηρησιμότητα**: Τα συστήματα σε μία έξυπνη πόλη που μεγαλώνουν με κριτήριο τη μεγάλη χρονική διάρκεια τους μπορούν να είναι αιώνια, επομένως η βιωσιμότητα και η συντηρησιμότητα είναι πολύ βασικό θέμα. Ένα ενδιάμεσο λογισμικό που είναι κεντρικά διαχειριζόμενο μπορεί να αντιμετωπίσει αυτό το ζήτημα σε μεγάλο βαθμό δίνοντας τη δυνατότητα να λειτουργεί όπως οι ενέργειες με βάση τον κανόνα που υπάρχει, την αυτόνομη λήψη των αποφάσεων και η ειδοποίηση σε πραγματικό χρόνο όσον αφορά την παρακολούθηση μίας συγκεκριμένης κατάστασης κ.λπ.
- **Ουδετερότητα του προμηθευτή**: Σε όλο το σύστημα που χρησιμοποιούμε το ενδιάμεσες λογισμικό που είναι χτισμένο πάνω στο πρωτόκολλο της ανοιχτής βιομηχανίας όλοι οι προμηθευτές των υποσυστημάτων είναι υποχρεωμένοι να ακολουθήσουν τα πρότυπα. Η συγκεκριμένη τακτική αναγκάζει τους προμηθευτές να ακολουθήσουν ένα ουδέτερο διαλειτουργικό οικολογικό σύστημα. Την ίδια ώρα θα υπάρχει επίπτωση και στο κόστος των συστημάτων.

4.3 Ποιες είναι οι λειτουργικές απαιτήσεις ενός οικοσυστήματος πράσινου IoT για μία έξυπνη πόλη;

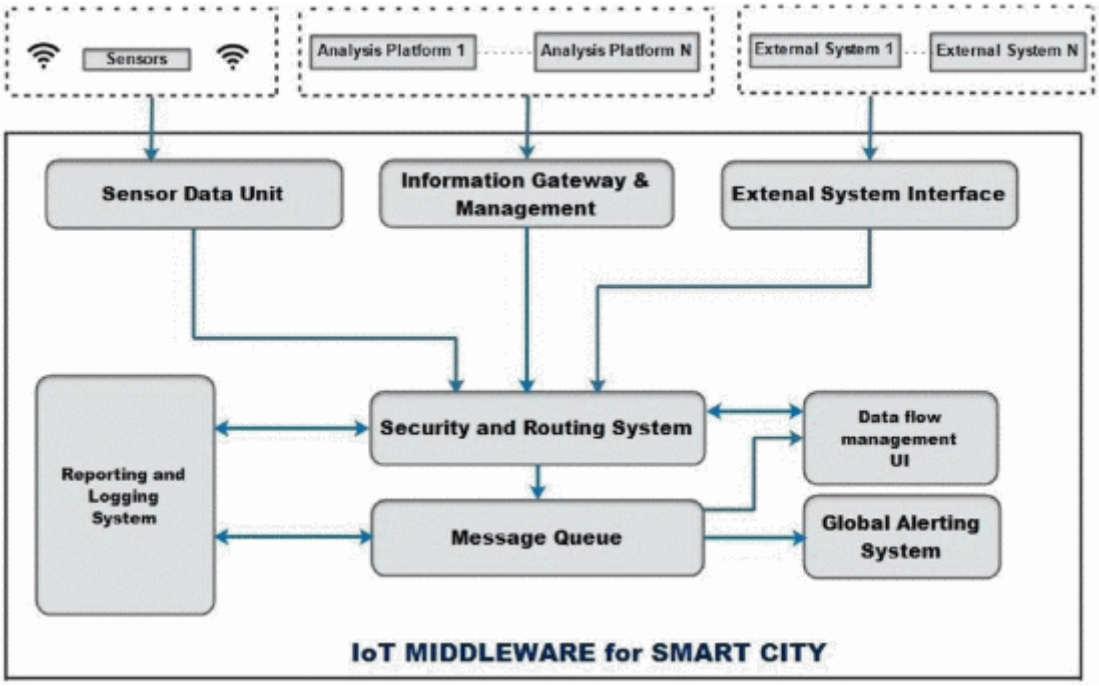
- **Ανοιχτή πύλη**: Το ενδιάμεσο λογισμικό είναι απαραίτητο να έχει μία πύλη που θα έχει τη δυνατότητα να δέχεται τα δεδομένα από διαφορετικά συστήματα που εκτελούν τα διαφορετικά πρωτόκολλα επιπέδου μεταφοράς ή εφαρμογής. Από αυτή την άποψη όσα πρωτόκολλα είναι κοινά από αυτό τον κλάδο θα πρέπει να συλλεχθούν για να μπορέσει να είναι δυνατή η ανενόχλητη ενσωμάτωση πολλών ετερογενών συστημάτων. Το μέσο επικοινωνίας μπορεί να είναι ένα δίκτυο Wi-Fi-Fiber που θα ανήκει σε όλη τη πόλη ή σε ένα σύστημα GPRS, αλλά και στις δύο αυτές καταστάσεις το ενδιάμεσο λογισμικό πρέπει να έχει τη δυνατότητα να ενσωματωθεί.
- **Ανοιχτό πρότυπο δεδομένων για επικοινωνία**: Τα συγκεκριμένα πρότυπα πρέπει να υποστηρίζονται όταν υπάρχουν απαιτήσεις διασύνδεσης και διαλειτουργικότητας γιατί είναι οι δύο μεγαλύτερες προκλήσεις που πρέπει να ξεπεράσει το IoT για να μπορέσει να αναπτυχθεί πλήρως σε πολύ μεγάλα έξυπνα περιβάλλονται. Εάν υπάρχει οποιοδήποτε πρότυπο ανοικτών δεδομένων σε οποιοδήποτε υποσύστημα θα πρέπει να εφαρμόζεται πλήρως.
- **Δρομολόγηση δεδομένων και δίαυλος των πληροφοριών**: Όλα τα δεδομένα που μαζεύονται από τους αισθητήρες ή τις συσκευές θα πρέπει να περάσουν μέσα από το ενδιάμεσο λογισμικό σε απαιτούμενα συστήματα που έχουν τεθεί για επεξεργασία. Το πέρασμα θα το αποφασίζουν οι αρχές βάση των εγκρίσεων που έχουν. Όσες πληροφορίες βγήκαν εντάξει από την επεξεργασία που έγιναν στα δεδομένα θα

πρέπει να καταλήγουν πίσω στο ενδιάμεσο λογισμικό για χρήση από οποιαδήποτε άλλο σύστημα είτε ίδιο είτε διαφορετικό που χρειάζονται αυτά τα δεδομένα. Η σημασία του διαύλου των πληροφοριών και των ανοιχτών δεδομένων έχει τη δυνατότητα να γίνει με αυτό το σκεπτικό δυνατή.

- **Τηλεπικοινωνιακή υποδομή**: Στην έξυπνη πόλη τα βοηθητικά συστήματα πρέπει να μπορούν να επικοινωνούν μεταξύ τους όταν μιλάμε για συγχρονισμένες λειτουργίες. Η αρχή της έξυπνης πόλης πρέπει να είναι σε θέση να οργανώνει τα δεδομένα και τις πληροφορίες στα απαιτούμενα υποσυστήματα ή στους χρήστες οπότε και με όποιον τρόπο χρειάζεται. Το μεσαίο λογισμικό οφείλει να μπορεί να συγχρονίζει την επικοινωνία μεταξύ των δύο διαφορετικών συστημάτων με διαφορετικές προσεγγίσεις όσον αφορά τη λειτουργία. Για παράδειγμα ένας γρήγορος παραγωγός δεδομένων και ένας αργός καταναλωτής στα δεδομένα.
- **Παρακολούθηση των σφαλμάτων σε πραγματικό χρόνο ή σε ένα σύστημα αυτόματης ανάδρασης**: Οι αισθητήρες ή συσκευές πρέπει να επιβλέπονται συνεχώς για να μπορούν αυτόματα να αναγνωρισθούν τα ελαττωματικά. Η ελαττωματική συσκευή μπορεί να εντοπιστεί είτε από την πλατφόρμα ανάλυσης, είτε από το ενδιάμεσο λογισμικό και να μπορεί να κοιτάζει τη ροή των μηνυμάτων που πηγαίνουν από τους αισθητήρες και φτάνουν στο ενδιάμεσο λογισμικό. Όταν εντοπίσουμε το πρόβλημα το σύστημα οφείλει να δώσει αναφορά στη πλατφόρμα όσον αφορά την κατάσταση και θα πρέπει να το ενημερώσει όταν γίνεται ανάκτηση.
- **Αυτόματη ειδοποίηση και συντήρηση**: Οι ειδοποιήσεις που πρέπει να παράγει το σύστημα πρέπει να είναι αυτόματες από τη στιγμή που η συσκευή έχει βγει από τη θέση με γεωγραφική υπόδειξη εάν κάποιος από τους αισθητήρες ή το σύστημα γίνει ελαττωματικό.
- **Σύστημα ανταλλαγής μηνυμάτων που αφορά πολλούς ενδιαφερόμενους**: Οι ειδοποιήσεις και τα μηνύματα που βγαίνουν αυτόματα θα πρέπει να έχουν κατεύθυνση προς τους σωστούς παραλήπτες. Τα μηνύματα θα χρειάζεται να αλλάξουν για να σταλούν από τα πολλαπλά μέσα με κριτήριο πάντα τη προτεραιότητα και τη κρισιμότητα που υπάρχει για να οριστεί αυτό το μήνυμα. Θα είναι απαραίτητο να υπάρχει ένα αρχείο που θα κρατάει μία λίστα με όσα μηνύματα θα περνούν μέσα από το ενδιάμεσο λογισμικό. Π.χ. Όταν υπάρχει ενημέρωση για τσουνάμι θα πρέπει να αναφέρεται στο κοινό, ενώ αντίθετα η ειδοποίηση για το ελαττωματικό φως θα πρέπει να πηγαίνει στον κοντινότερο ηλεκτρολόγο.
- **Αναφορές**: Οι Αυτοματοποιημένες αναφορές με βάση τα διάφορα συμβάντα που θα δημιουργεί το σύστημα θα πρέπει να δημιουργούνται με κριτήριο τα διάφορα συμβάντα και τα αρχεία καταγραφής των δεδομένων που υπάρχουν για να καλύπτουν τις απαιτήσεις και τις ανάγκες μίας έξυπνης πόλης. Θα ήταν καλό να υπάρχει μία διάταξη για να δημιουργηθούν δυναμικές αναφορές.

4.4 Αρχιτεκτονική οικοσυστήματος πράσινου IoT σε έξυπνες πόλεις

Η αρχιτεκτονική που αφορά το οικοσύστημα πράσινου IoT σε μία έξυπνη πόλη αποτυπώνεται χαρακτηριστικά στην παρακάτω εικόνα:



Εικόνα 14. Αρχιτεκτονική IoT για μια Έξυπνη Πόλη [7]

Τα βασικά στοιχεία από τα οποία αποτελείται το ενδιάμεσο λογισμικό ενός οικοσυστήματος πράσινου IoT για μία έξυπνη πόλη IoT είναι τα εξής:

1) **Πύλη**: Αυτή είναι το σημείο εισόδου στο σύστημα. Όσα δεδομένα που αποκτώνται μέσα από το σύστημα και πρωτίστως οι αισθητήρες, ή οι μονάδες ελέγχου στέλνουν τα δεδομένα στη πύλη. Από εκεί αυτή θα σχεδιαστεί για να επεξεργάζεται σωστά τον τεράστιο αριθμό πολλών συνδέσεων και τα όποια κινούμενα δεδομένα υπάρχουν χρησιμοποιώντας το μικρότερο δυνατό υλικό. Η πύλη θα στείλει πίσω ότι μπορεί να τα αναγνωρίσει στα συστήματα αναφοράς με το τι κατάσταση υπάρχει στα δεδομένα κάθε φορά. Όσα δεδομένα θα έρχονται θα έχουν πληροφορίες ταυτότητας για το σύστημα. Τα πρωτόκολλα που αναφέρονται στο επίπεδο πύλης για την υποστήριξη είναι:
   - MQTT
   - HTTPS
   - HTTP
   - Cap

   Η πύλη θα έχει τη δυνατότητα να συνδέει τα δεδομένα χρησιμοποιώντας πολλούς τύπους δεδομένων. Υπάρχει μία μονάδα δεδομένων των αισθητήρων που λαμβάνει δεδομένα από αισθητήρες και ελεγκτές όπως για παράδειγμα η εξωτερική διεπαφή για τη δρομολόγηση των δεδομένων από ένα εξωτερικό σύστημα μέσω των υπηρεσιών web στο ενδιάμεσο λογισμικό που θα μπορεί να χρησιμοποιηθεί από οποιοδήποτε εσωτερικό υποσύστημα. Ένας δίαυλος πληροφοριών στον οποίο θα βρίσκεται όλο το υποσύστημα και θα έχει τη δυνατότητα να μπορεί να δημοσιεύει τις επεξεργασίες πληροφορίας έτσι ώστε ένα τελείως διαφορετικό σύστημα ακόμη και ίδιο θα μπορεί να το χρησιμοποιήσει από τη στιγμή που έχει πάρει την κατάλληλη έγκριση. Στο Gateway θα βρίσκεται επίσης το πρώτο επίπεδο ασφάλειας όπως η

επαλήθευση των πιστοποιητικών SSL, το τείχος προστασίας, τα ACLs, το DoS Mitigation και το Σύστημα Πρόληψης Εισβολής στο επίπεδο κέντρου δεδομένων. Από τη στιγμή που μιλάμε για μία κοινή πλατφόρμα όλη η υποδομή θα μπορεί να διαμοιράζεται σε όλα τα έργα.

2) **Ασφάλεια**: Το κομμάτι της ασφάλειας που ορίστηκε για το ενδιάμεσο λογισμικό IoT έχει τη δυνατότητα να χρησιμοποιεί την υποδομή του δημόσιου κλειδιού και τον μηχανισμό SASL με σκοπό να προσφέρει τα επιθυμητά επίπεδα ασφάλειας. Αυτό το πλαίσιο με την ασφάλεια έχει τα παρακάτω βασικά στοιχεία:
   - Η Αρχή της έκδοσης του πιστοποιητικού για τη διαχείριση του πιστοποιητικού των στοιχείων των πελατών
   - Η Μονάδα ελέγχου ταυτότητας για να πιστοποίει το πελάτη

   Ο έλεγχος της ταυτότητας χρησιμοποιεί Ψηφιακά Πιστοποιητικά τα οποία εκδίδονται από την Αρχή των πιστοποιητικών. Η εμπιστευτικότητα των δεδομένων δίνεται με κρυπτογράφηση των δεδομένων όταν αυτά αποθηκεύονται και μεταφέρονται. Η ακεραιότητα στα δεδομένα συμβαίνει με υπογραφή των μηνυμάτων. Για να γίνει η κρυπτογράφηση των δεδομένων στην ουρά των πληροφοριών με τη χρήση συμμετρικού κλειδιού υπάρχει η ανταλλαγή μετά τον έλεγχο που έχει γίνει στη ταυτότητα του χρήστη. Η συγκεκριμένη διαδικασία εξασφαλίζει ότι το συμμετρικό κλειδί πηγαίνει σε πιστοποιημένους πελάτες. Το συγκεκριμένο πλαίσιο δίνει τα ακόλουθα τρία επίπεδα ασφαλείας σχετικά με τα δεδομένα που περνούν μέσα από το ενδιάμεσο λογισμικό IoT:
   - Επίπεδο 0: Εδώ τα δεδομένα μεταδίδονται σαν απλό κείμενο
   - Επίπεδο 1: Πάλι τα δεδομένα μεταδίδονται σαν απλό κείμενο, αλλά πρώτα εξασφαλίζεται ότι υπάρχει η ανταποδοτικότητα επαλήθευση της ταυτότητας μεταξύ των αποστάσεων και των πελατών
   - Επίπεδο 2: Πριν τη μετάδοση τα δεδομένα κρυπτογραφούνται μαζί με τον αμοιβαίο έλεγχο ταυτότητας που γίνεται μεταξύ του αποστολέα και του πελάτη. Στο συγκεκριμένο επίπεδο τα δεδομένα είναι δυνατό να κρυπτογραφηθούν με AES 256 και AES 128

   Σχετικά με την οποιαδήποτε συναλλαγή των δεδομένων από το ενδιάμεσο λογισμικό υπάρχουν οι παρακάτω ενέργειες:
   - Εγγραφή χρήστη
   - Ο έλεγχος της ταυτότητας και της ανταλλαγής κλειδιών
   - Επικοινωνία των δεδομένων

3) **Δρομολόγηση**: Σύμφωνα με τις πληροφορίες της ταυτότητας, αυτό το υποσύστημα θα στείλει το πακέτο των δεδομένων στο προορισμό που έχει τεθεί. Όσα δεδομένα φτάσουν στο συγκεκριμένο σύστημα θα μπορούν να κρυπτογραφούνται με κριτήριο το επίπεδο ασφαλείας που θα έχει προσδιοριστεί από το υποσύστημα της ασφάλειας. Το σύστημα δρομολόγησης θα περιέχει ένα σύνολο από ουρές που θα δημοσιεύον τα δεδομένα σε ουρές τις οποίες θα έχει υπό τη διαχείριση το σύστημα της ανταλλαγής των μηνυμάτων.

4) **Ουρά μηνυμάτων**: Το συγκεκριμένο στοιχείο είναι ένα σύστημα που προωθεί τα δεδομένα τα οποία έχουν κατεύθυνση προς τον προορισμό. Ο προορισμός συνήθως είναι μία πλατφόρμα ανάλυσης που χρησιμοποιεί τα δεδομένα τα οποία έχουν τεθεί για ανάλυση. Από την άλλη η ούρα θα έχει τη δυνατότητα για συνεχή μετάδοση και για να μεταδίδει τα δεδομένα με βάση τη συγκεκριμένη προδιαγραφή. Επίσης θα έχει τη δυνατότητα να επιλέξει προσωρινά να αποθηκεύσει τα δεδομένα στη περίπτωση συστημάτων με διαφορετική ταχύτητα από αυτή που επεξεργάζεται, όπως για παράδειγμα ένας γρήγορος παραγωγός των δεδομένων και ένας αργός καταναλωτής. Το συγκεκριμένο σύστημα θα έχει τη δυνατότητα ενός μηχανισμού ανακατεύθυνσης γιατί στη περίπτωση που κάποιος καταναλωτής αποτύχει, το σύστημα θα είναι σε θέση να ρυθμιστεί με σκοπό να βρεθεί μία άλλη ευκολότερη διαδρομή προς τον προορισμό.

5) **Διαχείριση ροής δεδομένων διεπαφής χρήστη**: Η διεπαφή χρήστη (User Interface) που υπάρχει στο σύστημα είναι για να μπορεί ένας χρήστης να αλλάξει το σύστημα με τον τρόπο που θέλει το σύστημα. Αυτή η αλλαγή θα αφορά στις ρυθμίσεις της ασφάλειας, στη δρομολόγηση δεδομένων, στην επιλογή ανακατεύθυνσης, στη προτεραιότητα κ.λπ. Ο διαχειριστής θα έχει τη δυνατότητα μέσω της διεπαφής του χρήστη να το τροποποιήσει χωρίς προβλήματα το σύστημα. Αυτή η διεπαφή θα εμφανίζει παράλληλα έναν πίνακα εργαλείων που θα παρουσιάζει όλη τη πορεία του συστήματος, αλλά και την απόδοση όσων ουρών δεδομένων υπάρχουν στο σύστημα. Τέλος παρέχεται η επιλογή του να διαχειριζόμαστε και να καθορίζουμε συγκεκριμένες ουρές μηνυμάτων που θα διαμορφώνουν το σύστημα.

6) **Σύστημα Αναφορών και Καταγραφής**: Ο συγκεκριμένος τομέας έχει υπό την επίβλεψη του την αναφορά και την καταγραφή της κατάστασης όσον αφορά τα σφάλματα που υπάρχουν στο σύστημα. Οι οποιεσδήποτε αστοχίες στο σύστημα θα εντοπίζονται και θα αναφέρονται στους διαχειριστές αλλά και σε οποιουσδήποτε άλλους χρήστες έχουν εξουσιοδότηση. Το σύστημα θα έχει τη δυνατότητα να ανταλλάξει τα μηνύματα SMS που παρέχονται από τα SMS, από τα email και από τις εφαρμογές των κινητών στους διαχειριστές των συστημάτων. Η αναφορά που θα γίνεται και η καταγραφή θα μπορούν να τροποποιηθούν με τη επαφή του χρήστη που διαχειρίζεται το σύστημα.

7) **Εργαλειοθήκη**: Εδώ πέρα είναι ένας ολόκληρος πίνακας εργαλείων που ικανοποιεί όλες τις απαιτήσεις του μεσαίου εξοπλισμού. Ο πίνακας των εργαλείων θα έχει από όλο το υποσύστημα γραφικές παραστάσεις που θα δείχνουν το πως πηγαίνει σε πραγματικό χρόνο. Επίσης, αποτελεί διάφορες τακτικές του ενδιάμεσου λογισμικού όπως τον Αριθμό υποσυστημάτων που βρίσκονται τη συγκεκριμένη στιγμή στο σύστημα, αλλά και από ουρές από αριθμούς που έχει το σύστημα, την κατάσταση της κάθε ουράς στα συστήματα που τη καταναλώνουν σε κάθε περίπτωση, τον ρυθμό που προχωρούν τα δεδομένα, τη χρήση του συστήματος, τους συνδέσμους που αφορούν τις διεπαφές του χρήστη, τους πίνακες εργαλείων κ.λπ.

8) **Λεωφόρος Πληροφοριών**: Σε όλα τα υποσυστήματα προτείνεται το να δημοσιεύουμε όλα τα επεξεργασμένα δεδομένα και τις πληροφορίες στο ενδιάμεσο λογισμικό, ώστε να μπορούν να χρησιμοποιηθούν από άλλους χρήστες ή από άλλα υποσυστήματα. Κάθε σύστημα που χρειάζεται δεδομένα από τα άλλα υποσυστήματα πρέπει να πάρει την έγκριση από τις αρχές για να μπορέσει να αξιοποιήσει τα δεδομένα του σε πραγματικό χρόνο μέσω του ενδιάμεσου λογισμικού έχοντας τους κατάλληλους ελέγχους ταυτότητας όσον άφορα την ασφάλεια. Με αυτόν τον τρόπο το ενδιάμεσο λογισμικό θα έχει έναν δίαυλο για τις πληροφορίες που περιέχονται εκεί πέρα όσες έχουνε επεξεργαστεί από όλα τα υποσυστήματα και θα μπορούν να είναι σε θέση να αξιοποιηθούν από κάθε χρήστη. Εάν παρθεί η απόφαση για να είναι διαθέσιμα στο κοινό μπορούν να γίνουν Ανοιχτά δεδομένα.

9) **Σύστημα Έγκαιρης Προειδοποίησης**: Σε μία έξυπνη πόλη υπάρχει μία ομάδα που είναι υπεύθυνη για τον χειρισμό των ειδοποιήσεων και για τις έκτακτες ανάγκες που παρέχονται από όλα τα υποσυστήματα. Συνεπώς για όλα τα υποσυστήματα στις έξυπνες πόλεις είναι απαραίτητη η χρήση μίας κοινής πλατφόρμας που θα αναφέρει τις ειδοποιήσεις και τιε καταστάσεις της έκτακτης ανάγκης που θα φτάνουν στο εκάστοτε άτομο που τις έχει υποβάλλει με τον τρόπο που έχει διαμορφωθεί το σύστημα. Θα υπάρχει ένας μηχανισμός που θα χειρίζεται τις προειδοποιήσεις στα πολλά επίπεδα και μέσα από αυτόν οι ειδοποιήσεις και οι προειδοποιήσεις θα μπορούν να πηγαίνουν από το κάθε υποσύστημα στους υπεύθυνους που τις απαντούν και θα τις παρουσιάζουν στο ευρύ κοινό. Π.χ. Μία διαρροή στο σύστημα που μοιράζει το νερό θα ειδοποιεί τις αρμόδιες υπηρεσίες και η προειδοποίηση για το τσουνάμι θα φτάνει στο ευρύ κοινό.

5. Μηχανισμοί Ασφάλειας στο Πράσινο Διαδίκτυο των Πραγμάτων

Όταν αναφερόμαστε σε μία εφαρμογή IoT αυτή περιλαμβάνει τη σύζευξη πολλών τεχνολογιών, συσκευών, τοποθεσιών και υποδομών. Για οποιοδήποτε σύστημα IoT πάντα ελλοχεύει ο κίνδυνος να εκτεθεί και να παραβιαστεί αν δεν τηρηθούν συγκεκριμένα μέτρα και μηχανισμοί ασφαλείας. Ορισμένες από τις παραμέτρους που πρέπει να ληφθούν υπόψιν για την ενίσχυση της ασφάλειας και της αξιοπιστίας ενός συστήματος IoT (που κάποια από αυτά απέκτησαν δημοτικότητα με τα χρόνια), είναι η εμπιστευτικότητα, η ακεραιότητα, η αποδοτικότητα, το κόστος, κλπ.

5.1 Σύγχρονες Τεχνολογίες για τις Προκλήσεις Ασφαλείας στο IoT

Σχετικά με την ενίσχυση της ασφάλειας σε ένα οικοσύστημα πράσινου IoT μπορούν να αξιοποιηθούν διάφορες σύγχρονες τεχνολογίες όπως, η τεχνολογία blockchain, η υπολογιστική νέφους (cloud computing), η μηχανική μάθηση (machine learning), η υπολογιστική νέφους (cloud computing), η υπολογιστική ομίχλης (fog computing) και η υπολογιστική άκρων (edge computing).

5.1.1 Τεχνολογία Blockchain για τις Προκλήσεις Ασφαλείας στο IoT

Στη σημερινή εποχή το IoT δεν μας έχει επηρεάσει μόνο προσωπικά αλλά και επαγγελματικά με τη μεγέθυνση των συσκευών που είναι πάντα συνδεδεμένες με τη δημιουργία μεγάλων δεδομένων. Η τεχνολογία blockchain αποτελεί μια απάντηση στις προκλήσεις ασφαλείας που αντιμετωπίζουν τα συστήματα IoT παρέχοντας λειτουργίες όπως την αποτροπή διπλών δεδομένων, την παρακολούθηση δεδομένων με αισθητήρες και τη μεταφορά δεδομένων με ασφαλή τρόπο. Συμπερασματικά, η τεχνολογία blockchain είναι νέα τεχνολογία, διαρκώς εξελισσόμενη, που μπορεί να προσφέρει καθολική προστασία στα δεδομένα των συστημάτων IoT από επιθέσεις, γιατί συνδυάζει τη χρήση διαφορετικών τεχνικών κρυπτογράφησης. Τα πλεονεκτήματα μεταξύ του συνδυασμού IoT και της τεχνολογίας blockchain είναι τα ακόλουθα:

- Σε περίπτωση βλάβης ή προσπάθειας παραβίασης της ασφάλειας σε κάποιο τμήμα του συστήματος IoT, λόγω του τρόπου λειτουργίας της τεχνολογίας blockchain δεν επηρεάζεται ολόκληρο το σύστημα IoT, αλλά απομονώνεται το μπλοκ που αντιμετωπίζει το πρόβλημα και λαμβάνονται τα κατάλληλα αντίμετρα.
- Η τεχνολογία blockchain έχει τη δυνατότητα να εφαρμοστεί σε κάθε επίπεδο του IoT που σημαίνει ότι είναι μία κατάλληλη λύση για την ασφαλή μεταφορά και αποθήκευση των δεδομένων.
- Μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα του blockchain. Ακόμη και αν παραβιαστεί ένας κόμβος του συστήματος IoT, δεν μπορεί να παραβιαστεί το περιεχόμενο των δεδομένων του, καθώς τα μπλοκ δεδομένων είναι κρυπτογραφημένα με ισχυρά κλειδιά και ασφαλείς μηχανισμούς κρυπτογράφησης.
- Οι κρυπτογραφικές συναρτήσεις hash χρησιμοποιούνται για την εγγραφή των δεδομένων που κυκλοφορούν ανάμεσα στους κόμβους αντί να αποθηκεύονται στο

κεντρικό διανομέα cloud που έχει ως στόχο το δίκτυο peer-to-peer να στοχοποιηθεί λιγότερο από τις κυβερνοεπιθέσεις.

5.1.2 Τεχνολογίες Μηχανικής Μάθησης για τις Προκλήσεις Ασφαλείας στο IoT

Η Μηχανική Μάθηση (Machine Learning) αποτελεί ένα κλάδο της Τεχνητής Νοημοσύνης (Artificial Intelligence) που αναπτύσσεται διαρκώς και αξιοποιείται ολοένα και περισσότερο σε σύγχρονα συστήματα κι εφαρμογές, μεταξύ των οποίων και στο IoT. Σε αυτή τη περίπτωση ένα σύστημα IoT έχει τη δυνατότητα να μάθει και να βελτιωθεί από την εμπειρία, ανεξάρτητα από το γεγονός πως δεν έχει προγραμματιστεί σκόπιμα για να κάνει κάτι τέτοιο. Ένα από τα πιο δημοφιλή παραδείγματα είναι το siri που χρησιμοποιεί προηγούμενες τεχνικές μηχανικής μάθησης. Μερικά από τα πλεονεκτήματα του συνδυασμού IoT με μηχανική μάθηση είναι ότι:

- Το κόστος μπορεί να μειωθεί, το ίδιο η εξυπηρέτηση πελατών και η αποτελεσματικότητα και η βελτιωμένη κατανάλωση ενέργειας μπορεί να διατηρηθεί χρησιμοποιώντας ιδιότητες μηχανικής μάθησης.
- Ο αυτοματισμός είναι ένα από τα σημαντικότερα πλεονεκτήματα που μπορεί και βοηθούν σε μεγάλο βαθμό. Για παράδειγμα, ο κύριος υπολογιστής ενός αυτοκινήτου μπορεί να ενσωματωθεί με μηχανική μάθηση που θα μπορεί να μάθει μόνο του την οδήγηση και οι επικίνδυνες καταστάσεις βοηθούν εύκολα στην εμπλοκή συστημάτων ασφαλείας όταν χρειάζεται.
  Ο ρυθμός ψευδούς συναγερμού και το μέσο ποσοστό σφάλματος μπορούν να ελαχιστοποιηθούν και η ακρίβεια και η ταξινόμηση της ανίχνευσης μπορεί να αυξηθεί με την αποφυγή επιθέσεων πλαστογράφησης χρησιμοποιώντας διάφορες τεχνικές μάθησης κυρίως

5.1.3 Υπολογιστική Ομίχλης και Νέφους για τις Προκλήσεις Ασφαλείας στο IoT

Η Υπολογιστική Ομίχλης (Fog Computing) μαζί με την Υπολογιστική Νέφους (Cloud Computing) αποτελούν δύο από τις πιο ισχυρές και ανεξάρτητες τεχνολογίες του IoT. Έχοντας το IoT μπορεί κάποιος να αποκτήσει πλεονέκτημα με τη χρήση και τη λειτουργία έξυπνων εφαρμογών και με το σύννεφο (cloud) υπάρχει απεριόριστος χώρος και λειτουργία που σχετίζονται με τη διαχείριση αποθήκευσης και επεξεργασίας των δεδομένων. Το IoT είναι μία ετερογενής σύμπτυξη διαφόρων συσκευών, υπηρεσιών και τεχνολογιών που παρέχουν πλούσια δεδομένα όλο το 24ωρο, συνεπώς υπάρχει χώρος που συντονίζει τα πολλά δεδομένα.

Με την πάροδο του χρόνου έγινε αντιληπτό ότι το Cloud Computing δεν μπορούσε να παρέχει μεγάλα οφέλη σε συστήματα IoT, όποτε δημιουργήθηκε το Fog Computing για να στηρίξει το Cloud Computing και να ξεπεράσει τα όποια μειονεκτήματά του. Ορισμένα από τα οφέλη της ενσωμάτωσης το Fog Computing σε συστήματα IoT είναι τα εξής:

- Όταν υπάρχει επίθεση στο σύστημα του IoT να πρέπει να πάει μέσα από το στρώμα υπολογιστικής ομίχλης όπου θα μπορεί να εντοπιστεί η επίθεση και το θύμα. Στο συγκεκριμένο επίπεδο εκτελείται το έργο ενός μεσάζοντα μεταξύ του τελικού χρήστη και του συστήματος υπολογιστικής ομίχλης ή νέφους.

- Η δυνατότητα του να αποθηκεύονται τα δεδομένα σε κόμβους ομίχλης, έναντι συσκευών των χρηστών έχει μειώσει τον κίνδυνο επιθέσεων σε μεγάλο βαθμό.
- Υπάρχει η δυνατότητα διευκόλυνσης που προσφέρει ο υπολογιστής ομίχλης που μπορεί να βοηθήσει στην ανακάλυψη οποιουδήποτε κακόβουλου λογισμικού και στην αντιμετώπιση του προβλήματος κατά τη διαδικασία, δημιουργώντας μία συσκευή κάθε φορά που υπάρχει μία αίσθηση
- Οι πληροφορίες από μερικούς χρήστες κοινοποιούνται με τον κόμβο ομίχλης και όχι του συνολικού δικτύου, άρα οι πιθανότητες για υποκλοπή μειώνονται δραστικά, διότι η κίνηση στο δίκτυο καταρρίπτεται.

5.1.4 Υπολογιστική Άκρων (Edge computing) για τις Προκλήσεις Ασφαλείας στο IoT

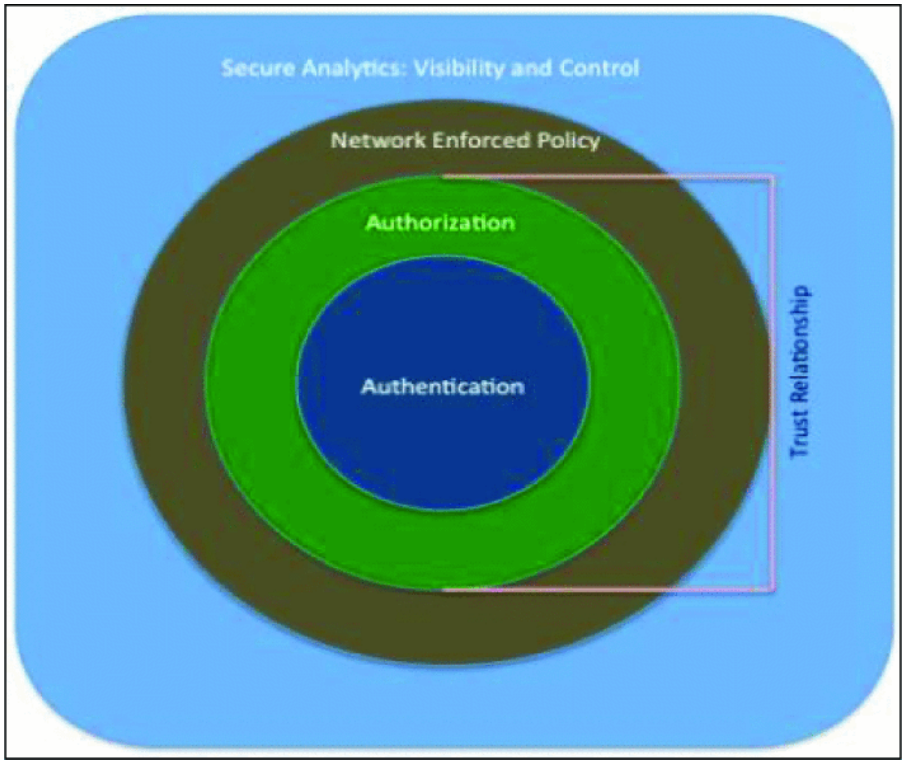
Ο κύριος στόχος του υπολογιστή των άκρων είναι να εξοικονομηθεί το εύρος ζώνης του δικτύου και να βελτιωθεί ο χρόνος απόκρισης που αφορά την αποθήκευση δεδομένων και υπολογισμού πολύ πιο κοντά στη θέση. Ο υπολογισμός είναι σχεδόν παρόμοιος με το cloud computing αλλά η βασική διαφορά είναι ότι το edge λειτουργεί ως ενδιάμεσος μεσολαβητής μεταξύ του cloud και του χρήστη. Το ίδιο ισχύει και για το σύννεφο που βρίσκεται σε μία μακρινή τοποθεσία από τον τελικό χρήστη με τη πολυπλοκότητα και τον υπολογισμό να αυξάνονται και άρα να τοποθετείται ένας διακομιστής άκρων μεταξύ των δύο, με σκοπό όλη η επεξεργασία να μπορεί να προχωρήσει στην άκρη για να είναι πιο κοντά στον χρήστη. Κάποιες θετικές επιδράσεις που έχουν οι εφαρμογές υπολογιστικών ακρών IoT είναι:

- Η διαδικασία της σύνταξης και στοίβας των δεδομένων μπορεί να γίνει εύκολα στην άκρη και μόνο όσα δεδομένα είναι απαραίτητα μπορούν να σταλούν στο cloud για να εξοικονομηθεί κόστος εύρος ζώνης
- Όταν το συγκρίνεις με την ομίχλη όπου υπάρχει η δυνατότητα μετακίνησης δεδομένων, ενώ είναι στη μετάδοση αποτρέπεται καθώς τα δεδομένα υποβάλλονται σε επεξεργασία στο τοπικό διαδίκτυο ή εντός της ίδιας της συσκευής.
- Support Vector Μηχανήματα (SVM), διανεμημένα Frank Wolfe (dfW) κ.λπ.

5.2 Προτεινόμενοι μηχανισμοί ασφάλειας στο Πράσινο IoT

Όταν αντιμετωπίζουμε ένα περιβάλλον πολύ διαφορετικά για τις προκλήσεις ασφαλείας του IoT είναι σημαντικό να υπάρχει μία εύκολη αρχιτεκτονική που θα παρέχει ασφάλεια. Τον τελευταίο καιρό πολλά πλαίσια και πρότυπα του IoT έχουν αναπτυχθεί με στόχο να προασπιστούν τα συμφέροντα του προγράμματος σχεδιάζοντας παράλληλα προϊόντα που θα συμβαδίζουν με τις πολλές ανάγκες που έχουν οι καταναλωτές. Η παρακάτω εικόνα έχει ένα πλαίσιο που προωθεί την ασφάλεια στο περιβάλλον του IoT και αυτή αποτελείται από τέσσερα στοιχεία:

- Πιστοποίηση Ταυτότητας – Αυθεντικοποίηση (Authentication)
- Εξουσιοδότηση (Authorization)
- Επιβολή Πολιτικής Δικτύου (Network Enforced Policy)
- Ασφαλής Ανάλυση: Ορατότητα και Έλεγχος



Εικόνα 15. Πλαίσιο Ασφαλείας στο οικοσύστημα IoT [7]

5.2.1 Πιστοποίηση Ταυτότητας - Αυθεντικοποίηση

Ο πυρήνας της αρχιτεκτονικής είναι το επίπεδο ελέγχου ταυτότητας που το χρειαζόμαστε για να επιβεβαιώσει τις πληροφορίες έτσι ώστε να είμαστε σε θέση να αναγνωρίσουμε μία οντότητα IoT. Αυτό το πετυχαίνουν όταν οι συσκευές χρειάζονται πρόσβαση στην υποδομή του IoT, δηλαδή να κερδίσουμε την εμπιστοσύνη. Η αποθήκευση και η παρουσία της πληροφορίες μπορεί να είναι κάθε φορά διαφορετική ανάλογα με το τι συσκευή IoT έχουμε. Αυτές οι συσκευές πρέπει να εξασφαλίζει ότι είναι αληθινές με τον τρόπο που δεν θα αποσυντονίζουν την ύπαρξη των ανθρώπων. Παραδείγματα τέτοιων τρόπων είναι η αναγνώριση των ραδιοσυχνοτήτων RFID, το κοινό απόρρητο, τα πιστοποιητικά X.509, η διεύθυνση MAC του τελικού σημείου η ακόμη και με μία βάση δεδομένων που στηρίζεται στο υλικό.

5.2.2 Εξουσιοδότηση

Το δεύτερο επίπεδο αυτής της αρχιτεκτονικής ασφαλείας είναι η εξουσιοδότηση που ο ρόλος της είναι να ελέγχει το ποιοι έχουν πρόσβαση σε μία συσκευή μέσα στο διαδίκτυο. Το συγκεκριμένο επίπεδο στηρίζεται στο επίπεδο ελέγχου στη ταυτότητα που χρησιμοποιεί τις συγκεκριμένες πληροφορίες όσον αφορά την οντότητα του δηλαδή το που βρίσκεται ο κάθε χρήστης. Έχοντας τα στοιχεία του ελέγχου της ταυτότητας και των εξουσιοδοτών καλλιεργείται η εμπιστοσύνη ανάμεσα στις συσκευές IoT στην ανταλλαγή των πληροφοριών. Π.χ. Ένα αυτοκίνητο μπορεί να έχει αξιόπιστη σύνδεση με ένα άλλο από τον ίδιο πωλητή. Η συγκεκριμένη σχέση εμπιστοσύνης μπορεί να επιτρέψει στα αυτοκίνητα να ανταλλάξουν διάφορους τρόπους για την ασφάλεια. Εφόσον δημιουργήσει μία ασφάλεια στη σύνδεση μεταξύ του μηχανήματος και της εταιρείας που αγοράστηκε δίνει τη

δυνατότητα στο ίδιο το μηχάνημα να βάζει επιπλέον πληροφορίες όπως για παράδειγμα για την μέτρηση των χιλιομέτρων η το πότε συντηρήθηκε τελευταία φορά (service). Το καλό που προκύπτει στην όλη υπόθεση είναι πως οι μηχανισμοί που διαχειρίζονται και ελέγχουν την πρόσβαση στα καταναλωτικά και εταιρικά δίκτυα έχουν προσαρμοστεί στις ανάγκες που έχει το IoT. Έπειτα υπάρχει μία αρχιτεκτονική που έχει τη δυνατότητα να διαχειρίζεται δισεκατομμύριο συσκευές IoT με ένα σωρό τρόπους εμπιστοσύνης και αυτή είναι η μεγαλύτερη πρόκληση που προκύπτει. Παράλληλα εφαρμόζονται διάφορες μέθοδοι της κυκλοφορίας που γίνεται σε όλο το δίκτυο για να ξεχωρίζουμε τη κίνηση στα δεδομένα και τον τρόπο που επικοινωνούν από άκρο σε άκρο.

5.2.3 Επιβολή Πολιτικής Δικτύου

Το συγκεκριμένο επίπεδο με επιβολή πολιτικής δικτύου ικανοποιεί όλες τις υπηρεσίες που μεταφέρονται με ασφάλεια και κατευθύνουν τη κυκλοφορία είτε αφορά τον έλεγχο, τη διαχείριση και τη πραγματική κίνηση δεδομένων,.

5.2.4 Ασφαλής Ανάλυση – Ορατότητα και Έλεγχος

Σε αυτό το ασφαλές επίπεδο ανάλυσης καθορίζει το ποιες υπηρεσίες θα χρησιμοποιηθούν για να δώσουμε τηλεμετρία με σκοπό να αποκτήσουμε ορατότητα και έλεγχο για το δίκτυο του IoT. Από τη στιγμή που έχουν εξελιχθεί τα συστήματα δεδομένων μία πλατφόρμα παράλληλης βάσης δεδομένων MPP που να μπορεί να μπορεί να προχωρήσει για να επεξεργαστούμε δεδομένα που έχουν μεγάλο όγκο σε πραγματικό χρόνο.

6. Μελέτη περίπτωσης με χρήση του Πράσινου Διαδίκτυο των Πραγμάτων

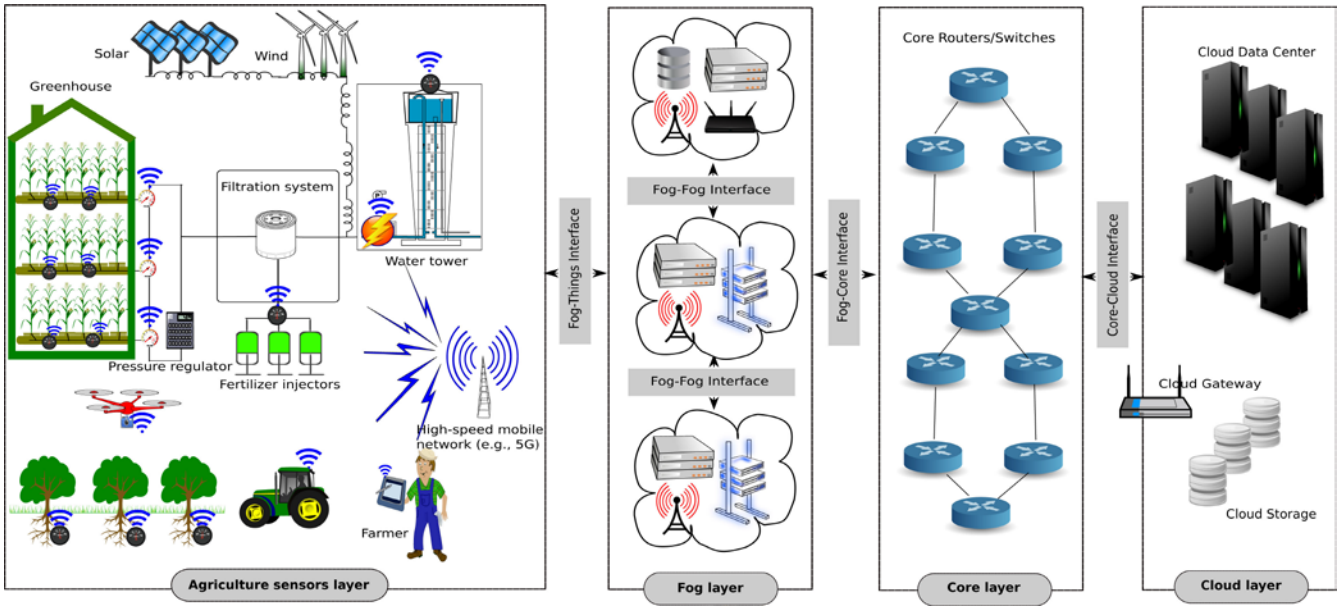
Αυτή η μελέτη περίπτωσης παρουσιάζει τις ερευνητικές προκλήσεις σε θέματα ασφάλειας και απορρήτου στην περιοχή της **έξυπνης γεωργίας (smart agriculture)** που βασίζεται στο πράσινο Διαδίκτυο των Πραγμάτων (Green IoT). Η έξυπνη γεωργία που βασίζεται στην τεχνολογία IoT έχει δώσει τη δυνατότητα στους αγρότες για τη βελτίωση των αποδόσεων των καλλιεργειών, τη βελτιστοποίηση της αποτελεσματικότητας της άρδευσης και μείωση του αγροτικού κόστους. Είναι μια έξυπνη γεωργική λύση συνδυάζοντας τη γεωργία με τις σύγχρονες τεχνολογίες της πληροφορίας και των επικοινωνιών (ΤΠΕ). Η τεχνολογία IoT συνέβαλε στην ανάπτυξη της έξυπνης γεωργίας σε τρεις πτυχές της:

- **Γεωργία ακριβείας**: Χρησιμοποιεί προηγμένη τεχνολογία για τη βελτίωση της απόδοσης των καλλιεργειών. Το ασύρματο δίκτυο αισθητήρων (WSN) είναι ο κύριος μοχλός για την ανάπτυξή της γεωργίας ακριβείας. Αποτελεσματικά μειώνει τους πιθανούς κινδύνους στην παραγωγική διαδικασία και βοηθά τους αγρότες να κάνουν ακριβή και ελεγχόμενη γεωργία πρακτικές με την ανάπτυξη μεγάλου αριθμού χαμηλής ισχύος, πολυλειτουργικοί αισθητήρες ασύρματης επικοινωνίας σε αγροτοκτηνοτροφικά περιβάλλοντα (όπως αγροί και καλλιέργειες, ορνιθοτροφεία, στάβλοι εκτροφής ζώων αναπαραγωγής, κλπ.) και συλλογή σχετικών δεδομένων στη γεωργική παραγωγή (όπως δεδομένα περιβάλλοντος, δεδομένα ανάπτυξης καλλιεργειών, δεδομένα για την υγεία των ζώων, κλπ.)
- **Υποβοηθούμενη Γεωργία**: Είναι ένας βιομηχανοποιημένος τρόπος γεωργικής παραγωγής που στοχεύει σε καλή ποιότητα και υψηλή απόδοση, με τη χρήση βιοτεχνολογίας, μηχανικής, φυτοκομίας, μετεωρολογίας, περιβαλλοντικών τεχνολογιών, τεχνολογίες υπολογιστών, επικοινωνιών και IoT. Ο πυρήνας της υποβοηθούμενης γεωργίας βρίσκεται στο σύστημα ελέγχου που βασίζεται στα ιστορικά δεδομένα που συλλέγονται από αισθητήρες IoT, στο μοντέλο πρόβλεψης και στη διαχείριση αποφάσεων. Ανήκει σε μια βιομηχανία υψηλής εισροής, υψηλής παραγωγής, έντασης κεφαλαίου, έντασης τεχνολογίας και έντασης εργασίας. Παρέχει προστασία της φυτικής παραγωγής με εγκαταστάσεις που υποστηρίζονται από τεχνολογία μηχανικής, με στόχο να μην περιορίζεται η αγροτική παραγωγή από περιβαλλοντικούς παράγοντες και να απελευθερώνεται η παραδοσιακή γεωργία από τα δεσμά της φύσης, με τα προϊόντα να ανταποκρίνονται στην κατανάλωση πολλαπλών επιπέδων και την ολοένα αυξανόμενη ζήτηση που προέρχεται από την παγκόσμια κοινωνική ανάπτυξη.
- **Συμβολαιακή Γεωργία**: Είναι ένα νέο μοντέλο αγροτικής παραγωγής και διαχείρισης. Αναθέτει εκ των προτέρων την παραγωγή στους συνεργαζόμενους αγρότες με βάση τη ζήτηση ορισμένων αγροτικών προϊόντων, μειώνει τη φύτευση και τους κινδύνους παραγωγής των καλλιεργητών και την αποφυγή της τυφλής παραγωγής. Είναι ένα αποτελεσματικό μοντέλο παραγωγής και μάρκετινγκ προσανατολισμένο στην αγορά. Η συμβολαιακή γεωργία περιλαμβάνει σύστημα εμπορίας γεωργικών προϊόντων, τη διαχείριση της εφοδιαστικής αλυσίδας logistics

αγροτικών προϊόντων, την ιχνηλασιμότητα αγροτικών προϊόντων, την ασφάλεια γεωργικών προϊόντων, κλπ. Η τεχνολογία IoT χρησιμοποιείται για την παρακολούθηση της αλυσίδας εφοδιασμού τροφίμων (δηλ. ιχνηλασιμότητα από τη φάρμα στο πιάτο του καταναλωτή). Για παράδειγμα, αναπτύσσεται ένα σύστημα που βασίζεται στο IoT για την παρακολούθηση της ασφάλειας των τροφίμων καθ' όλη τη διάρκεια του κύκλου ζωής του προϊόντος, προκειμένου να βοηθηθούν οι καταναλωτές στη λήψη καλύτερων αποφάσεων αγοράς, με παροχή πληροφοριών γεωγραφικής θέσης σχετικά με τα τρόφιμα, την αποθήκευση και μεταφορά τους.

6.1 Έξυπνη Γεωργία βασισμένη στο Πράσινο IoT (Green IoT-based agriculture)

Η Εικόνα 16 απεικονίζει την αρχιτεκτονική τεσσάρων επιπέδων της έξυπνης γεωργίας που βασίζεται στο πράσινο IoT, η οποία αποτελείται από τα ακόλουθα τέσσερα επίπεδα: **1) Agriculture Sensors layer; 2) Fog layer; 3) Core layer; 4) Cloud layer.**



Εικόνα 16. Αρχιτεκτονική τεσσάρων επιπέδων έξυπνης γεωργίας βασισμένης στο πράσινο IoT.

6.1.1 Επίπεδο Αισθητήρων Έξυπνης Γεωργίας (Agriculture Sensors Layer)

Αυτό το επίπεδο αποτελείται από συσκευές που χρησιμοποιούν το IoT όπως για παράδειγμα οι κόμβοι αισθητήρων, τα smartphone κ.λπ που είναι συνδεδεμένες στο Παγκόσμιο Σύστημα Εντοπισμού Θέσης (Global Positioning System – GPS) για να υποστηρίζουν διαφορετικούς τύπους εφαρμογών του IoT που αφορούν την έξυπνη γεωργία, συμπεριλαμβανομένων των εφαρμογών IoT για θερμοκήπια, για αγροκτήματα με φωτοβολταϊκά, κτηνοτροφικές εγκαταστάσεις με συστήματα εξοικονόμησης ενέργειας, κ.ά.

Συνεπώς, προσθέτοντας και προσαρμόζοντας συσκευές IoT στα διάφορα επίπεδα γεωργίας, έχουν σκοπό να επιτευχθούν δύο στόχοι: Ο πρώτος είναι να ξέρουμε ότι υπάρχει η αξιοπιστία στη διαδικασία της παραγωγής, αλλά και στη διανομή των αγροτικών και κτηνοτροφικών προϊόντων. Ο δεύτερος είναι να δίνεται ένας καλύτερος έλεγχος όσον αφορά την κατανάλωση αυτών των προϊόντων, που να έχει χαμηλό κόστος, καθώς και να

μειώνονται οι αστοχίες ως προς την επίτευξη του στόχου. Πέρα από τα οικονομικά θέματα, το θέμα των περιβαλλοντικών επιπτώσεων θα μειωθεί σημαντικά. Με την πράσινη γεωργία που βασίζεται στο IoT, οι αγρότες έχουν στην κατοχή τους ένα ψηφιακό σύστημα ελέγχου που αφορά τον εποπτικό έλεγχο όλων των διαδικασιών παραγωγής και διανομής των προϊόντων τους.

Για παράδειγμα, ως προς την ένταξη εξοπλισμού κι εφαρμογών IoT στο θερμοκήπιο προτείνονται διάφοροι κόμβοι αισθητήρων και μετρήσεων, ως εξής:

- Οι συσκευές του IoT στο σύστημα της άντλησης του νερού, που θα αφορά τις επιφάνειες που πρέπει να ποτιστούν, τις αναμενόμενες πιέσεις και του ρυθμού ροής του καθενός σταλάκτη ποτίσματος.
- Οι μετρήσεις στάθμης νερού σε δεξαμενές νερού, για να μπορούν να εμφανίζουν τις ενημερώσεις σε πραγματικό χρόνο.
- Οι συσκευές του IoT που είναι κατάλληλες σε κάθε εξοπλισμό φιλτραρίσματος όπως το φίλτρο άμμου το οποίο αφορά τις φυσικές ιδιότητες του νερού και τους σταλάκτες.
- Οι μετρητές των λιπασμάτων, τόσο κατά την αποθήκευσή τους, όσο και κατά τη λίπανση από τους εγχυτήρες των λιπασμάτων, παρέχοντας ενημερώσεις σε πραγματικό χρόνο.
- Οι συσκευές του IoT που ελέγχουν το pH και την ηλεκτρική αγωγιμότητα του εδάφους για να επιτυγχάνεται η τιμή που θέλουν όσον αφορά το θρεπτικό διάλυμα κατά τη λίπανση.
- Οι μικροί ηλιακοί συλλέκτες που έχουν αισθητήρες IoT έτσι ώστε να είναι υπό έλεγχο το επίπεδο υγρασίας και θερμοκρασίας εδάφους και αέρα.

Αυτές οι συσκευές και οι μετρητές του IoT μπορούν να επικοινωνούν με το επίπεδο υπολογισμού ομίχλης μέσα από το δίκτυο κινητής τηλεφωνίας 4G και 5G καθώς και της δορυφορικής επικοινωνίας.

6.1.2 Επίπεδο Υπολογιστικής Ομίχλης (Fog Computing Layer)

Θεωρώντας ως δεδομένο ότι υπάρχουν ορισμένα αγροτικά δεδομένα IoT τα οποία πρέπει να τίθενται σε επεξεργασία όταν βρίσκονται πιο κοντά σε συσκευές και μετρητές IoT, το επίπεδο υπολογιστικής ομίχλης (Fog Computing Layer) [8] έχει προτιμηθεί για αυτή την εργασία, που θα μπορεί παράλληλα να μειώνει δραστικά τον χρόνο της επεξεργασίας. Το συγκεκριμένο επίπεδο ονομάζεται επίσης επίπεδο υπολογιστικής ακμής (Edge Computing Layer). Οι κόμβοι ομίχλης παίρνουν τα δεδομένα γεωργίας IoT μέσω των γεωκατανεμημένων συσκευών τα οποία διαχειρίζονται ένα κατανεμημένο δίκτυο που συμπεριλαμβάνει τα σημεία πρόσβασης (access points), τις πύλες (gateways), τους μεταγωγείς (switches) και τους δρομολογητές (routers).

Το επίπεδο υπολογιστικής ομίχλης παρέχει πολλά πλεονεκτήματα και ένα από αυτά είναι να μειώνεται η επιβάρυνση της κυκλοφορίας του δικτύου, ενισχύοντας παράλληλα την ασφάλεια των δεδομένων IoT που αφορούν την πράσινη γεωργία. Έτσι λοιπόν υπάρχουν τρεις ιεραρχικές αρχιτεκτονικές οι οποίες μπορούν να αξιοποιηθούν στο επίπεδο υπολογιστικής ομίχλης στην πράσινη γεωργία που στηρίζεται στο IoT. Η πρώτη ιεραρχική

αρχιτεκτονική περιλαμβάνει τρία επίπεδα: το Tier1-Things/End Device, το Tier2-Fog και το Tier-3-Cloud και είναι η βασική αρχιτεκτονική της υπολογιστικής ομίχλης. Η δεύτερη αρχιτεκτονική περιλαμβάνει τέσσερα επίπεδα και είναι συνδυασμένη αρχιτεκτονική υπολογιστικής ομίχλης και υπολογιστικής νέφους.

6.1.3 Επίπεδο Δικτυακού Κορμού (Core Network Layer)

Ο ρόλος του επιπέδου δικτυακού κορμού (Core Network Layer) είναι να μεταφέρει δεδομένα πράσινης γεωργίας που εξαρτάται από το IoT από το επίπεδο της υπολογιστικής ομίχλης στο επίπεδο της υπολογιστικής νέφους. Για να επιβεβαιώσουμε ότι τα πακέτα δεδομένων μεταφέρονται με ασφάλεια μέσα από τα ενδιάμεσα δίκτυα, το επίπεδο δικτυακού κορμού περιλαμβάνει τις ζεύξεις υψηλής ταχύτητας, όπως τα καλώδια οπτικών ινών και τους μεταγωγείς υψηλής τεχνολογίας. Επιπρόσθετα το επίπεδο δικτυακού κορμού έχει ως στόχο τη δρομολόγηση των πακέτων δεδομένων, δίνοντας τη δυνατότητα για διασύνδεση δικτύου που στηρίζεται σε στρατηγικές, όπως η στρατηγική QoS, η στρατηγική μετάδοσης ελέγχου, η στρατηγική πολλαπλής μετάδοσης, κ.λπ.

6.1.4 Επίπεδο Υπολογιστικής Νέφους (Cloud Computing Layer)

Το συγκεκριμένο επίπεδο υπολογιστικής νέφους (Cloud Computing Layer) είναι ένα κεντρικό σύστημα που περιλαμβάνει κέντρα δεδομένων (data centers), παραδοσιακούς διακομιστές (cloud servers) που διαθέτουν πολλούς υπολογιστικούς πόρους για επεξεργασία μεγάλου όγκου δεδομένων, καθώς και μεγάλη χωρητικότητα αποθήκευσης δεδομένων. Το επίπεδο υπολογιστικής νέφους είναι υπεύθυνο για να παρέχει πρόσβαση στα δεδομένα και συγχρονισμό, επεξεργασία, αποθήκευση, κλπ.

6.2 Μοντέλα Απειλών Ασφαλείας (Threat Models)

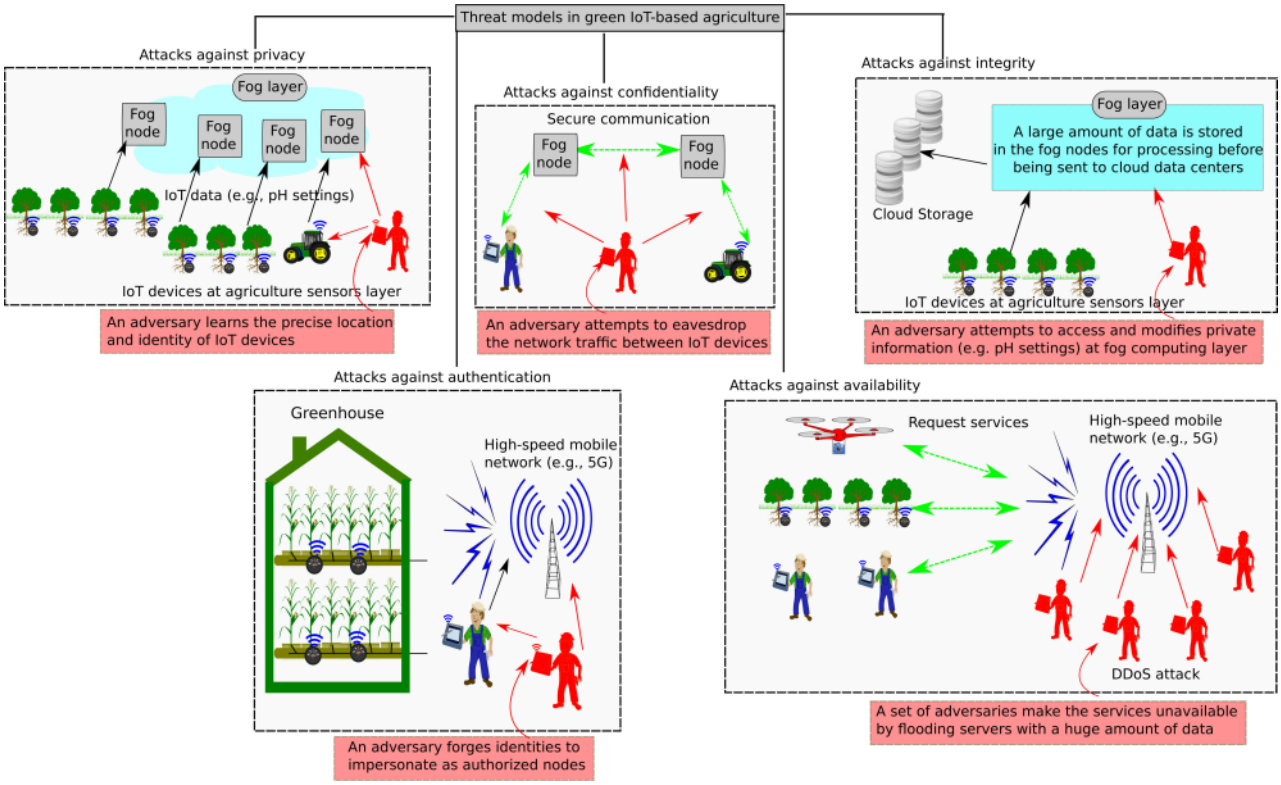
Θα μπορούσαμε να πούμε με απλά λόγια πως η ταξινόμηση των επιθέσεων για εφαρμογές IoT γίνεται χρησιμοποιώντας τα δύο παρακάτω κριτήρια:

1) Εσωτερική ή Εξωτερική Επίθεση
2) Παθητική ή Ενεργητική Επίθεση

Συνεπώς σύμφωνα με τα παραπάνω κριτήρια, καθεμία επίθεση προσπαθεί να δημιουργήσει μεγάλα προβλήματα στους κόμβους της πράσινης γεωργίας που βασίζεται στο IoT, δηλαδή σε συσκευές IoT, σε κόμβους υπολογιστικής ομίχλης και σε κόμβους υπολογιστικής νέφους.

Έτσι, όπως φαίνεται και στο παρακάτω σχήμα, τοποθετούμε τα μοντέλα των απειλών και επιθέσεων ασφαλείας στις ακόλουθες πέντε βασικές αρχές ασφάλειας που αφορούν:

1) τη διατήρηση απορρήτου,
2) τον έλεγχο πιστοποίησης ταυτότητας,
3) την εμπιστευτικότητα των δεδομένων,
4) την ακεραιότητα των δεδομένων,
5) και τη διαθεσιμότητα των δεδομένων



Εικόνα 17. Threat models in green IoT-based agriculture.

6.2.1 Επιθέσεις κατά του Απορρήτου (Attacks against privacy)

Η συγκεκριμένη κατηγορία επιθέσεων στο επίπεδο των αισθητήρων της έξυπνης γεωργίας έχει ως κύριο σκοπό να γίνουν γνωστές, σε μη εξουσιοδοτημένες οντότητες, οι ακριβείς τοποθεσίες των συσκευών IoT, καθώς και οι ταυτότητές τους. Κατά συνέπεια, πρέπει να λαμβάνονται τα κατάλληλα μέτρα διαφύλαξης του απορρήτου στο σύστημα IoT. Στην πράσινη γεωργία η οποία στηρίζεται στο IoT, ορισμένα δεδομένα όπως η σύνθεση του νερού, η θερμοκρασία και η υγρασία, καταγράφονται και συλλέγονται πολλές φορές την ώρα, από συσκευές-αισθητήρες IoT και έξυπνους μετρητές, που ανήκουν στο επίπεδο των αισθητήρων της έξυπνης γεωργίας. Η διεξοδική ανάλυση των παραπάνω δεδομένων IoT μπορεί με ευκολία να υποστηρίξει τις αγροτικές εργασίες.

Για παράδειγμα, εάν το pH του εδάφους έχει αυξητική τάση, τότε αυτό θα πρέπει να οδηγήσει τον αγρότη να αυξήσει την λίπανση των φυτών με θρεπτικά διαλύματα (με κύριο συστατικό την αμμωνία) και εάν το pH έχει μειούμενη τάση, τότε ο αγρότης θα πρέπει να μειώσει αυτόματα την αντίστοιχη λίπανση. Με βάση τις παραπάνω πληροφορίες μια κακόβουλη οντότητα μπορεί να σχεδιάσει φυσικές επιθέσεις, όπως την αποστολή ενός drone για μη ορθή λίπανση των φυτών, με σκοπό να παραβιάσει τις ρυθμίσεις του pH. Είναι προφανές ότι το απόρρητο ιδιωτικών πληροφοριών για την πράσινη γεωργία, όπως είναι οι ρυθμίσεις pH, θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.

6.2.2 Επιθέσεις κατά της Πιστοποίησης Ταυτότητας (Attacks against authentication)

Σε αυτή τη κατηγορία επιθέσεων, κακόβουλες οντότητες πλαστογραφούν ταυτότητες για να μπορέσουν να μοιάσουν με τους εξουσιοδοτημένους κόμβους του συστήματος IoT

της πράσινης γεωργίας, δηλαδή συσκευές-αισθητήρες IoT, κόμβους υπολογιστικής ομίχλης ή κόμβους υπολογιστικής νέφους, με σκοπό να αποκτήσουν την πρόσβαση στο πληροφοριακό σύστημα IoT της πράσινης γεωργίας. Για παράδειγμα, ένας αντίπαλος μπορεί να δοκιμάσει τις ακόλουθες επιθέσεις για να παρακάμψει τον έλεγχο πιστοποίησης ταυτότητας σχετικά και πιο συγκεκριμένα, στην επίθεση αναμετάδοσης μέσω ενδιάμεσου χρήστη, στην επίθεση μεταμφίεσης, στην επίθεση πλαστοπροσωπίας και στην επίθεση πλαστογράφησης.

- Μία επίθεση αναμετάδοσης μέσω ενδιάμεσου χρήστη σύμφωνα με τη μορφή Man-in-the-Middle (MITM) Attack, έχει ως στόχο το επίπεδο αισθητήρων έξυπνης γεωργίας και πιο συγκεκριμένα, να υποκλέψει πακέτα δεδομένων που ανταλλάσσονται μεταξύ των συσκευών IoT ή μεταξύ μίας συσκευής IoT και του σημείου πρόσβασης στο δίκτυο IoT, οπότε στη συνέχεια είναι εφικτή η κακόβουλη αναμετάδοσή τους. Για την αντιμετώπιση τέτοιων επιθέσεων, αξιοποιούνται τρεις τεχνικές ελέγχου και πιστοποίησης ταυτότητας, μέσω κρυπτογράφησης της ροής δεδομένων στη ζεύξη, τη χρήση ασφαλών συναρτήσεων κατακερματισμού (hash), καθώς και τη χρονοσήμανση των κρυπτογραφημένων δεδομένων.
- Μία επίθεση μεταμφίεσης (masquerade attack) έχει ως στόχο το επίπεδο αισθητήρων έξυπνης γεωργίας και πιο συγκεκριμένα, τη μεταμφίεση του επιτιθέμενου σε νόμιμο (εξουσιοδοτημένο) κόμβο για να μπορέσει να συνδεθεί με το διακομιστή υπηρεσίας IoT, δηλαδή να μπορέσει να συνδεθεί με το σημείο πρόσβασης του δικτύου IoT ή με τον αντίστοιχο κόμβο στο επίπεδο της υπολογιστικής ομίχλης. Για την αντιμετώπιση τέτοιων επιθέσεων, αξιοποιούνται διάφορες τεχνικές που αφορούν την πιστοποίηση ταυτότητας των χρηστών για τον έλεγχο πρόσβασής τους στα συστήματα IoT και πιο συγκεκριμένα:
  1) Με βάση τα βιομετρικά χαρακτηριστικά των νόμιμων (εξουσιοδοτημένων) χρηστών, όπως το δακτυλικό αποτύπωμα του χεριού, την ίριδα του ματιού, ή το σχήμα προσώπου.
  2) Με βάση τα δευτερεύοντα χαρακτηριστικά των νόμιμων (εξουσιοδοτημένων) χρηστών που εξαρτώνται από την επιμέρους συμπεριφορά τους, όπως ο ρυθμός πληκτρολόγησης, η χειρόγραφη υπογραφή, ο βηματισμός και η χροιά της φωνή τους.
  3) Ασφαλείς συναρτήσεις κατακερματισμού (hash).
  4) Κρυπτοσύστημα ελλειπτικής καμπύλης.
  5) Κρυπτογράφησης της ροής δεδομένων στη ζεύξη.

6.2.3 Επιθέσεις κατά της Εμπιστευτικότητας (Attacks against confidentiality)

Η συγκεκριμένη κατηγορία επιθέσεων στο επίπεδο των αισθητήρων της έξυπνης γεωργίας έχει ως κύριο σκοπό την υποκλοπή της κίνησης δεδομένων που ανταλλάσσονται μεταξύ των συσκευών IoT ή μεταξύ μίας συσκευής IoT και του σημείου πρόσβασης στο δίκτυο IoT, οπότε στη συνέχεια να είναι εφικτή η αποκρυπτογράφησή τους, παραβιάζοντας την αρχή της εμπιστευτικότητας. Για παράδειγμα ένας αντίπαλος μπορεί να δοκιμάσει τις ακόλουθες επιθέσεις για να θέσει σε κίνδυνο την εμπιστευτικότητα των δεδομένων του

συστήματος IoT, που περιλαμβάνει τις επιθέσεις εντοπισμού, τις επιθέσεις ωμής βίας και τις επιθέσεις του γνωστού κλειδιού.

- Η επίθεση εντοπισμού έχει σκοπό να συλλέγει πακέτα δεδομένων από τις συσκευές IoT για να επιτευχθεί η παραβίαση του απορρήτου και η υποκλοπή διαπιστευτηρίων νομίμων χρηστών για τη δημιουργία κακόβουλων συνδέσεων. Για να αντιμετωπιστεί αυτή η κατηγορία επιθέσεων θα πρέπει να χρησιμοποιούνται εξελιγμένες μέθοδοι κρυπτογράφησης των δεδομένων.
- Η επίθεση ωμής βίας (brute force attack) στο επίπεδο των αισθητήρων έξυπνης γεωργίας έχει σκοπό την εξαντλητική δοκιμή όλων των πιθανών συνδυασμών κωδικών πρόσβασης οι οποίοι μπορεί να έχουν χρησιμοποιηθεί από τις συσκευές IoT. Για να αντιμετωπιστεί αυτή η επίθεση θα πρέπει να χρησιμοποιούνται σύνθετοι κωδικοί πρόσβασης και να διατηρείται η μυστικότητά τους.
- Η επίθεση γνωστού κλειδιού έχει σκοπό τη δημιουργία νέου κλειδιού συνόδου (session key) με βάση την παραβίαση κλειδιού που έχει επιτευχθεί σε προηγούμενη σύνοδο. Για να αντιμετωπιστεί αυτή η επίθεση θα πρέπει να χρησιμοποιούνται εξελιγμένες μέθοδοι δημιουργίας κλειδιών μέσω κρυπτογράφησης δημοσίου κλειδιού.

6.2.4 Επιθέσεις κατά της Ακεραιότητας (Attacks against integrity)

Η συγκεκριμένη κατηγορία επιθέσεων αφορά τη μη εξουσιοδοτημένη πρόσβαση και παραβίαση της ακεραιότητας των δεδομένων με κακόβουλη τροποποίησή τους. Σε αυτή την κατηγορία μπορούμε να βρούμε τα παρακάτω είδη επιθέσεων: Επίθεση πλαστογραφίας, επίθεση αναμετάδοσης μέσω ενδιάμεσου χρήστη (MITM), επίθεση μέσω πλαστοπροσωπίας (βιομετρικών χαρακτηριστικών), επίθεση μέσω δούρειων ίππων, κλπ. Για να αντιμετωπιστεί αυτή η κατηγορία επιθέσεων θα πρέπει να εξελιχθούν τα σχήματα συλλογής δεδομένων που εξαρτώνται από τη συμμετρική κρυπτογράφηση και τις συναρτήσεις κατακερματισμού.

6.2.5 Επιθέσεις κατά της Διαθεσιμότητας (Attacks against availability)

Η συγκεκριμένη κατηγορία επιθέσεων αφορά την άρνηση παροχή υπηρεσίας (Denial of Service – DoS) από τις εξουσιοδοτημένες οντότητες (διακομιστές υπηρεσίας). Το βασικό πλάνο αυτής της κατηγορίας επιθέσεων είναι να μπορέσει να διακόψει την παροχή υπηρεσιών που προσφέρει ένα οικοσύστημα IoT στην πράσινη γεωργία, όπως ο έλεγχος ταυτότητας στις συσκευές IoT, μέσω της εξάντλησης των υπολογιστικών πόρων ή/και των δικτυακών υποδομών, ως εξής:

- Αποστέλλοντας στους διακομιστές υπηρεσίας, τεράστιο όγκο δεδομένων και κακόβουλων αιτήσεων εξυπηρέτησης με στόχο την εξάντληση των υπολογιστικών πόρων τους και καθιστώντας τους μη ικανούς να παρέχουν υπηρεσίες στις εξουσιοδοτημένες συσκευές IoT.
- Με υπερφόρτωση των δικτυακών υποδομών (δρομολογητών, μεταγωγέων, σημείων πρόσβασης, κλπ.) του συστήματος IoT με επιθέσεις παραπλάνησης (spoofing attacks) σε και με κακόβουλη ροή μεγάλου όγκου δεδομένων για εξάντληση των δικτυακών πόρων.

6.3 Μηχανισμοί Ασφάλειας

6.3.1 Μηχανισμοί Διαφύλαξης Απορρήτου (Privacy-preserving Solutions)

6.3.1.1 Privacy-preserving data aggregation

Κατά τη διάρκεια της συγκέντρωσης δεδομένων στα άκρα του δικτύου που χρησιμοποιεί το IoT στην πράσινη γεωργία, οι συσκευές της υπολογιστικής ομίχλης δεν μπορούν να δουν τα δεδομένα της καθεμίας συσκευής του πράσινου IoT. Ο μηχανισμός συλλογής και συγκέντρωσης των δεδομένων κάθε πράσινης συσκευής IoT είναι πολύ σημαντικός για την προστασία του απορρήτου και περιλαμβάνει τρία επίπεδα, δηλαδή το κατώτερο επίπεδο που βρίσκονται οι έξυπνες συσκευές, το μεσαίο επίπεδο στους κόμβους υπολογιστικής ομίχλης και το ανώτερο επίπεδο στην υπολογιστική νέφους.

6.3.1.2 Location privacy

Οι υπηρεσίες που βασίζονται στον εντοπισμό γεωγραφικής θέσης (Location Based Services –LBS) που χρησιμοποιούνται στην πράσινη γεωργία που εξαρτάται από το IoT, με τη γρήγορη ανάπτυξη της έξυπνης γεωργίας θα έχουν έναν πολύ σημαντικό ρόλο. Έτσι λοιπόν ένας αντίπαλος θα είναι σε θέση να βλέπει τις συσκευές του IoT στην έξυπνη γεωργία και αυτό θα έχει πιθανότητα να προκαλέσει προβλήματα απώλειας της ιδιωτικότητας. Ο Sun πρότεινε την προσθήκη σε εφαρμογές του IoT αλγόριθμου διατήρησης απορρήτου για τον εντοπισμός της γεωγραφικής θέσης, ο οποίος θα είναι σε θέση να προσαρμοστεί στις ανάγκες της πράσινης γεωργίας που αξιοποιεί το IoT. Αυτός ο αλγόριθμος θα μπορεί να αποτρέπει δύο κατηγορίες επιθέσεων, την επίθεση των συμπερασμάτων και τις επιθέσεις συμπαιγνίας, όμως η ακεραιότητα των δεδομένων και ο έλεγχος ταυτότητας δεν εξετάζονται.

6.3.1.3 Content-oriented protection

Όταν συλλέγονται και συνδυάζονται τα διαφορετικά δεδομένα IoT από το επίπεδο των αισθητήρων της πράσινης γεωργίας, η προστασία του απορρήτου του περιεχομένου των εφαρμογών IoT για την πράσινη γεωργία, είναι πολύ σημαντική. Ο Gai μας προτείνει ένα δυναμικό μοντέλο προστασίας του απορρήτου για τους χρήστες που ονομάζεται DPP για να υπάρξει η διασφάλιση του απορρήτου των χρηστών των κινητών συσκευών με τις εφαρμογές IoT. Η ιδέα του μοντέλου DPP βασίζεται στην κατηγοριοποίηση των επιπέδων προστασίας του απορρήτου σε κλάσεις.

6.3.1.4 Anonymity

Μία πολύ σημαντική ιδιότητα ασφάλειας στα συστήματα IoT της πράσινης γεωργίας είναι να υπάρξει ισχυρή ανωνυμία κάτι που έχει ως αποτέλεσμα ότι, εκτός από τους κόμβους της υπολογιστικής ομίχλης, η ταυτότητα των δεδομένων της γεωργίας IoT δεν μπορεί να αποκαλυφθεί. Η λύση CPAL που έχει προταθεί από τον Lai αρχειοθετεί την ανωνυμία του χρήστη στην εφαρμογή IoT. Η λύση αυτή ορίζει τη διατήρηση του απορρήτου στα τρία επίπεδα που περιλαμβάνει, τους εξουσιοδοτημένους ανώνυμους χρήστες, του ελέγχου της ταυτότητας τους και της διατήρησης της ανωνυμίας τους. Επομένως, η συγκεκριμένη λύση μπορεί να προσαρμοστεί στην πράσινη γεωργία που

βασίζεται στο IoT εφαρμόζοντας την κρυπτογράφηση του υβριδικού συνδυασμού μεταξύ των επικοινωνιών των συσκευών IoT στο επίπεδο των αισθητήρων της έξυπνης γεωργίας.

6.3.1.5 Privacy-preserving trust evaluation

Η αξιολόγηση της εμπιστοσύνης με τη διατήρηση του απορρήτου έχει ένα πολύ σημαντικό ρόλο για τη διασφάλιση των σχέσεων εμπιστοσύνης μεταξύ των οντοτήτων της πράσινης γεωργίας που στηρίζεται στο IoT. Ο Yan προτείνει δύο συστήματα που αξιολογούν την εμπιστοσύνη για να διατηρηθεί το απόρρητο. Το πρώτο σύστημα θεωρεί ότι ο εξουσιοδοτημένος πληρεξούσιος είναι τελείως αξιόπιστος και παράλληλα δεν υπάρχει συμπαιγνία μεταξύ των μερών, του αξιολογητή και του εξουσιοδοτημένου πληρεξούσιου. Το δεύτερο σύστημα θεωρεί ότι ο εξουσιοδοτημένος πληρεξούσιος δεν είναι εντελώς αξιόπιστος και πως το μέρος που συμβάλλει στην αξιολόγηση με τον εξουσιοδοτημένο πληρεξούσιο δεν συνεργάζονται. Και στα δύο σχήματα έχουμε μία φάση αξιολόγησης εμπιστοσύνης, η οποία αφού λάβει τα κρυπτογραφημένα στοιχεία τα αποστέλλει σε κόμβο που αποκρυπτογραφεί τα δεδομένα και στη συνέχεια αξιολογεί την εμπιστοσύνη του αποτελέσματος μέσω αλγορίθμου αξιολόγησης εμπιστοσύνης.

6.3.1.6 Personalized privacy

Το εξατομικευμένο απόρρητο προτείνεται στην παροχή θυρίδας που δεν θα είναι εύκολα φανερή όπως και στο θέμα του ευρετηρίου. Ο Li μας προτείνει ένα σύστημα κρυπτογράφησης που θα έχει τη δυνατότητα να αναζητά ένα εξατομικευμένο απόρρητο στην εφαρμογή IoT που θα μπορεί να προσαρμοστεί στην πράσινη γεωργία που χρησιμοποιεί το IoT. Το σχήμα που προτάθηκε εξετάζει ένα μοντέλο του δικτύου IoT που περιλαμβάνει τρεις οντότητες, οι οποίες είναι ο κάτοχος δεδομένων, ο διακομιστής υπολογιστικού νέφους και ο χρήστης των δεδομένων. Ο ρόλος του διακομιστή υπολογιστικού νέφους αξιοποιείται για να αποθηκεύει και να ανακτά τα κρυπτογραφημένα χαρακτηριστικά που έχουν λάβει τις κρυπτογραφικές λειτουργίες από τον κάτοχο των δεδομένων. Με βάση τη συγκεκριμένη λέξη-κλειδί, ο χρήστης των δεδομένων ρωτά ποια είναι τα κρυπτογραφικά χαρακτηριστικά. Το σχήμα που προτάθηκε επιβεβαιώνει με τη χρήση δύο μεθόδων πρόκλησης-απόκρισης που ικανοποιεί τη θυρίδα που δεν είναι φανερή, όπως και το ευρετήριο που βρίσκεται κάτω από επιλεγμένη επίθεση ζεύγους λέξεων-κλειδιών όσον αφορά τα χαρακτηριστικά. Συνεπώς, το σχήμα που προτάθηκε θα είναι σε θέση να να ικανοποιεί τις απαιτήσεις για την πράσινη γεωργία η οποία στηρίζεται στο IoT δίνοντας έτσι τη δυνατότητα σε ένα σχήμα κρυπτογράφησης που θα έχει δυνατότητα αναζήτησης να χρησιμοποιεί τις ακόλουθες συναρτήσεις:

1) Ρυθμίσεις για να εκτελούνται οι παράμετροι της ασφάλειας
2) Γεννήτρια κλειδιών (KeyGen) για να δημιουργούνται ιδιωτικά και δημόσια κλειδιά. Η λειτουργία KeyGen εκτελείται από τον κόμβο υπολογιστικής ομίχλης και τη συσκευή IoT.
3) Δημιουργία πίνακα ευρετηρίου για τους εξουσιοδοτημένους χρήστες
4) Trapdoor για να δημιουργούνται ερωτήματα trapdoor. Η λειτουργία trapdoor εκτελείται από τη συσκευή IoT.
5) Αναζήτηση. Οι συναρτήσεις setup και store εκτελούνται από τον κόμβο υπολογιστικής ομίχλης. Η λειτουργία αναζήτησης εκτελείται διαδραστικά μεταξύ της συσκευής IoT και του διακομιστή υπολογιστικού νέφους.

6.3.2 Μηχανισμοί Ακεραιότητας Δεδομένων (Data Integrity Solutions)

Για να προστατέψουμε την ακεραιότητα των δεδομένων και τον έλεγχο ταυτότητας που αφορά εφαρμογές IoT. Ο Song μας προτείνει ένα πρωτόκολλο το οποίο διατηρεί την ιδιωτικότητα που χρησιμοποιεί κωδικούς για τον έλεγχο ταυτότητας των μηνυμάτων (Message Authentication Code – MAC). Η λύση MAC εφαρμόζεται μπει στα αρχικά δεδομένα IoT, όπου εκεί ο αποστολέας θα μπορεί να επιβεβαιώνει ότι τα δεδομένα IoT δεν έχουν παραβιαστεί κατά τη μετάδοσή τους. Η συγκεκριμένη λύση μπορεί να εφαρμοστεί στην πράσινη γεωργία που στηρίζεται στο IoT και πιο συγκεκριμένα μεταξύ μίας ομάδας συσκευών IoT και κόμβων υπολογιστικής ομίχλης, με στόχο να διαφυλαχθεί η ακεραιότητα των δεδομένων των πράσινων συσκευών IoT. Ο έλεγχος ταυτότητας του χρήστη πετυχαίνεται με το να επαληθεύσουμε την ακεραιότητα των δεδομένων. Η αξιολόγηση της απόδοσης δείχνει ότι το MD5 είναι πιο αποτελεσματικό από το SHA-1 στο περιβάλλον IoT.

Το έργο του Li μπορεί να δίνει τη δυνατότητα να επαληθεύεται η ακεραιότητα του περιεχομένου που ονομάζεται δικτύωση δεδομένων που θα μπορεί κάλλιστα να προσαρμόζεται στην επικοινωνία μεταξύ των αγροτικών κόμβων IoT στη πράσινη γεωργία που χρησιμοποιεί το IoT. Πιο συγκεκριμένα οι συγγραφείς μας προτείνουν μια ελαφριά αρχιτεκτονική επαλήθευσης της ακεραιότητας που ονομάζεται LIVE για να διασφαλιστεί η ασφαλής πρόσβαση στο περιεχόμενο. Η αρχιτεκτονική LIVE χρησιμοποιεί τα παρακάτω τρία επίπεδα ασφαλείας.

1) Χωρίς προσωρινή αποθήκευση
2) 1-Cacheable;
3) All-Cacheable

Για την παραγωγή των διακριτικών στη δημιουργία των υπογραφών η αρχιτεκτονική LIVE χρησιμοποιεί έναν αλγόριθμο υπογραφής που θα εξαρτάται από το δέντρο κατακερματισμού (αλγόριθμος Merkle Hash Tree)

6.3.3 Μηχανισμοί Ελέγχου Ταυτότητας (Authentication Solutions)

6.3.3.1 RFID Authentication

Η αναγνώριση των ραδιοσυχνοτήτων (RFID) είναι μία τεχνολογία η οποία έχει τη δυνατότητα για να λαμβάνει και να αυτοματοποιεί αναγνώριση πληροφοριών σε ηλεκτρονικές ετικέτες. Με την προσομοίωση της τεχνολογίας RFID στην πράσινη γεωργία που εξαρτάται από το IoT, οι αγρότες θα έχουν πιο καλό έλεγχο των καλλιεργειών τους από και οι κτηνοτρόφοι θα έχουν καλύτερη επίβλεψη των κοπαδιών τους. Έτσι λοιπόν, έαν ένα μη εξουσιοδοτημένο μέρος είναι σε θέση να ρυθμίζει την ετικέτα RFID θα μπορεί να θέσει σε κατάσταση κινδύνου το σύστημα της έξυπνης γεωργίας. Ο Gope μας προτείνει μία εύκολη ανώνυμη λύση για τον έλεγχο της ταυτότητας για εφαρμογές IoT. Συγκεκριμένα το μοντέλο που εξετάστηκε από μελέτη που έγινε, χρησιμοποιεί τέσσερις οντότητες, δύο διακομιστές, ένα πιστοποιημένο υπολογιστικό νέφος και μια βάση δεδομένων υποστήριξης ενός αναγνώστη και μιας ετικέτας RFID. Με κριτήριο τη μη συνδεδεμένη ψευδο-ταυτότητα, το κλειδί έκτακτης ανάγκης για τη λειτουργία του κατακερματισμού μας προτείνει λύση που θα μπορεί να στέκεται έναντι των παρακάτω πέντε επιθέσεων: επίθεση επανάληψης, επίθεση πλαστογραφίας, επίθεση κλωνοποίησης, επίθεση DoS και επίθεση εντοπισμού

γεωγραφικής θέσης. Έτσι λοιπόν αυτή η λύση θα έχει τη δυνατότητα να επιτυγχάνει πέντε ιδιότητες ασφαλείας και συγκεκριμένα τον αμοιβαίο έλεγχο ταυτότητας, την ανωνυμία ετικέτας, τη διαθεσιμότητα και την επεκτασιμότητα, αλλά δεν θα αξιολογούνται οι επιθέσεις εισαγωγής των ψευδών δεδομένων και η επίθεση DDoS.

6.3.3.2 Delegated Authentication

Με δεδομένο ότι τα αγροτικά δεδομένα IoT μπορούν να μεταφέρονται μέσα από μη αξιόπιστες δημόσιες συσκευές, οι λύσεις της ασφάλειας πρέπει να προσφέρουν τον προγραμματισμένο έλεγχο ταυτότητας. Το έργο του Zhang μας προτείνει ένα σύστημα ημι-εξωτερικής αποθήκευσης που θα διατηρεί την ιδιωτική ζωή που ονομάζεται SOPP για να συλλέγει τα δεδομένα IoT. Το σχήμα SOPP εξετάζει τρία στα οποία περιλαμβάνεται το κέντρο δεδομένων του δημοσίου (μη αξιόπιστου) cloud και των συσκευών IoT. Για να μειωθεί η απόδοση και να επιτευχθεί μεγαλύτερη διάρκεια ζωής της μπαταρίας, το σχήμα SOPP εφάρμοσε κρυπτογραφία ελλειπτικής καμπύλης ως μονόδρομο, δηλαδή έναν μη διαδραστικό έλεγχο ταυτότητας μεταξύ των μη αξιόπιστων δημοσιών νεφών και των συσκευών IoT. Για τον αποκλεισμό της μη έγκυρης πρόσβασης η ευθύνη του ελέγχου ταυτότητας τίθεται στα δημόσια σύννεφα. Η παροχή της ακεραιότητας των δεδομένων χρησιμοποιείται από το κέντρο δεδομένων με τη τεχνική της αποκρυπτογράφησης.

6.3.4 Μηχανισμοί Ελέγχου Πρόσβασης (Access Control Solutions)

Για να υποστηρίξουμε τη διατήρηση της ιδιωτικότητας στην πράσινη γεωργία που στηρίζεται στο IoT, μπορούμε να έχουμε ένα αποτελεσματικό σύστημα για τον έλεγχο πρόσβασης. Το έργο του Fan έχει σχεδιάσει ένα πρωτόκολλο ελέγχου πρόσβασης για το IoT που θα έχει τη δυνατότητα της υπολογιστικής ομίχλης. Η μελέτη αυτή εξέτασε συνδυαστικά συστήματα υπολογιστικής ομίχλης–υπολογιστικής νέφους που περιλαμβάνει πέντε οντότητες, έναν πάροχος υπηρεσιών υπολογιστικής νέφους, μία ομάδα κόμβων υπολογιστικής ομίχλης, μία ομάδα κατόχων δεδομένων, μία αρχή πιστοποιητικών και μίας ομάδας συσκευών IoT. Για να παρέχεται η ανάκληση της εμπιστευτικότητας των δεδομένων με τη δυνατότητα της επαλήθευσης, η κρυπτογράφηση εξυπηρετεί τις ανάγκες σε περίπτωση που μία συσκευή IoT με αναγνωριστικά υποβάλλει αίτημα πρόσβασης στα δεδομένα.

Η τεχνολογία blockchain μπορεί να έχει στη χρήση της την παροχή του ελέγχου πρόσβασης στην πράσινη γεωργία που βασίζεται στο IoT. Ο Ouaddah μας προτείνει ένα πλαίσιο που θα ελέγχει τη πρόσβαση που ονομάζεται Fair Access που αφορά εφαρμογή IoT. Το πλαίσιο αυτό αξιοποιεί τη τεχνολογία blockchain για να κερδίσει, να εκχωρήσει και να ανακαλέσει την πρόσβαση. Ο Zhang εξέτασε ένα σύστημα IoT που θα έχει μεγάλο αριθμό συσκευών (διακομιστές αποθήκευσης, διακομιστές υπηρεσίας, συσκευές χρηστών και πύλες IoT). Αυτή η μελέτη χρησιμοποιεί ένα πλαίσιο ελέγχου πρόσβασης που θα στηρίζεται στη πλατφόρμα έξυπνων συμβολαίων Ethereum. Η συγκεκριμένη πλατφόρμα περιέχει πέντε χαρακτηριστικά όπως το έξυπνο συμβόλαιο, ο λογαριασμός ή η διεύθυνση, το blockchain, η συναλλαγή ή μήνυμα και η εξόρυξη. Για τη διαχείριση των πολιτικών και για τις εφαρμογές του ελέγχου πρόσβασης το συγκεκριμένο πλαίσιο παρέχει κάποια λειτουργία ή δυαδικές διεπαφές εφαρμογών όπως για παράδειγμα η προσθήκη νέας

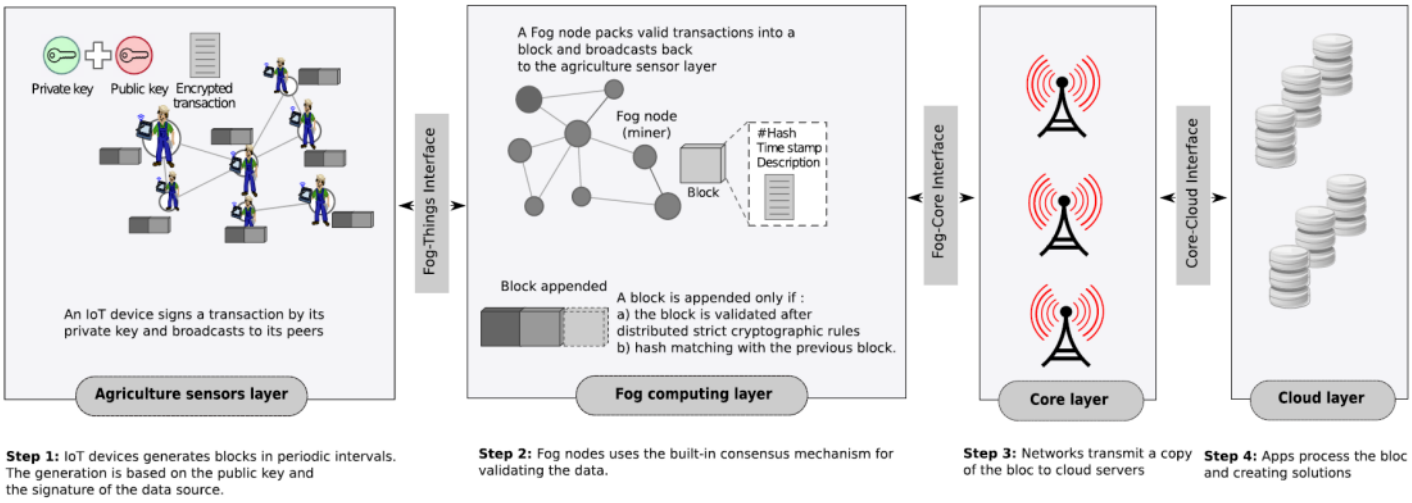
πολιτικής ελέγχου πρόσβασης, η ενημέρωση της πολιτικής, η επιστροφή του αποτελέσματος πρόσβασης, η ποινή κ.λπ.

6.3.5 Μηχανισμοί Διαφύλαξης Απορρήτου μέσω blockchain (Privacy-preserving over blockchain)

Η τεχνολογία blockchain μπορεί να έχει αποτελεσματική χρήση σε όλους τους τομείς IoT και φυσικά που περιλαμβάνει και την πράσινη γεωργία που στηρίζεται στο IoT. Η εφαρμογή της τεχνολογίας blockchain για το IoT εφαρμόζεται για την προστασία της ιδιωτικότητας. Πιο συγκεκριμένα η τεχνολογία blockchain χρησιμοποιείται για την κρυπτογραφημένη κοινή χρήση των δεδομένων. Συνεπώς, μπορούμε να χρησιμοποιήσουμε το blockchain ως ένα κατανεμημένο ψηφιακό βιβλίο που θα περιέχει όλα τα μηνύματα στην πράσινη γεωργία που στηρίζεται στο IoT. Αυτό το κατανεμημένο καθολικό ψηφιακό βιβλίο αναπαράγεται και αποθηκεύεται σε διαφορετικούς κόμβους IoT στο επίπεδο των αισθητήρων της έξυπνης γεωργίας.

Σύμφωνα με τα χαρακτηριστικά της κάθε λύσης που είναι προσανατολισμένη στο απόρρητο, οι λύσεις που εξαρτώνται από την τεχνολογία blockchain που βασίζονται σε blockchain για την πράσινη γεωργία με βάση το IoT ταξινομούνται σε έξι κατηγορίες.

1) Λύση μηχανικής εκμάθησης που βασίζεται σε blockchain
2) Λύση διαχείρισης κατανεμημένων σχεδίων που βασίζεται σε blockchain
3) Λύση ελέγχου πρόσβασης που βασίζεται σε blockchain
4) Λύση αξιολόγησης της εμπιστοσύνης που βασίζεται στο blockchain
5) Λύση ελέγχου ταυτότητας και ταυτοποίησης που βασίζεται σε blockchain
6) Ασφαλής λύση SDN που βασίζεται σε blockchain



Εικόνα 18. An illustration of blockchain working methodology for green IoT based agriculture architecture.

6.4 Υλοποίηση Οικοσυστήματος IoT για την Έξυπνη Γεωργία (Deploying IoT in agriculture)

Το IoT στην γεωργία μπορεί να χωριστεί σε διαφορετικά επίπεδα και από διαφορετικές προοπτικές. Όταν μιλάμε για τα Ασύρματα Δίκτυα Αισθητήρων (Wireless Sensor Networks –

WSN), θα πρέπει να έχουμε υπόψη τα ειδικά χαρακτηριστικά του περιβάλλοντος όπου θα αναπτυχθούν οι κόμβοι. Οι καλλιέργειες, ή τα άλλα εμπόδια στις γεωργικές εκτάσεις, μπορεί να αναγκάσουν την αλλαγή στις θέσεις των κόμβων, δημιουργώντας σημαντικά προβλήματα στην επικοινωνία μεταξύ των κόμβων. Τα κινούμενα εμπόδια επηρεάζουν την ποιότητα των συνδέσεων διαμορφώνοντας τις συνθήκες των καναλιών κατά τη διάρκεια του χρόνου, που επηρεάζει τους αλγορίθμους δρομολόγησης των πακέτων, τις μεθόδους διάγνωσης των αστοχιών, καθώς και άλλες πτυχές του WSN. Οι περιβαλλοντικοί παράγοντες όπως η θερμοκρασία, η βροχόπτωση, η υψηλή ηλιακή ακτινοβολία, μαζί με τη μεταβαλλόμενη σκίαση από τα φύλλα των φυτών, καθώς και ο θόρυβος που παράγεται από κτιριακές κατασκευές όπως τα θερμοκήπια, αυξάνουν σημαντικά τη χωρο-χρονική κλιματική διακύμανση και σε μεγάλο βαθμό δημιουργούνται προβλήματα στην επικοινωνία μεταξύ των κόμβων που αναπτύσσονται σε ένα τόσο δυσμενές περιβάλλον. Το μεταβαλλόμενο περιβάλλον θέτει τις δικές του απαιτήσεις και απαιτεί έναν νέο κύκλο ελέγχου της εργασίας, της δειγματοληψίας και του προγραμματισμού, τη συλλογή και καταγραφή των δεδομένων, την αποθήκευση και αναζήτηση των δεδομένων, τον έξυπνο έλεγχο, αλλά και για άλλες λύσεις.

Οι μονάδες που χρησιμοποιούνται για την ανίχνευση και την αναφορά οποιασδήποτε κατάστασης πρέπει να είναι αρκετά ακριβείς και κατάλληλα θωρακισμένες έναντι των περιβαλλοντικών παραγόντων που μπορεί, είτε να δώσουν ψεύτικες αναφορές, είτε να οδηγήσουν σε μόνιμη καταστροφή των αισθητήρων IoT. Επιπλέον, η αντικατάσταση της πηγής ισχύος σε κατανεμημένους κόμβους αισθητήρων οι οποίοι είναι διάσπαρτοι σε μεγάλες περιοχές μπορεί να είναι μία εργασία που θα έχει πολλές δυσκολίες, ή ενδεχομένως να είναι αδύνατον να αντικατασταθεί και θα πρέπει να λαμβάνονται υπόψη κατά τη διάρκεια του σχεδιασμού τέτοιων συστημάτων.

Σχετικά, με την επικοινωνία μεταξύ των κόμβων πολλές διαφορετικές τεχνολογίες μπορούν να συνδυαστούν από GSM έως WPAN και P2P, με τη διαλειτουργικότητα να είναι η βασικότερη πρόκληση στο σχεδιασμό ή στην ανάπτυξη τέτοιων συστημάτων, ειδικά στην έξυπνη γεωργία, όπου το φαινόμενο της υψηλής θερμοκρασίας και της υψηλής υγρασίας μπορεί να επηρεάζουν αρνητικά σε μεγάλο βαθμό τη διαλειτουργικότητα. Επίσης, σε μια περιοχή όπου έχουμε διαφορετικές μεθόδους ασύρματης επικοινωνίας, σε τοπικό επίπεδο, όπως το Bluetooth, το Zigbee και το Wi-Fi, οι παρεμβολές είναι ένα θέμα που θα πρέπει να εξεταστεί.

Με δεδομένο ότι οι συσκευές των αισθητήρων κατανέμονται σε μεγάλες εκτάσεις που δεν μπορούν να επιβλέπονται συνεχώς, το σύστημα μπορεί εύκολα να υποστεί φυσική επίθεση. Επιπλέον, οι συσκευές των αισθητήρων που διαθέτουν συστήματα εντοπισμού γεωγραφικής θέσης έχουν πιο πολύπλοκη δομή υλικού και καταναλώνουν περισσότερη ενέργεια. Τελειώνοντας, η συστηματική επίβλεψη της φυσικής ασφάλειας των συσκευών αισθητήρων, που εκτείνονται σε μεγάλες αγροτικές εκτάσεις, δεν είναι εφικτή σε ικανοποιητικό βαθμό και είναι πιο εύκολο να προστεθούν κακόβουλοι κόμβοι που θα είναι σε θέση να κρυφακούν ή/και να υποκλέπτουν τα δεδομένα που μεταδίδονται, ή να μπορούν να πραγματοποιήσουν πολλές επιθέσεις, όπως Man-in-the-Middle (MITM) ή Distributed Denial of Service (DDoS) ή.

Συμπεράσματα

Με την ολοκλήρωση της παρούσας πτυχιακής εργασίας το συμπέρασμα που βγαίνει ξεκάθαρα είναι ότι το Διαδίκτυο των Πραγμάτων (IoT) και οι εφαρμογές του έχουν γίνει πλέον μέρος της καθημερινότητας μας και όσο περνά ο καιρός βελτιώνεται όλο και περισσότερο με την τεχνολογία να εξελίσσεται.

Το Πράσινο Διαδίκτυο των Πραγμάτων έχει ως στόχο να συνδέσει δισεκατομμύρια έξυπνα πράγματα με το Διαδίκτυο, με κύριο γνώμονα την εξοικονόμηση ενέργειας και τη μεγιστοποίηση της αποδοτικότητας των συστημάτων IoT, μέσω της συνολικής και διαρκούς παρακολούθησής τους, με αποτέλεσμα να γίνεται πιο εύκολη η συλλογή και καταγραφή δεδομένων από πληθώρα αισθητήρων, καθώς και η επικοινωνία και μετάδοσή τους σε όλα τα επίπεδα, η απομακρυσμένη αποθήκευση και επεξεργασία των δεδομένων αυτών και η λήψη αποφάσεων για το συνολικό έλεγχο της βιωσιμότητας τους, σε ποικίλες περιπτώσεις της καθημερινής ζωής (έξυπνες πόλεις, έξυπνες μεταφορές, έξυπνη υγεία, έξυπνη βιομηχανία, έξυπνη γεωργία, κ.ά.).

Ένας από τους πιο σημαντικούς τομείς αφορά την πράσινη γεωργία όπου παρέχονται διάφοροι τρόποι για το πως οι αγρότες θα αξιοποιούν καλύτερα τις αγροτικές εκτάσεις τους από διάφορες άσχημες καιρικές δυσκολίες ή από προσπάθειας κλοπής της περιουσίας τους, θα ενισχύουν την απόδοση των καλλιεργειών τους και θα βελτιώνουν την ποιότητα των προϊόντων τους. Ένα άλλο θετικό στοιχείο, είναι πως το IoT εφαρμόζεται πλέον σε όλους τους τομείς της ανθρώπινης δραστηριότητας, χωρίς να είναι ιδιαίτερα ακριβό και θα βοηθήσει ακόμη περισσότερο στη καθημερινή μας ζωή.

Σε αυτή την εργασία παρουσιάστηκαν και αναλύθηκαν οι πιο σημαντικές απειλές και προκλήσεις ασφαλείας που αντιμετωπίζει σήμερα το Πράσινο Διαδίκτυο των Πραγμάτων. Επίσης, δίνεται έμφαση σε μελέτη περίπτωσης για το οικοσύστημα «πράσινου» IoT την έξυπνης γεωργίας, με ανάλυση των βασικών απειλών και προκλήσεων σε θέματα ασφάλειας που αντιμετωπίζει, καθώς και τους κύριους μηχανισμούς για την προστασία της ασφάλειας του, όπως είναι ο έλεγχος πιστοποίησης ταυτότητας των οντοτήτων που εμπλέκονται σε αυτό το οικοσύστημα IoT, καθώς και η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα των δεδομένων του, με λύσεις που βασίζονται σε τεχνολογία blockchain για να μπορέσει κάποιος να διατηρήσει το απόρρητο με τη χρήση αλγορίθμων συναίνεσης για εφαρμογές που βασίζονται σε IoT.

Προτάσεις για Μελλοντικές Επεκτάσεις

Αν και το Πράσινο Διαδίκτυο των Πραγμάτων (Green IoT) έχει πολλά πλεονεκτήματα, υστερεί από μερικές προκλήσεις και τα προβλήματα που αναφέρονται παρακάτω θα πρέπει μα εξεταστούν από ερευνητές σε μελλοντικές μελέτες.

Τεχνικές προκλήσεις

Σε γενικές γραμμές ορισμένα τεχνικά ζητήματα εμποδίζουν το να χρησιμοποιείται πάντα η εφαρμογή του GIoT. Οι οικονομικοί περιορισμοί και οι περιορισμοί υλικών εμποδίζουν σοβαρά την εφαρμογή νέων ορισμών και ιδεών στην επικράτηση των υλικών. Το ίδιο συμβαίνει και στην έλλειψη γρήγορων ανανεώσιμων υλικών και σε ορισμένες περιπτώσεις οι ασυμβατότητες των διαφορετικών υλικών μπορεί να θέσουν νέες προκλήσεις όσον αφορά το Green IoT. Επιπλέον ένα Green IoT μπορεί να συνδυαστεί με άλλα πράσινα δίκτυα για να υπάρξει η συνεργασία μίας ετερογενής δομής. Με αυτόν τον τρόπο κρατώντας τα πράσινα χαρακτηριστικά σε αυτά τα ετερογενή δίκτυα, το να διατηρήσουν την επικοινωνία είναι μία μεγάλη πρόκληση. Επιπρόσθετα, η μεγάλη διάρκεια ζωής είναι μόνιμη απαίτηση της τεχνολογίας Green IoT, συνεπώς η διάρκεια ζωής των συσκευών Green IoT θα πρέπει να είναι συμβατές με το κάθε είδος της εφαρμογής. Άρα λοιπόν αν οι συσκευές Green IoT είναι διατεθειμένες στο εμπόριο το βασικό που πρέπει να ικανοποιεί τον πελάτη αφορά τη διάρκεια ζωής που θα έχουνε. Τελειώνοντας μπορεί η ισχύς της μπαταρίας να είναι σημαντική όσον αφορά τον εξοπλισμό Green IoT που βασίζεται σε μπαταρίες αλλά οι μπαταρίες της πρέπει να είναι επίσης πράσινες.

Τυποποίηση

Η τυποποίηση είναι συνήθως μία σημαντική προϋπόθεση που αφορά τη διεισδυτικότητα της νέας τεχνολογίας λόγω των πλεονεκτημάτων της συμπεριλαμβανομένης της μείωσης κόστους, της αυξημένης απλότητας και της διασφάλισης της ποιότητας. Η έλλειψη κατάλληλων προτύπων για το Green IoT οδηγεί στην παραγωγή διάφορου εξοπλισμού των συσκευών με διαφορετικό υλικό και λογισμικό που δεν είναι συμβατό μεταξύ τους. Επομένως, ο καθορισμός των ισχυρών προτύπων είναι απαραίτητος για να επεκταθεί το Green IoT στο μέλλον. Τα συγκεκριμένα πρότυπα πρέπει να είναι ανεπτυγμένα με τέτοιο τρόπο ώστε να καλύπτουν τις απαιτήσεις των διαφόρων εφαρμογών, συμπεριλαμβανομένου των τυπικών αναγκών της βιομηχανικής ζώνης, των περιβαλλοντικών αναγκών και τις ανάγκες των ανθρώπων στις αστικές και στις αγροτικές περιοχές. Επιπλέον τα πρότυπα Green IoT θα πρέπει να κωδικοποιηθούν για τη βελτιστοποίηση της κατανάλωσης ενέργειας και της αύξησης της χωρητικότητας των πόρων του δικτύου. Ταυτόχρονα είναι απαραίτητο να εξεταστούν και άλλοι περιορισμοί στους διαθέσιμους κανόνες για τις επιτρεπόμενες ζώνες συχνοτήτων και των επιπέδων ενέργειας για τις διάφορες ραδιοεπικοινωνίες. Πέρα από αυτά τα πρότυπα θα πρέπει να αναπτυχθούν και άλλα πρότυπα σχετικά με το πράσινο χαρακτηριστικό του εξοπλισμού και των αντικειμένων. Με δεδομένο ότι αναπτύσσεται γρήγορα η αγορά του Green IoT και οι προβλέψεις για τα επόμενα χρόνια είναι σημαντικό να καθοριστούν πρότυπα για την κατανάλωση ενέργειας, την ανακύκλωση και την εκπομπή GHz και των επιβλαβών αερίων ώστε οι άνθρωποι να μην έχουν προβλήματα που θα αφορούν στο περιβάλλον.

Συμπερασματικά, μαζί με τη γρήγορο πρόοδο του Green IoT χρειάζονται τα απαραίτητα πρότυπα που πρέπει να ενημερώνονται και να αναθεωρούνται ανάλογα.

Ασφάλεια και προστασία της ιδιωτικής ζωής

Γενικά, οι απειλές για την ασφάλεια του Green IoT προέρχονται από ευάλωτα σημεία και αδυναμίες στα διάφορα επίπεδα που αφορούν εφαρμογές, διεπαφές, στοιχεία δικτύου, λογισμικού, υλικού και αντικειμένων. Στις περισσότερες εφαρμογές Green IoT ακόμη και ένα μικρό πρόβλημα ασφάλειας μπορεί να οδηγήσει σε σημαντικά προβλήματα στον έλεγχο και στο αυξημένο κόστος. Επομένως, είναι απαραίτητο να αντιμετωπιστούν τα ζητήματα ασφάλειας και να ελέγχεται η πρόσβαση των χρηστών στο Green IoT για να οριστούν τα δικαιώματα. Όσον αφορά τα αντικείμενα Green IoT συνδέονται μέσω των ασύρματων καναλιών και έχουν πολλές κοινές επιθέσεις όπως η υποκλοπή, το man in the middle, το Sybil και την παρεμβολή που όλα αυτά συμβαίνουν εύκολα στη συγκεκριμένη τεχνολογία. Η χρήση αποτελεσματικών τεχνικών κρυπτογράφησης των συστημάτων ανίχνευσης εισβολής(IDS) και των ασφαλή συστημάτων ελέγχου ταυτότητας είναι απαραίτητα για να αντιμετωπιστούν αυτές οι απειλές. Σαν συμπέρασμα μπορεί να υποστηριχθεί πως η βελτίωση στα θέματα της τεχνολογίας ασφάλειας που περιλαμβάνει την διαχείριση εμπιστοσύνης, την ασφάλεια επικοινωνίας, το απόρρητο επικοινωνίας και την ασφάλεια των εφαρμογών και των υπηρεσιών είναι προκλήσεις για το Green IoT.

Καινοτομία στο περιβάλλον Green IoT

Με δεδομένο τον μεταβαλλόμενο τρόπο ζωής και τις αυξανόμενες ανάγκες για ενέργεια, η διαχείριση αυτής θα είναι η μεγαλύτερη πρόκληση που θα έχουν να αντιμετωπίσουν οι άνθρωποι τα επόμενα χρόνια. Έτσι λοιπόν οι ενεργειακοί πόροι και τα αποθέματα πρέπει να χρησιμοποιούνται με έναν τέτοιο τρόπο που θα μπορούν να παρέχουν την ενέργεια που χρειάζεται ο παγκόσμιος πληθυσμός. Το Green IoT μπορεί να αποτελέσει το κατάλληλο εργαλείο για την επίτευξη του συγκεκριμένου σκοπού. Άλλωστε, πρέπει να αναπτυχθούν νέες τεχνολογίες και εργαλεία έτσι ώστε η διαχείριση στην κατανάλωση ενεργειών και στο Green IoT και είναι συμβατή με αυτή χωρίς καμία βασική αλλαγή.

Βιβλιογραφία

[1] "Internet of things," 24 April 2022. [Online]. Available: https://en.wikipedia.org/wiki/Internet_of_things. [Accessed 27 April 2022].

[2] S. Anand and A. Sharma, "Assessment of security threats on IoT based applications," in *Materials Today* , 2020.

[3] L. Antão, R. Pinto, J. P. Reis and G. M. Gonçalves, "Requirements for Testing and Validating the Industrial Internet of Things," in *2018 11th IEEE Conference on Software Testing, Validation and Verification*, Västerås, Sweden, 2018.

[4] N. Kaushik and T. Bagga, "Smart Cities Using IoT," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, 2021.

[5] A. E. Varjovi and S. Babaie, "Green Internet of Things (Green IoT): Vision, applications and research challenges," *Sustainable Computing: Informatics and Systems,* vol. 28, no. 100448, pp. 1-9, 18 September 2020.

[6] J. Tintu, J. Roopesh, K. A. Ajmal, K. V. A. Sajith, P. M. Sasi and G. Alexander, "IoT middleware for smart city: (An integrated and centrally managed IoT middleware for smart city)," in *2017 IEEE Region 10 Symposium (TENSYMP)*, Cochin, India, 2017.

[7] O. G. Dorobantu and S. Halunga, "Security threats in IoT," in *2020 International Symposium on Electronics and Telecommunications (ISETC)*, Timisoara, Romania, 2020.

[8] J. TAO, S. JIN, J. TANG, Y. JI and N. ZHANG, "Application of Cloud Edge Collaboration Architecture in Power IoT," in *2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA)*, Chongqing, China, 2020.