ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Διαδίκτυο των Πραγμάτων

Γιαννικουλη Αικατερινη

ΕΠΙΤΡΟΠΗ ΑΞΙΟΛΟΓΗΣΗΣ

1. Ι. Τζήμας , Αναπληρωτής Καθηγητής

2.Ι. Τσακνάκης , Αναπληρωτής Καθηγητής

3. Π. Κίτσος , Αναπληρωτής Καθηγητής

Υπεύθυνη Δήλωση Φοιτητή

Βεβαιώνω ότι είμαι συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη εργασία. Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Περίληψη

Το Internet of Things (IoT) αποτελεί μια πλατφόρμα στην οποία οι συσκευές καθημερινής χρήσης και οι διάφορες καθημερινές διαδικασίες γίνονται εξυπνότερες. Μετατρέποντας τα αντικείμενα του πραγματικού κόσμου σε πράγματα (things), προβάλει ως μια τεχνολογία που ενσωματώνει πολλές άλλες αναδυόμενες τεχνολογίες, για να αποτελέσει το μέλλον της πληροφόρησης και της επικοινωνίας. Ως φιλοσοφία λειτουργίας του IoT θεωρείται η ένωση όλων των πραγμάτων σε παγκόσμιο επίπεδο, στο πλαίσιο μιας κοινής υποδομής και έτσι ώστε να υπάρχει η δυνατότητα ελέγχου τους, αλλά και παροχής τακτικών και έγκαιρων ενημερώσεων. Η ιδέα του IoT δεν είναι νέα αλλά αποτελεί εξέλιξη πολλών σχετικών προτάσεων του παρελθόντος, που αναφέρονταν σε μια ενοποίηση των πάντων σε παγκόσμιο επίπεδο.

Σκοπός της παρούσας εργασίας, είναι η παρουσίαση μιας όσο το δυνατόν πιο ολοκληρωμένης βιβλιογραφικής ανασκόπησης του IoT, με βάση τις πλέον πρόσφατες εξελίξεις σε διάφορες πτυχές του, όπως είναι οι χρησιμοποιούμενες τεχνολογίες, οι εφαρμογές και οι προκλήσεις που αντιμετωπίζει. Για το λόγο αυτό είναι ουσιαστικά διαρθρωμένη σε τέσσερα μέρη. Αρχικά δίνεται μια συνοπτική περιγραφή και ανάλυση της έννοιας του IoT, καθώς και μια αναφορά στην ιστορική του εξέλιξη. Στη συνέχεια, γίνεται μια γενική ανάλυση των τεχνολογιών επικοινωνίας που περιλαμβάνει. Το τρίτο μέρος της εργασίας ασχολείται με τις πολυάριθμες εφαρμογές της τεχνολογίες, καλύπτοντας όσο το δυνατόν περισσότερους κλάδους στους οποίους μπορούν να υλοποιηθούν. Επιπρόσθετα, παρουσιάζονται οι τρέχουσες προκλήσεις που πρέπει να αντιμετωπίσει η τεχνολογία για να μπορέσει να ανταπεξέλθει στην υιοθέτησή της σε όλους αυτούς του τομείς. Η εργασία ολοκληρώνεται με κάποια συμπεράσματα που προκύπτουν από την ανάλυση όλων των παραπάνω θεμάτων, επισημαίνοντας κάποιες μελλοντικές ερευνητικές κατευθύνσεις που μπορούν να χρησιμοποιηθούν ως βάση αξιοποίησης καινοτόμων ιδεών πάνω στον τομέα του IoT.

Λέξεις κλειδιά: Ασφάλεια, εφαρμογές, πρωτόκολλα επικοινωνίας, τεχνολογίες πληροφοριών και επικοινωνίας, IoT.

Abstract

The Internet of Things (IoT) is a platform on which everyday devices and various daily processes become smarter. Turning real-world objects into things, IoT is an incorporation field for many emerging technologies so as to be the future of information and communication systems. IoT's operating philosophy is to unite all global things within a common infrastructure and in such a way that people can control the things but provide them with regular and timely updates. The basic idea behind IoT is not new but it is the evolution of many relevant past proposals about the unification of everything in global level.

The purpose of this study is to present the most comprehensive literature review of IoT based on the latest developments in various aspects, such as used technologies, applications and challenges. The study is structured in four parts. In the first part, a brief description and analysis of the concept of IoT is given, along with a reference to IoT historical development. In the second part, a general analysis of the communication technologies involving in IoT architecture is made. The third part of the study deals with the numerous applications of the technology, covering as many fields as possible in which IoT can be used. Finallly, the current challenges that the technology must face in order to be able to cope with its adoption in all these areas are presented. The work concludes with some aspects that emerge from the analysis of all the above issues, highlighting some future research directions that can be used as a basis for exploiting some innovative ideas in the field of IoT.

Keywords: Applications, communication protocols, information and communication technologies, IoT, security.

Πίνακας περιεχομένων

Περίληψη ..... ***iii***

Abstract ..... ***v***

1 Εισαγωγή ***1***

1.1 Θεωρητικό υπόβαθρο ***1***

1.2 Σκοπός της πτυχιακής εργασίας ***1***

1.3 Δομή της πτυχιακής εργασίας ***2***

2 Internet of Things (IoT) ***4***

2.1 Ορισμοί και εννοιολογική σημασία ***4***

2.2 Το Διαδίκτυο του μέλλοντος ***7***

2.3 Οπτικές ***10***

2.3.1 Πραγματοστρεφής οπτική *11*

2.3.2 Διαδικτυοστρεφής οπτική *12*

2.3.3 Σημασιολογικοστρεφής οπτική *14*

2.4 Τεχνικά στοιχεία ***14***

2.5 Γενικά χαρακτηριστικά και απαιτήσεις ***18***

2.6 Πλεονεκτήματα και μειονεκτήματα ***22***

3 Αρχιτεκτονική και τεχνολογίες IoT ***26***

3.1 Δομικά στοιχεία και βασική αρχιτεκτονική ***26***

3.2 Αρχιτεκτονικές δομές IoT ***28***

3.2.1 Απαιτήσεις αρχιτεκτονικών δομών *29*

3.2.2 Ταξινόμηση αρχιτεκτονικών δομών IoT *31*

3.3 Επικοινωνία IoT ***38***

3.3.1 Μοντέλα επικοινωνίας *40*

3.3.2 Είδη δικτύων IoT *42*

3.3.3 Τοπολογίες δικτύων IoT *44*

3.3.4 Κατανάλωση ενέργειας *45*

3.3.5 Χρονική ευαισθησία *46*

3.4 Τεχνολογίες και πρωτόκολλα επικοινωνίας IoT ***47***

3.4.1 Τεχνολογίες επικοινωνίας IoT μικρού εύρους κάλυψης *50*

3.4.2 Τεχνολογίες επικοινωνίας IoT μεγάλου εύρους κάλυψης *54*

3.5 Πρωτόκολλα ανωτέρου στρώματος ***57***

4 Εφαρμογές IoT ***63***

4.1 Γενικά ***63***

4.2 Εφαρμογές υγειονομικής περίθαλψης ***64***

4.3 Εφαρμογές περιβάλλοντος ***68***

4.4 Εφαρμογές έξυπνης πόλης ***71***
4.5 Εμπορικές εφαρμογές ***75***
4.6 Βιομηχανικές εφαρμογές ***78***
5 Ζητήματα & Προκλήσεις IoT ***82***
5.1 Ταξινόμηση των προκλήσεων ***82***
5.2 Τυποποίηση ***83***
5.3 Αρχιτεκτονική δομή ***84***
5.3.1 Αρχιτεκτονικές hardware υλικού και δικτύου *85*
5.3.2 Αρχιτεκτονικές λογισμικού *86*
5.4 Διαλειτουργικότητα ***87***
5.4.1 Τεχνική διαλειτουργικότητα *88*
5.4.2 Συντακτική διαλειτουργικότητα *92*
5.4.3 Σημασιολογική διαλειτουργικότητα *92*
5.4.4 Οργανωτική διαλειτουργικότητα *93*
5.5 Διαθεσιμότητα και αξιοπιστία ***93***
5.6 Αποθήκευση, επεξεργασία και οπτικοποίηση δεδομένων ***95***
5.7 Επεκτασιμότητα ***98***
5.8 Ποιότητα QoS ***99***
5.9 Κατανάλωση ενέργειας ***100***
5.10 Ασφάλεια και προστασία της ιδιωτικότητας ***101***
Συμπεράσματα ***106***
Βιβλιογραφία ***109***
Συντομογραφίες ***127***

Πίνακας πινάκων

Πίνακας 3-1: Λειτουργία στρωμάτων αρχιτεκτονικής δομής IoT [57].....38
Πίνακας 3-2: Βασικά στοιχεία ασύρματων τεχνολογιών IoT μικρού εύρους κάλυψης.....50
Πίνακας 3-3: Βασικά στοιχεία ασύρματων τεχνολογιών IoT μεγάλου εύρους κάλυψης 55
Πίνακας 3-4: Σύγκριση δημοφιλών πρωτοκόλλων μηνυμάτων IoT 58
Πίνακας 4-1: Σύνοψη εφαρμογών υγειονομικής περίθαλψης IoT.....67
Πίνακας 4-2: Σύνοψη εφαρμογών περιβάλλοντος IoT 70
Πίνακας 4-3: Σύνοψη εφαρμογών IoT στο πλαίσιο των έξυπνων πόλεων 73
Πίνακας 4-4: Σύνοψη εμπορικών εφαρμογών IoT 77
Πίνακας 4-5: Σύνοψη βιομηχανικών εφαρμογών IoT 80

Πίνακας εικόνων

Εικόνα 2-1: Ορισμός του IoT σύμφωνα με το IERC [12] 6
Εικόνα 2-2: Μετασχηματισμός του Διαδικτύου – από την προ-Διαδικτυακή φάση στο IoT [15] 8
Εικόνα 2-3: Αριθμός διασυνδεδεμένων έξυπνων συσκευών σε παγκόσμιο επίπεδο [16] 9
Εικόνα 2-4: Gartner Hype Cycle για την τεχνολογία IoT (2020) [19] 10
Εικόνα 2-5: Οι τρεις προοπτικές του IoT [4] 11
Εικόνα 2-6: Διαφορετικές απόψεις σχετικά με το σύνολο των τεχνικών στοιχείων του IoT [34] 15
Εικόνα 2-7: Τεχνολογικός χάρτης της πορείας του IoT [47] 22
Εικόνα 3-1: Δομικά στοιχεία της αρχιτεκτονικής του IoT [50] 26
Εικόνα 3-2: Βασική αρχιτεκτονική δομή του IoT [51] 27
Εικόνα 3-3: Ταξινόμηση αρχιτεκτονικών IoT [57] 32
Εικόνα 3-4: Μοντέλα επικοινωνίας συσκευών IoT [70] 40
Εικόνα 3-5: Είδη δικτύων IoT [73] 42
Εικόνα 3-6: Τοπολογίες δικτύων IoT [74] 44
Εικόνα 3-7: Ασύρματες τεχνολογίες επικοινωνίας IoT [71] 49
Εικόνα 4-1: Ταξινόμηση εφαρμογών IoT 64
Εικόνα 5-1: Ζητήματα ασφάλειας και ιδιωτικότητας IoT [222] 102

1 Εισαγωγή

1.1 Θεωρητικό υπόβαθρο

Τα τελευταία χρόνια, η χρήση του Διαδικτύου και των τεχνολογιών πληροφορίας και επικοινωνίας έχει επεκταθεί τόσο πολύ σε όλους τους τομείς της καθημερινότητας που έχει καταστήσει το έργο των ερευνητών ιδιαίτερα δύσκολο ως προς τον εντοπισμό της βέλτιστης δυναμικής της. Η επέκταση αυτή έχει ξεπεράσει τα όρια της απλής σύνδεσης υπολογιστών ή υπολογιστικών συστημάτων με σκοπό τη δημιουργία ενός δικτύου ανταλλαγής πληροφοριών, καθώς με την πάροδο του χρόνου όλο και μεγαλύτερος αριθμός συσκευών, πολλών διαφορετικών ειδών, μπορεί να χρησιμοποιήσει το Διαδίκτυο ως μέσω διασύνδεσης. Με τον τρόπο αυτό, ο όρος του Διαδικτύου έχει εξελιχθεί σε κάτι ευρύτερο που περιλαμβάνει τη διασύνδεση μεταξύ συσκευών καθώς και τη διασύνδεση των ανθρώπων με τις συσκευές και είναι γνωστό ως Διαδίκτυο των Πραγμάτων (Internet of Things – IoT). Στο πλαίσιο του IoT καθετί που μπορεί να συνδεθεί στο Διαδίκτυο λογίζεται ως οντότητα και παίρνει την ονομασία του "πράγματος" (thing). Τα "πράγματα" συμπεριλαμβάνουν μια τεράστια γκάμα οντοτήτων, όπως συσκευές, αισθητήρες, εξοπλισμούς, λογισμικά, υπηρεσίες, κλπ. [1]

Το IoT θεωρείται ως το Διαδίκτυο του μέλλοντος το οποίο θα μπορεί να υποστηρίξει την ευφυή επικοινωνία μεταξύ δισεκατομμυρίων "πραγμάτων". Η επικοινωνία αυτή μπορεί να γίνει μέσω πολλών και διαφορετικών τεχνολογιών, όπως τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks - WSN), οι ραδιοσυχνότητες αναγνώρισης (Radio-Frequency Identification - RFID), το Bluetooth, η επικοινωνία κοντινού πεδίου (Near Field Communication - NFC), τα ασύρματα δίκτυα κινητής τηλεφωνίας LTE (Long Term Evolution), τα δίκτυα 5G και πολλές άλλες [2]. Συνεπώς, το IoT δεν είναι τίποτα άλλο παρά μια υποδομή δικτύου πληροφοριών, παγκόσμιας κλίμακας και δυναμικού χαρακτήρα, που βασίζεται σε πλήθος προτύπων και πρωτοκόλλων επικοινωνίας, στο οποίο μπορούν να συνδεθούν φυσικά και τα εικονικά "πράγματα" μέσω έξυπνων διασυνδέσεων. Το εν λόγω δίκτυο δίνει τη δυνατότητα μεταφοράς πληροφοριών που συλλέγονται από διάφορες συσκευές σε όλο τον κόσμο μέσω του Διαδικτύου [3].

1.2 Σκοπός της πτυχιακής εργασίας

Σκοπός της παρούσας πτυχιακής εργασίας είναι η ανάλυση της τρέχουσας κατάστασης του IoT. Σε αυτό το πλαίσιο, θα γίνει μια βιβλιογραφική επισκόπηση των μελετών που έχουν

εμφανιστεί με αντικείμενο το IoT τα τελευταία πέντε χρόνια. Η βιβλιογραφική επισκόπηση αφορά την προέλευση και την ιστορική εξέλιξη του IoT, την τρέχουσα κατάστασή του, τις τεχνολογίες που χρησιμοποιεί, τις εφαρμογές του και τους κλάδους που αυτές μπορούν να καλύψουν, καθώς και τις προκλήσεις που αντιμετωπίζει όσον αφορά την μελλοντική του εξέλιξη. Μια τέτοια βιβλιογραφική επισκόπηση μπορεί να λειτουργήσει ως σημείο αναφοράς κατανόησης των βασικών στοιχείων της τεχνολογίας.

Η επίτευξη αυτού του σκοπού θα πραγματοποιηθεί μέσα από μια όσο το δυνατόν πιο διεξοδική και περιεκτική ανασκόπηση της διεθνούς βιβλιογραφίας. Η βιβλιογραφία που θα χρησιμοποιηθεί θα περιλαμβάνει μελέτες, άρθρα και πηγές που θα βρεθούν στο Διαδίκτυο, η αναζήτηση των οποίων θα γίνει μέσω χρήσης των βάσεων δεδομένων PubMed, Google Scholar και Google.

1.3 Δομή της πτυχιακής εργασίας

Στα πλαίσια της παρούσας πτυχιακής εργασίας, για την βιβλιογραφική ανασκόπηση της τεχνολογίας του IoT επιλέχθηκε η ακόλουθη δομή.

Το κεφάλαιο 2 αναλύει την έννοια του IoT, την εξελικτική του πορεία και τους στόχους εφαρμογής του. Αρχικά δίνονται κάποιοι ορισμοί και αναλύεται η εννοιολογική σημασία της τεχνολογίας. Στη συνέχεια δίνεται μια περιγραφή του συσχετισμού Διαδικτύου και IoT. Έπειτα, αναλύονται στοιχεία του IoT, όπως οι προοπτικές του, τα τεχνικά στοιχεία, τα γενικά χαρακτηριστικά και οι απαιτήσεις εφαρμογής του. Το κεφάλαιο ολοκληρώνεται με μια αναφορά στα πλεονεκτήματα και μειονεκτήματα που παρουσιάζει η τεχνολογία.

Το κεφάλαιο 3 ασχολείται με την αρχιτεκτονική δομή του IoT και τα πρότυπα και πρωτόκολλα που εμπεριέχει κάθε στρώμα της. Αρχικά γίνεται μια αναφορά των δομικών στοιχείων του IoT. Στη συνέχεια γίνεται μια ταξινόμηση των αρχιτεκτονικών δομών της τεχνολογίας. Έπειτα δίνονται κάποια στοιχεία σχετικά με τις επικοινωνίες στο IoT και αναφέρονται τα πρωτόκολλα ασύρματης επικοινωνίας τα οποία έχουν ταξινομηθεί με βάση

της εμβέλεια κάλυψής τους. Τέλος γίνεται μια μικρή περιγραφή των πρωτοκόλλων που εμπεριέχονται στο στρώμα εφαρμογών του IoT.

Στο κεφάλαιο 4 γίνεται μια ταξινόμηση των δημοφιλέστερων εφαρμογών του IoT με βάση την μεγαλύτερη εμφάνισή τους στις μελέτες της τελευταίας πενταετίας.

Στο κεφάλαιο 5 αναλύονται οι μεγαλύτερες προκλήσεις που παρουσιάζει η τεχνολογία ως προς την πλήρη υιοθέτησή της, δίνοντας μεγάλη έμφαση σε κάποιες από αυτές, όπως είναι η ασφάλεια και η προστασία της ιδιωτικότητας.

Τέλος, η εργασία ολοκληρώνεται με κάποια συμπέρασμα που απεικονίζουν την ουσία της παρούσας βιβλιογραφικής εργασίας με θέμα το IoT.

2 Internet of Things (IoT)

2.1 Ορισμοί και εννοιολογική σημασία

Μελετώντας τη βιβλιογραφία σχετικά με τον όρο του IoT, μπορεί εύκολα να γίνει αντιληπτό ότι δεν υπάρχει κάποιος ορισμός του που να είναι αποδεκτός από όλους. Ο λόγος είναι ότι η μελέτη της τεχνολογίας έχει γίνει από τόσο διαφορετικές σκοπιές που είναι εύλογο να της αποδοθούν διαφορετικοί ορισμοί οι οποίοι αντανακλούν τις διαφορετικές προοπτικές προσέγγισής της. Πολλοί από τους ορισμούς που έχουν δοθεί στο IoT από διάφορους ερευνητές έχουν εκφραστεί με βάση τη στάση τους απέναντι στα δυνατά σημεία της ιδέας. Ο λόγος αυτής της ασάφειας προέρχεται από το ίδιο το όνομα της έννοιας "Διαδίκτυο των Πραγμάτων" που αποτελείται από δύο λέξεις. Η πρώτη λέξη δίνει έμφαση στην οπτική της δικτύωσης αυτής της έννοιας, ενώ η δεύτερη λέξη τονίζει τη χρήση του όρου "πράγματα" ως γενικά αντικείμενα που αντιμετωπίζονται με τον ίδιο τρόπο ανάλογα με το περιβάλλον στο οποίο χρησιμοποιούνται [4].

Ο πρώτος ορισμός του IoT προήλθε από μία "πραγματοστρεφή" οπτική (things oriented perspective), σύμφωνα με την οποία οι ετικέτες RFID θεωρήθηκαν ως πράγματα. Σύμφωνα με την κοινότητα RFID, το IoT μπορεί να οριστεί ως [5]: *"Το παγκόσμιο δίκτυο διασυνδεδεμένων αντικειμένων, μοναδικά διευθυνσιοδοτημένων βάσει τυπικών πρωτοκόλλων επικοινωνίας"*.

Σύμφωνα με τους Dorsemaine και συν. (2015) [6]: *"Το IoT είναι μια ομάδα υποδομών διασύνδεσης αισθητήρων και / ή ενεργοποιητών με (περιορισμένες) υπολογιστικές δυνατότητες υπολογιστών, που επιτρέπουν τη διαχείρισή τους και την πρόσβαση και μεταφορά των δεδομένων που δημιουργούν μέσω του Διαδικτύου, χωρίς να απαιτείται η ανθρώπινη παρέμβαση"*.

Οι Minerva, Biru & Rotondi (2015).πιστεύουν ότι [7]: *"Το IoT είναι ένα παγκόσμιο δίκτυο και υποδομή υπηρεσιών μεταβλητής ευαισθησίας και συνδεσιμότητας, με δυνατότητα αυτο-*

διαμόρφωσης βάσει προτύπων, διαλειτουργικών προτύπων και μορφών, που αποτελούνται από ετερογενή πράγματα τα οποία έχουν ταυτότητα, φυσικές και εικονικές ιδιότητες και είναι αδιάλειπτα και ασφαλώς ενσωματωμένα στο Διαδίκτυο".

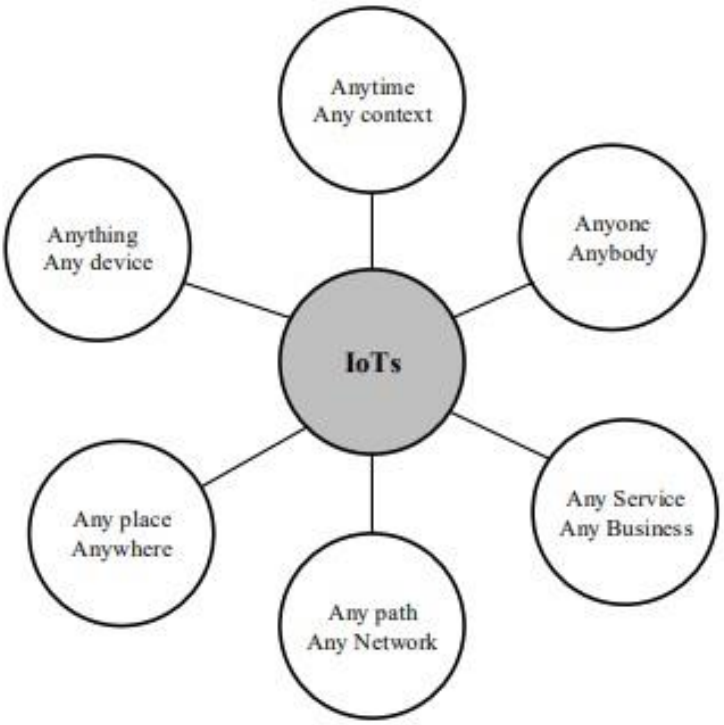
Το 2015, το Συμβούλιο Αρχιτεκτονικής Διαδικτύου (Internet Architecture Board - IAB) δημοσίευσε το περιοδικό *" Architectural Considerations in Smart Object Networking"* στο οποίο αναφέρεται ότι [8]: *"Ο όρος "Internet of Things" (IoT) υποδηλώνει μια τάση όπου ένας μεγάλος αριθμός συσκευών χρησιμοποιούν υπηρεσίες επικοινωνίας που προσφέρονται από πρωτόκολλα του Διαδικτύου. Πολλές από αυτές τις συσκευές, που συχνά ονομάζονται "έξυπνα αντικείμενα", δεν ελέγχονται άμεσα από τους ανθρώπους, αλλά αποτελούν στοιχεία κτιρίων ή οχημάτων, ή είναι διασκορπισμένες στο περιβάλλον"*.

Κοινή συνισταμένη όλων αυτών των ορισμών που έχουν δοθεί στο IoT, αποτελεί ένα σενάριο συνύπαρξης αντικειμένων, συσκευών και αισθητήρων που έχουν δυνατότητες αυτό-διαμόρφωσης, δικτυακής συνδεσιμότητας και υπολογιστικής ισχύος, τα οποία όμως δεν θεωρούνται ως υπολογιστές. Κύριο χαρακτηριστικό αυτών των συσκευών αποτελεί επίσης η ελάχιστη έως καμία ανθρώπινη παρέμβαση στη δημιουργία, ανταλλαγή και αποθήκευση πληροφοριών. Στο πλαίσιο του IoT, δυνατότητα διασύνδεσης έχουν οι ομογενείς αλλά και οι ετερογενείς συσκευές. Επίσης, δίνεται η δυνατότητα χρήσης εργαλείων (πράγματα) που να αλληλοεπιδρούν και να συντονίζονται μεταξύ τους, μειώνοντας έτσι την ανθρώπινη παρέμβαση στη βασική καθημερινή τους λειτουργία [9].

Το IoT συνδυάζει διαφορετικές τεχνολογίες σε ένα ημιαυτόνομο δίκτυο. Συνδέει μεμονωμένες συσκευές στο δίκτυο αλλά και μεταξύ τους. Σε ένα δίκτυο IoT περιλαμβάνονται επίσης συστήματα ελεγκτών (λογισμικό και υπηρεσίες), τα οποία αναλύουν και επεξεργάζονται τα δεδομένα που συλλέγονται από τις συνδεδεμένες συσκευές, με απώτερο σκοπό τη λήψη αποφάσεων και την έναρξη ανάλογων διαδικασιών [10]. Βασικός στόχος του IoT αποτελεί η χρήση του Διαδικτύου για την ανά πάσα στιγμή και σε οποιδήποτε χώρο αναγνώριση, απόκτηση πρόσβασης και έλεγχο των διασυνδεδεμένων πραγμάτων [11]. Το IoT έχει τη δυνατότητα να εκτείνει το δυναμικό χαρακτήρα του Διαδικτύου πέρα από τη

διασύνδεση υπολογιστών και smartphone και να την εφαρμόσει σε μια ευρεία γκάμα πραγμάτων, διεργασιών και περιβαλλόντων. Τα διασυνδεδεμένα δίκτυα συσκευών μπορούν να οδηγήσουν στη δημιουργία ενός μεγάλου αριθμού έξυπνων και αυτόνομων εφαρμογών και υπηρεσιών με σημαντικά προσωπικά, επαγγελματικά και οικονομικά οφέλη, συμβάλλοντας όμως παράλληλα στην πολυπλοκότητα του IoT [9].

Με βάση τα όσα αναφέρθηκαν, προκύπτει το συμπέρασμα ότι ο πιο περιεκτικός ορισμός που έχει δοθεί για το IoT, εκφράζοντας την εννοιολογική του σημασία, είναι αυτός που δόθηκε από το IERC (IoT European Research Cluster), σύμφωνα με τον οποίο (Εικ. 2-1) [12]: *"Το IoT επιτρέπει σε άτομα και πράγματα να συνδεθούν οποτεδήποτε, οπουδήποτε, με οτιδήποτε και οποιονδήποτε, ιδανικά χρησιμοποιώντας οποιαδήποτε διαδρομή / δίκτυο και υπηρεσία"*.



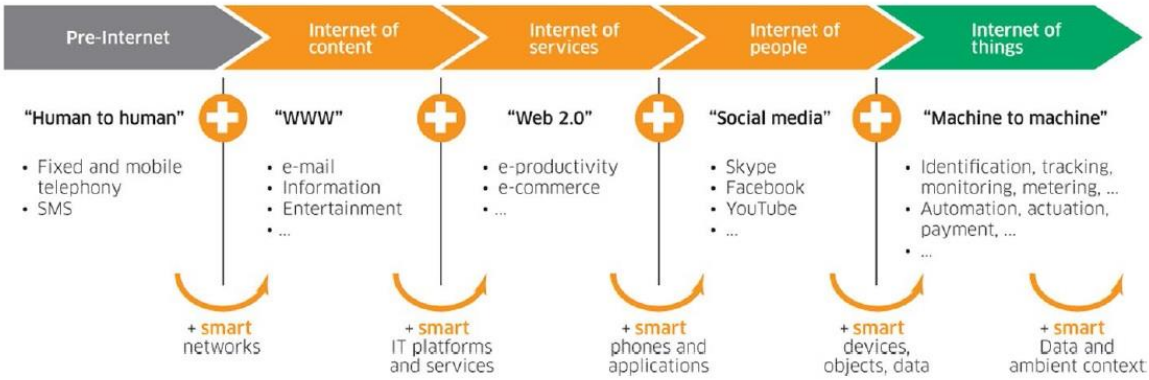
Εικόνα 2-1: Ορισμός του IoT σύμφωνα με το IERC [12]

2.2 Το Διαδίκτυο του μέλλοντος

Η εμφάνιση του IoT θεωρείται από πολλούς ως ένα από τα πλέον αξιοσημείωτα φαινόμενα στην ιστορία της ψηφιακής υπολογιστικής, που βασίστηκε στην ανάπτυξη και εξέλιξη του ευρέως χρησιμοποιούμενου παγκόσμιου δικτύου, του Διαδικτύου, σε συνδυασμό με την ανάπτυξη της διάχυτης υπολογιστικής (ubiquitous computing) και το μετασχηματισμό των υπολογιστών και των κινητών σε έξυπνα αντικείμενα που δημιουργεί νέες ευκαιρίες υλοποίησης καινοτόμων λύσεων σε διάφορες πτυχές της ζωής [13]. Στα τέλη της δεκαετίας του ’90, ο Kevin Ashton, ένας από τους συνιδρυτές του Auto-ID Center του MIT (Massachusetts Institute of Technology), ήταν ο πρώτος που ανέφερε τον όρο IoT, περιγράφοντάς τον ως ένα σύστημα διασύνδεσης του φυσικού κόσμου με το Διαδίκτυο, μέσω της χρήσης ετικετών RFID και διάχυτων συσκευών αισθητήρων, που παρατηρούν και αναγνωρίζουν τον πραγματικό κόσμο [14].

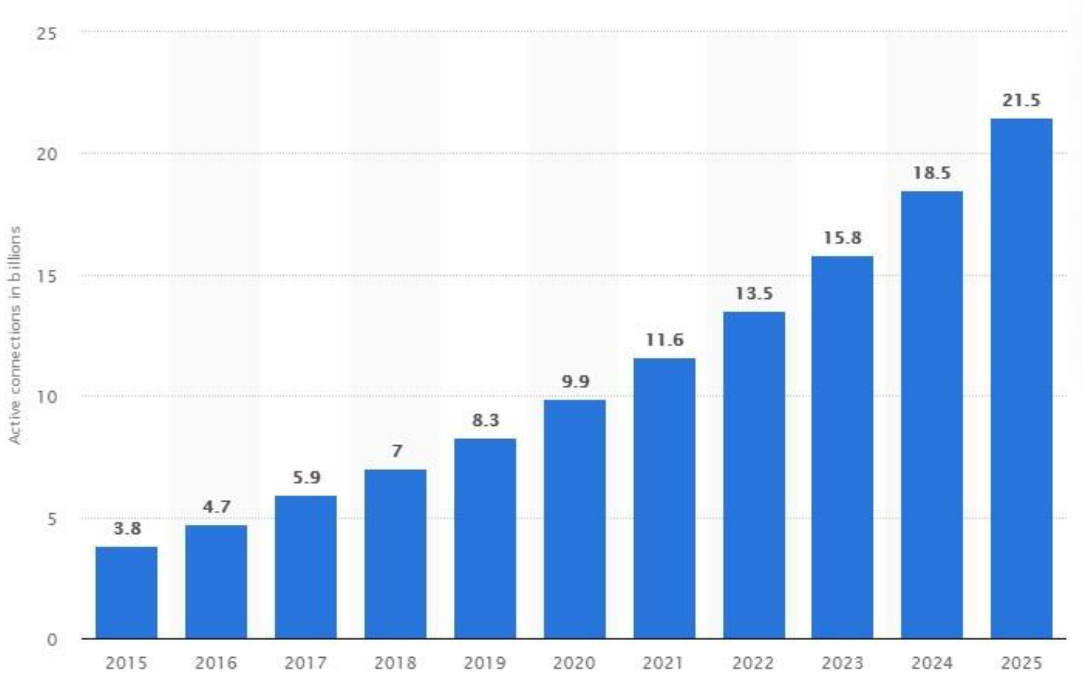
Κατά την εξέλιξη του Διαδικτύου στο IoT, μεσολάβησαν πολλές φάσεις (Εικ. 2-2). Στην πρώτη φάση, γνωστή ως προ-Διαδικτυακή φάση, η επικοινωνία ήταν δυνατή μέσω της σταθερής τηλεφωνίας. Αργότερα το μέσο επικοινωνίας αναβαθμίστηκε με τη χρήση των συσκευών κινητής τηλεφωνίας, μέσω των οποίων ήταν δυνατή η εφαρμογή της υπηρεσίας σύντομων μηνυμάτων (SMS). Η δεύτερη φάση αποτελεί τη φάση του Διαδικτύου του Περιεχομένου. Σε αυτή τη φάση ήταν δυνατή η αποστολή μηνυμάτων μεγάλου μεγέθους με τη μορφή μηνυμάτων ηλεκτρονικού ταχυδρομείου (e-mail) που ήταν ικανά να περιέχουν και συνημμένα αρχεία. Βασικές δυνατότητες αυτής της φάσης ήταν η υποστήριξη της μεταφοράς πληροφοριών, η ψυχαγωγία κ.λπ. Το Διαδίκτυο των Υπηρεσιών αποτελεί την τρίτη φάση αυτής της εξέλιξης. Βασικό στοιχείο αυτής της φάσης, γνωστής και ως Web 2.0, ήταν η παροχή υπηρεσιών με τη μορφή ηλεκτρονικών εφαρμογών, όπως το ηλεκτρονικό εμπόριο (e-commerce), κ.λπ. Η τέταρτη φάση, δηλαδή το Διαδίκτυο των Ανθρώπων, αποτέλεσε τη φάση κατά την οποία οι άνθρωποι συνδέθηκαν μεταξύ τους μέσω των κοινωνικών και πολλών άλλων μέσων, όπως τα Facebook, Skype, Youtube κ.λπ. Η τελευταία φάση, δηλαδή η εποχή του IoT, αφορά τη δυνατότητα σύνδεσης πολλών συσκευών μέσω του Διαδικτύου και της μεταξύ τους επικοινωνίας για την εκτέλεση διάφορων κατευθυνόμενων δραστηριοτήτων,

ανάλογα με το σχεδιασμό και τις λειτουργικές δυνατότητές τους. Ωστόσο, η σύγχρονη φάση μπορεί να μην αποτελεί το τέλος της εξέλιξης του Διαδικτύου στο IoT. Οι ερευνητές προσπαθούν να ενσωματώσουν την έννοια της τεχνητής νοημοσύνης (Artificial Intelligence - AI) σε αυτές τις διασυνδεδεμένες συσκευές, έτσι ώστε να μπορούν να λαμβάνουν τις απαραίτητες αποφάσεις και να ενεργούν με μηδενική ανθρώπινη παρέμβαση [15].



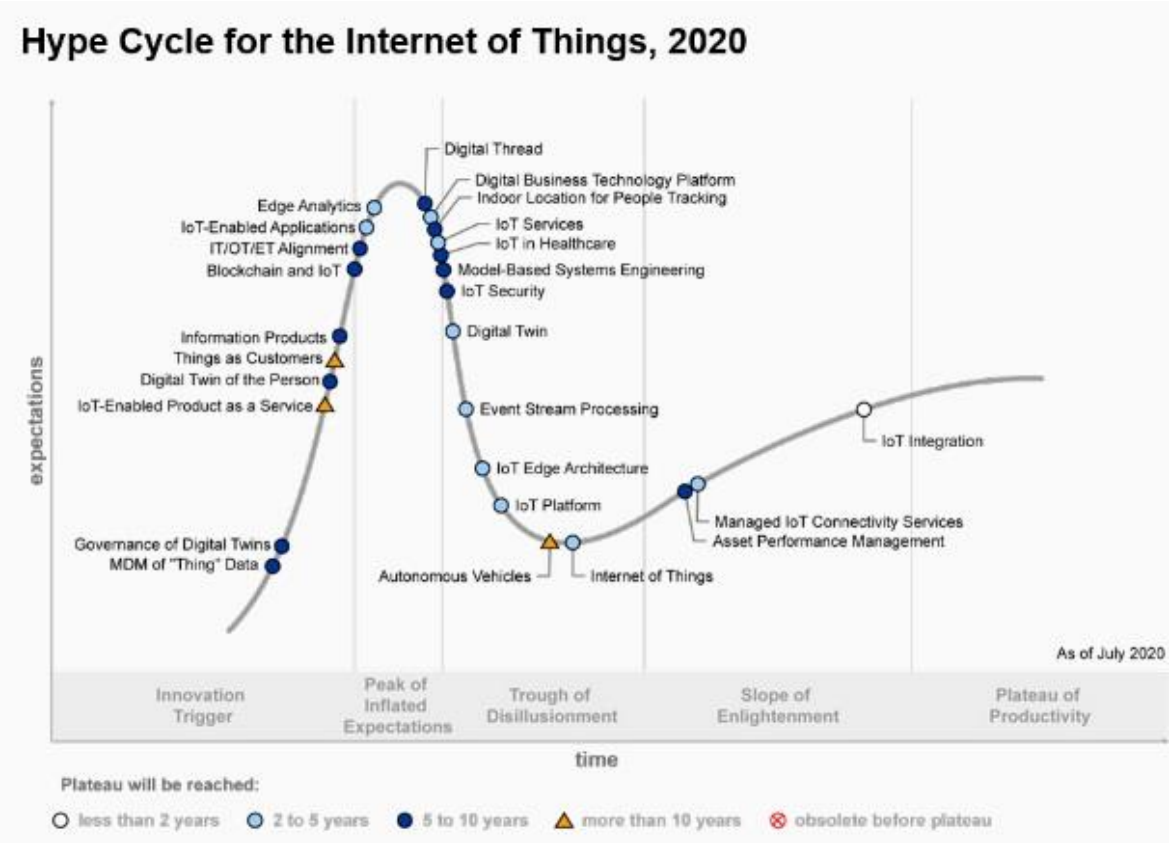
Εικόνα 2-2: Μετασχηματισμός του Διαδικτύου – από την προ-Διαδικτυακή φάση στο IoT [15]

Η τελευταία δεκαετία, στιγματίστηκε από δύο σημαντικά στοιχεία: (α) το Διαδίκτυο έχει αναμφίβολα γίνει σημείο αναφοράς όσον αφορά την επικοινωνία και (β) παρατηρήθηκε μια απότομη ροπή προς την υιοθέτηση των αναδυόμενων τεχνολογιών επικοινωνίας σε όλους τους τομείς. Σύμφωνα με πρόσφατη έρευνα της Statista (Ιανουάριος 2021), ο αριθμός των έξυπνων συσκευών που έχουν χρησιμοποιηθεί μέχρι το τέλος του 2020, ανήλθε σε σχεδόν 10 δισεκατομμύρια, ένας αριθμός που πιστεύεται να φτάσει τις 21,5 δισεκατομμύρια συσκευές το 2025. Σε αυτόν τον αριθμό περιλαμβάνονται ενεργοί κόμβοι/συσκευές ή πύλες που περιέχουν αισθητήρες και όχι καταναλωτικές συσκευές όπως υπολογιστές και κινητά τηλέφωνα (Εικ. 2-3) [16]. Το αγοραίο εισόδημα της τεχνολογίας έφτασε τα 100 δισεκατομμύρια δολάρια για πρώτη φορά το 2017, ενώ έως το 2025 αναμένεται να φτάσει τα 1,6 τρισεκατομμύρια [17].



Εικόνα 2-3: Αριθμός διασυνδεδεμένων έξυπνων συσκευών σε παγκόσμιο επίπεδο [16]

Κάτι ανάλογο προκύπτει και από τη μελέτη του γραφήματος Hype Cycle του IoT. Το Hype Cycle είναι ένα γράφημα που απεικονίζει την ωριμότητα των αναδυόμενων τεχνολογιών και δημιουργήθηκε από το αμερικανικό ερευνητικό και συμβουλευτικό ινστιτούτο Gartner με σκοπό την αποτύπωση του κύκλου ζωής των αναδυόμενων τεχνολογιών. Το συγκεκριμένο γράφημα χωρίζεται σε πέντε (5) φάσεις, ξεκινώντας από την στιγμή που εμφανίζεται μια τεχνολογία (Innovation trigger), μέχρι να φτάσει στο επόμενο στάδιο, στο οποίο έχει την μέγιστη προβολή και τις μέγιστες προσδοκίες (Peak of Inflated Expectations). Οι προσδοκίες για τις τεχνολογίες που βρίσκονται στο σημείο αυτό είναι πολύ μεγάλες, αλλά μόνο λίγες φτάνουν σχετικά άμεσα στην εμπορική αξιοποίηση (Plateau of Productivity) [18]. Το Hype Cycle που δημιούργησε το ινστιτούτο Gartner για το IoT το 2020 (Εικ. 2-4) δείχνει ότι η πλατφόρμα IoT βρίσκεται στο μέγιστο επίπεδο προσδοκιών, όπου το ποσοστό εξάρτησης και οι αυξημένες προσδοκίες δημιουργούν τις κατάλληλες προϋποθέσεις για νέες έρευνες ως προς τις νέες εξελίξεις της τεχνολογίας. Ως προς την εμπορική της αξιοποίηση, το γράφημα δείχνει ότι αυτή απέχει μόλις 2 χρόνια από την υλοποίηση [19].

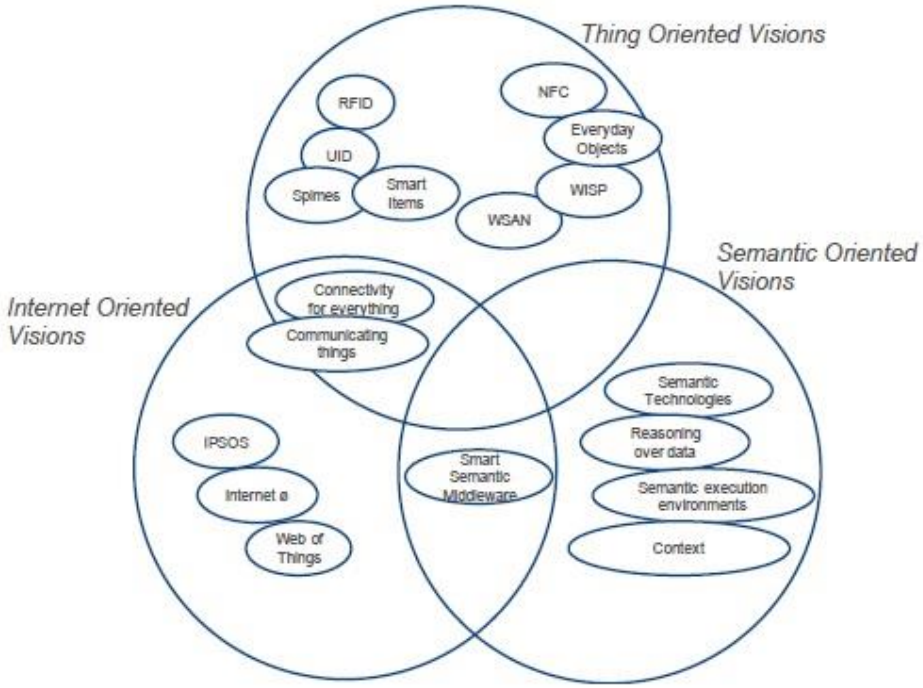


Εικόνα 2-4: Gartner Hype Cycle για την τεχνολογία IoT (2020) [19]

2.3 Οπτικές

Όπως προαναφέρθηκε σε προηγούμενη ενότητα, το IoT στερείται ενός κοινώς αποδεκτού και καθιερωμένου ορισμού, λόγω του ενδιαφέροντος που έχει παρουσιαστεί ως προς την ανάλυσή του από πολλούς ερευνητές σε διαφορετικούς τομείς. Κάθε ένας από αυτούς τους τομείς επικεντρώνεται σε διαφορετικές πτυχές των βασικών ιδεών του IoT και εισέρχεται σε διαφορετικά στάδια της εξελικτικής του πορείας. Με τον τρόπο αυτό εκτός από μια πλειάδα ορισμών, διαμορφώνεται και ένα πλήθος διαφορετικών οπτικών των προοπτικών του IoT. Επί της ουσίας όμως, οι θεμελιώδεις οπτικές της τεχνολογίας, όπως αυτές είχαν παρουσιαστεί στη μελέτη των Atzori και συν. (2010), δεν έχουν μεταβληθεί ιδιαίτερα στη διάρκεια της εξελικτικής πορείας της. Οι οπτικές είναι τρεις (Εικ. 2-5) [4]: (α) η Πραγματοστρεφής οπτική

(Thing Oriented Perspective), (β) η Διαδικτυοστρεφής οπτική (Internet Oriented Perpective) και (γ) η Σημασιολογικοστρεφής οπτική (Semantic Oriented Perspective).



Εικόνα 2-5: Οι τρεις προοπτικές του IoT [4]

Η ανάλυση των οπτικών αυτών, που θα ακολουθήσει, σε συνδυασμό με την σύντομη αναφορά στην εξέλιξη του IoT, θα δώσει μια πιο σαφή εικόνα της δημιουργίας τόσο πολλών ορισμών που του δόθηκαν στην προσπάθεια των μελετητών να καθορίσουν την έννοια του.

2.3.1 Πραγματοστρεφής οπτική

Αυτή η οπτική μπορεί να θεωρηθεί ως η πρώτη οπτική του IoT. Εστιάζοντας στην τεχνολογία RFID, τα δίκτυα WSN και τα έξυπνα αντικείμενα, θεωρεί τα "πράγματα" (μαζί με την ταυτότητα, τη λειτουργικότητα και τις πληροφορίες τους) ως τον πυρήνα του IoT [12]. Σύμφωνα με τους Atzori και συν. (2010), οι βασικές τεχνολογίες αυτής της οπτικής είναι οι RFID και NFC, που παρέχουν ασύρματη επικοινωνία μικρής έως μεσαίας εμβέλειας. Η χρήση αυτών των τεχνολογιών στις εφαρμογές των καθημερινών αντικειμένων δημιουργεί την έννοια των spime.

Τα spime είναι θεωρητικά αντικείμενα, χαρακτηριστικό του IoT, που μπορούν να παρακολουθούνται μέσω του χώρου και του χρόνου καθόλη τη διάρκεια του κύκλου ζωής τους. Ένας spime συσχετίζεται με τον κάτοχό του και περιέχει πληροφορίες σχετικά με τους προηγούμενους κατόχους του και το περιεχόμενό του (π.χ. από ποιο υλικό είναι κατασκευασμένο, κ.λπ.). Επιπλέον, αυτά τα αντικείμενα αναγνωρίζονται μοναδικά, κάτι που απαιτεί προηγμένα σχήματα διευθυνσιοδότησης, ικανά να διατηρούν μεγάλο αριθμό αντικειμένων [20]. Η έννοια του spime είναι μάλλον θεωρητική, ωστόσο έχει ήδη πρακτική εφαρμογή με τη μορφή των έξυπνων αντικειμένων.

Τα έξυπνα αντικείμενα είναι συσκευές με δυνατότητες ανίχνευσης, αποθήκευσης, ασύρματης επικοινωνίας και επεξεργασίας. Επιπλέον, πρέπει να είναι ικανά για αυτόνομες ενέργειες με βάση τη συνειδητοποίηση και τη συνεργατική επικοινωνία [21]. Αυτές οι απαιτήσεις των έξυπνων αντικειμένων συνάδουν με τις προαναφερθείσες βασικές ιδέες του IoT. Τα έξυπνα αντικείμενα ουσιαστικά αντιπροσωπεύουν την έννοια των “πραγμάτων”, τα οποία δεν χρειάζεται να περιορίζονται σε φυσικά αντικείμενα, αλλά μπορούν να αφορούν και εικονικές οντότητες [7]. Τα πράγματα είναι υπεύθυνα για τη συλλογή, βραχυπρόθεσμη αποθήκευση και μετάδοση πληροφοριών και ανάλογα με το σκοπό τους παρουσιάζουν διάφορες ιδιότητες [22]. Στη βιβλιογραφία, σε αυτές τις ιδιότητες των πραγμάτων αποδίδονται διαφορετικά ονόματα αλλά ουσιαστικά έχουν την ίδια σημασία. Κάποιες από τις ιδιότητες των πραγμάτων είναι [23]: (α) η μοναδική αναγνώριση, (β) η συνεχής παρακολούθηση, (γ) η ανίχνευση, (δ) η ενεργοποίηση και (ε) η επεξεργασία.

2.3.2 Διαδικτυοστρεφής οπτική

Αυτή η οπτική στοχεύει στην ενσωμάτωση της εκάστοτε εξέλιξης του Διαδικτύου στη νέα υποδομή του IoT ή το αντίστροφο. Θεωρώντας ότι το IoT μπορεί να αποτελεί επέκταση ή και εξέλιξη του σύγχρονου Διαδικτύου, οι prosumer δεν είναι πλέον απαραίτητο να είναι άνθρωποι. Ο όρος prosumer προέρχεται από σύντμηση των όρων producer και consumer. Επομένως, ένας prosumer δημιουργεί και καταναλώνει πληροφορίες / περιεχόμενο, κάτι πολύ συνηθισμένο από την εποχή του Web 2.0 και μετά, όπου ο σαφής διαχωρισμός μεταξύ

δημιουργών και καταναλωτών περιεχομένου είναι κάτι παραπάνω από ασαφής [24]. Ωστόσο, η ετερογενής φύση του IoT, απαιτεί την προσαρμογή του υφιστάμενου Διαδικτύου ώστε να είναι σε θέση να επιτρέπει τη διασύνδεση του οποιουδήποτε και του οτιδήποτε, οποιαδήποτε στιγμή και οπουδήποτε [25].

Στο πλαίσιο του IoT, η πλειονότητα των συσκευών που είναι συνδεδεμένες στο Διαδίκτυο παρουσιάζει περιορισμούς όσον αφορά την κατανάλωση ενέργειας, την υπολογιστική ισχύ και την αποθήκευση δεδομένων και πρέπει να βασίζεται στην ευκαιριακή διαθεσιμότητα επικοινωνίας. Η χρήση του πρωτοκόλλου TCP/IP απαιτεί σχετικά μεγάλες ποσότητες ισχύος και υπολογιστική χωρητικότητα, κάτι που καθιστά τη σύνδεση των συσκευών, με τους περιορισμούς που αναφέρθηκαν, στο Διαδίκτυο μέσω του πρωτοκόλλου IP μια πραγματική πρόκληση. Ως εκ τούτου, μία από τις βασικές ιδέες αυτής της οπτικής του IoT είναι η απλοποίηση του πρωτοκόλλου IP για την υποστήριξη των συσκευών με περιορισμένους πόρους [26].

Η Διαδικτυοστρεφής οπτική ευνοεί τη δυνατότητα του πρωτοκόλλου IP να ενσωματώνει δίκτυα διαφορετικών τεχνολογιών. Η δυνατότητα αυτή εκφράζεται με τον όρο “IP over anything” και δηλώνει τη δυνατότητα του πρωτοκόλλου να λειτουργήσει πάνω από ένα υποκείμενο δίκτυο οποιασδήποτε τεχνολογίας (π.χ., IP over Ethernet). Η Internet Protocol for Smart Objects (IPSO) Alliance, μία μη κερδοσκοπική, διεθνή σύμπραξη εταιρειών και βιομηχανιών, έχει ως σκοπό τη χρήση του IP σε εμπορικές λύσεις του IoT ως ελαφρού πρωτοκόλλου επικοινωνίας για όλα τα είδη συσκευών [27]. Παρόλα αυτά, πολλές από τις συσκευές IoT που έχουν ήδη κατασκευαστεί, έχουν δημιουργηθεί με τη χρήση ιδιόκτητων πρωτοκόλλων, κάτι που καθιστά την επικοινωνία μεταξύ τους δύσκολη [28]. Μία λύση, που θα εκμεταλλευτεί την ήδη υπάρχουσα κατάσταση και που αποτελεί στόχο της Διαδικτυοστρεφούς οπτικής του IoT, είναι η υιοθέτηση του πρωτοκόλλου 6LoWPAN, το οποίο μπορεί να υποστηρίξει την επικοινωνία μεταξύ ετερογενών συσκευών με περιορισμένους πόρους [29].

2.3.3 Σημασιολογικοστρεφής οπτική

Η σύγχρονη αρχιτεκτονική του Διαδικτύου αντιμετωπίζει προκλήσεις όταν αντιμετωπίζει πολλά είδη διεπαφών, οι οποίες στην παρούσα φάση είναι σχεδιασμένες για χρήση από ανθρώπους ή απλές και καλά καθορισμένες υπηρεσίες, Η σύνδεση όμως ενός μεγάλου αριθμού συσκευών, στο πλαίσιο του IoT, τείνει να αυξάνει περαιτέρω τη δυσκολία αντιμετώπισης αυτής της πρόκλησης. Έτσι, η σημασιολογικοστρεφής οπτική επικεντρώνεται στις σημασιολογικές τεχνολογίες για την αντιπροσώπευση, αναζήτηση και αποθήκευση πληροφοριών στο IoT. Επιπλέον, αυτή η οπτική στοχεύει στη χρήση σημασιολογικών περιγραφών για διεπαφές, υπηρεσίες, πράγματα και τις αντίστοιχες ταυτότητές τους [30].

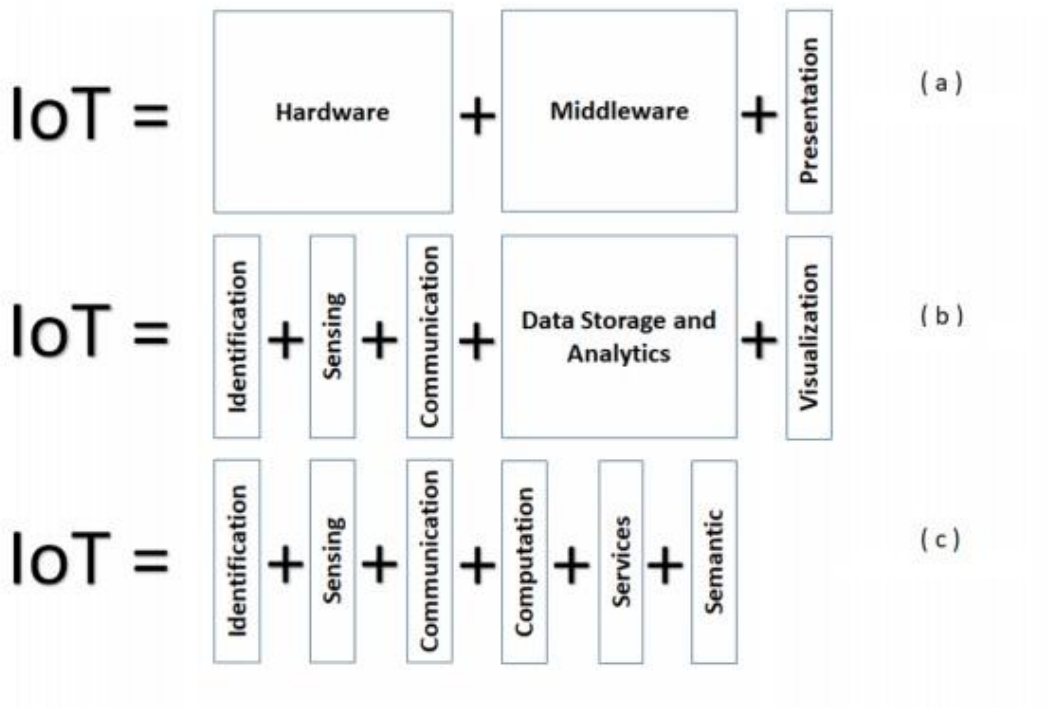
Οι Maarala, Su & Riekki (2016) θεωρούν τις οντολογικές γλώσσες, τις ευέλικτες αποθήκες (π.χ. βάσεις δεδομένων χωρίς σχήμα) και τις μηχανές συλλογιστικής, ως σημαντικές βασικές τεχνολογίες αυτής της οπτικής. Η χρήση αυτών των τεχνολογιών προωθεί τη σημασιολογική διαλειτουργικότητα των πόρων του IoT και τη χρήση μοντέλων πληροφοριών και σημασιολογικού σχολιασμού των δεδομένων [31].

Ένα ακόμα επίκεντρο αυτής της οπτικής είναι η χρήση σημασιολογικών περιβαλλόντων εκτέλεσης ή σημασιολογικών ενδιάμεσων λογισμικών πλαισίου. Τα σημασιολογικά ενδιάμεσα λογισμικά μπορούν να χρησιμοποιούνται ως διαμεσολαβητές μεταξύ των διαφορετικών ειδών συσκευών που έχουν διαφορετικά μοντέλα δεδομένων ή πληροφοριών [32]. Η χρήση του πλαισίου, για παράδειγμα η παροχή υπηρεσιών βάσει περιβαλλοντικών πληροφοριών, μπορεί επίσης να βασιστεί σε σημασιολογικούς σχολιασμούς και περιγραφές [33].

2.4 Τεχνικά στοιχεία

Από την ανάλυση των οπτικών του IoT που παρουσιάστηκαν στην προηγούμενη ενότητα, προκύπτουν κάποια συμπεράσματα. Η πραγματοστρεφής οπτική σχετίζεται με την συνεχή παρακολούθηση των αντικειμένων μοναδικής ταυτότητας από αισθητήρες, με σκοπό τη συλλογή δεδομένων μέσω ενσωματωμένων συστημάτων. Η διαδικτυοστρεφής οπτική

επικεντρώνεται στη χρήση του Διαδικτύου ως μέσω διασύνδεσης διαφόρων φυσικών συσκευών, με σκοπό τη δυνατότητα μεταξύ τους αλληλεπίδρασης. Η σημασιολογικοστρεφής οπτική λαμβάνει υπόψη το μεγάλο όγκο δεδομένων που συλλέγονται μέσω των αισθητήρων και καθορίζει την αποτελεσματική επεξεργασία του. Τα αρχικά δεδομένα υπόκεινται σε μια σειρά διαδικασιών με σκοπό την αφαίρεση των περιττών πληροφοριών, ώστε η ανάλυση και η ερμηνεία τους να γίνεται πιο εύκολη και καλύτερη. Επομένως, αυτές οι τρεις οπτικές ουσιαστικά παρέχουν μια περιγραφή των βασικών τεχνικών στοιχείων IoT [34].



Εικόνα 2-6: Διαφορετικές απόψεις σχετικά με το σύνολο των τεχνικών στοιχείων του IoT [34]

Πολλοί συγγραφείς υποστηρίζουν ότι η σημαντικότερη τεχνική πρόκληση στο πλαίσιο του IoT είναι η ικανότητα μοναδικού προσδιορισμού των βασικών τεχνικών στοιχείων του [35]. Αυτός άλλωστε είναι και ο λόγος που στη βιβλιογραφία ο αριθμός των στοιχείων αυτών ποικίλλει. Στην εικόνα 2-6 παρουσιάζονται τρεις τέτοιες περιπτώσεις. Στην εικόνα φαίνεται ξεκάθαρα ότι ενώ ορισμένοι συγγραφείς θεωρούν ότι τα τεχνικά στοιχεία του IoT είναι τρία, άλλοι προσδιορίζουν στο IoT πέντε βασικά τεχνικά στοιχεία και ορισμένοι του προσδίδουν

έξι στοιχεία. Με μια πιο προσεκτική ματιά, προκύπτει ότι ενώ οι εικόνες 2-6(α) και (β) περιλαμβάνουν πιο γενικά τεχνικά στοιχεία, στην εικόνα 2-6(γ) τα στοιχεία αυτά είναι πιο συγκεκριμένα [34].

Στο πλαίσιο της παρούσας εργασίας επιλέχθηκε η άποψη των έξι στοιχείων, καθώς έτσι προσδιορίζεται σωστότερα η έννοια του IoT, με βάση τους ορισμούς που παρουσιάστηκαν σε προηγούμενη ενότητα. Τα έξι βασικά τεχνικά στοιχεία του IoT αφορούν [36]: (1) την ταυτοποίηση (identification), (2) την ανίχνευση (sensing), (3) την επικοινωνία (communication), (4) την υπολογιστική ικανότητα (computation), (5) τις υπηρεσίες (services) και (6) την σημασιολογία (semantics).

Καθώς όλο και περισσότερες συσκευές προστίθενται μέρα με τη μέρα στο οικοσύστημα του IoT, η σημασία της ταυτοποίησής τους αυξάνεται από τη στιγμή που συμβάλλει στην επιτυχή μεταξύ τους επικοινωνία. Η ετερογένεια των πλατφορμών καθώς και η αντιστοίχιση των υπηρεσιών με τη ζήτησή τους, αποτελούν σημαντικά ζητήματα τα οποία καθιστούν την ταυτοποίηση των συσκευών στοιχείο ζωτικής σημασίας για το IoT. Κάποιες από τις μεθόδους ταυτοποίησης συσκευών που χρησιμοποιούνται είναι η χρήση του ηλεκτρονικού κώδικα προϊόντος (Electronic Product Code - EPC) και του uCode (ubiquitous code) [37]. Από τη στιγμή που οι μέθοδοι ταυτοποίησης δεν είναι παγκοσμίως μοναδικές, η διευθυνσιοδότηση είναι επίσης μια μέθοδος καθορισμού των αντικειμένων IoT, καθώς ενισχύει τον μοναδικό προσδιορισμό τους δείχνοντας τη διεύθυνση που παρουσιάζουν εντός του δικτύου επικοινωνιών. Η διευθυνσιοδότηση των αντικειμένων IoT γίνεται με χρήση των πρωτοκόλλων IPv6 και IPv4.

Η διαδικασία της συλλογής δεδομένων από τα διάφορα αντικείμενα του δικτύου IoT και της αποστολή τους σε αποθήκες δεδομένων, σε βάσεις δεδομένων ή στο cloud, είναι γνωστή ως ανίχνευση. Τα δεδομένα αυτά μπορεί να συλλέγονται από μια μεγάλη ποικιλία συσκευών, διαφορετικών πλατφορμών και αρχιτεκτονικών. Καθώς οι συσκευές IoT έχουν συνήθως περιορισμένες δυνατότητες αποθήκευσης δεδομένων, η ανίχνευση χρήσιμων δεδομένων, που απαιτούνται για επεξεργασία και εξαγωγή χρήσιμων συμπερασμάτων, είναι πολύ σημαντική.

Η διαδικασία ανίχνευσης δεδομένων στο IoT σχετίζεται πάντα με τις δυνατότητες αποθήκευσης του εκάστοτε συστήματος.

Οι τεχνολογίες επικοινωνίας στο IoT χρησιμοποιούνται για τη σύνδεση των ετερογενών αντικειμένων, με σκοπό την παροχή έξυπνων υπηρεσιών. Εκτός από μια μεγάλη ποικιλία αρχιτεκτονικών, οι συσκευές IoT χρησιμοποιούν και διαφορετικές τεχνολογίες επικοινωνίας. Στο IoT, η ομαλή επικοινωνία μεταξύ όλων αυτών των ετερογενών συσκευών αποτελεί πραγματική πρόκληση. Οι κόμβοι IoT έχουν σχεδιαστεί για να λειτουργούν με χαμηλή ισχύ σε περιβάλλοντα που χαρακτηρίζονται από παρουσία θορύβων ζεύξεων επικοινωνίας [38]. Κάποια από τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στο IoT είναι τα Wi-Fi (Wireless Fidelity), Bluetooth, IEEE 802.15.4, Z-wave και LTE-Advanced.

Η υπολογιστική ικανότητα του IoT καθορίζεται από τις μονάδες επεξεργασίας, όπως μικροελεγκτές, μικροεπεξεργαστές, SOC και FPGA, που χρησιμοποιούνται στο εκάστοτε σύστημα, αλλά και από τις πλατφόρμες hardware υλικού, όπως οι Arduino, Friendly ARM, Intel Galileo, Raspberry PI, Beagle Bone, WiSense, Mule, κλπ, που χρησιμοποιούνται για την υποστήριξη του λογισμικού των συσκευών IoT. Διάφορα λειτουργικά συστήματα, όπως το RTOS Contiki έχουν χρησιμοποιηθεί ευρέως στο IoT. Τα Tiny OS, Lite OS και RIoT OS αποτελούν επίσης ελαφριά λειτουργικά συστήματα, σχεδιασμένα για περιβάλλοντα IoT. Οι πλατφόρμες cloud συνεισφέρουν επίσης στην υπολογιστική ικανότητα του IoT. Η χρήση τους αποσκοπεί στην παροχή διευκολύνσεων κατά την αποστολή των δεδομένων που συλλέγονται από τα έξυπνα αντικείμενα στο cloud, καθώς και την επεξεργασία των Big Data σε πραγματικό χρόνο. Υπάρχουν πολλές δωρεάν και εμπορικές πλατφόρμες και πλαίσια cloud για τη φιλοξενία υπηρεσιών IoT.

Οι υπηρεσίες IoT μπορούν να ομαδοποιηθούν σε 4 κατηγορίες [39]: (α) υπηρεσίες που σχετίζονται με την ταυτότητα, (β) υπηρεσίες συγκέντρωσης πληροφοριών, (γ) υπηρεσίες συνεργασίας και (δ) διάχυτες υπηρεσίες. Οι υπηρεσίες που σχετίζονται με την ταυτότητα περιλαμβάνουν εφαρμογές για τη χαρτογράφηση των αντικειμένων του πραγματικού κόσμου στον εικονικό κόσμο, με σκοπό την ταυτοποίηση. Οι υπηρεσίες συγκέντρωσης πληροφοριών

ασχολούνται με τη συλλογή και ομαδοποίηση των μετρήσεων που λαμβάνονται από τους αισθητήρες καθώς και με την αποστολή των συγκεκριμένων μετρήσεων στην αντίστοιχη εφαρμογή IoT για επεξεργασία. Οι υπηρεσίες συνεργασίας χρησιμοποιούν τα δεδομένα που έχουν αναλυθεί, για να λαμβάνουν αποφάσεις και να αντιδρούν ανάλογα. Τέλος, οι διάχυτες υπηρεσίες βεβαιώνουν ότι οι υπηρεσίες συνεργασίας είναι διαθέσιμες σε οποιονδήποτε και ανά πάσα στιγμή.

Με τον όρο εξόρυξη γνώσης εννοείται η ανακάλυψη πληροφοριών με ορθή χρήση πόρων και μοντελοποίηση. Επίσης, εννοείται η λήψη σωστών αποφάσεων μέσω ανάλυσης και αναγνώρισης δεδομένων για την παροχή συγκεκριμένων υπηρεσιών. Η εξόρυξη γνώσης υποστηρίζεται από τεχνολογίες του Σημασιολογικού Ιστού, όπως το πλαίσιο περιγραφής πόρων (Resource Description Framework - RDF) και η γλώσσα οντολογίας ιστού (Web Ontology Language - OWL) [40].

2.5 Γενικά χαρακτηριστικά και απαιτήσεις

Βάσει των όσων αναλύθηκαν μέχρι τώρα, προκύπτει το συμπέρασμα ότι το IoT μπορεί να ανοίξει νέες ευκαιρίες για τη δημιουργία καινοτόμων εφαρμογών. Μερικές από αυτές τις εφαρμογές, όπως θα γίνει κατανοητό και από την παρουσίασή τους σε άλλο κεφάλαιο, μπορούν να υλοποιηθούν μόνο σε συγκεκριμένους τομείς, εμφανίζοντας ιδιότυπα χαρακτηριστικά του τομέα που υπηρετούν. Αντίθετα, άλλες εφαρμογές μπορούν να υλοποιηθούν σε μια ευρύτερη γκάμα τομέων και κλάδων, γεγονός που απαιτεί την εμφάνιση κοινών χαρακτηριστικών [41]. Με τον τρόπο αυτό, δημιουργείται ένα πολύπλοκο σύστημα με πολλά χαρακτηριστικά τα οποία ποικίλουν μεταξύ των τομέων εφαρμογή της τεχνολογίας [42].

Αν και τα γενικά χαρακτηριστικά του IoT που αναφέρονται στη βιβλιογραφία είναι πολυάριθμα, εντούτοις είναι δυνατή η ταξινόμησή τους σε έξι μεγάλες κατηγορίες [43]: (α) την νοημοσύνη, (β) την αρχιτεκτονική, (γ) την πολυπλοκότητα, (δ) την εκτίμηση μεγέθους, (ε) την εκτίμηση χρόνου και (στ) την εκτίμηση του χώρου.

Με τον όρο νοημοσύνη εννοείται η εφαρμογή της γνώσης, η οποία δημιουργείται από την ανάλυση των δεδομένων που συλλέγονται. Με την ανάλυση ουσιαστικά πραγματοποιείται ένας μετασχηματισμός των συλλεγμένων πρωτογενών δεδομένων σε γνώση (πληροφορίες υψηλού επιπέδου). Μετά την απόκτηση της γνώσης, η χρήση της μπορεί να πραγματοποιηθεί μέσω ευφυούς αλληλεπίδρασης και επικοινωνίας. Επομένως, η νοημοσύνη αποτελείται από δύο διαφορετικές συνιστώσες : (α) την περιβαλλοντική νοημοσύνη και τον αυτόνομο έλεγχο και (β) την ενσωματωμένη νοημοσύνη. Αν και η πρώτη συνιστώσα δεν αποτελούσε μέρος της αρχικής ιδέας του IoT, η ενσωμάτωση της έννοιας του IoT με τον αυτόνομο έλεγχο δημιούργησε μια νέα προοπτική [44]: τον συνδυασμό της τεχνικής νοημοσύνης με το IoT. Βάσει αυτής της προοπτικής, διευκολύνεται η ικανότητα συλλογής και ανάλυσης των ψηφιακών ιχνών που αφήνουν οι άνθρωποι όταν αλληλοεπιδρούν με ευρέως διαδεδομένα έξυπνα πράγματα, με στόχο την απόκτηση γνώσης για τις ανθρώπινες δραστηριότητες, τις αλληλεπιδράσεις τους με το περιβάλλον και τις κοινωνικές επαφές και συμπεριφορές τους.

Το IoT πρέπει να διευκολύνεται από μια υβριδική αρχιτεκτονική που να περιλαμβάνει πολλές διαφορετικές αρχιτεκτονικές. Η αρχική ιδέα περιλάμβανε δύο αρχιτεκτονικές: την αρχιτεκτονική βάσει συμβάντων και την αρχιτεκτονική βάσει χρόνου. Στην πρώτη περίπτωση, η συλλογή δεδομένων από τους αισθητήρες πραγματοποιείται όταν συμβαίνει ένα συμβάν (π.χ. αισθητήρας πόρτας), ενώ στη δεύτερη περίπτωση, η συλλογή πραγματοποιείται συνεχώς, με βάση καθορισμένα χρονικά πλαίσια (π.χ. αισθητήρας θερμοκρασίας). Η πιο κοινά χρησιμοποιούμενη αρχιτεκτονική βασίζεται σε συμβάντα. Επομένως, άλλα μοντέλα και λειτουργικές προσεγγίσεις των συστημάτων IoT συνυπάρχουν με την συγκεκριμένη αρχιτεκτονική, με σκοπό την αντιμετώπιση των εξαιρέσεων και την ασυνήθιστη εξέλιξη των διεργασιών. Παρόλα αυτά, σε ένα σύστημα IoT, ένα συμβάν δεν θα πρέπει να βασίζεται απαραίτητα σε κάποιο ντετερμινιστικό ή συντακτικό μοντέλο, αλλά στο ίδιο το πλαίσιο του [45].

Το IoT περιλαμβάνει μεγάλο αριθμό αντικειμένων (αισθητήρες και ενεργοποιητές) που αλληλοεπιδρούν αυτόνομα. Επί του παρόντος, υπάρχουν εκατομμύρια αισθητήρες που έχουν αναπτυχθεί σε όλο τον κόσμο. Οι αλληλεπιδράσεις μεταξύ τους μπορεί να διαφέρουν

σημαντικά, ανάλογα με τις δυνατότητές τους. Τα περισσότερα αντικείμενα στο πλαίσιο του IoT παρουσιάζουν περιορισμένους πόρους, επομένως η αποθήκευση και η επεξεργασία των πληροφοριών που συλλέγουν είναι μηδαμινές. Υπάρχουν όμως και αντικείμενα που διαθέτουν μεγαλύτερη μνήμη και επεξεργαστική ισχύ, στοιχεία που τα καθιστούν πιο έξυπνα. Η συνύπαρξη όλων αυτών των αντικειμένων σε ένα σύστημα το καθιστά αυτόματα σύνθετο και πολύπλοκο καθότι θα πρέπει να διαχειρίζεται ένα τεράστιο αριθμό συνδέσεων μεταξύ των αντικειμένων, τις αλληλεπιδράσεις τους και τη δυνατότητα ενσωμάτωσης περισσότερων. Για το λόγο αυτό, στην πράξη, ένα σύστημα IoT, χωρίζεται σε υποσυστήματα με σκοπό την αντιμετώπιση των θεμάτων της ασφάλειας και της διατήρησης του απορρήτου, αλλά και την αύξηση της αξιοπιστίας του [45].

Σε προηγούμενη ενότητα αναφέρθηκε ότι ο αριθμός των έξυπνων συσκευών που έχουν χρησιμοποιηθεί μέχρι το τέλος του 2020, ανήλθε σε σχεδόν 10 δισεκατομμύρια, ένας αριθμός που αναμένεται να φτάσει τις 21,5 δισεκατομμύρια συσκευές το 2025. Από τη στιγμή που τα μεγέθη των διασυνδεδεμένων συσκευών στο IoT δεν πρόκειται ποτέ να μειωθούν, αλλά αναμένεται να αυξάνονται συνεχώς, η δυνατότητα υποστήριξης της αδιάλειπτης μεταξύ τους επικοινωνίας και των αλληλεπιδράσεων αποτελεί σημαντικό χαρακτηριστικό της τεχνολογίας. Επίσης, η εκτίμηση του μεγέθους του αριθμού των αντικειμένων που θα μπορούν να υποστηρίζονται σε ένα σύστημα IoT αποτελεί βασικό παράγοντα κατά το σχεδιασμό του.

Η εκτίμηση χρόνου αποτελεί ένα ακόμα βασικό χαρακτηριστικό του IoT, καθώς η τεχνολογία θα πρέπει να μπορεί να υποστηρίζει την διαχείριση δισεκατομμύριων γεγονότων που συμβαίνουν ή πραγματοποιούνται ταυτόχρονα. Σε αυτό το πλαίσιο η δυνατότητα υποστήριξης διεργασιών επεξεργασίας δεδομένων σε πραγματικό χρόνο είναι ιδιαίτερα κρίσιμη. Στο IoT, ο χρόνος δεν χρησιμοποιείται πλέον ως γραμμική διάσταση, αλλά εξαρτάται από κάθε οντότητα (αντικείμενο, διαδικασία, σύστημα πληροφοριών, κ.λπ.) [43].

Η ακριβής γεωγραφική θέση ενός αντικειμένου είναι επίσης ζωτικής σημασίας, καθώς η τοποθεσία παίζει σημαντικό ρόλο στη διάχυτη υπολογιστική. Η σημασία της εκτίμησης

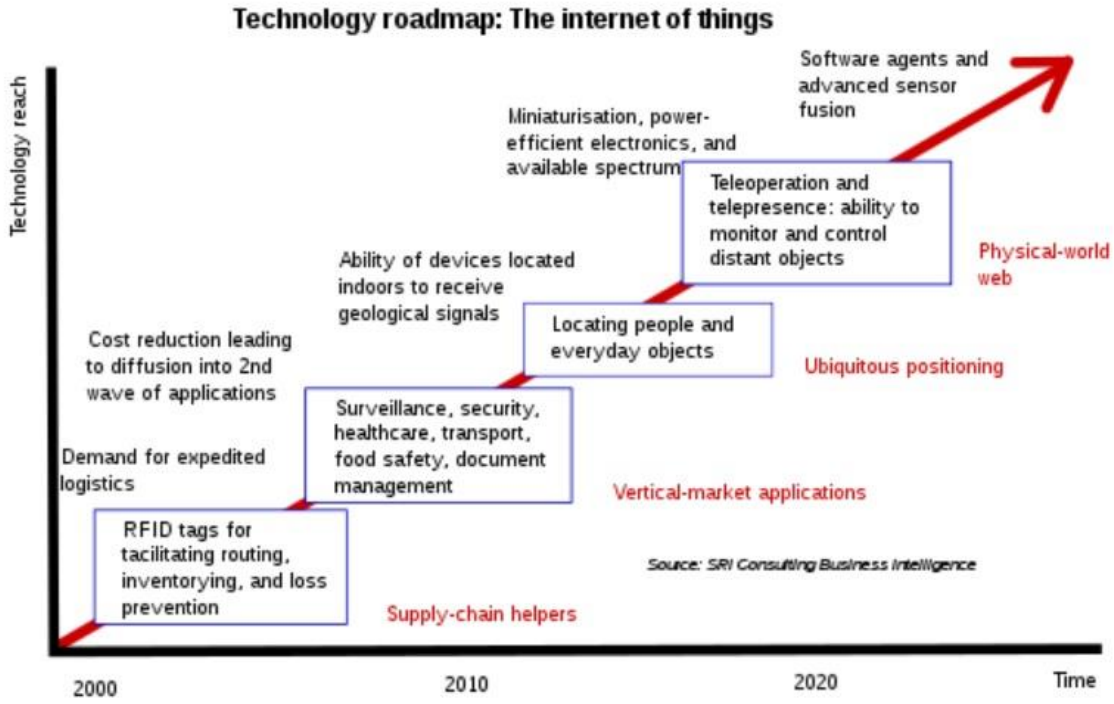
χώρου γίνεται μεγαλύτερη καθώς ο αριθμός των αντικειμένων αυξάνεται και η συνεχής παρακολούθησή τους αποτελεί βασική απαίτηση. Οι αλληλεπιδράσεις μεταξύ των αντικειμένων εξαρτώνται σε μεγάλο βαθμό από τη θέση τους, το γύρω περιβάλλον τους και την παρουσία άλλων οντοτήτων (π.χ. αντικείμενα και άτομα) [43].

Με βάση τα γενικά χαρακτηριστικά του IoT που αναλύθηκαν παραπάνω, οι Madakam και συν. (2015), κατέληξαν στο συμπέρασμα, ότι οι απαιτήσεις και παράλληλα προϋποθέσεις για την επιτυχή εφαρμογή του είναι οι εξής [46]:

- Δυναμική ζήτηση πόρων
- Υποστήριξη πραγματικού χρόνου
- Υποστήριξη της εκθετικής αύξησης της ζήτησης
- Διαθεσιμότητα των εφαρμογών
- Προστασία δεδομένων και απόρρητο χρήστη
- Αποτελεσματική κατανάλωση ισχύος των εφαρμογών
- Εκτέλεση των εφαρμογών κοντά στους τελικούς χρήστες
- Πρόσβαση σε ανοιχτό και διαλειτουργικό σύστημα cloud

Παρόλα αυτά, η αποδεδειγμένη δυναμικότητα που παρουσιάζει η τεχνολογία του IoT έχει ως αποτέλεσμα τη συνεχή μεταβολή των απαιτήσεων αυτών. Η δημιουργία επομένως ενός ολοκληρωμένου τεχνολογικού χάρτη της πορείας του IoT, που να περιλαμβάνει τις ακριβείς παρατηρήσεις που έχουν γίνει τις προηγούμενες περιόδους, καθώς και τις αναμενόμενες προβλέψεις για το εγγύς μέλλον, είναι πολύ σημαντική. Ένας τέτοιος χάρτης επίσης να καθορίσει το χρονικό διάστημα στο οποίο μπορεί να υλοποιηθεί μια νέα απαίτηση που έχει δημιουργηθεί από την εξέλιξη των άλλων τεχνολογιών που εμπεριέχονται στο IoT. Κάτι τέτοιο μπορεί επίσης να αποτελέσει τη βάση για μια βαθύτερη επισκόπηση της τεχνολογίας του IoT γύρω από τα σύγχρονα οικοσυστήματα και τις πλατφόρμες στις οποίες βασίζονται σε μεγάλο βαθμό. Στην εικόνα 2-7 παρουσιάζεται ένας ενδιαφέρων και ολοκληρωμένος τεχνολογικός χάρτης της πορείας του IoT που επισημαίνει το χρονοδιάγραμμα, τα χαρακτηριστικά και τις εφαρμογές σημαντικών τεχνολογικών ορόσημων, στοιχεία που είναι

απαραίτητα για το σχεδιασμό επιτυχημένων εφαρμογών που είναι πιθανό να υλοποιηθούν μέχρι το 2025 [47].



Εικόνα 2-7: Τεχνολογικός χάρτης της πορείας του IoT [47]

2.6 Πλεονεκτήματα και μειονεκτήματα

Όπως θα φανεί από τα επόμενα κεφάλια της παρούσας εργασίας, οι εφαρμογές του IoT μπορούν να καλύψουν μεγάλο πλήθος τομέων και κλάδων κάτι που αντικατοπτρίζει περίτρανα τη σημασία της τεχνολογίας. Η χρήση αυτών των εφαρμογών, όμως, δημιουργεί και πολλές προκλήσεις και ζητήματα τα οποία δεν μπορούν να αγνοηθούν και θα πρέπει να αντιμετωπιστούν με τέτοιο τρόπο ώστε να μπορεί να γίνει πλήρη υιοθέτηση της τεχνολογίας. Ο συνδυασμός εφαρμογών και προκλήσεων δημιουργούν ένα πλαίσιο πλεονεκτημάτων και μειονεκτημάτων που παρουσιάζει το IoT, μια σύνοψη των οποίων είναι παρατίθεται στη συνέχεια [9].

I. Πλεονεκτήματα

Οι συσκευές IoT έχουν σχεδιαστεί με σκοπό την ενίσχυση των καταναλωτών στις προσπάθειές τους για εξοικονόμηση χρημάτων, μείωσης της κατανάλωσης ενέργειας και βελτίωσης των καθημερινών δραστηριοτήτων τους, παρέχοντας αυτοματοποίηση, αποτελεσματικότητα, ασφάλεια και άνεση. Όλα αυτά τα στοιχεία μπορούν να βοηθήσουν τα μεμονωμένα άτομα αλλά και την κοινωνία γενικότερα σε καθημερινή βάση. Οι υπηρεσίες που προσφέρει το IoT μπορούν να βελτιώσουν τις διαδικασίες λήψης αποφάσεων και των αποτελεσμάτων τους σε ένα ευρύ φάσμα εφαρμογών.

Η σωστή εφαρμογή του IoT μπορεί να δημιουργήσει σημαντικά οφέλη στις επιχειρήσεις, όπως ενισχυμένη παραγωγικότητα και ανταγωνιστικά πλεονεκτήματα. Οι επιχειρήσεις που έχουν ήδη υιοθετήσει την τεχνολογία έχουν τη δυνατότητα να παράγουν καινοτόμα προϊόντα και να παρέχουν καινοτόμες υπηρεσίες, μειώνοντας παράλληλα τα λειτουργικά κόστη και δημιουργώντας επιπλέον ροές εσόδων. Η πραγματική αξία του IoT έγκειται στην ενσωμάτωση των δεδομένων που συλλέγονται από συσκευές στις επιχειρηματικές διαδικασίες, επιτυγχάνοντας βελτιστοποίηση κρίσιμων λειτουργικών τομέων και βελτίωση της λειτουργικής απόδοσης και αποτελεσματικότητας.

Το IoT επιτρέπει την αυτοματοποίηση και τον έλεγχο των εργασιών που γίνονται σε καθημερινή βάση, αποφεύγοντας την ανθρώπινη παρέμβαση. Κάτι τέτοιο οδηγεί σε ομοιομορφία στην εκτέλεση των καθηκόντων και την καλή ποιότητα των παρεχόμενων υπηρεσιών. Η αλληλεπίδραση μεταξύ των μηχανών βοηθά στη διατήρηση της διαφάνειας των διαδικασιών, με παράλληλη αύξηση της αποδοτικότητας. Ως εκ τούτου, ακριβή αποτελέσματα μπορούν να ληφθούν γρηγορότερα και επομένως εξοικονομείται πολύτιμος χρόνος. Αντί για την επανάληψη των ίδιων καθημερινών καθηκόντων, οι εργαζόμενοι έχουν τη δυνατότητα να κάνουν άλλες δημιουργικές εργασίες. Η τεχνολογία επιτρέπει επίσης την άμεση λήψη των απαραίτητων ενεργειών σε περιπτώσεις έκτακτης ανάγκης.

Η υιοθέτηση της τεχνολογίας και η διατήρηση των έξυπνων συσκευών υπό επιτήρηση, μπορεί να βελτιστοποιήσει την αποτελεσματική χρήση των ενεργειακών πόρων, συμβάλλοντας στα ζητήματα της έλλειψης τους. Επιπλέον, πιθανά σημεία συμφόρησης,

βλάβες και ζημιές στο σύστημα μπορεί να αποφευχθούν ουσιαστικά. Η επίλυση αυτών των ζητημάτων συνεισφέρει στην εξοικονόμηση χρημάτων, ένα ακόμα βασικό πλεονέκτημα της τεχνολογίας του IoT.

II. Μειονεκτήματα

Το IoT φέρνει επανάσταση στην καθημερινότητα των ανθρώπων. Καθώς οι καταναλωτές προσελκύονται όλο και περισσότερο από τις ανέσεις, την ευκολία και οφέλη των συσκευών IoT, οι περισσότεροι δεν γνωρίζουν τους κινδύνους που σχετίζονται με κάτι τέτοιο. Οι μεγαλύτεροι κίνδυνοι που σχετίζονται με το IoT είναι η παραβίαση του απορρήτου (ζήτημα προστασίας της ιδιωτικότητας), η παρεχόμενη ασφάλεια, η πλήρης εμπιστοσύνη στην τεχνολογία και η απώλεια θέσεων εργασίας.

Το IoT βασίζεται στη διασύνδεση των έξυπνων συσκευών μέσω του Διαδικτύου για τη συλλογή και την ανάλυση δεδομένων. Όπως συμβαίνει όμως και με οποιαδήποτε συσκευή που συνδέεται στο Διαδίκτυο, οι συσκευές IoT παρουσιάζουν πιθανές ευπάθειες ασφαλείας. Σαν αποτέλεσμα, τα προσωπικά δεδομένα και το απόρρητο των καταναλωτών βρίσκονται σε κίνδυνο ακόμη και χωρίς τη γνώση τους. Συσκευές IoT, όπως οι έξυπνες τηλεοράσεις, οι δρομολογητές δικτύου ή και τα ψυγεία είναι επιρρεπείς σε κυβερνοεπιθέσεις. Εάν μια συσκευή IoT προσβληθεί από κακόβουλο λογισμικό, είναι εύλογο και άλλες συσκευές, όπως οι υπολογιστές ή τα smartphone, που βρίσκονται στο ίδιο δίκτυο να πέσουν θύματα κυβερνοεπιθέσεων, εάν δεν προστατεύονται από κατάλληλα διαμορφωμένα firewall και λογισμικά προστασίας από ιούς.

Σε σχετικά πρόσφατη έρευνα του Σεπτεμβρίου του 2019, αποκαλύφθηκε ότι αν και υπάρχει μια ευρεία γκάμα διασυνδεδεμένων συσκευών, όπως υπολογιστές και έξυπνες οικιακές συσκευές (τηλεοράσεις, κουζίνες, ψυγεία, κλπ.), το 47% των πιο ευάλωτων IoT συσκευών είναι οι κάμερες ασφαλείας εγκατεστημένες σε οικιακά δίκτυα, ακολουθούμενες από έξυπνους οικιακούς κόμβους (15%), όπως το Google Home και το Amazon Alexa, και διασυνδεδεμένες συσκευές αποθήκευσης (12%). Τα συστήματα καμερών ασφαλείας είναι οι

συσκευές IoT που παρουσιάζουν μεγαλύτερο ποσοστό ευπάθειας κυβερνοεπιθέσεων, καθώς οι εισβολείς μπορούν να παρακάμψουν τις διατάξεις ασφαλείας που περιλαμβάνουν τα φθηνά μοντέλα καμερών IP. Πολλές από αυτές τις συσκευές έχουν παρόμοια σχεδιαγράμματα, επομένως εάν εντοπιστεί μια ευπάθεια σε μία συσκευή, η ίδια ευπάθεια πιθανότατα θα βρίσκεται και σε άλλες συσκευές [48].

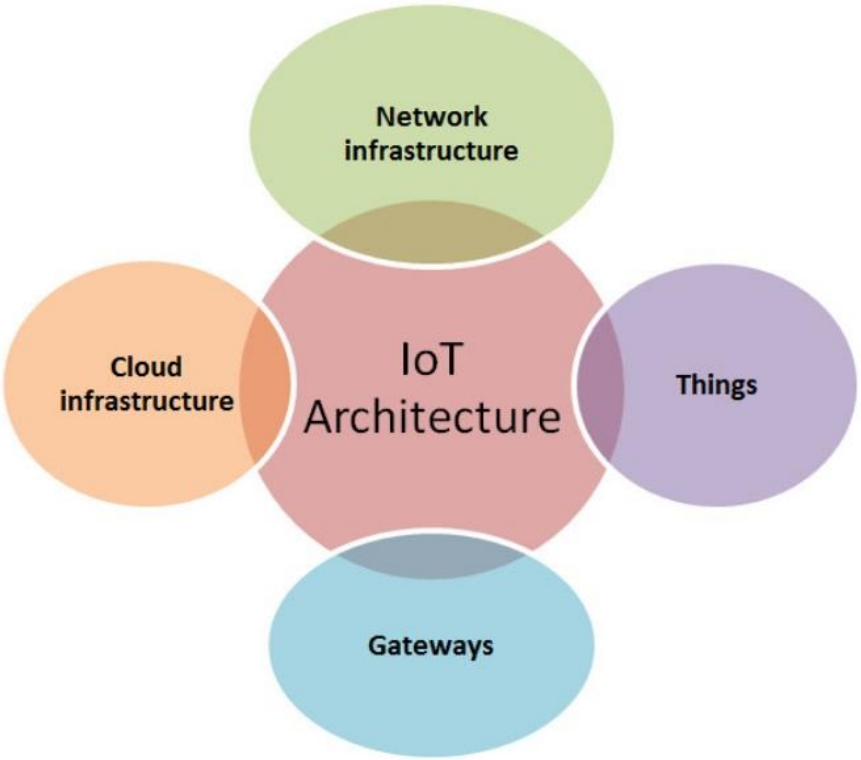
Επιπλέον, η πλήρης εμπιστοσύνη σε μια τεχνολογία σε καθημερινή βάση και η λήψη αποφάσεων σύμφωνα με τις πληροφορίες που παρέχει, θα μπορούσαν να αποβούν μοιραία. Οι τεχνολογίες που περιλαμβάνουν τη χρήση του Διαδικτύου είναι συνεχώς επιρρεπείς σε δυσλειτουργίες, καθώς ο σχεδιασμός όλων των συστημάτων είναι τέτοιος που να μην μπορεί να εμφανίζει 100% σταθερότητα. Η κατάρρευση ενός συστήματος μπορεί να αποβεί λιγότερο ή περισσότερο επιζήμια, ανάλογα με το ποσοστό με το οποίο η οποιαδήποτε ενέργεια και δράση βασίζεται στις πληροφορίες που αυτό παρέχει. Εάν αυτό το ποσοστό είναι μεγάλο, η οποιαδήποτε δυσλειτουργία του συστήματος θα μπορούσε να οδηγήσει σε δυνητικά καταστροφικά συμβάντα Το IoT χαρακτηρίζεται από μεγάλη ετερογένεια και πολυπλοκότητα. Επομένως, οποιοδήποτε σφάλμα ή δυσλειτουργία του λογισμικού ή του hardware υλικού του συστήματος θα δημιουργήσει σοβαρά ζητήματα.

Μια άλλη σημαντική ανησυχία είναι ότι η αυτοματοποίηση του IoT θα έχει καταστροφικό αντίκτυπο στις προοπτικές απασχόλησης των λιγότερο εκπαιδευμένων εργαζομένων, κάτι που μπορεί να οδηγήσει σε ανεργία και τελικά να επηρεάσει την κοινωνία στο σύνολό της [49].

3 Αρχιτεκτονική και τεχνολογίες IoT

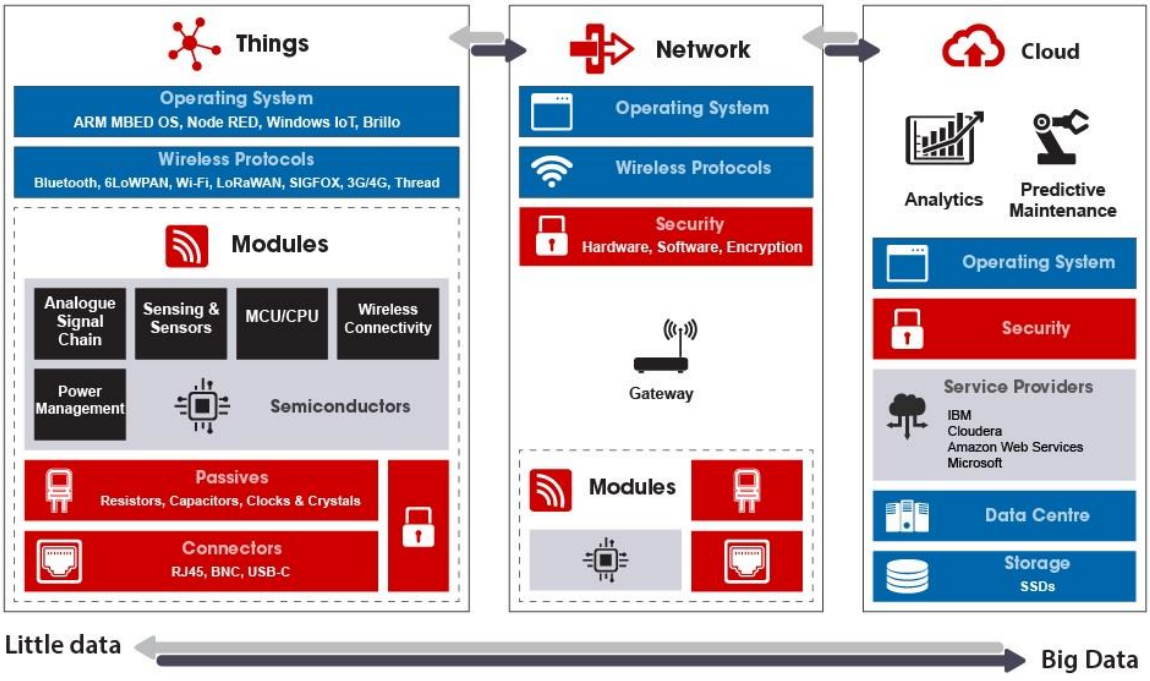
3.1 Δομικά στοιχεία και βασική αρχιτεκτονική

Η φιλοσοφία του IoT μπορεί να εξηγηθεί με μεγαλύτερη σαφήνεια μέσω της αρχιτεκτονικής του, η οποία ποικίλει ανάλογα με την εφαρμογή στην οποία υλοποιείται. Με τη σειρά της, η εκάστοτε αρχιτεκτονική IoT μπορεί να γίνει περισσότερο κατανοητή, λαμβάνοντας υπόψη την έννοια των δομικών στοιχείων από τα οποία αποτελείται. Τα δομικά στοιχεία της αρχιτεκτονικής του IoT είναι παρόμοια και ανεξάρτητα από την εκάστοτε εφαρμογή και αφορούν ως επί το πλείστο το hardware υλικό που χρησιμοποιείται. Η κατανόηση της φιλοσοφίας των δομικών υλικών, των συστατικών που σχηματίζουν αλλά και των μεταξύ τους αλληλεπιδράσεων, είναι σημαντική στην ανάλυση των διάφορων προοπτικών αρχιτεκτονικής του IoT που έχουν παρουσιαστεί στη βιβλιογραφία.



Εικόνα 3-1: Δομικά στοιχεία της αρχιτεκτονικής του IoT [50]

Ένα οποιοδήποτε σύστημα IoT περιλαμβάνει τέσσερα βασικά δομικά στοιχεία (Εικ. 3-1) [50]: τα πράγματα, τις πύλες, την υποδομή του δικτύου και την υποδομή του cloud. Στο προηγούμενο κεφάλαιο αναφέρθηκε ότι τα πράγματα αποτελούν κόμβους του δικτύου IoT με μοναδική ταυτότητα, που περιέχουν αισθητήρες ή/και ενεργοποιητές, οι οποίοι έχουν δυνατότητα για μεταξύ τους επικοινωνία και συλλέγουν πληροφορίες από το γύρω περιβάλλον τους χωρίς την απαίτηση ανθρώπινης παρέμβασης. Οι πύλες (gateways) λειτουργούν ως ενδιάμεσα στοιχεία σύνδεσης των πραγμάτων με την υποδομή του δικτύου ή του cloud και παρέχουν την απαιτούμενη συνδεσιμότητα, ασφάλεια και διαχείριση. Η υποδομή του δικτύου αποτελείται από δρομολογητές, αθροιστές, πύλες και επαναλήπτες και έχει ως σκοπό την παροχή ελέγχου στις παρεχόμενες από τα πράγματα πληροφορίες και την ασφαλή και ομαλή ροή τους προς την υποδομή του cloud. Η υποδομή του cloud αποτελείται από δίκτυα εικονικών διακομιστών και μονάδων αποθήκευσης δεδομένων, των οποίων οι υπολογιστικές δυνατότητες είναι τέτοιες που να τους δίνεται η δυνατότητα να επεξεργάζονται και να αποθηκεύουν τα δεδομένα που συλλέγονται από τα πράγματα.



Εικόνα 3-2: Βασική αρχιτεκτονική δομή του IoT [51]

Μέσω της βασικής αρχιτεκτονικής δομής του IoT είναι η ευκολότερη κατανόηση της λειτουργικής ροής των διαδικασιών των εφαρμογών του. Βάσει αυτού του σκεπτικού, η βασική αρχιτεκτονική δομή ενός οποιουδήποτε συστήματος IoT, αποτελείται από (Εικ. 3-2) [51]: τα πράγματα, το δίκτυο και το cloud. Τα πράγματα είναι οι εξοπλισμένες με αισθητήρες συσκευές που συλλέγουν τις πληροφορίες που αφορούν τη συγκεκριμένη περιοχή εφαρμογής και συνδέονται μεταξύ τους (ενσύρματα ή ασύρματα) για το σχηματισμό ενός ευρύτερου δικτύου. Το δίκτυο χρησιμοποιείται ως μέσο επικοινωνίας μεταξύ των συσκευών και συνδέει (συνήθως μέσω μια πύλης) τα πράγματα στο cloud. Το cloud περιλαμβάνει αποθήκες δεδομένων που αποθηκεύουν τις συλλεγόμενες πληροφορίες σε διάφορες μορφές, και μηχανές ανάλυσης και επεξεργασίας, οι οποίες επιτρέπουν την αλληλεπίδραση ανθρώπου-μηχανής, την ανάλυση των πληροφοριών σύμφωνα με το επιλεγμένο υπολογιστικό μοντέλο και την απεικόνιση των αποτελεσμάτων της ανάλυσης των πληροφοριών, ανάλογα με τις ανθρώπινες απαιτήσεις.

3.2 Αρχιτεκτονικές δομές IoT

Το IoT είναι μια πλατφόρμα που μπορεί να παρέχει λύσεις στα περισσότερα προβλήματα της καθημερινότητας. Η εκάστοτε λύση δημιουργείται από τον τρόπο συνδυασμού του λογισμικού και του hardware υλικού των τεχνολογιών πληροφορίας και επικοινωνίας που χρησιμοποιούνται. Στο IoT, τα στοιχεία λογισμικού και hardware υλικού συνεργάζονται και ενεργούν με βάση τις προτεραιότητες που δίνονται κατά το σχεδιασμό ενός συστήματος. Εν συντομία, το hardware υλικό του συστήματος που καθορίζεται από λογισμικό βοηθά στην επεξεργασία των πρωτογενών πληροφοριών με σκοπό τη δημιουργία, την αποθήκευση, την ανάκτηση και την ανάλυση δεδομένων, μέσω προηγμένων υπολογιστικών εργαλείων τα οποία είναι ενσωματωμένα στα συστήματα IoT. Τα επικοινωνιακά συστήματα βοηθούν στην παροχή πρωτοκόλλων που να επιτρέπουν την επικοινωνία μεταξύ των αντικειμένων, των πραγμάτων και γενικότερα κάθε συστατικού του IoT. Η καλύτερη, ταχύτερη, αξιόπιστη και ασφαλής σύγκλιση των τεχνολογιών πληροφορίας και επικοινωνίας μπορεί να επιτευχθεί μόνο μέσα από τη δημιουργία αποτελεσματικής αρχιτεκτονικής δομής του IoT [52].

Η αρχιτεκτονική δομή στο πλαίσιο του IoT δεν είναι σταθερή και ποικίλλει με βάση τις απαιτήσεις που παρουσιάζει η εκάστοτε εφαρμογή αλλά και του τρόπου με τον οποίο υλοποιείται το κάθε σύστημα. Με τον τρόπο αυτό, σύμφωνα με την υπάρχουσα βιβλιογραφία, δημιουργούνται πολλές και διαφορετικές αρχιτεκτονικές δομές του IoT [53]. Στο πλαίσιο της παρούσας εργασίας παρέχεται μια επισκόπηση των ευρέως αποδεκτών αρχιτεκτονικών δομών του IoT.

3.2.1 Απαιτήσεις αρχιτεκτονικών δομών

Για το σχεδιασμό της αρχιτεκτονικής δομής ενός συστήματος IoT, στη βιβλιογραφία έχουν παρουσιαστεί πολλές προσεγγίσεις, οι οποίες βάσει του μοντέλου αρχιτεκτονικού σχεδιασμού που χρησιμοποιούν μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες [54]: τις αρχιτεκτονικές top-down και τις αρχιτεκτονικές bottom-up.

Οι αρχιτεκτονικές top-down χρησιμοποιούν ως βάση την υπηρεσιοστρεφή αρχιτεκτονική (Service Oriented Architecture – SOA) και ξεκινώντας από το στρώμα εφαρμογών Διαδικτύου (που βρίσκεται στο πάνω μέρος των στρωμάτων της αρχιτεκτονικής δομής), οργανώνουν την παροχή υπηρεσιών στον φυσικό κόσμο, μέσω των υπηρεσιών του Ιστού, προσπαθώντας να επιτύχουν συμβατότητα με τα χαρακτηριστικά των πραγμάτων (που βρίσκονται στο κάτω μέρος των στρωμάτων) [55]. Αντίθετα, η φιλοσοφία των αρχιτεκτονικών bottom-up είναι τελείως αντίστροφη, ξεκινόντας από τη δομή των πραγμάτων για να επεκταθούν προς το στρώμα του Διαδικτύου.

Τα δυο μοντέλα αρχιτεκτονικού σχεδιασμού παρουσιάζουν διαφορετικά χαρακτηριστικά. Η προσέγγιση top-down δίνει έμφαση στην παροχή υπηρεσιών και στην ομοιότητα των υπηρεσιών που παρέχονται από το Διαδίκτυο στα πράγματα, προσπαθώντας να επεκτείνει τους κανόνες του Διαδικτύου στο IoT. Επικεντρώνεται δηλαδή στην αρχιτεκτονική λογισμικού του συστήματος IoT. Η προσέγγιση bottom-top δίνει έμφαση στη σύνδεση των αντικειμένων του IoT και τις μεταξύ τους σχέσεις. Εστιάζει επομένως περισσότερο στη φυσική αρχιτεκτονική που σχηματίζεται από την σύνδεση των αντικειμένων στο σύστημα IoT [54].

Ανεξάρτητα από το χρησιμοποιούμενο μοντέλο σχεδιασμού, η αρχιτεκτονική δομή του IoT θα πρέπει να πληροί ορισμένες σημαντικές απαιτήσεις, όπως [56]:

- ***Ταυτόχρονη συλλογή δεδομένων:*** Υποστήριξη συλλογής, ανάλυσης και ελέγχου δεδομένων από μεγάλο αριθμό αισθητήρων ή ενεργοποιητών
- ***Αποτελεσματικό χειρισμό δεδομένων:*** Ελαχιστοποίηση των ακατέργαστων δεδομένων και μεγιστοποίηση των πληροφοριών από τις οποίες μπορούν να ληφθούν οι καταλληλότερες αποφάσεις για τη λήψη των απαραίτητων μέτρων και ενεργειών
- ***Συνδεσιμότητα και επικοινωνίες:*** Δημιουργία ενός δικτύου με δυνατότητα συνδεσιμότητας και ευελιξίας και σχεδιασμός πρωτοκόλλων υποστήριξης της επικοινωνίας μεταξύ αισθητήρων / ενεργοποιητών και cloud
- ***Κλιμάκωση και ανεξαρτησία από κατασκευαστικές πλατφόρμες:*** Δημιουργία ενός δικτύου με δυνατότητα κλιμάκωσης χρησιμοποιώντας την ίδια αρχιτεκτονική. Κάθε στρώμα της αρχιτεκτονικής δομής θα πρέπει να μπορεί να υποστηρίξει την σύνδεση στο δίκτυο συσκευών με διαφορετικά χαρακτηριστικά, hardware υλικά και υποδομή από διάφορους κατασκευαστές
- ***Ασφάλεια:*** Υποστήριξη κρυπτογράφησης και συνεχούς παρακολούθησης από άκρο σε άκρο
- ***Διαθεσιμότητα και ποιότητα εξυπηρέτησης:*** Δημιουργία ενός δικτύου που να παρουσιάζει ελάχιστους λανθάνοντες χρόνους (καθυστερήσεις) και μεγάλη ανοχή σε σφάλματα
- ***Ανοιχτά πρότυπα και διαλειτουργικότητα:*** Δημιουργία ανοχτών προτύπων και πρωτοκόλλων επικοινωνίας μεταξύ των στρωμάτων της αρχιτεκτονικής που να διασφαλίζουν τη διαλειτουργικότητα
- ***Διαχείριση συσκευών:*** Κάθε δίκτυο θα πρέπει να υποστηρίζει αυτοματοποιημένη και απομακρυσμένη διαχείριση των συσκευών του και να δίνει τη δυνατότητα για αυτοματοποιημένη και απομακρυσμένη εγκατάσταση των ενημερώσεων των λογισμικών τους

- ***Καθορισμένες διεπαφές API:*** Κάθε στρώμα της αρχιτεκτονικής πρέπει να διαθέτει καθορισμένες διεπαφές API (Application Programming Interface) που να επιτρέπουν την εύκολη ενσωμάτωση με υπάρχουσες εφαρμογές και με άλλες λύσεις IoT

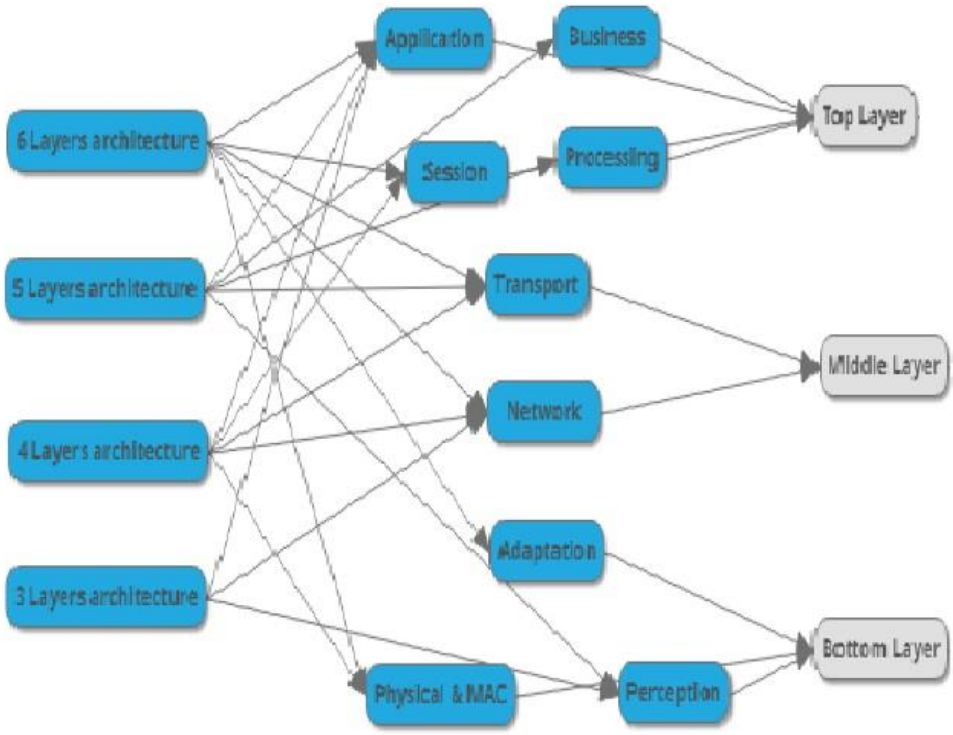
Φυσικά, οποιοσδήποτε αρχιτεκτονικός σχεδιασμός μπορεί να υποστηρίζει περαιτέρω απαιτήσεις. Μερικές από αυτές ενδέχεται να πληρούνται ήδη από τον αρχικό σχεδιασμό, άλλες ενδέχεται να απαιτούν την προσθήκη περαιτέρω στοιχείων και άλλες μπορεί να προκύψουν μετά την υλοποίηση και εφαρμογή της αρχιτεκτονικής.

3.2.2 Ταξινόμηση αρχιτεκτονικών δομών IoT

Στη βιβλιογραφία δεν υπάρχει μια ενιαία και γενική αρχιτεκτονική δομή του IoT που να είναι κοινά αποδεκτή από την ακαδημαϊκή και ερευνητική κοινότητα και να χρησιμοποιείται σε όλες τις εφαρμογές. Κατά καιρούς έχουν προταθεί και παρουσιαστεί πολλές και διαφορετικές αρχιτεκτονικές δομές συστημάτων IoT, ανάλογα με τον σκοπό εφαρμογής τους [57]. Η πολυπλοκότητα ενός συστήματος IoT εξαρτάται από την ετερογένεια των συσκευών που περιέχει και την επεκτασιμότητα που θέλει να υποστηρίζει. Η αρχιτεκτονική δομή ενός συστήματος IoT πρέπει να περιλαμβάνει συσκευές, δίκτυα και εφαρμογές που να έχουν δυνατότητα απρόσκοπτης συνεργασίας, με σκοπό την δημιουργία έξυπνων αποτελεσμάτων ανάλυσης και επεξεργασίας που παρέχονται στους χρήστες μέσω υπηρεσιών, λαμβάνοντας υπόψη τις δικλείδες ασφαλείας [58]. Με βάση την ανάλυση των αρχιτεκτονικών δομών του IoT που έχουν παρουσιαστεί στη βιβλιογραφία, μια αρχιτεκτονική, ανεξαρτήτως φιλοσοφίας και οπτικής, περιέχει στρώματα τεχνολογιών, πρωτοκόλλων και προτύπων επικοινωνίας, τα οποία επιτρέπουν τη συνεργασία μεταξύ διάφορων τεχνολογιών, με σκοπό την υποστήριξη βασικών χαρακτηριστικών του IoT, όπως η επεκτασιμότητα, η ετερογένεια και η διαλειτουργικότητα, σε όλες τις υλοποιήσεις του [59].

Οι αρχιτεκτονικές δομές που έχουν παρουσιαστεί στη βιβλιογραφία κατά καιρούς βασίζονται στη λογική του μοντέλου αναφοράς ανοικτής διασύνδεσης συστημάτων (Open Systems Interconnection – OSI). Βάσει αυτού του στοιχείου, ο αριθμός των στρωμάτων που περιέχεται σε κάθε αρχιτεκτονική IoT δημιουργεί διάφορους τύπους αρχιτεκτονικής, οι

οποίοι μπορεί να χωριστούν σε πέντε κατηγορίες [60]: τριών, τεσσάρων, πέντε, έξι και εφτά στρωμάτων. Η αρχιτεκτονική των τριών στρωμάτων θεωρείται ως η βασική ή θεμελιώδης αρχιτεκτονική του IoT. Παρόλα αυτά, σύμφωνα με τους περισσότερους ερευνητές, η συγκεκριμένη αρχιτεκτονική δεν μπορεί να εκφράσει το σύνολο των χαρακτηριστικών του IoT, λόγω της εξελικτικής πορείας που παρουσιάζει η τεχνολογία. Αντίθετα, η αρχιτεκτονική των πέντε στρωμάτων μπορεί να ενισχύσει την πλήρη κατανόηση της ουσίας του IoT και να υποστηρίξει την περαιτέρω εξέλιξή του [43].



Εικόνα 3-3: Ταξινόμηση αρχιτεκτονικών IoT [57]

Στο πλαίσιο της παρούσας εργασίας και στην προσπάθεια παρουσίασης μιας γενικευμένης ανάλυσης των διαφόρων αρχιτεκτονικών δομών που έχουν εμφανιστεί στη βιβλιογραφία θα ακολουθηθεί η προσέγγιση των Aman και συν. (2020). Οι συγγραφείς αγνόησαν τις διαφορές των στρωμάτων που περιέχονται στις διάφορες αρχιτεκτονικές δομές του IoT και ομαδοποίησαν τις λειτουργίες όλων των πιθανών στρωμάτων, δημιουργώντας τρία στρώματα (Εικ. 3-3) [57]: το ανώτερο στρώμα, το μεσαίο στρώμα και το κατώτερο στρώμα. Η

ταξινόμηση αυτή βασίζεται στα χρησιμοποιούμενα πρωτόκολλα και τις λειτουργικές απαιτήσεις των στρωμάτων των διαφόρων αρχιτεκτονικών. Με βάση αυτή την προσέγγιση, το ανώτερο στρώμα χρησιμοποιείται κυρίως για την υλοποίηση των λειτουργικών απαιτήσεων του συστήματος που έχει ο χρήστης, το μεσαίο στρώμα υλοποιεί τις λειτουργικές απαιτήσεις του συστήματος που έχει το δίκτυο και το κατώτερο στρώμα είναιν σχεδιασμένο ώστε να υλοποιεί τις λειτουργικές απαιτήσεις του συστήματος που έχουν οι συσκευές [57]. Με άλλα λόγια, στη συγκεκριμένη προσέγγιση ακολουθείται η φιλοσοφία της θεμελιώδους αρχιτεκτονικής δομής του IoT, χωρίς όμως να παραλείπονται τα χαρακτηριστικά των άλλων αρχιτεκτονικών δομών.

I) Ανώτερο στρώμα

Το ανώτερο στρώμα της προσέγγισης των Aman και συν. (2020) αφορά το στρώμα διαχείρισης των χρηστών και περιλαμβάνει [57]:

- το στρώμα εφαρμογών (application layer)
- το στρώμα επιχειρήσεων (business layer)
- το στρώμα διεπαφής (interface layer)
- το στρώμα υποστήριξης (support layer) και
- το στρώμα υπηρεσίας / δεδομένων (service / data layer)

Το στρώμα εφαρμογών ορίζει όλες τις εφαρμογές που χρησιμοποιούν το IoT και έχει την ευθύνη παροχής των υπηρεσιών στις εφαρμογές αυτές. Οι παρεχόμενες υπηρεσίες κάθε εφαρμογής είναι διαφορετκές, καθώς είναι αλληλένδετες με τις πληροφορίες που έχουν προκύψει από την ανάλυση των δεδομένων των αισθητήρων. Στο στρώμα αυτό χρησιμοποιούνται επίσης πολλά διαφορετικά λειτουργικά συστήματα και τεχνολογίες. Η διαφορετικότητα όμως αυτή συνδυάζεται και με πολλά άλλα ζητήματα τα οποία προκύπτουν λόγω της μη ύπαρξης ενός συγκεκριμένου και πιστοποιημένου προτύπου υλοποίησης του στρώματος εφαρμογών του IoT [61]. Η εφαρμογή ενός τέτοιου προτύπου θα μπορούσε να επιλύσει πολλά ζητήματα του IoT, όπως θα γίνει κατανοητό από τα όσα θα αναφερθούν στο τελευταίο κεφάλαιο.

Το στρώμα επιχειρήσεων εισήχθη στην αρχιτεκτονική δομή των πέντε στρωμάτων, με σκοπό τη διαχείριση και την ιδιαίτερη απεικόνιση των δεδομένων που λαμβάνονται από το στρώμα εφαρμογών, έτσι ώστε να είναι δυνατή η δημιουργία επιχειρηματικών μοντέλων, γραφημάτων και διαγραμμάτων ροής, τα οποία είναι χρήσιμα για την αξιολόγηση και την υποστήριξη της τεχνολογίας του IoT. Επίσης, αναφέρεται στις επιδιωκόμενες συμπεριφορές των εφαρμογών και ενεργεί σαν διαχειριστής ολόκληρου του συστήματος. Ευθύνη του είναι η διαχείριση και ο έλεγχος των εφαρμογών και των μοντέλων επιχειρήσεων και κερδών του IoT. Το συγκεκριμένο στρώμα διαχειρίζεται επίσης το απόρρητο του χρήστη και έχει τη δυνατότητα να καθορίσει τον τρόπο δημιουργίας, αποθήκευσης και τροποποίησης των πληροφοριών [62].

Το στρώμα υποστήριξης εισήχθη στην αρχιτεκτονική των τεσσάρων στρωμάτων με σκοπό την ενίσχυση της ασφάλειας των συστημάτων IoT. Στην αρχιτεκτονική αυτή, οι πληροφορίες του στρώματος αντίληψης αποστέλλονται στο στρώμα δικτύου μέσω του στρώματος υποστήριξης. Το στρώμα υποστήριξης παίζει δύο ρόλους: (α) επιβεβαιώνει ότι οι πληροφορίες αποστέλλονται από αυθεντικούς χρήστες και επαληθεύει την ταυτοποίηση χρηστών και πληροφοριών και (β) μεταφέρει τις επαληθευμένες πληροφορίες στο στρώμα δικτύου. Το μέσο μετάδοσης των πληροφοριών που χρησιμοποιεί το στρώμα υποστήριξης μπορεί να είναι ασύρματο ή ενσύρματο [63].

Το στρώμα υπηρεσίας / δεδομένων υφίσταται σε περιπτώσεις αρχιτεκτονικής SOA. Βασική λειτουργία αυτού του στρώματος είναι η υποστήριξη των προδιαγραφών υπηρεσίας του μεσαίου λογισμικού (middleware) ενός συστήματος IoT, οι οποίες καθορίζονται από διάφορες εταιρείες. Ο σωστός σχεδιασμός του στρώματος υπηρεσίας δίνει τη δυνατότητα αναγνώρισης των απαιτήσεων των εφαρμογών και παροχής διεπαφών API και πρωτοκόλλων, ώστε οι απαιτούμενες υπηρεσίες, εφαρμογές και ανάγκες των χρηστών να μπορούν να υποστηριχθούν κατάλληλα. Το στρώμα υποστήριξης είναι επίσης σε θέση να επεξεργαστεί τα όποια ζητήματα των παρεχόμενων υπηρεσιών, όπως η ανταλλαγή και αποθήκευση των πληροφοριών, η διαχείριση των δεδομένων και η επικοινωνία [64].

Με βάση τα χαρακτηριστικά και τις λειτουργίες αυτές, το ανώτερο στρώμα της προσέγγισης των Aman και συν. (2020) χειρίζεται ολόκληρο το σύστημα IoT και διαχειρίζεται και ελέγχει την μορφοποίηση και παρουσίαση των δεδομένων στο πλαίσιο της αλληλεπίδρασης αντικειμένων και συστήματος. Κάτι τέτοιο είναι εφικτό μέσω χειρισμού των κανόνων επιχειρηματικών μοντέλων (business rule engines), οι οποίοι ενεργοποιούν αυτοματοποιημένες διαδραστικές διαδικασίες για την υλοποίηση ενός συστήματος IoT μεγαλύτερης απόκρισης στις ανάγκες τις εκάστοτε εφαρμογής. Τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται σε αυτό το στρώμα είναι τα MQTT και CoAP, που θα αναλυθούν σε επόμενη ενότητα [57].

II) Μεσαίο στρώμα

Το μεσαίο στρώμα της προσέγγισης των Aman και συν. (2020) αφορά την επικοινωνία του δικτύου και περιλαμβάνει [57]:

- το στρώμα δικτύου (network layer)
- το στρώμα μεταφοράς (transport layer)
- το στρώμα μεσαίου λογισμικού (middleware layer) και
- το στρώμα Διαδικτύου (Internet layer)

Το στρώμα μεταφοράς της αρχιτεκτονικής δομής του IoT των πέντε στρωμάτων ουσιαστικά πραγματοποιεί τις ίδιες λειτουργίες με το στρώμα δικτύου των αρχιτεκτονικών δομών με τρία και τέσσερα στρώματα. Ευθύνη του στρώματος μεταφοράς αποτελεί η ασφαλή μετάδοση των δεδομένων που έχουν ήδη συλλεχθεί από τις συσκευές του στρώματος αντίληψης. Σε αυτό το στρώμα υπάρχει πληθώρα διαφορετικών τεχνολογιών που χρησιμοποιούνται για τη μετάδοση των δεδομένων, όπως είναι οι ασύρματες επικοινωνίες, τα δορυφορικά δίκτυα και οι ενσύρματες επικοινωνίες χαλκού και οπτικών ινών [65].

Το στρώμα μεσαίου λογισμικού συλλέγει τις πληροφορίες που αποστέλλονται από το στρώμα μεταφοράς τις οποίες και επεξεργάζεται. Έχει την ευθύνη εξάλειψης των περιττών πληροφοριών, εξάγοντας τα χρήσιμα δεδομένα. Επίσης, αφαιρεί μεγάλο μέρος των Big Data του IoT, στοιχείο το οποίο όμως μπορεί να θέσει σε κίνδυνο την αποδοτικότητα της

τεχνολογίας. Εκτός από την επεξεργασία των δεδομένων, το συγκεκριμένο στρώμα είναι υπεύθυνο για τη σύνδεση του συστήματος με το cloud και τις βάσεις δεδομένων καθώς και για την αποθηκευσή τους σε αυτά. Με τη συνεχή εξέλιξη των τεχνολογιών του cloud και του IoT, το στρώμα μεσαίου λογισμικού μπορεί να παρέχει πιο ισχυρές δυνατότητες υπολογισμού και αποθήκευσης. Επίσης, αυτό το στρώμα παρέχει διεπαφές API για κάλυψη των απαιτήσεων του στρώματος εφαρμογών [66].

Με βάση τα χαρακτηριστικά και τις λειτουργίες αυτές, το μεσαίο στρώμα της προσέγγισης των Aman και συν. (2020) μπορεί να παρέχει διάφορες υπηρεσίες στα κατώτερα και ανώτερα στρώματα και ευθύνεται για συνδέσεις με άλλες έξυπνες συσκευές και κόμβους δικτύου, όπως πύλες, διακομιστές ή δρομολογητές. Επίσης, διαχειρίζεται τη μετάδοση των δεδομένων αισθητήρα, τη δρομολόγηση των πακέτων και την επεξεργασία, χρησιμοποιώντας τεχνολογίες ασύρματης επικοινωνίας όπως ZigBee, Wi-Fi, RFID, Bluetooth χαμηλής ενέργειας (Bluetooth Low Energy - BLE), NFC, τοπικά δίκτυα (Local Area Networks - LAN) και υπερ-ευρυζωνικά ή δίκτυα ευρείας περιοχής (Wide Area Networks - WAN) όπως GSM (Global System for Mobile communications), GPRS (General Packet Radio Service) και LTE. Βασικό χαρακτηριστικό όλων αυτών των δικτύων και τεχνολογιών είναι η χαμηλής ισχύος λειτουργία τους με απώλειες. Για το λόγο αυτό, η ομάδα έργου μηχανικής του Διαδικτύου (Internet Engineering Task Force – IETF), έχοντας λάβει σοβαρά υπόψη τις απαιτήσεις και τα ιδιαίτερα χαρακτηριστικά που παρουσιάζουν τα δίκτυα IoT, δημιούργησε μια ομάδα εργασίας, που ονομάζεται ROLL (Routing Over Low power and Lossy), με σκοπό την προτυποποίηση της δρομολόγησης στα συγκεκριμένα δίκτυα, έχοντας ως βάση το IPv6. Το αποτέλεσμα των εργασιών της συγκεκριμένης ομάδας οδήγησε στη δημιουργία του πρωτοκόλλου δρομολόγησης RPL (Routing Protocol for LLNs), ένα πρωτόκολλο που λειτουργεί στο επίπεδο IP και επιτρέπει την πραγματοποίηση διαδικασιών δρομολόγησης πάνω από διάφορα επίπεδα ζεύξης [67].

III) Κατώτερο στρώμα

Το κατώτερο στρώμα της προσέγγισης των Aman και συν. (2020) αποτελεί τη διασύνδεση των συσκευών με ενσωματωμένους αισθητήρες και της ψηφιακής επικοινωνίας και περιλαμβάνει [57]:

- το στρώμα προσαρμογής (adaptation layer)
- το φυσικό / ελέγχου πρόσβασης στο μέσο στρώμα (PHY/MAC layer)
- το στρώμα υποδομής (infrastructure layer)
- το στρώμα ανίχνευσης (sensing layer) και
- το στρώμα αντίληψης (perception layer)

Το στρώμα προσαρμογής εισήχθη στην αρχιτεκτονική δομή των συστημάτων IoT στην περίπτωση χρήσης της τεχνολογίας 6LoWPAN σε δίκτυα LLN (Low-power and Lossy Network). Η δημιουργία του στρώματος προσαρμογής είχε ως σκοπό τη δυνατότητα προώθησης των πακέτων δεδομένων μεταξύ των στρωμάτων δικτύου και ζεύξης δεδομένων καθώς και τη δρομολόγησή τους. Το στρώμα προσαρμογής παρέχει επίσης μηχανισμούς συμπίεσης, κατακερματισμού και ενθυλάκωσης, με σκοπό τη μεταφορά των πακέτων IPv6 στα δίκτυα LLN [68].

Το PHY/MAC στρώμα χρησιμοποιείται για την κάλυψη του τρόπου με τον οποίο μια συσκευή συνδέεται σε ένα δίκτυο μέσω ενσύρματων ή ασύρματων μηχανισμών, αλλά του τρόπου μοναδικής αναγνώρισης των συσκευών μέσω των διευθύνσεων MAC. Τα περισσότερα πρότυπα που χρησιμοποιούνται σε αυτό το στρώμα έχουν ως σκοπό τη δημιουργία καναλιών επικοινωνίας. Ο σχεδιασμός του στρώματος PHY/MAC θα πρέπει να καλύπτει το γεγονός ότι οι συσκευές που ενσωματώνονται σε ένα σύστημα IoT πρέπει να λειτουργούν με μπαταρίες μεγάλης διάρκειας ζωής, απαιτούν χαμηλή κατανάλωση ενέργειας και διαθέτουν από ελάχιστους έως καθόλου υπολογιστικούς πόρους. Επίσης, σε περιπτώσεις σύνδεσης και λειτουργίας πολλών συσκευών σε ένα μονό περιβάλλον, ο σχεδιασμός του στρώματος PHY/MAC θα πρέπει είναι τέτοιος που να λαμβάνονται υπόψη η διαθεσιμότητα μικρού εύρους ζώνης και η ανάγκη για κλιμάκωση [69].

Το στρώμα αντίληψης αποτελεί το πρώτο στρώμα πολλών αρχιτεκτονικών δομών του IoT. Το συγκεκριμένο στρώμα αποτελείται ουσιαστικά από συσκευές οι οποίες αντιλαμβάνονται, συλλέγουν, αποθηκεύουν, αναλύουν και μεταδίδουν τις αλλαγές που συμβαίνουν στο φυσικό περιβάλλον στο οποίο βρίσκονται, μέσω των αισθητήρων που περιλαμβάνουν. Για το λόγο αυτό, σε άλλες αρχιτεκτονικές αναφέρεται ως στρώμα συσκευών (device layer) και σε άλλες ως στρώμα ανίχνευσης (sensing layer) [68].

Με βάση τα χαρακτηριστικά και τις λειτουργίες αυτές, στο κατώτερο στρώμα της προσέγγισης των Aman και συν. (2020), οι αισθητήρες ανιχνεύουν το γύρω περιβάλλον τους και συγκεντρώνουν πληροφορίες, όπως φυσικές παραμέτρους ή στοιχεία για το περιβάλλον. Οι αισθητήρες έχουν την ικανότητα να αποκτήσουν ποσοτικές τιμές μεταβλητών φυσικών μεγεθών (θερμοκρασία, ταχύτητα του ανέμου, ποιότητα του αέρα, κλπ.), οι οποίες στη συνέχεια μεταφράζονται σε ψηφιακά σήματα, που τελικά μεταγλωττίζονται σε κάποια γλώσσα μηχανής [57].

Στον πίνακα 3-1 παρουσιάζεται μια σύνοψη των λειτουργιών των τριών προαναφερθέντων στρωμάτων καθώς και μερικών από τα πρωτόκολλα που χρησιμοποιούνται σε αυτά [57].

Πίνακας 3-1: Λειτουργία στρωμάτων αρχιτεκτονικής δομής IoT [57]

Στρώμα - Χειριστής	Λειτουργία	Πρωτόκολλα
Ανώτερο – Χρήστης	Εφαρμογές ή εργαλεία υποστήριξης αποφάσεων	AMQP, COAP, DDS, DNS-SD, MQTT, MDNS, REST, XMPP
Μεσαίο - Δίκτυο	Ενσωμάτωση εφαρμογών, δικτύων και συσκευών. Απόκρυψη πολυπλοκότητας από το χρήστη	UDP, IPv6 –v4, RPL, DODAG
Κατώτερο - Συσκευή	Φυσική υποδομή πολλαπλής πρόσβασης και τεχνικές διαμόρφωσης	6LoWPAN, LTE-A, Z-WAVE, IEEE 802.15.4

3.3 Επικοινωνία IoT

Οι έξυπνες συσκευές παίζουν βασικό ρόλο στην υλοποίηση της συνολικής οπτικής του IoT, η οποία σε γενικές γραμμές αφορά τη σύνδεση ετερογενών αντικειμένων τόσο μεταξύ τους όσο

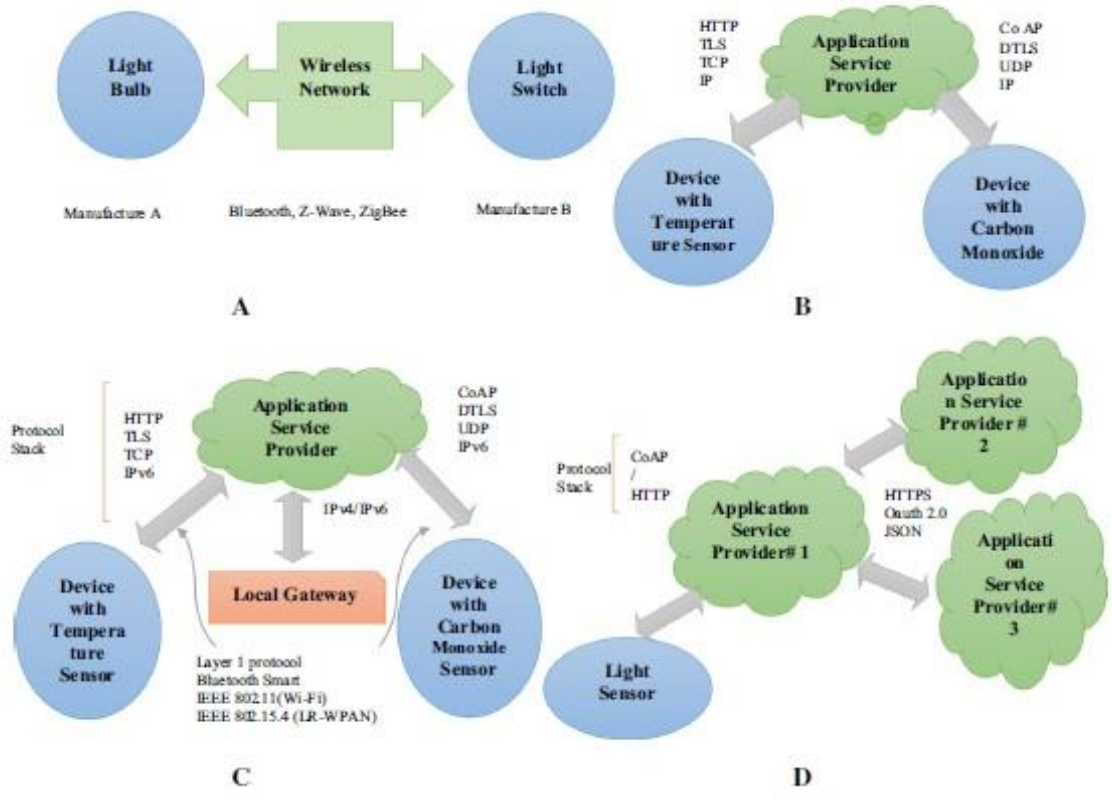
και στο Διαδίκτυο. Από λειτουργικής άποψης, ο καθορισμός του τρόπου σύνδεσης και του τρόπου επικοινωνίας των συσκευών IoT, αποτελεί ιδιαίτερα βασικό στοιχείο. Η επικοινωνία των συσκευών στο πλαίσιο του IoT περιλαμβάνει τη χρήση πολλών τεχνολογιών, οι οποίες μπορούν να υλοποιηθούν σε συγκεκριμένα στρώματα της αρχιτεκτονικής δομής της τεχνολογίας, όπως είναι τα στρώματα που εμπεριέχονται στο μεσαίο στρώμα της αρχιτεκτονικής που παρουσιάστηκε στην προηγούμενη ενότητα, δηλαδή τα στρώματα δικτύου, μεταφοράς, μεσαίου λογισμικού και Διαδικτύου [70]. Τα στρώματα αυτά, ανεξάρτητα από την αρχιτεκτονική δομή που ακολουθείται στην εκάστοτε εφαρμογή IoT, περιλαμβάνουν τις τεχνολογίες και τα πρωτόκολλα που υποστηρίζουν την συνδεσιμότητα μεταξύ των αντικειμένων και μεταξύ των αντικειμένων και του Διαδικτύου [71].

Τα συστήματα IoT χρησιμοποιούν μια τεράστια ποικιλία τεχνολογιών επικοινωνίας που πρέπει να χαρακτηρίζονται από διαλειτουργικότητα, προκειμένου να πληρούν τις απαιτήσεις τους. Επίσης, τα δίκτυα IoT θα πρέπει να είναι σε θέση να πληρούν ορισμένες απαιτήσεις υψηλού επιπέδου, όπως συνδεσιμότητα βάσει ταυτοποίησης, αυτόνομη δικτύωση, παροχή αυτόνομων υπηρεσιών, δυνατότητες βάσει τοποθεσίας, ασφάλεια, προστασία της ιδιωτικότητας, ποιότητα παρεχόμενων υπηρεσιών, δυνατότητα σύνδεσης συσκευών μέσω plug and play και διαχείριση. Η πλήρωση όλων αυτών των απαιτήσεων θα δώσει τη δυνατότητα στα συστήματα IoT να αντιμετωπίσουν ευκολότερα τα φαινόμενα καθυστέρησης, συμφόρησης και απώλειας πακέτων τα οποία δημιουργούνται από τη συνεχή αύξηση του όγκου των δεδομένων και των πληροφοριών που πρέπει να μεταφέρονται σε αυτά τα συστήματα [71].

Η χρήση των κατάλληλων τεχνολογιών και πρωτοκόλλων επικοινωνίας σε κάθε περίπτωση εξαρτάται από διάφορους σημαντικούς παράγοντες, όπως [72]: (α) το μοντέλο επικοινωνίας των συσκευών IoT, (β) το είδος και την εμβέλεια του δικτύου IoT, (γ) την τοπολογία του δικτύου, (δ) την κατανάλωση ενέργειας και (ε) την χρονική ευαισθησία.

3.3.1 Μοντέλα επικοινωνίας

Σύμφωνα με δημοσίευμα του συμβουλίου IAB, του Σεπτεμβρίου του 2015, το οποίο αφορούσε την δικτύωση των έξυπνων αντικειμένων, η σύνδεση μεταξύ των τριών μερών της βασικής αρχιτεκτονικής δομής ενός οποιουδήποτε συστήματος IoT, που παρουσιάστηκε σε προηγούμενη ενότητα, μπορεί να πραγματοποιηθεί με τέσσερεις δυνατούς τρόπους (Εικ. 3-4) [71]: α) συσκευή με συσκευή, β) συσκευή με cloud, γ) συσκευή με πύλη και δ) με χρήση μοντέλου back-end κοινής χρήσης δεδομένων. Οι τέσσερεις αυτοί τρόποι σύνδεσης δημιουργούν τέσσερα αντίστοιχα μοντέλα επικοινωνίας των συσκευών IoT [73], [74].



Εικόνα 3-4: Μοντέλα επικοινωνίας συσκευών IoT [70]

I) Μοντέλο επικοινωνίας συσκευής με συσκευή (D2D)

Στο μοντέλο επικοινωνίας συσκευής με συσκευή (Device-to-Device – D2D) (Εικ. 3-4 (α)), δύο ή περισσότερα έξυπνα αντικείμενα επικοινωνούν απευθείας, χωρίς την ύπαρξη κάποιου ενδιάμεσου, με σκοπό την ανταλλαγή πληροφοριών σε πραγματικό χρόνο. Τυπικά, το μοντέλο επικοινωνίας D2D βασίζεται στη μεταφορά πακέτων δεδομένων μικρού μήκους και παρουσιάζει σχετικά χαμηλό ρυθμό μεταφοράς δεδομένων, χρησιμοποιώντας πρωτόκολλα οικιακού αυτοματισμού.

II) Μοντέλο επικοινωνίας συσκευής με cloud (D2C)

Στο μοντέλο επικοινωνίας συσκευής με cloud (Device-to-Cloud – D2C), τα έξυπνα αντικείμενα IoT δημιουργούν μια απευθείας σύνδεση με τις εφαρμογές cloud, όπως φαίνεται στην εικόνα 3-4 (β). Σκοπός της σύνδεσης μεταξύ των συσκευών IoT και του συστήματος αποθήκευσης δεδομένων (cloud) είναι η ανταλλαγή δεδομένων και ο έλεγχος της κίνησης των μηνυμάτων. Το μοντέλο D2C χρησιμοποιεί τυπικούς μηχανισμούς επικοινωνίας, όπως ενσύρματες συνδέσεις Ethernet ή Wi-Fi, με στόχο τη σύνδεση της συσκευής και του δικτύου IP, που τελικά συνδέεται με ένα κεντρικό σύστημα αποθήκευσης δεδομένων.

III) Μοντέλο επικοινωνίας συσκευής με πύλη (D2G)

Στο μοντέλο επικοινωνίας συσκευής με πύλη (Device-to-Gateway – D2G) (Εικ. 3-4 (γ)), η συσκευή IoT συνδέεται στην υπηρεσία cloud μέσω του στρώματος εφαρμογών της πύλης. Με απλούστερους όρους, αυτό σημαίνει ότι η εκάστοτε τοπική συσκευή, που λειτουργεί ως πύλη, παίζει το ρόλο του μεσάζοντα μεταξύ των έξυπνων συσκευών και του κεντρικού συστήματος αποθήκευσης δεδομένων (cloud) Η πύλη, στο μοντέλο D2G, έχει δύο βασικές λειτουργίες: συλλέγει δεδομένα από τους αισθητήρες τα οποία και δρομολογεί στο κεντρικό σύστημα αποθήκευσης (cloud) μέσω του Διαδικτύου.

IV) Μοντέλο back-end κοινής χρήσης δεδομένων

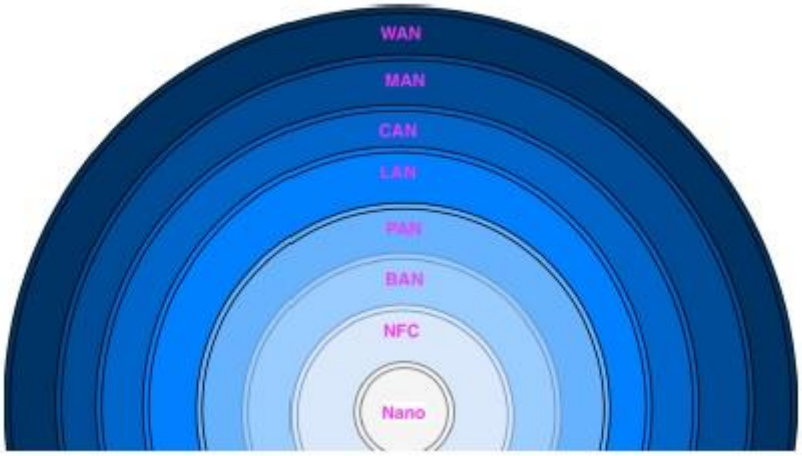
Στο συγκεκριμένο μοντέλο επικοινωνίας, οι πληροφορίες είναι κοινής χρήσης μεταξύ του κεντρικού συστήματος αποθήκευσης δεδομένων και των παρόχων εφαρμογών και υπηρεσιών (Εικ. 3-4 (δ)). Το συγκεκριμένο μοντέλο υποστηρίζει την επιθυμία των χρηστών να συνδυάζουν τα δεδομένα από πολλές πηγές (αισθητήρες, έξυπνα αντικείμενα, κλπ.) και να

παραχωρούν την πρόσβαση σε αυτά σε τρίτους προς ανάλυση. Οι χρήστες μπορεί να είναι μεμονωμένα άτομα ή επιχειρήσεις. Το μοντέλο υποστηρίζει τη χρήση πρωτοκόλλων επικοινωνίας που παρουσιάζουν υψηλή διαθεσιμότητα, χωρητικότητα και αξιοπιστία όσον αφορά την ανάκαμψη από δυσλειτουργίες [75].

3.3.2 Είδη δικτύων IoT

Τα δίκτυα IoT μπορούν να ταξινομηθούν σε διαφορετικά είδη ανάλογα με την εμβέλεια που παρουσιάζουν και τον αριθμό των συσκευών που είναι σε θέση να υποστηρίξουν. Στην εικόνα 3-5 παρουσιάζεται μια τέτοια ταξινόμηση των δικτύων IoT [73].

Ένα νανοδίκτυο (nano) είναι ένα σύνολο μικροσκοπικών συσκευών (μέγιστου μεγέθους λίγων μικρόμετρων) που πραγματοποιούν πολύ απλές λειτουργίες, όπως ανίχνευση, επεξεργασία, αποθήκευση και ενεργοποίηση. Τέτοια δίκτυα χρησιμοποιούνται σε στρατιωτικές εφαρμογές, στον τομέα της βιοϊατρικής και γενικότερα σε τομείς όπου μπορεί να εφαρμοστεί η νανοτεχνολογία.



Εικόνα 3-5: Είδη δικτύων IoT [73]

Τα NFC είναι δίκτυα χαμηλής ταχύτητας που μπορούν να συνδέουν ηλεκτρονικές συσκευές που έχουν μέγιστη απόσταση μεταξύ τους της τάξης των 4 εκατοστών. Τα δίκτυα NFC

χρησιμοποιούνται συνήθως σε εφαρμογές συστημάτων ανέπαφης πληρωμής, ταυτοποίησης ηλεκτρονικών εγγράφων (ψηφιακές ταυτότητες), κλπ.

Τα δίκτυα περιοχής σώματος (Body Area Network - BAN) είναι δίκτυα που έχουν τη δυνατότητα σύνδεσης έξυπνων υπολογιστικών συσκευών, γνωστών ως wearables, οι οποίες μπορούν να φορεθούν ή ακόμα και να εμφυτευτούν στο ανθρώπινο σώμα. Τέτοιες συσκευές αφορούν έξυπνα ρολόγια (smartwatches), ζώνες καρπού (wrist bands), έξυπνα γυαλιά (smart glasses), έξυπνα κοσμήματα (smart jewellery), ηλεκτρονικά ενδύματα (electronic garments), επιθέματα δέρματος (skin patches), κλπ.

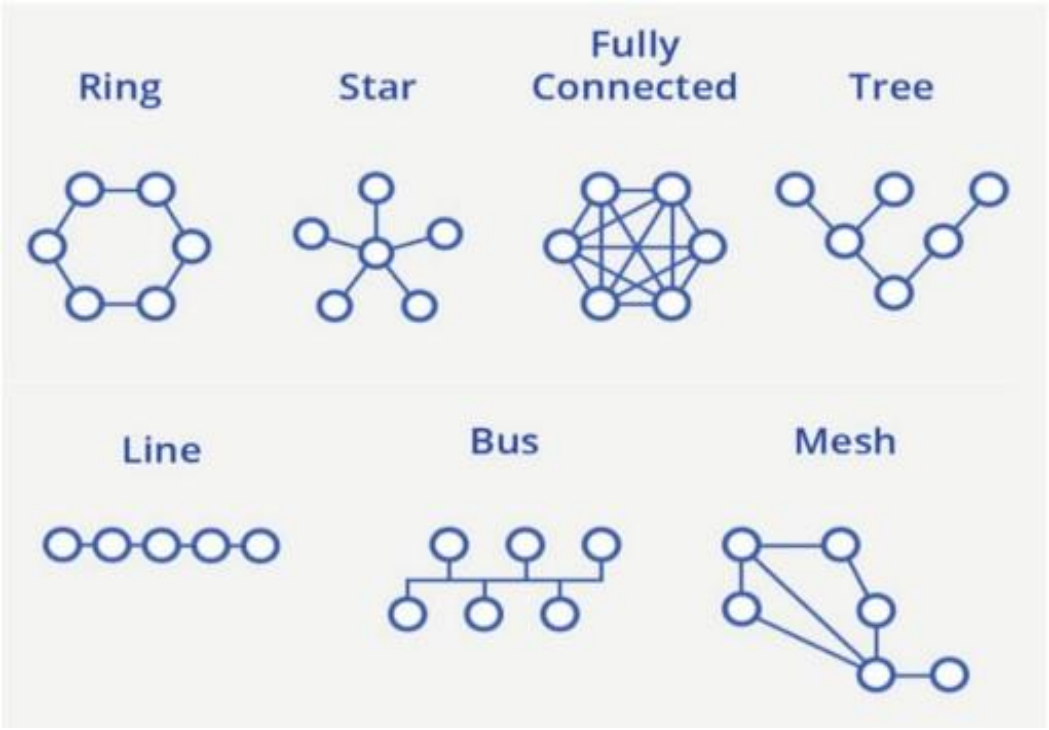
Τα δίκτυα προσωπικής περιοχής (Personal Area Network - PAN) χρησιμοποιούνται για τη σύνδεση συσκευών που συνήθως βρίσκονται σε μέγιστη απόσταση ακτίνας της τάξης των 7 μέτρων, δηλαδή καλύπτουν την επιφάνεια ενός ή δύο δωματίων.

Τα τοπικά δίκτυα (LAN) χρησιμοποιούνται για τη σύνδεση συσκευών IoT ή αισθητήρων που εκτείνονται στο χώρο ενός κτιρίου. Τα δίκτυα CAN (Campus / Corporate Area Network) αποτελούν συλλογή πολλών δικτύων LAN σε μια περιορισμένη γεωγραφική περιοχή, όπως επιχείρηση ή πανεπιστήμιο. Τα μητροπολιτικά δίκτυα (Metropolitan Area Network - MAN) αφορούν δίκτυα μεγάλης (μητροπολιτικής) έκτασης που για τη μετάδοση δεδομένων χρησιμοποιούν τεχνολογίες μικροκυμάτων. Τέλος, τα δίκτυα ευρείας περιοχής (WAN) αφορούν δίκτυα IoT πολύ μεγάλων γεωγραφικών περιοχών κάλυψης τα οποία ενώνουν πολλά μικρότερα δίκτυα LAN και MAN.

Όλα αυτά τα διαφορετικά είδη δικτύων IoT χρησιμοποιούνται σε διάφορα είδη εφαρμογών, ανάλογα με το εύρος κάλυψής τους και τον αριθμό των συσκευών που είναι σε θέση να υποστηρίξουν. Αυτή η διαφορετικότητα συναντάται και στον τύπο των πρωτοκόλλων επικοινωνίας που μπορούν να χρησιμοποιηθούν σε κάθε μελέτη περίπτωσης. Ανάλογα με την εκάστοτε μελέτη περίπτωσης, το χρησιμοποιούμενο πρωτόκολλο επικοινωνίας θα πρέπει να παρουσιάζει και άλλα σχετικά χαρακτηριστικά, όπως την ικανότητα υπερπήδησης των εμποδίων ή την απαίτηση για ύπαρξη οπτικής επαφής μεταξύ των συσκευών [76].

3.3.3 Τοπολογίες δικτύων IoT

Τα ασύρματα δίκτυα μπορούν επίσης να κατηγοριοποιηθούν σύμφωνα με την τοπολογία τους, δηλαδή τη διαμόρφωση συνδεσιμότητας που παρουσιάζουν. Βάσει της τοπολογίας του δικτύου στο οποίο ανήκουν, η διάταξη των κόμβων IoT μπορεί να παρουσιάζει σύνδεση (Εικ. 3-6) [74]: γραμμής (line), δακτυλίου (ring), αστέρα (star), πλέγματος (mesh), δέντρου (tree) ή διάυλου (bus).



Εικόνα 3-6: Τοπολογίες δικτύων IoT [74]

Όσον αφορά την τοπολογία ενός δικτύου IoT το στοιχείο που είναι μείζονος σημασίας είναι ο τρόπος σύνδεσης των συσκευών, ώστε να παρέχουν δεδομένα ή να έχουν τη δυνατότητα ελέγχου του περιβάλλοντος. Επίσης, σημαντικό παράγοντα παίζει η επικοινωνία των συσκευών και το αν αυτή θα γίνεται μεταξύ των συσκευών ή μέσω ενός κεντρικού κόμβου. Τα δίκτυα πλέγματος έχουν τα περισσότερα οφέλη σε σύγκριση με άλλους τύπους δικτύων, δεδομένου ότι δεν χαρακτηρίζονται από ιεραρχία και το hub και κάθε κόμβος συνδέονται με όσο το δυνατόν περισσότερους άλλους κόμβους. Οι πληροφορίες μπορούν να

δρομολογούνται πιο άμεσα και αποτελεσματικά, γεγονός που αποτρέπει τα προβλήματα επικοινωνίας. Αυτό καθιστά τα δίκτυα πλέγματος μια εξαιρετική λύση για τα συνδεδεμένα αντικείμενα [74].

Εκτός από τη τοπολογία του δικτύου, σημαντικό παράγοντα επιλογής των πρωτοκόλλων επικοινωνίας παίζει και ο αριθμός που θα μπορεί να υποστηρίξει το σύστημα IoT στην εκάστοτε εφαρμογή. Πολλές ασύρματες τεχνολογίες μπορούν να υποστηρίξουν έναν σχετικά μικρό αριθμό συσκευών στις παρυφές του δικτύου. Το Bluetooth είναι ένα πρωτόκολλο επικοινωνίας που βασίζεται στην αρχιτεκτονική master – slave, σύμφωνα με την οποία, στη συγκεκριμένη περίπτωση, κάθε master μπορεί να επικοινωνήσει με έως και 7 slave, σε σύνδεση σημείου με σημείο (point-to-point) είτε σημείου με πολλαπλά σημεία (point-to-multipoint). Το BLE επιτρέπει τη σύνδεση περισσότερων συσκευών, σχεδόν από 10 έως 20. Τα σημεία πρόσβασης Wi-Fi μπορούν να υποστηρίξουν γενικά 30 με 40 ενεργούς κινητούς χρήστες και υπό προϋποθέσεις έως και 4096 συνδέσεις. Οι σταθμοί βάσης έξι τομέων 4G/LTE παρέχουν κάλυψη σε 10 με 15 χιλιάδες συσκευές, αν και μπορεί να υποστηρίζουν μόνο έως 1000 ταυτόχρονες φωνητικές κλήσεις ή 50 με 100 χρήστες δεδομένων. Το Zigbee υποστηρίζει έως και 65.000 κόμβους [77].

3.3.4 Κατανάλωση ενέργειας

Η κατανάλωση ενέργειας αποτελεί ένα από τα σημαντικότερα κριτήρια επιλογής της τεχνολογίας επικοινωνίας σε ένα σύστημα IoT. Το μεγαλύτερο μέρος της ενέργειας μιας συσκευής IoT καταναλώνεται λόγω του πρωτοκόλλου επικοινωνίας. Πράγματι, τυχόν περιττά δεδομένα που μεταφέρονται, αποθηκεύονται και υποβάλλονται σε επεξεργασία φαίνεται να αποτελούν πιθανή σπατάλη ενέργειας. Ο σχεδιασμός ενός αλγόριθμου βελτιστοποίησης της κατανάλωσης ενέργειας σε ένα δίκτυο IoT δεν είναι ικανός να επιλύσει το συγκεκριμένο ζήτημα, αν ο αλγόριθμος αυτός δεν συνοδεύεται από αποτελεσματικά πρωτόκολλα επικοινωνίας. Το ευτύχημα είναι ότι υπάρχει μια τεράστια γκάμα διαφορετικών πρωτοκόλλων επικοινωνίας, τα οποία παρουσιάζουν διαφορές ως προς αυτό το θέμα. Τα πρωτόκολλα επικοινωνίας μπορούν να ταξινομηθούν με βάση την ενέργεια που

καταναλώνουν και διακρίνονται σε αυτά που επιτρέπουν τη μετάδοση μικρής ποσότητας δεδομένων σε μεγάλες αποστάσεις με χαμηλή κατανάλωση ενέργειας και σε εκείνα που μπορούν να μεταδίδουν μεγάλη ποσότητα δεδομένων σε μεγάλες αποστάσεις με υψηλή κατανάλωση [77].

Η επιλογή της βέλτιστης τεχνολογίας ασύρματης πρόσβασης επηρεάζει επίσης το κόστος κατασκευής μιας συσκευής καθώς και τη διάρκεια ζωής της ενσωματωμένης μπαταρίας της. Οι συσκευές που λειτουργούν με μπαταρία πρέπει να εξοικονομούν ενέργεια για ελαχιστοποίηση του κύκλου αντικατάστασης / επαναφόρτισης μπαταρίας. Κάτι τέτοιο όμως δημιουργεί περιορισμό όσον αφορά τον όγκο μετάδοσης των δεδομένων [78]. Η επιλογή της τεχνολογίας συγκομιδής ενέργειας που εστιάζει στη συλλογή ενέργειας από το περιβάλλον λειτουργίας του δικτύου και που μπορεί να προσφέρει οικονομικά αποδοτικές και πιο φιλικές προς το περιβάλλον λύσεις, θα μπορούσε να αποτελέσει μία ορθή επιλογή. Επειδή όμως η λύση αυτή βρίσκεται ακόμη σε σχετικά πρώιμο στάδιο και μπορεί να αποδειχθεί αρκετά ακριβή όσον αφορά την ενσωμάτωσή της στο σχεδιασμό των συσκευών IoT, η επιλογή της σωστής ασύρματης τεχνολογίας εξακολουθεί να αποτελεί σημαντικό παράγοντα [79].

3.3.5 Χρονική ευαισθησία

Η χρονική ευαισθησία (time sensitivity) των συλλεγόμενων δεδομένων αποτελεί ένα ακόμη πολύ σημαντικό κριτήριο επιλογής του πρωτοκόλλου επικοινωνίας ενός συστήματος IoT. Στις περιπτώσεις που είναι αναγκαία η ανταλλαγή πληροφοριών σε πραγματικό χρόνο, τότε διαφοροποιούνται οι επιθυμητές απαιτήσεις από την τεχνολογία, ακόμη και αν το μέγεθος της ποσότητας των μεταφερόμενων δεδομένων είναι μικρό. Εάν οι μεταδόσεις των δεδομένων είναι κρίσιμες για την αποδοτικότητα μιας εφαρμογής, όπως για παράδειγμα στην περίπτωση του ελέγχου μια βιομηχανικής διαδικασίας ή στην περίπτωση συνεχούς παρακολούθησης της κατάστασης της υγείας ενός ασθενούς, οι συσκευές απαιτείται να είναι συνδεδεμένες ανά πάσα στιγμή.

Άλλες περιπτώσεις χρήσης παρουσιάζουν λιγότερο αυστηρές απαιτήσεις χρονικής ευαισθησίας. Για παράδειγμα, ένας έξυπνος κάδος απορριμμάτων στέλνει μήνυμα αναφοράς

κατάστασης μόνο όταν γεμίσει, επομένως η επικοινωνία του είναι εφικτό να είναι απενεργοποιημένη την περισσότερη ώρα και να ενεργοποιηθεί μόνο για τη σύντομη μετάδοση της αναφοράς κατάστασής του. Αντίθετα, μια καφετιέρα αυτοεξυπηρέτησης σε μια καφετέρια μεγάλου πελατειακού όγκου μπορεί να χρειαστεί να αναφέρει ότι ξεμένει από υλικά αρκετές φορές μέσα στη μέρα. Από τα παραπάνω παραδείγματα προκύπτει το συμπέρασμα ότι η χρονική ευαισθησία είναι ένας παράγοντας που συνάδει με την κατανάλωση ενέργειας ενός συστήματος IoT και ότι στις περιπτώσεις που η μεταφορά δεδομένων δεν είναι απαραίτητο να γίνεται σε πραγματικό χρόνο, το μέγεθος των μεταφερόμενων δεδομένων καθίσταται λιγότερο σημαντικό ζήτημα, καθώς τα δεδομένα μπορεί να αποθηκεύονται και να προωθούνται περιοδικά ακόμη και με χαμηλό ρυθμό μετάδοσης.

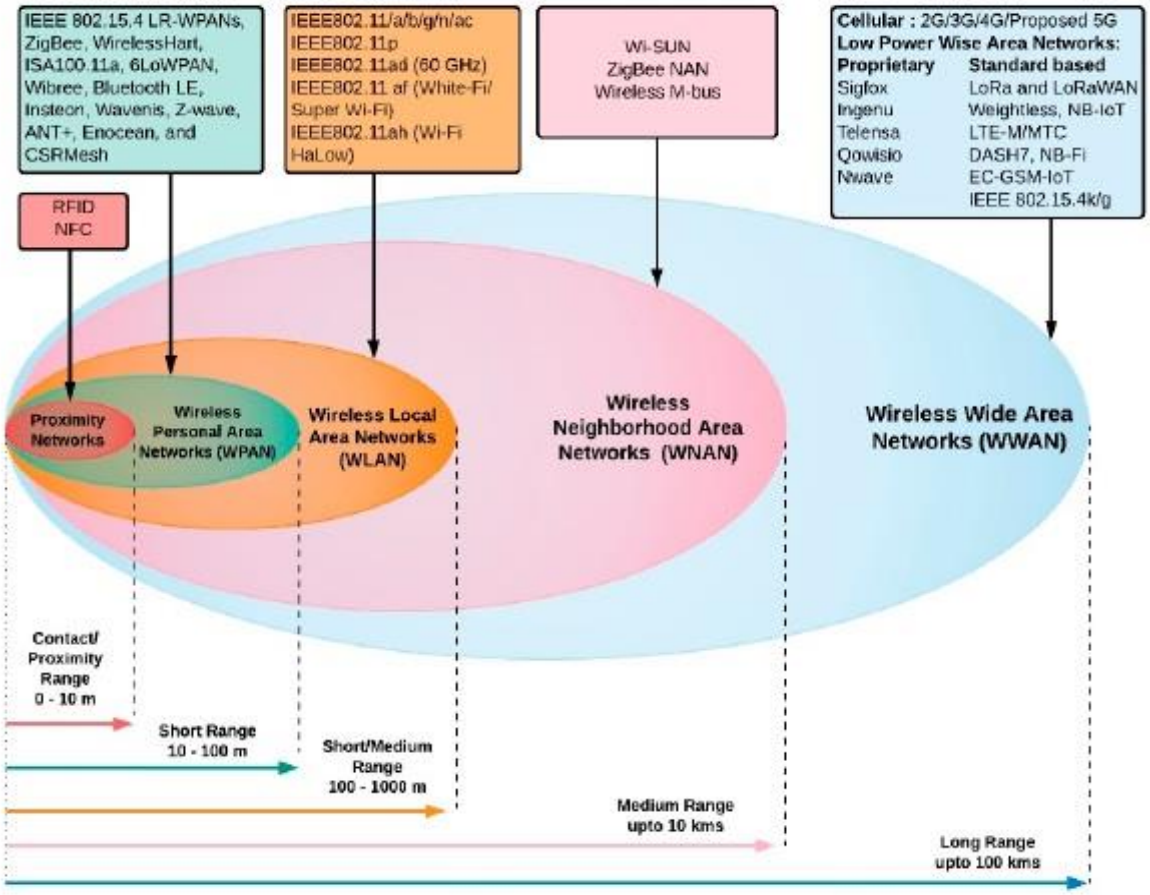
3.4 Τεχνολογίες και πρωτόκολλα επικοινωνίας IoT

Οι επικοινωνίες IoT περιλαμβάνουν πολλά πρωτόκολλα που εξυπηρετούν ένα συγκεκριμένο στρώμα της αρχιτεκτονικής δομής της τεχνολογίας. Η επικοινωνία των συσκευών IoT μπορεί να πραγματοποιείται σε παγκόσμιο ή τοπικό επίπεδο και για το λόγο αυτό, τα πρωτόκολλα επικοινωνίας θα πρέπει να υποστηρίζουν τις απαιτήσεις επικοινωνίας, ανεξάρτητα από το αν αυτές αφορούν την εντός και μεταξύ των συσκευών επικοινωνία (intra-device & inter-device communication) [57].

Εκτός από το πρωτόκολλο TCP και το UDP (User Datagram Protocol) στο μεσαίο στρώμα της αρχιτεκτονικής IoT, έχουν εμφανιστεί και ορισμένα άλλα πρωτόκολλα μεταφοράς που χρησιμοποιούνται σε πειραματικές φάσεις, όπως το QUIC (Quick UDP Internet Connections) και το NanoIP (Nano Internet Protocol) [71]. Το QUIC έχει σχεδιαστεί από την Google για να υποστηρίζει ένα σύνολο πολλαπλών συνδέσεων μεταξύ δύο τελικών σημείων πάνω από το UDP. Αυτό το πρωτόκολλο σχεδιάστηκε για να παρέχει προστασία ασφαλείας ισοδύναμη με αυτή του TLS/SSL, έλεγχο ροής ισοδύναμη με αυτόν του HTTP/2 και μείωση της καθυστέρησης σύνδεσης και μεταφοράς, καθώς και αποφυγή συμφόρησης, χρησιμοποιώντας μηχανισμό ελέγχου συμφόρησης ισοδύναμο με του TCP [80]. Το NanoIP είναι μια ιδέα που

βασίζεται σε δύο τεχνικές μεταφοράς: την nanoUDP για μη αξιόπιστη και απλή μεταφορά και την nanoTCP που παρέχει αναμεταδόσεις και έλεγχο ροής. Το NanoIP παρέχει μια εναλλακτική στοίβα δικτύου για έλεγχο, αυτοματισμό και δίκτυα αισθητήρων χωρίς την ύπαρξη κεφαλίδας TCP/IP [71].

Το IPv6 είναι ένας από τους βασικότερους παράγοντες διευθυνσιοδότησης των συσκευών IoT, καθώς οι διευθύνσεις που μπορεί να παρέχει πλέον το IPv4 τείνουν προς εξάντληση [81]. Πρόκειται για ένα πρωτόκολλο για δίκτυα μεταγωγής πακέτων που παρέχει μετάδοση δεδομένων από άκρο σε άκρο σε πολλά δίκτυα IP. Μια διεύθυνση IPv6 αποτελείται από δύο μέρη των 64 bit, που αποτελούν το πρόθεμα (prefix) και το αναγνωριστικό διεπαφής (interface identifier). Το πρόθεμα λαμβάνεται από τις πύλες για τον προσδιορισμό του δικτύου στο οποίο ανήκει η διεύθυνση και το αναγνωριστικό διεπαφής χρησιμοποιείται για την αναγνώριση της συσκευής η διεύθυνση της οποίας ανήκει στο δίκτυο. Επομένως, εκτός από τη περίπτωση που το πρόθεμα δεν χρησιμοποιείται ως διεύθυνση τοπικής σύνδεσης, η διεύθυνση IPv6 128-bit αποτελεί παγκόσμια μοναδική τιμή αναγνώρισης κάθε συσκευής [82].



Εικόνα 3-7: Ασύρματες τεχνολογίες επικοινωνίας IoT [71]

Το πλείστο των υπηρεσιών και εφαρμογών IoT βασίζονται στη χρήση ασύρματων τεχνολογιών επικοινωνίας, πληρώντας με τον τρόπο αυτό τις απαιτήσεις διαθεσιμότητας και κινητικότητας. Το θέμα της παρουσίασης, ανάλυσης και ταξινόμησης των τεχνολογιών και πρωτοκόλλων επικοινωνίας στο πλαίσιο του IoT είναι αρκετά δημοφιλές. Μια τέτοια ταξινόμηση μπορεί να γίνει με βάση πολλές παραμέτρους, όπως το εύρος κάλυψης, η τοπολογία του δικτύου, η ταχύτητα μεταφοράς δεδομένων, η συχνότητα λειτουργίας και το εύρος ζώνης. Στο πλαίσιο της παρούσας εργασίας η συγκεκριμένη ταξινόμηση θα ακολουθήσει την προσέγγιση των Aman και συν. (2020) και θα γίνει με βάση το εύρος κάλυψης των δικτύων IoT [57]. Βάσει αυτής της ταξινόμησης, οι τεχνολογίες επικοινωνίας IoT μπορούν να χωριστούν σε δύο μεγάλες κατηγορίες: (α) του μικρού εύρους κάλυψης

(short range) και (β) του μεγάλου εύρους κάλυψης (long range). Στην εικόνα 3-7 παρουσιάζεται μια τέτοια κατηγοριοποίηση των ασύρματων τεχνολογιών επικοινωνίας του IoT [71].

3.4.1 Τεχνολογίες επικοινωνίας IoT μικρού εύρους κάλυψης

Στην κατηγορία αυτή περιλαμβάνονται οι τεχνολογίες και τα πρωτόκολλα που καλύπτουν τα δίκτυα BAN, PAN και LAN. Κάποια βασικά στοιχεία των τεχνολογιών αυτών παρουσιάζονται στον πίνακα 3-2.

Πίνακας 3-2: Βασικά στοιχεία ασύρματων τεχνολογιών IoT μικρού εύρους κάλυψης

Είδος δικτύου IoT	Τεχνολογία	Ρυθμός μετάδοσης δεδομένων	Εύρος κάλυψης (εσωτ./εξωτ. χώρων)	Συχνότητα λειτουργίας	Τοπολογία δικτύου
BAN	NFC	424Kbps	0-4cm	13,56MHz	P2P
BAN	RFID	640Kbps	10cm - 1m	13,56MHz	P2P
PAN	BLE	1Mbps	10m / 50m	2,4GHz	Αστέρα
PAN	Bluetooth 5	2Mbps	40m / 200m	2.4GHz	Αστέρα
PAN	ZigBee	250Kbps	10-100m	2,4GHz	Αστέρα, πλέγματος, δέντρου
PAN	Z-Wave	100Kbps	100m	868/915MHz	Πλέγματος
PAN	6LowPAN	40 – 250Kbps	10-100m	868/921MHz	Αστέρα, πλέγματος, P2P
LAN	Wi-Fi	11Mbps	30m / 150m	2,4GHz ή 5GHz	Αστέρα, πλέγματος, P2P
LAN	HaLow Wi-Fi	350Mbps	140m / 500m	900MHz	Αστέρα

Οι τεχνολογίες RFID και NFC έπαιξαν καθοριστικό ρόλο στην υλοποίηση και εξέλιξη του IoT [82]. Το RFID είναι μια τεχνολογία επικοινωνίας μικρής εμβέλειας, στην οποία η αυτόματη αναγνώριση και συνεχής παρακολούθηση των ετικετών (tags) που έχουν προσαρτηθεί στα αντικείμενα πραγματοποιείται μέσω χρήσης ηλεκτρομαγνητικού πεδίου. Η

τεχνολογία χρησιμοποιεί ζώνες ISM (Industrial, Scientific and Medical) κάτω του 1GHz, σχεδιασμένες ειδικά έτσι ώστε ακόμα και συσκευές χωρίς μπαταρίες να μπορούν να στέλνουν σήμα. Τα συστήματα RFID δεν πρέπει να παρεμβάλλονται σε άλλα συστήματα, όπως υπηρεσίες έκτακτης ανάγκης ραδιοφώνου ή ραδιοτηλεοπτικούς σταθμούς τηλεοπτικών σημάτων κ.λπ. Η ενσωμάτωση των τεχνολογιών αισθητήρων και του RFID έδωσε πολλές νέες δυνατότητες στο πρότυπο IoT, ενώ παράλληλα ενίσχυσε πολλά παθητικά συστήματα με δυνατότητες ανίχνευσης, υπολογισμού και συνδεσιμότητας. Ένα από τα οφέλη της τεχνολογίας RFID αφορά τη δυνατότητα συνεχούς παρακολούθησης των ετικετών, καθιστώντας με τον τρόπο αυτό τα δεδομένα τους προσβάσιμα μέσω του Διαδικτύου [83].

Το NFC βασίζεται στο πρότυπο ISO/IEC 18092: 2004 και στην τεχνολογία RFID για να μπορέσει να υποστηρίξει επικοινωνίες μικρής εμβέλειας. Λειτουργεί στα 13,56MHz και έχει σχεδιαστεί για την ανταλλαγή δεδομένων με άλλες συσκευές NFC, επιτρέποντας αμφίδρομες επικοινωνίες. Κάθε ετικέτα NFC έχει μία μοναδική ταυτότητα αναγνώρισης. Όταν έχει συνδεσιμότητα στο Διαδίκτυο υπάρχει η δυνατότητα ανταλλαγής δεδομένων με διαδικτυακές υπηρεσίες για την επέκταση των πλεονεκτημάτων της. Ο χαμηλός ρυθμός μετάδοσης δεδομένων και η μικρή απόσταση επικοινωνίας το καθιστούν κατάλληλο μόνο για εξειδικευμένες εφαρμογές IoT [84].

Το Bluetooth (IEEE 802.15.1) λειτουργεί στη ζώνη συχνοτήτων ISM (2,4 - 2,4835GHz) και αποτελεί μία από τις πιο χρησιμοποιούμενες τεχνολογίες επικοινωνίας σε εφαρμογές IoT μικρής εμβέλειας. Επειδή το Wi-Fi είναι μια τεχνολογία που λειτουργεί στην ίδια ζώνη συχνοτήτων με το Bluetooth, αλλά παρουσιάζει συγκριτικά πολύ μεγαλύτερες ταχύτητες μεταφοράς δεδομένων, ο οργανισμός τυποποίησης Bluetooth Special Interest Group (SIG) στράφηκε προς το στοιχείο της κατανάλωσης ενέργειας με σκοπό τη δημιουργία μιας νέας τεχνολογίας που να παρουσιάζει δυνατότητα συλλογής και συγκέντρωσης δεδομένων από συσκευές (αισθητήρες) που παράγουν δεδομένα με πολύ χαμηλό ρυθμό και καταναλώνουν ελάχιστα ποσά ενέργειας [85]. Έτσι, προτάθηκε το BLE, στην προδιαγραφή Bluetooth 4.0, το οποίο έχει σχεδιαστεί για εφαρμογές μικρής εμβέλειας (έως 50 m) κάτι που το καθιστά κατάλληλο για εφαρμογές ελέγχου και συνεχούς παρακολούθησης. Το BLE είναι επίσης

γνωστό για την ικανότητά του πραγματοποιεί επικοινωνίες μικρής εμβέλειας με χαμηλή κατανάλωση ενέργειας. Η νέα έκδοσή του, το Bluetooth 5, εστιάζει στη βελτίωση της ταχύτητας, της εμβέλειας, της ασφάλειας, της ενεργειακής απόδοσης, των λειτουργιών βάσει τοποθεσίας, της διαλειτουργικότητας και της συνύπαρξης με άλλες τεχνολογίες. Το Bluetooth 5 χρησιμοποιεί λιγότερη ισχύ, υποστηρίζει δίκτυα τοπολογίας πλέγματος και δίκτυα συσκευών μεγάλης κλίμακας και επιτρέπει την πραγματοποίηση επικοινωνίας πολλών συσκευών με πολλές συσκευές (many-to-may). Το Bluetooth 5 πληροί τις απαιτήσεις των νεότερων συσκευών IoT, παρουσιάζοντας μεγαλύτερη εμβέλεια, αυξημένη ταχύτητα έως 2Mbps και δυνατότητα λειτουργίας μεγάλης εμβέλειας με υψηλότερη ευαισθησία σε χαμηλότερους ρυθμούς μετάδοσης δεδομένων [86]. Όλες αυτές οι σημαντικές εξελίξεις στην συγκεκριμένη τεχνολογία μπορούν να την καταστήσουν βασικό παράγοντα υποστήριξης των εφαρμογών IoT.

Το ZigBee είναι ένα ακόμα από τα πρότυπα επικοινωνίας IoT που μπορούν να χρησιμοποιηθούν σε δίκτυα PAN. Έχοντας ως βάση το πρότυπο IEEE 802.15.4 και με κύρια εφαρμογή του τον τομέα των ασύρματων δικτύων αισθητήρων (WSN) σε συστήματα έξυπνης παροχής ενέργειας και οικιακού αυτοματισμού (έξυπνο σπίτι), το ZigBee μπορεί να χρησιμοποιηθεί και σε διάφορους άλλους τομείς, όπως σε έξυπνες πόλεις, γεωργία, έξυπνα συστήματα μεταφοράς και υγειονομική περίθαλψη. Το ZigBee λειτουργεί κυρίως στα 2,4GHz, αλλά υποστηρίζει επίσης τις ζώνες ISM των 868MHz και 916MHz [87].

Μια άλλη λύση δικτύων PAN αποτελεί το Z-Wave, ένα πρωτόκολλο δικτύου πλέγματος που λειτουργεί στην μπάντα κάτω του 1GHz. Χρησιμοποιείται συχνά για συστήματα ασφαλείας, οικιακούς αυτοματισμούς και έλεγχο φωτισμού. Παρόμοια με το Zigbee, το Z-Wave είναι μια τεχνολογία χαμηλής ισχύος που έχει ως βάση το πρότυπο IEEE 802.15.4 και μεταφέρει μικρές ποσότητες δεδομένων σε μικρές και μεσαίες αποστάσεις. Το Z-wave χρησιμοποιεί ένα proprietary ραδιοσύστημα και διαθέτει αυστηρά ελεγχόμενο οικοσύστημα προϊόντων που μπορούν να χρησιμοποιηθούν σε εφαρμογές έξυπνων σπιτιών, σε αντίθεση με τις συσκευές Zigbee που μπορούν να βρουν χρήση σε ποικιλία εφαρμογών και δεν είναι πλήρως διαλειτουργικές [88].

Μετά τις απαιτήσεις της αγοράς για άμεση συνδεσιμότητα που να βασίζεται στο πρωτόκολλο IP, έχουν αναπτυχθεί νέα πρότυπα ασύρματης δικτύωσης πλέγματος, όπως το 6LoWPAN. Το 6LoWPAN είναι ένα ελαφρύ και ανοικτό πρωτόκολλο επικοινωνίας δικτύων IoT. Βασίζεται στο πρωτόκολλο IP και αποτελείται από πολλά πρωτόκολλα όπως τα UDP, IPv6, IEEE 802.15.4, ICMP και RPL, ο συνδυασμός των οποίων επιτρέπει τον έλεγχο σε συστήματα οικιακού και κτιριακού αυτοματισμού. Το 6LoWPAN παρέχει ασύρματη σύνδεση μεταξύ των στοιχείων των συστημάτων αυτών, επιτρέποντας την πραγματοποίηση διάφορων διαδικασιών, όπως έξυπνη μέτρηση, έξυπνη διαχείριση και συνεχή παρακολούθηση [89]. Σε αντίθεση με τις υπόλοιπες ασύρματες τεχνολογίες των δικτύων PAN που απαιτούν την ύπαρξη πύλης στρώματος εφαρμογών που εκτελεί τη στοίβα των στρωμάτων TCP/IP μέσω Ethernet ή WiFi, οι λύσεις που βασίζονται στο 6LoWPAN χρησιμοποιούν έναν δρομολογητή παρυφών (edge router) που προωθεί πακέτα μόνο στο στρώμα δικτύου και δεν εφαρμόζεται στο στρώμα εφαρμογών, επιτρέποντας γεφύρωση χαμηλού κόστους με άλλα δίκτυα IP [77].

Το IEEE 802.11 είναι ένα σύνολο προδιαγραφών MAC και PHY για δίκτυα LAN, γνωστό ως Wi-Fi. Τα δίκτυα Wi-Fi χρησιμοποιούν τα σημεία πρόσβασης (access points) ως Διαδικτυακή πύλη και παρουσιάζουν καλή κάλυψη εντός κτιρίων. Μέχρι σχετικά πρόσφατα, η ενσωμάτωση συνδεσιμότητας Wi-Fi σε συσκευές με χαμηλή υπολογιστική απόδοση ήταν αρκετά δαπανηρή, λόγω του μεγέθους και της πολυπλοκότητας του λογισμικού Wi-Fi και της υψηλής κατανάλωσης ενέργειας που το καθιστούσαν ακατάλληλο για χρήση σε συσκευές με μπαταρία, σε σύγκριση με τα πρωτόκολλα Bluetooth και Zigbee [90]. Το ζήτημα αυτό του Wi-Fi αντιμετωπίστηκε μέσω βελτιώσεων, οι οποίες μπορούν να ενισχύσουν την τεχνολογία και σε άλλα ζητήματα, όπως η κινητικότητα, η περιαγωγή και η απόδοση QoS. Οι σύγχρονες συσκευές υποστηρίζουν το λογισμικό Wi-Fi και παρουσιάζουν μειωμένη κατανάλωση ενέργειας. Η κατανάλωση ενέργειας αυτών των συσκευών μπορεί να μειωθεί περαιτέρω με περιοδική ενεργοποίηση του πρωτοκόλλου μόνο για σύντομα χρονικά διαστήματα, επιτρέποντάς τους να λειτουργούν για περισσότερο από ένα χρόνο με δύο μπαταρίες AA [83].

Πολλά διαφορετικά πρωτόκολλα Wi-Fi είναι διαθέσιμα και λειτουργούν στα 2,4GHz ή στα 5GHz. Για παράδειγμα, τα IEEE 802.11n και IEEE 802.11ac είναι τα πιο ευρέως

χρησιμοποιούμενα πρωτόκολλα, αλλά τα τελευταία χρόνια έχουν αναπτυχθεί διαφορετικές εκδόσεις στη προσπάθεια της IEEE για βελτίωση της τεχνολογίας Wi-Fi. Μια από αυτές τις προσπάθειες αφορά τη δημιουργία του IEEE 802.11ah, γνωστού και ως Wi-Fi χαμηλής ισχύος (Wi-Fi HaLow), που έχει σχεδιαστεί για συσκευές χαμηλού ρυθμού μεταφοράς δεδομένων και δίκτυα μεγάλης εμβέλειας [91]. Λειτουργεί στη ζώνη ISM σε συχνότητα κάτω του 1GHz και εφαρμόζει τεχνικές εξοικονόμησης ενέργειας, όπως ο χρόνος αφύπνισης στόχου (target wake time) που ξυπνά τη συσκευή σε καθορισμένα διαστήματα για πολύ μικρό χρονικό διάστημα. Με τον τρόπο αυτό, μπορεί να υποστηρίξει ένα ευρύ φάσμα εφαρμογών IoT, ενώ παράλληλα μπορεί να παρουσιάσει μεγαλύτερη ενεργειακή απόδοση, ποιότητα QoS (Quality of Service), επεκτασιμότητα (υποστηρίζοντας μεγαλύτερο αριθμό συσκευών) και οικονομικά αποδεκτές λύσεις [92].

3.4.2 Τεχνολογίες επικοινωνίας IoT μεγάλου εύρους κάλυψης

Στην κατηγορία αυτή περιλαμβάνονται οι τεχνολογίες και τα πρωτόκολλα που καλύπτουν τα δίκτυα MAN και WAN. Κάποια βασικά στοιχεία των τεχνολογιών αυτών παρουσιάζονται στον πίνακα 3-3.

Το LoRa (Long Range) είναι μια τεχνολογία ευρείας περιοχής χαμηλής ισχύος (Low Power Wide Area Network - LPWAN) [93]. Βασίζεται σε τεχνικές διαμόρφωσης ραδιοφάσματος και είναι ανοιχτό, δηλαδή η χρήση του είναι δωρεάν, χωρίς συνδρομές και χωρίς περιορισμούς στην εγκατάσταση πυλών και διακομιστών δικτύου. Η χρήση του σε εφαρμογές IoT μπορεί να γίνει κάτω από ορισμένες προϋποθέσεις [94]. Για παράδειγμα, η εφαρμογή του συνδυασμού μηχανικής εκμάθησης με το LoRa ως πρωτόκολλο μετάδοσης χαμηλής ισχύος, επιτρέπει τη μείωση του όγκου των μεταδιδόμενων δεδομένων και την επέκταση της διάρκειας ζωής της μπαταρίας των συσκευών IoT [95]. Στις σύγχρονες εφαρμογές IoT, η πιο κοινή στρατηγική επεξεργασίας των δεδομένων είναι η χρήση του cloud, αλλά η μετάδοση μεγάλων ποσοτήτων δεδομένων απαιτεί συχνή επαναφόρτιση των συσκευών, καταργώντας έτσι ένα από τα μεγάλα πλεονεκτήματα του IoT. Επιπλέον, οι εφαρμογές IoT απαιτούν μετάδοση δεδομένων σε μεγάλες αποστάσεις, όπως για παράδειγμα σε εφαρμογές συνεχούς

παρακολούθησης της κυκλοφορίας. Οι συσκευές IoT πρέπει, συνεπώς, να παρουσιάζουν χαμηλή κατανάλωση ενέργειας σε συνδυασμό με όσο το δυνατόν μεγαλύτερο εύρος μετάδοσης. Υπό αυτές τις συνθήκες, η αποτελεσματική χρήση της μείωσης δεδομένων και της τοπικής επεξεργασίας πρέπει να συνδυαστεί με πρωτόκολλα μετάδοσης μεγάλου εύρους κάλυψης και μικρού εύρους ζώνης, στοιχεία που παρουσιάζει το LoRa [96].

Πίνακας 3-3: Βασικά στοιχεία ασύρματων τεχνολογιών IoT μεγάλου εύρους κάλυψης

Είδος δικτύου IoT	Τεχνολογία	Ρυθμός μετάδοσης δεδομένων	Εύρος κάλυψης (εσωτ./εξωτ. χώρων)	Συχνότητα λειτουργίας	Τοπολογία δικτύου
LPWAN	LoRa	0,3 - 50Kbps	5 – 10Km	868/915MHz	Αστέρα, πλέγματος
LPWAN	SigFox	100 - 600bps	30 – 50Km	868/902MHz	Αστέρα
Κυψελοειδές	NB-IoT	200Kbps	280m / 1Km	800/900/1800MHz	Αστέρα
Κυψελοειδές	LTE-M1	1Mbps	5 – 100Km	1,08MHz	Αστέρα σε αστέρα
Κυψελοειδές	4G/LTE	150Mbps	15Km	850/1700/1900 /2100MHz	Αστέρα σε αστέρα
Κυψελοειδές	5G	10 – 50Gbps	2Km	600MHz/2,5/28 /39GHz	Αστέρα σε αστέρα

Το SigFox αποτελεί μια ακόμα τεχνολογία LPWAN, που σε αντίθεση με το LoRa είναι proprietary. Λειτουργεί στην μπάντα κάτω του 1GHz και είναι σε θέση να υποστηρίξει την εφαρμογή συσκευών που διατίθενται από διαφορετικούς κατασκευαστές. Ωστόσο, απαιτεί τη χρήση εξελιγμένων και ακριβών πυλών και σημείων πρόσβασης. Όπως και το LoRa, παρουσιάζει πολύ μεγάλο εύρος κάλυψης και πολύ χαμηλή κατανάλωση ισχύος. Τα συγκεκριμένα χαρακτηριστικά του επιτυγχάνονται χρησιμοποιώντας ασύρματη μετάδοσης πολύ χαμηλής ταχύτητας δεδομένων (Ultra Narrowband - UNB) [97].

Το LTE, κοινώς γνωστό ως “4G LTE”, είναι ένα πρότυπο για ασύρματη ευρυζωνική επικοινωνία, που βασίζεται στις τεχνολογίες GSM/EDGE και UMTS/HSPA [98]. Μετά την εισαγωγή του και όσον αφορά την υλοποίηση των εφαρμογών IoT, άρχισε να ανταγωνίζεται αναδυόμενες τεχνολογίες, όπως το BLE, το IoT στενής ζώνης (Narrow Band IoT - NB-IoT),

το ZigBee και το LoRa. Παρά το γεγονός ότι το 4G έχει βελτιώσει τις δυνατότητες των κυψελοειδών δικτύων, δεν μπορεί να θεωρηθεί ως βέλτιστη τεχνολογία για εφαρμογές IoT [99].

Το NB-IoT δημιουργήθηκε με σκοπό την παροχή κυψελοειδούς συνδεσιμότητα ευρείας ζώνης χαμηλού κόστους και χαμηλής ισχύος ειδικά για το IoT [100]. Πρόκειται για μια τεχνολογία LPWA που αναπτύχθηκε με σκοπό τη βελτίωση της κατανάλωσης ενέργειας των συσκευών, της αύξησης της χωρητικότητας του συστήματος και τη βέλτιστη χρήση του φάσματος, ιδιαίτερα σε εφαρμογές εξαιρετικά μεγάλου εύρους κάλυψης. Η τεχνολογία δημιουργήθηκε από υπάρχουσες λειτουργίες του LTE με ουσιαστικές απλοποιήσεις και βελτιστοποιήσεις [101]. Στο φυσικό στρώμα, καταλαμβάνει φάσμα 180kHz, το οποίο είναι ουσιαστικά μικρότερο από το εύρος ζώνης των 1,4 - 20MHz του LTE. Στα υψηλότερα στρώματα υποστηρίζονται απλοποιημένες λειτουργίες δικτύου LTE. Σε σύγκριση με άλλες λύσεις LPWAN, το NB-IoT έχει το μεγάλο πλεονέκτημα ότι μπορεί να εξαλείψει την ανάγκη για χρήση συγκεκριμένων πυλών, οπότε τα δεδομένα των αισθητήρων αποστέλλονται απευθείας στους διακομιστές cloud, μειώνοντας με τον τρόπο αυτό το κόστος υποδομής.

Το LTE Cat-M1 είναι επίσης μια τεχνολογία LPWAN που επιτρέπει την παροχή κυψελοειδών υπηρεσιών σε εφαρμογές IoT [102]. Σε σύγκριση με το NB-IoT, αυτή η τεχνολογία παρέχει υψηλότερο ρυθμό μεταφοράς δεδομένων και δυνατότητα χρήσης φωνής μέσω του δικτύου (voice over network), αλλά απαιτεί περισσότερο εύρος ζώνης και, επομένως, οι συσκευές που τη χρησιμοποιούν είναι πιο περίπλοκες και ακριβές. Τα NB-IoT και Cat-M1 έχουν διαφορετικές και κάπως συμπληρωματικές εφαρμογές, με τις εφαρμογές του πρώτου να είναι κατάλληλες για μικρούς αισθητήρες και μετρητές και του δεύτερου για συσκευές που απαιτούν υψηλότερους ρυθμούς μετάδοσης δεδομένων και διαθέτουν περισσότερους πόρους ισχύος.

Σκοπός του 5G, της πέμπτης γενιάς ασύρματων δικτύων κινητής τηλεφωνίας, είναι η επίλυση των ζητημάτων που παρουσιάζει το 4G. Παρόλο που δεν δημιουργήθηκε αποκλειστικά για το IoT, αναμένεται να αποτελέσει τον κύριο μοχλό ανάπτυξής του. Το 5G IoT είναι ένα

πρωτοποριακό, έξυπνο δίκτυο που βασίζεται στην επικοινωνία 5G, η οποία έχει σχεδιαστεί για τη σύνδεση των περιοχών ανίχνευσης (αισθητήρες) με τα κέντρα επεξεργασίας (cloud), χρησιμοποιώντας αλγόριθμους AI [103]. Το δίκτυο 5G IoT εκμεταλλεύεται διάφορες αναδυόμενες τεχνολογίες, όπως τα μαζικά δίκτυα πολλαπλών εισόδων πολλαπλών εξόδων (Multiple Input Multiple Output - MIMO) και τα πυκνά στατικά και κινητά δίκτυα μικρών κυψελών.

Το 5G είναι ικανό να ικανοποιεί ανάγκες του IoT, όπως [104]:

- υψηλές ταχύτητες μετάδοσης δεδομένων
- αύξηση της επεκτασιμότητας του δικτύου
- πολύ μικρός λανθάνων χρόνος (μικρή καθυστέρηση)
- βελτιστοποίηση της χωρητικότητας των μπαταριών των συσκευών, χαρακτηριστικό που μπορεί να επεκτείνει τη διάρκεια ζωής τους και επομένως να συμβάλει στην υποστήριξη των συσκευών χαμηλής ισχύος που μπορούν να χρησιμοποιηθούν σε εφαρμογές IoT

Μειώνοντας τον λανθάνοντα χρόνο στις επικοινωνίες, το 5G εξαλείφει μέρος της συμφόρησης που σχετίζεται με την απομακρυσμένη εκτέλεση αλγορίθμων μηχανικής μάθησης [105].

3.5 Πρωτόκολλα ανωτέρου στρώματος

Τα πρωτόκολλα του στρώματος εφαρμογών που χρησιμοποιούνται στις παραδοσιακές υπηρεσίες Διαδικτύου δεν μπορούν να αποτελέσουν αντίστοιχη επιλογή για το IoT, λόγω των περιορισμών των δικτύων LLN. Εξαιτίας αυτού, έχουν δημιουργηθεί πρωτόκολλα ανταλλαγής μηνυμάτων για να υποστηρίξουν τη χρήση του IoT και να διευκολύνουν τη χρήση του. Βασικός σκοπός των μηνυμάτων είναι η διασφάλιση της σύνδεσης μεταξύ των συσκευών [106]. Με βάση τα όσα αναφέρθηκαν σε προηγούμενη ενότητα, τα συγκεκριμένα πρωτόκολλα μπορούν να υλοποιηθούν στο ανώτερο στρώμα της αρχιτεκτονικής δομής του

IoT, δηλαδή στα στρώματα εφαρμογών, επιχειρήσεων, διεπαφής, υποστήριξης και υπηρεσιών / δεδομένων.

Τα πιο συχνά χρησιμοποιούμενα πρωτόκολλα μηνυμάτων του ανώτερου στρώματος είναι τα εξής [107]:

- το πρωτόκολλο περιορισμένης εφαρμογής (Constrained Application Protocol - CoAP)
- το πρωτόκολλο μεταφοράς τηλεμετρίας ουράς μηνυμάτων (Message Queuing Telemetry Transport - MQTT)
- το προηγμένο πρωτόκολλο ουράς μηνυμάτων (Advanced Message Queuing Protocol - AMQP)
- το επεκτάσιμο πρωτόκολλο μηνυμάτων και παρουσίας (Extensible Messaging and Presence Protocol - XMPP) και
- η υπηρεσία διανομής δεδομένων (Data Distribution Service - DDS)

Στον πίνακα 3-4 περιλαμβάνονται κάποιες βασικές πληροφορίες σχετικά με τα πρωτόκολλα αυτά.

Πίνακας 3-4: Σύγκριση δημοφιλών πρωτοκόλλων μηνυμάτων IoT

Πρωτόκολλο	Πρότυπο	Υποστήριξη REST	Πρωτόκολλο μεταφοράς	Ασφάλεια	Υποστήριξη QoS
CoaP	IETF RFC 7252	✓	UDP	DTLS	✓
MQTT	OASIS Standard	–	TCP	TLS/SSL	✓
XMPP	IETF RFC 6120,6121	–	TCP	TLS/SSL	–
AMQP	ISO & IEC	–	TCP	TLS/SSL	✓
DDS	OMG (Object Management Group)	–	UDP	DTLS	✓

I) CoAP

Το CoAP είναι ένα πρωτόκολλο του στρώματος εφαρμογών της αρχιτεκτονικής του IoT, που δημιουργήθηκε από τον οργανισμό IETF (Internet Engineer Task Force), και είναι σε θέση να

επεκτείνει την αρχιτεκτονική REST (REpresentational State Transfer) στα δίκτυα LoWPAN [108]. Έχοντας ως προεπιλεγμένο πρωτόκολλο μεταφοράς το UDP, και όχι το TCP, καθίσταται καταλληλότερο για εφαρμογές IoT [109]. Καθώς λειτουργεί πάνω από το UDP, παρέχει αξιοπιστία από άκρο σε άκρο και πρωταρχικό έλεγχο για περιπτώσεις συμφόρησης. Επιπλέον, το CoAP τροποποιεί ορισμένες από τις λειτουργίες του HTTP για να ανταποκριθεί σε συγκεκριμένες απαιτήσεις του IoT, όπως η μικρή κατανάλωση ενέργειας και η λειτουργία σε περιπτώσεις απώλειας ζεύξης ή ζεύξης με μεγάλο θόρυβο. Επίσης, παρέχει αξιοπιστία μέσω του μηχανισμού αναμετάδοσης χρονικού ορίου [110].

Το CoAP μπορεί να χωριστεί σε δύο υπο-επίπεδα: το υπο-επίπεδο ανταλλαγής μηνυμάτων και το υπο-επίπεδο αιτήματος / απόκρισης. Το υπο-επίπεδο ανταλλαγής μηνυμάτων ανιχνεύει την ύπαρξη διπλών μηνυμάτων και παρέχει αξιόπιστη επικοινωνία μέσω του στρώματος μεταφοράς UDP χρησιμοποιώντας εκθετικό backoff. Το υπο-επίπεδο αιτήματος / απόκρισης χειρίζεται τις επικοινωνίες REST [111].

Λειτουργώντας στο στρώμα εφαρμογών, το CoAP είναι υπεύθυνο για τη μορφοποίηση των μηνυμάτων χειραψίας που ανταλλάσσουν οι συσκευές πριν τη σύνδεσή τους [112]. Οι τύποι μηνυμάτων που υποστηρίζονται είναι τέσσερις [113]: τα μηνύματα που απαιτούν επιβεβαίωση (confirmable message), τα μηνύματα που δεν απαιτούν επιβεβαίωση (non-confirmable message), τα μηνύματα επιβεβαίωσης (acknowledgement message) και το μήνυμα επαναφοράς (reset message). Συνολικά, το CoAP λειτουργεί ακολουθώντας την προσέγγιση αιτήματος / απόκρισης.

II) MQTT

Το MQTT είναι ένα ελαφρύ πρωτόκολλο για επικοινωνία και συνδεσιμότητα μεταξύ μηχανών (Machine-to-Machine - M2M) και συσκευών IoT, το οποίο εστιάζει στη συλλογή δεδομένων [114]. Όπως υποδηλώνει το όνομά του, το MQTT έχει σχεδιαστεί για να υποστηρίζει την τηλεμετρία (δηλαδή απομακρυσμένη παρακολούθηση) συλλέγοντας δεδομένα από απομακρυσμένες συσκευές και μεταφέροντας μηνύματα στην υποδομή του διακομιστή [115]. Το MQTT στο IoT λειτουργεί όπως το πρωτόκολλο HTPP στο Διαδίκτυο,

χρησιμοποιώντας κεντρική αρχιτεκτονική πελάτη-διακομιστή. Όλες οι συσκευές πρέπει να είναι συνδεδεμένες στην υποδομή του διακομιστή, ενώ το πρωτόκολλο εκτελείται πάνω από το TCP. Αυτό το είδος αρχιτεκτονικής εγγυάται τη μη απώλεια δεδομένων, καθώς και απλή και αξιόπιστη ροή δεδομένων. Η απλότητα του πρωτοκόλλου δεν προσφέρει πολλές επιλογές ελέγχου.

Κύριος στόχος του είναι η σύνδεση συσκευών και δικτύων σε εφαρμογές. Ορισμένες από τις εφαρμογές του IoT που το χρησιμοποιούν αφορούν τη συνεχή παρακολούθηση διεργασιών στον βιομηχανικό τομέα, την ιατρική παρακολούθηση, την παρακολούθηση της ενεργειακής κατανάλωσης, τον οικιακό αυτοματισμό, τον έλεγχο φωτισμού κλπ. Όλες αυτές οι εφαρμογές εκμεταλλεύονται το μικρό μέγεθος των πακέτων δεδομένων και την αποτελεσματική διανομή τους σε μία ή περισσότερες συσκευές. Στα πλεονεκτήματά του περιλαμβάνεται επίσης, η ικανότητά του να διασφαλίζει τη δρομολόγηση σε περιπτώσεις χρήσης συσκευών μικρής μνήμης και χαμηλής κατανάλωσης ενέργειας, σε ευαίσθητα και χαμηλού εύρους ζώνης δίκτυα [116].

III) XMPP

Το XMPP είναι ένα πρωτόκολλο επικοινωνίας που έχει ως βάση τη γλώσσα σήμανσης XML (eXtensible Markup Language) και χρησιμοποιείται κυρίως για την ανταλλαγή άμεσων μηνυμάτων (Instant Messaging - IM), υιοθετώντας τη φιλοσοφία της επικοινωνίας των ατόμων μέσω μηνυμάτων κειμένου [117]. Για τους σκοπούς του IoT, το πρωτόκολλο αναπτύχθηκε μέσω μιας σειράς επεκτάσεων που επιτρέπουν την επικοινωνία μεταξύ αισθητήρων και ενεργοποιητών IoT. Το XMPP επικεντρώνεται στην υποστήριξη αποστολής και λήψης μηνυμάτων μεταξύ κατανεμημένων συστημάτων (δηλαδή μεσαίου λογισμικού προσανατολισμένου σε μηνύματα) και εφαρμογών, βασιζόμενο στο πρωτόκολλο άμεσων μηνυμάτων σε πραγματικό χρόνο και πληροφοριών παρουσίας (Instant Messaging/Presence Protocol – IMPP) του IETF που χρησιμοποιείται για συνομιλία πολλών μερών, φωνητικές κλήσεις και βιντεοκλήσεις [118].

Το XMPP, όπως συμβαίνει και με το MQTT, λειτουργεί μέσω TCP ή, περιστασιακά, μέσω HTTP στην κορυφή του TCP. Τα κύρια χαρακτηριστικά του, όπως ο ισχυρός έλεγχος ταυτότητας και η ασφάλεια, η επεκτασιμότητα και το σχήμα διευθύνσεων ονομάτων-τομέα που βοηθά στη σύνδεση των διαφόρων συσκευών μέσω του IoT και στην προώθηση των δεδομένων όπου χρειάζεται, καθιστούν το XMPP ως ένα ισχυρό εργαλείο για τις εφαρμογές IoT. Αυτές οι δυνατότητες του XMPP προσφέρουν έναν εύκολο τρόπο διευθυνσιοδότησης μιας συσκευής, που είναι ιδιαίτερα χρήσιμη, στην περίπτωση όπου τα δεδομένα ανταλλάσσονται μεταξύ μακρινών, κυρίως άσχετων μεταξύ τους, σημείων του δικτύου [119].

Παρόλο που το XMPP δεν έχει σχεδιαστεί για να είναι γρήγορο (ο "πραγματικός χρόνος" στο XMPP είναι σε ανθρώπινη κλίμακα, μετρούμενος σε δευτερόλεπτα), αυτό το είδος "καθυστέρησης" δεν αποτελεί πρόβλημα για τις περισσότερες εφαρμογές, καθώς είναι συγκρίσιμο με το χρόνο χρονισμού που παρατηρείται γενικά σε συστήματα που χρησιμοποιούν άλλα πρωτόκολλα ανταλλαγής μηνυμάτων, όπως το MQTT [120]. Στις περισσότερες εφαρμογές XMPP, ο έλεγχος για ενημερώσεις πραγματοποιείται μόνο κατόπιν αιτήματος.

Τα κύρια πλεονεκτήματά του, όπως αυτά που αναφέρθηκαν παραπάνω, καθιστούν το XMPP ιδανικό για εφαρμογές IoT που προσανατολίζονται στους καταναλωτές, όπως ο οικιακός αυτοματισμός ή η παρακολούθηση και ο έλεγχος χρήσης της ενέργειας [121].

IV) AMQP

Το AMQP είναι ένα πρωτόκολλο IoT εταιρικού επιπέδου που προέκυψε από τον τραπεζικό κλάδο [106]. Πρόκειται για ένα ανοιχτό πρωτόκολλο του στρώματος εφαρμογών της αρχιτεκτονικής IoT που παρέχει αξιόπιστη επικοινωνία μέσω ανταλλαγής μηνυμάτων. Χρησιμοποιημένο για την αξιοπιστία και τη διαλειτουργικότητά του, το AMQP παρέχει ένα ευρύ φάσμα λειτουργιών που σχετίζονται με την ανταλλαγή μηνυμάτων, όπως δημιουργία αξιόπιστης ουράς μηνυμάτων, μηνύματα δημοσίευσης και εγγραφής βάσει θεμάτων, ευέλικτη δρομολόγηση και ασφάλεια [122].

Το κύριο μέλημα του AMQP είναι η ελαχιστοποίηση της απώλειας των μηνυμάτων συναλλαγών. Για αυτό το λόγο, χρησιμοποιεί στις επικοινωνίες το πρωτόκολλο TCP, το οποίο παρέχει αξιόπιστες συνδέσεις από σημείο σε σημείο, ενώ τα τελικά σημεία έχουν τη δυνατότητα να αναγνωρίζουν την αποδοχή κάθε μηνύματος. Το πρωτόκολλο δίνει επίσης ιδιαίτερη προσοχή στην παρακολούθηση όλων των κατανεμημένων μηνυμάτων και στη διασφάλιση της αποστολής κάθε μηνύματος [123].

Ορισμένες από τις εφαρμογές IoT που χρησιμοποιούν το AMQP περιλαμβάνουν λειτουργίες ανάλυσης βάσει διακομιστή και αποστολή επιχειρηματικών μηνυμάτων.

V) DDS

Το DDS είναι ένα πρωτόκολλο που επιτρέπει τη διαλειτουργικότητα του δικτύου IoT και την ανταλλαγή δεδομένων μεταξύ κινητών συσκευών και διασυνδεδεμένων μηχανημάτων [124]. Το πρωτόκολλο παρέχει ευελιξία, αξιοπιστία, επεκτασιμότητα, υψηλή απόδοση, ασφάλεια και ποιότητα υπηρεσίας (QoS) που είναι απαραίτητα για την υποστήριξη σύνθετων εφαρμογών IoT σε πραγματικό χρόνο. Οι διάφορες εκδόσεις του μπορούν να αναπτυχθούν σε πολλές πλατφόρμες, από μικρές συσκευές έως το cloud. Υποστηρίζει την ευέλικτη επεκτασιμότητα του συστήματος σε πραγματικό χρόνο, καθώς είναι ικανό να παραδίδει εκατομμύρια μηνύματα ανά δευτερόλεπτο σε πολλούς ταυτόχρονους δέκτες [125].

Ορισμένες από τις εφαρμογές IoT που χρησιμοποιούν DDS αφορούν τα στρατιωτικά συστήματα, την ιατρική παρακολούθηση, τα συστήματα παρακολούθησης και διαχείρισης περιουσιακών στοιχείων, τις δοκιμές ασφάλειας οχημάτων κλπ.

4 Εφαρμογές IoT

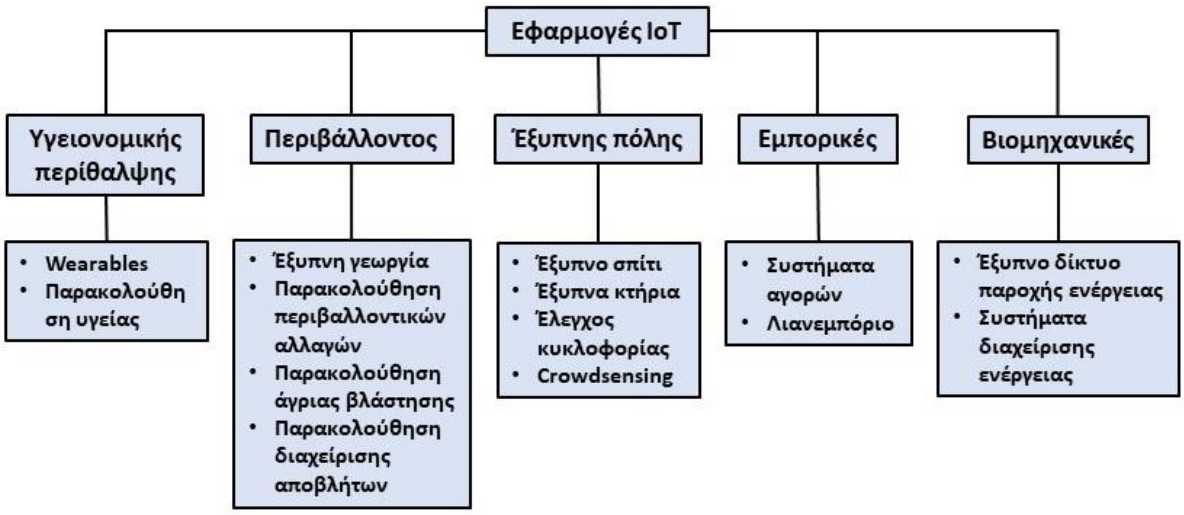
4.1 Γενικά

Το IoT έχει τόσες πολλές δυνατότητες ώστε η πλήρης υιοθέτησή του μπορεί να έχει τεράστιο κοινωνικό, περιβαλλοντικό και οικονομικό αντίκτυπο. Συνδέοντας δισεκατομμύρια πράγματα στο Διαδίκτυο, το IoT δημιούργησε μια πληθώρα εφαρμογών που αγγίζουν κάθε πτυχή της ανθρώπινης ζωής, όπως τα wearable και η παρακολούθηση της κατάστασης των ασθενών, οι στρατιωτικές εφαρμογές ανίχνευσης εισβολέων, η περιβαλλοντική παρακολούθηση, τα έξυπνα σπίτια, οι έξυπνες πόλεις, τα έξυπνα δίκτυα παροχής ενέργειας και πολλές άλλες [126].

Τα τελευταία χρόνια, η εξέλιξη των τεχνολογιών που εμπεριέχονται στο IoT είναι τέτοια ώστε δημιουργούνται τεράστιες προοπτικές ως προς την αναμενόμενη χρηστικότητα όλων των εφαρμογών του. Η χρήση του IoT σε ένα τεράστιο πλήθος διάφορων τομέων και κλάδων δίνει σαφή εικόνα της σημασίας του στην μελλοντική ανάπτυξη της σύγχρονης τεχνολογικής κατάστασης [127]. Η μελέτη των εφαρμογών IoT ενισχύει την βαθύτερη κατανόηση της τεχνολογίας και συμβάλλει στη δημιουργία ιδεών, για το σχεδιασμό συστημάτων IoT σε νέες περιπτώσεις χρήσης [128]. Όπως έχει ήδη αναφερθεί, η βασική φιλοσοφία του IoT αφορά την ανίχνευση, συλλογή και επεξεργασία δεδομένων και πληροφοριών από διάφορα αντικείμενα και τη μεταφορά τους σε άλλα. Επομένως, η σωστή επικοινωνία μεταξύ όλων των στοιχείων του IoT και η εξέλιξη των τεχνολογιών και των πρωτοκόλλων που την υποστηρίζουν, συμβάλλουν στη συνεχή μεταβολή και επέκταση του εύρους των εφαρμογών του IoT [129].

Στην εικόνα 4-1 παρουσιάζεται μια ταξινόμηση των πλέον σημαντικών τομέων εφαρμογής του IoT. Η συγκεκριμένη ταξινόμηση έγινε με βάση τις μελέτες που έχουν παρουσιαστεί κατά καιρούς στη βιβλιογραφία και αφορούν τις εφαρμογές του IoT. Με βάση τις μελέτες αυτές οι βασικοί τομείς των εφαρμογών του IoT αφορούν [106]: την υγεία, το περιβάλλον, τις έξυπνες πόλεις, το εμπόριο και τη βιομηχανία. Οι τομείς αυτοί θα αναλυθούν στις επόμενες ενότητες του κεφαλαίου. Η συγκεκριμένη ανάλυση βασίζεται στην παρουσίαση των βασικών

στοιχείων των λειτουργικών πτυχών των εφαρμογών και στη βιβλιογραφική ανασκόπηση των μελετών που έχουν εμφανιστεί την τελευταία πενταετία, όσον αφορά τις εφαρμογές αυτές.



Εικόνα 4-1: Ταξινόμηση εφαρμογών IoT

4.2 Εφαρμογές υγειονομικής περίθαλψης

Η εφαρμογή του IoT στον τομέα της υγείας δημιουργεί νέες δυνατότητες παροχής υπηρεσιών υγειονομικής περίθαλψης σε ανθρώπους που τις έχουν ανάγκη οπουδήποτε και ανά πάσα στιγμή. Η συνεχής παρακολούθηση της υγείας, κυρίως των ηλικιωμένων, έχει γίνει ευκολότερη με τη χρήση έξυπνων συσκευών που μπορούν να παίρνουν μετρήσεις και να αποστέλλουν ασύρματα πληροφορίες που αφορούν την αρτηριακή πίεση, το επίπεδο του σακχάρου στο αίμα, τους καρδιακούς παλμούς, τον κορεσμό του οξυγόνου στο αίμα, κ.λπ., στους επαγγελματίες υγείας και σε άλλα μέλη της οικογένειας [130].

Στα σύγχρονα συστήματα υγειονομικής περίθαλψης χρησιμοποιούνται πολλά και διάφορα είδη τεχνολογιών. Για παράδειγμα, τα ασύρματα δίκτυα αισθητήρων σώματος (Wireless Body Sensor Networks - WBSN) αφορούν δίκτυα αισθητήρων και βιοαισθητήρων που μπορούν να τοποθετηθούν, να φορεθούν ή ακόμα και να εμφυτευτούν οπουδήποτε στο σώμα, όπως, έξυπνα ρολόγια ή έξυπνες ζώνες, και να ενισχύσουν τη συνεχή παρακολούθηση της υγείας των ασθενών [131]. Η χρήση τέτοιων τεχνολογιών στο πλαίσιο του IoT εξασφαλίζει

καλύτερη υγειονομική περίθαλψη, βελτιώνει και εξατομικεύει τη θεραπεία, αλλά και μειώνει το κόστος διαχείρισης των συστημάτων υγείας. Το μέλλον του IoT στον τομέα της υγειονομικής περίθαλψης είναι σαφώς πολλά υποσχόμενο και για το λόγο αυτό η ακαδημαϊκή και ερευνητική κοινότητα έχει δείξει τεράστιο ενδιαφέρον, παρουσιάζοντας πλήθος μελετών και δοκιμίων σχετικών με το θέμα [132].

Οι Fafoutis και συν. (2016) παρουσίασαν ένα σύστημα παρακολούθησης υγείας με στόχο τη διάγνωση και την αποφυγή χρόνιων ασθενειών, όπως παχυσαρκία, διαβήτης και κατάθλιψη. Το προτεινόμενο σύστημα παρακολουθεί τις δραστηριότητες των χρηστών και βασίζεται στη χρήση wearable αισθητήρων, που τροφοδοτούνται μέσω επαγωγικής φόρτισης από το ύφασμα των ρούχων που φορούν οι χρήστες. Τα πειράματα που πραγματοποιήθηκαν στην πρωτότυπη υλοποίηση του συστήματος απέδειξαν την ενεργειακή αποτελεσματικότητά του [133].

Η μελέτη των Kim & Kim (2018), παρέχει έναν οδηγό για προγραμματιστές υπηρεσιών υγειονομικής περίθαλψης IoT, από τη σκοπιά του χρήστη της τεχνολογίας. Ειδικότερα, οι συγγραφείς καθόρισαν τους κατά τη γνώμη τους κρίσιμους παράγοντες που ενδέχεται να επηρεάσουν την αποδοχή από τους χρήστες των υπηρεσιών IoT διαχείρισης ασθενειών. Οι παράγοντες αυτοί αφορούν το επάγγελμα των παρόχων υπηρεσιών, το εύρος των εργασιών, τις συσκευές που χρησιμοποιούνται, την υποστήριξη των ειδικών και την κοινή χρήση μιας σειράς προσωπικών ιατρικών δεδομένων. Τα αποτελέσματα της έρευνας που διεξήχθη έδειξαν ότι οι πιθανοί χρήστες προτιμούν την ύπαρξη μιας ασφαλούς και αξιόπιστης υπηρεσίας υγειονομικής περίθαλψης, παρά μιας με μεγάλη λειτουργικότητα, ενώ η κοινή χρήση των δεδομένων του ιατρικού ιστορικού των ασθενών έχει τη μεγαλύτερη σημασία μεταξύ των παραγόντων που καθορίστηκαν από τους συγγραφείς [134].

Οι Subrahmanyam και συν. (2018) παρουσίασαν μια μελέτη η οποία επικεντρώνεται στην πρόταση τροποποίησης μιας αμελητέας ανακρίβειας που εμφανίζουν οι πομποδέκτες IEEE 802.15.4 σε εφαρμογές υγειονομικής περίθαλψης IoT. Η μελέτη αποσκοπούσε στη βελτίωση του αξιολογητή ρύθμισης της συχνότητας των πομποδεκτών, για την εξασφάλιση υψηλότερης

απόδοσής τους. Η προτεινόμενη τροποποίηση βοηθά στην ελαχιστοποίηση του συνολικού σφάλματος bit και στη συνολική εμφάνιση σφαλμάτων αποστολής πακέτων σε σύγκριση με την τυπική αρχιτεκτονική των πομποδεκτών. Επιπλέον, συμβάλλει στη μείωση της ισχύος που καταναλώνεται λόγω των λιγότερων αναμεταδόσεων που απαιτούνται, προκειμένου να διασφαλιστεί μια επιτυχημένη μετάδοση πακέτων [135].

Οι Damis και συν. (2018) παρουσίασαν μια θεωρητική και πειραματική ανάλυση τριών κεραιών επιδερμικού βρόχου για τη μέτρηση των βιολογικών παραμέτρων σε εφαρμογές υγειονομική περίθαλψη IoT. Στη μελέτη εξετάστηκε το μέγεθος του διανύσματος σφάλματος (Error Vector Magnitute - EVM) και αξιολογήθηκε το ποσοστό σφάλματος bit (Bit Error Rate – BER), ως παράμετροι που αποδεικνύουν την ακρίβεια που παρουσιάζουν οι κεραίες τετραπλού βρόχου (Quadruple Loop - QL) στις περιπτώσεις επικοινωνίας GSM και BLE. Τα αποτελέσματα των πειραματικών μετρήσεων έδειξαν οι συγκεκριμένες περιπτώσεις χρήσης παρουσιάζουν την κατάλληλη αξιοπιστία και σταθερότητα όσον αφορά την ύπαρξη ανακλώμενων κυμάτων και ακτινοβολίας [136].

Οι Malik και συν. (2018) πραγματοποίησαν ανάλυση και αξιολόγηση της τεχνολογίας NB-IoT όσον αφορά την καθυστέρηση και την απόδοση της στις υπηρεσίες υγειονομικής περίθαλψης και πιο συγκεκριμένα στα συστήματα συνεχούς παρακολούθησης της κατάστασης των ασθενών. Από τη διεξαχθείσα ανάλυση, οι συγγραφείς κατέληξαν στο συμπέρασμα ότι στα συγκεκριμένα συστήματα η απόδοση και ο αριθμός των ασθενών που μπορεί να υποστηριχτεί ανά κυψέλη είναι αντιστρόφως ανάλογα της καθυστέρησης του δικτύου. Αυτό οφείλεται στη μείωση της κεφαλίδας των πληροφοριών ελέγχου της μετάδοσης. Από τα αποτελέσματα, προέκυψε επίσης το συμπέρασμα ότι για την παροχή της καταλληλότερης λύσης σε διαφορετικά σενάρια χρήσης, θα πρέπει να γίνει προσπάθεια βελτιστοποίησης τριών παραμέτρων: της απαιτούμενης απόδοσης, καθυστέρησης και πυκνότητας συσκευών ανά κυψέλη [137].

Οι Dauwed και συν. (2018) παρουσίασαν μια μελέτη αξιολόγησης των ανθρώπινων παραγόντων που επηρεάζουν την ανταλλαγή πληροφοριών στον τομέα της υγειονομικής

περίθαλψης. Η μελέτη αποσκοπούσε στην παροχή των γνώσεων που απαιτούνται για την ανάπτυξη νέων εφαρμογών IoT στην υγειονομική περίθαλψη και επικεντρώθηκε στη συλλογή και ανταλλαγή πληροφοριών μεταξύ των επαγγελματιών υγείας. Τα αποτελέσματα που προέκυψαν απέδειξαν ότι οι κυριότεροι παράγοντες αφορούν την πρόθεση χρήσης, την ικανοποίηση των χρηστών, την ύπαρξη εμπιστοσύνης, την ποιότητα της παρεχόμενης υπηρεσίας και το περιβάλλον συνεργασίας [138].

Οι Shahidul Islam και συν. (2019) πρότειναν ένα σύστημα διαχείρισης υγειονομικής περίθαλψης που αναπτύχθηκε με χρήση της πλατφόρμας MySignals και ενός ασύρματου δικτύου LoRa. Το σύστημα περιλάμβανε επίσης μια σειρά αισθητήρων θερμοκρασίας σώματος, κορεσμού του οξυγόνου, ηλεκτροκαρδιογραφήματος και μέτρησης των παλμών της καρδιάς. Στόχος ήταν η συλλογή όσο το δυνατόν περισσότερων πληροφοριών από την πλατφόρμα MySignals και η μετάδοση τους σε έναν υπολογιστή μέσω του συστήματος υλοποίησης LoRa. Οι συγγραφείς αξιολόγησαν την αποδοτικότητα και την απόδοση κάθε αισθητήρα και κάθε συσκευής της ασύρματης πλατφόρμας, μετά από ανάλυση φυσιολογικών και στατιστικών δεδομένων [139].

Στον πίνακα 4-1 παρουσιάζεται μια σύνοψη των μελετών που αφορούν τις εφαρμογές υγειονομικής περίθαλψης του IoT. Στον πίνακα αυτόν αναφέρονται η εφαρμογή που μελετήθηκε, το πρωτόκολλο, η τεχνολογία ή η τεχνική που χρησιμοποιήθηκε, καθώς και οι συσκευές άντλησης των δεδομένων / πληροφοριών.

Πίνακας 4-1: Σύνοψη εφαρμογών υγειονομικής περίθαλψης IoT

Μελέτη	Εφαρμογή	Πρωτόκολλο / Τεχνική	Συσκευή
Fafoutis και συν. (2016)	Σύστημα παρακολούθησης υγείας	Μηχανική μάθηση	Wearables
Kim & Kim (2018)	Οδηγός παροχής υπηρεσιών υγειονομικής περίθαλψης IoT	–	Φορητές συσκευές Smartphone
Subrahmanyam και συν. (2018)	Πρόταση τροποποίησης πομποδεκτών IEEE 802.15.4 σε εφαρμογές υγειονομικής	IEEE 802.15.4	Wearables

	περίθαλψης IoT		
Damis και συν. (2018)	Εφαρμογή τηλεμετρίας μικρότερης κατανάλωσης ενέργειας	–	Wearable κεραίες
Malik και συν. (2018)	Αλγόριθμος συστήματος παρακολούθησης υγείας	NB-IoT	–
Dauwed και συν. (2018)	Αξιολόγηση παραγόντων ανταλλαγής πληροφοριών υγείας	–	–
Shahidul Islam και συν. (2019)	Σύστημα διαχείρισης υγειονομικής περίθαλψης IoT	LoRa	Βιοαισθητήρες

4.3 Εφαρμογές περιβάλλοντος

Οι εφαρμογές του IoT στην παρακολούθηση του περιβάλλοντος είναι πολλές, όπως η προστασία του περιβάλλοντος, η παρακολούθηση για ακραία καιρικά φαινόμενα, η προστασία των υδάτων από περιπτώσεις ρύπανσης, η προστασία των απειλούμενων ειδών, η γεωργία, κλπ. Σε αυτές τις εφαρμογές, η χρήση αισθητήρων αποσκοπεί στην ανίχνευση και μέτρηση κάθε τύπου περιβαλλοντικής αλλαγής [140].

Τα σύγχρονα συστήματα παρακολούθησης της ρύπανσης του αέρα και του νερού περιλαμβάνουν διεργασίες και διαδικασίες μέτρησης, επεξεργασίας και ανάλυσης των δεδομένων που λαμβάνονται από αισθητήρες, οι οποίοι αποτελούν μέρος προηγμένων οργάνων μετρήσεων. Η χρήση του IoT σε αυτά τα συστήματα μειώνει την ανάγκη για ανθρώπινη συμμετοχή στις διαδικασίες αυτές και βελτιώνει την απόδοση των συστημάτων. Μια τέτοια βελτίωση προέρχεται από την αύξηση της συχνότητας των δειγματοληψιών, από την αύξηση του εύρους των περιοχών παρακολούθησης και από τη δυνατότητα υποστήριξης επιτόπιων ελέγχων και λήψεων αποφάσεων, ως προσπάθεια απόκρισης στην ανάλυση των συγκεκριμένων ελέγχων. Μια τέτοια συνεχή παρακολούθηση επιτρέπει την αποφυγή περιπτώσεων μόλυνσης του αέρα αλλά και των υδάτων, καθώς των συναφών καταστροφών [141].

Τα προηγμένα συστήματα που χρησιμοποιούνται σήμερα για την παρακολούθηση εμφάνισης ακραίων καιρικών φαινομένων, βασίζονται στη χρήση μονάδων, όπως ραντάρ και δορυφόροι, που δεν διαθέτουν την ικανότητα εμφάνισης λεπτομερειών. Οι εξελίξεις των τεχνολογιών που εμπεριέχονται στην πλατφόρμα του IoT υπόσχονται τη συλλογή δεδομένων μεγαλύτερης ακρίβειας και λεπτομερειών, στοιχεία που οδηγούν σε πιο αποτελεσματικές προβλέψεις. Κάτι τέτοιο επιτρέπει πιο έγκαιρη ανίχνευση και απόκριση στις περιπτώσεις εμφάνισης ακραίων καιρικών φαινομένων, γεγονός που βελτιώνει την πρόληψη όσον αφορά την απώλεια ανθρώπινων ζωών και περιουσιών [142].

Οι εφαρμογές της συνεχούς παρακολούθησης του περιβάλλοντος, σε πολλές περιπτώσεις είναι αλληλένδετες με τις εφαρμογές της γεωργίας. Μεγάλο μέρος των γεωργικών διεργασιών εξαρτώνται από την κατάσταση του καιρού, επομένως η συνεχής παρακολούθηση του είναι αναγκαία. Τα σύγχρονα εξελιγμένα γεωργικά συστήματα εκμεταλλεύονται τις νέες αναδυόμενες τεχνολογίες, όπως η βιοτεχνολογία, εδώ και μερικά χρόνια, ωστόσο, η εισαγωγή του IoT μπορεί να εισάγει περισσότερο αυτοματισμό και ανάλυση. Τα συστήματα IoT μπορούν να εντοπίζουν τις μεταβολές στις καλλιέργειες, το έδαφος, το περιβάλλον κλπ. Μπορούν επίσης να βελτιστοποιήσουν τις τυπικές γεωργικές διαδικασίες μέσω ανάλυσης μεγάλων, πλούσιων συλλογών δεδομένων. Αποτρέπουν επίσης την εμφάνιση κινδύνων για τη δημόσια υγεία, επιτρέποντας καλύτερο έλεγχο των γεωργικών προϊόντων [143].

Η αξιολόγηση της χρήσης του IoT σε εφαρμογές περιβάλλοντος έχει πραγματοποιηθεί μέσα από ένα μεγάλο σύνολο μελετών που ασχολούνται με το συγκεκριμένο θέμα. Οι Kim και συν. (2015) παρουσίασαν ένα IoT σύστημα ελέγχου των κλιματικών αλλαγών για την προστασία περιοχών με άγρια βλάστηση. Το σύστημα περιλαμβάνει τη χρήση ενός δικτύου WSN χαμηλής κατανάλωσης ισχύος. Σκοπός του συστήματος είναι ο έλεγχος ενός περιβάλλοντος άγριας βλάστησης, μέσω μέτρησης πολλών σημαντικών στοιχείων του, όπως η υγρασία και η θερμοκρασία εδάφους, τα επίπεδα του διοξείδιο του άνθρακα και το μέγεθος ανάπτυξης της βλάστησης. Η αξιολόγηση του προτεινόμενου συστήματος έγινε μέσω δημιουργίας ενός μοντέλου ανάλυσης της αποτελεσματικότητάς του, χωρίς όμως να αναφέρονται τα αποτελέσματά της [144].

Οι Suparta, Alhasa & Singh (2017) παρουσίασαν ένα σύστημα παρακολούθησης των επιπέδων των αερίων του θερμοκηπίου. Στη μελέτη αναπτύχθηκε επίσης ένα σύστημα ελέγχου των συγκεκριμένων αερίων μέσω του μικροελεγκτή Netduino 3 WIFI. Το σύστημα ήταν σε θέση να συλλέγει μετεωρολογικά δεδομένα, όπως υγρασίας, θερμοκρασίας και πίεσης και να υπολογίζει την ποσότητα του κατακρημνίσιμου ύδατος (precipitable water vapour), μέσω του μοντέλου ANFIS PWV που έχει εισαχθεί στην πλακέτα του Netduino 3 WIFI. Οι πειραματικές εργαστηριακές μετρήσεις έδειξαν την μεγάλη αποτελεσματικότητα του προτεινόμενου συστήματος, ακόμα και στην περίπτωση που λειτουργεί απομακρυσμένα [145].

Οι Nordin και συν. (2017) επικεντρώθηκαν στην αναβίωση ενός παλιού συστήματος ελέγχου υδάτων σε μια αγροτική περιοχή της Μαλαισίας, χρησιμοποιώντας τεχνολογία NB-IoT. Η ερευνητική μελέτη συνέβαλε στην κατανόηση της αξιοπιστίας της ζεύξης ενός δικτύου WSN που χρησιμοποιεί ασύρματα δίκτυα 2G και LoRa και έχει κεντρικό αρχιτεκτονικό σχεδιασμό, και των περιορισμών της απόδοσης ενός δικτύου WSN χαμηλού ρυθμού μεταφοράς δεδομένων, ειδικά σε αγροτικό περιβάλλον [146].

Οι Ahamad και συν. (2019) μελέτησαν το θέμα του επιφανειακού όζοντος σε τρεις περιοχές της Μαλαισίας χρησιμοποιώντας IoT. Οι πληροφορίες που συλλέχθηκαν αναλύθηκαν για να εμφανιστεί η διακύμανση των επιπέδων του επιφανειακού όζοντος. Τα στατιστικά ληφθέντα αποτελέσματα έδειξαν τη σημαντική προσφορά της τεχνολογίας του IoT ως πρακτικού τρόπου προσδιορισμού της μεταβλητότητας των μετεωρολογικών συνθηκών [147].

Πίνακας 4-2: Σύνοψη εφαρμογών περιβάλλοντος IoT

Μελέτη	**Εφαρμογή**	**Πρωτόκολλο / Τεχνική**	**Συσκευή**
Kim και συν. (2015)	Σύστημα ελέγχου κλιματικών αλλαγών προστασίας περιοχών με άγρια βλάστηση	WSN	–
Suparta, Alhasa & Singh (2017)	Σύστημα παρακολούθησης επιπέδων των αερίων του θερμοκηπίου	WI-FI	NetDuino 3
Nordin και συν. (2017)	Αναβίωση παλιού συστήματος ελέγχου υδάτων σε αγροτική περιοχή της	NB-IoT LoRa	–

	Μαλαισίας	WAN TCP/IP	
Ahamad και συν. (2019)	Διακύμανση επιπέδων του επιφανειακού όζοντος περιοχών της Μαλαισίας	–	–

Στον πίνακα 4-2 παρουσιάζεται μια σύνοψη των μελετών που αφορούν τις εφαρμογές περιβάλλοντος του IoT. Στον πίνακα αυτόν αναφέρονται η εφαρμογή που μελετήθηκε, το πρωτόκολλο, η τεχνολογία ή η τεχνική που χρησιμοποιήθηκε, καθώς και οι συσκευές άντλησης των δεδομένων / πληροφοριών.

4.4 Εφαρμογές έξυπνης πόλης

Ο όρος "έξυπνη πόλη" χρησιμοποιείται εδώ και αρκετά χρόνια και χρησιμεύει ως περιγραφή της εφαρμογής σύνθετων συστημάτων, με σκοπό την ολοκλήρωση της λειτουργίας των αστικών υποδομών και υπηρεσιών όπως σπίτια, κτίρια, μεταφορές και δημόσια ασφάλεια [148]. Η εφαρμογή του IoT σε κτίρια και διάφορες άλλες αστικές υποδομές επιτρέπει την αυτοματοποίηση πολλών καθημερινών δραστηριοτήτων στο πλαίσιο μιας πόλης, με σκοπό την πλήρωση των αναγκών και τη βελτίωση του αστικού περιβάλλοντος διαβίωσης και εργασίας. Επομένως, σε γενικές γραμμές, η εφαρμογή του IoT στις έξυπνες πόλεις αποσκοπεί στην μείωση του κόστους διαβίωσης, στη βελτίωση της δημόσιας ασφάλειας, στη βελτίωση της ατομικής παραγωγικότητας και στη βελτίωση της ποιότητας ζωής [149].

Στη βιβλιογραφία έχει παρουσιαστεί τεράστιος όγκος μελετών που ασχολούνται με το θέμα της εφαρμογής του IoT στο πλαίσιο των έξυπνων πόλεων, καθώς οι τομείς εφαρμογής της τεχνολογίας σε αυτό το πλαίσιο είναι πολλοί. Σε πολλές περιπτώσεις μάλιστα η διάκριση των τομέων εφαρμογής είναι δύσκολο να επιτευχθεί, καθώς μια συγκεκριμένη εφαρμογή μπορεί κάλλιστα να υιοθετηθεί σε περισσότερους από έναν τομείς.

Η εγκατάσταση βιντεοκάμερων παρακολούθησης δεν είναι πλέον ο βέλτιστος τρόπος για την παροχή ασφάλειας στους πολίτες μιας πόλης. Ένα σύστημα επιτήρησης, στο πλαίσιο της έξυπνης πόλης, χρησιμοποείται για παρακολούθηση και ανίχνευση περιπτώσεων ύποπτων αντικειμένων, βανδαλισμών, λεηλασιών και εγκληματικής ταυτοποίησης. Η βιομετρία

διαδραματίζει πλέον θεμελιώδη ρόλο στις εφαρμογές προστασίας και παροχής ασφάλειας. Εκτός από τη χρήση τους σε εφαρμογές υγειονομικής περίθαλψης, εφαρμογές smartphone οι οποίες λαμβάνουν δεδομένα από ηλεκτροκαρδιογραφήματα, φωτοπλαστικογραφήματα, τεχνικές αναγνώρισης προσώπων και δακτυλικών αποτυπωμάτων μπορούν να χρησιμοποιηθούν, σύμφωνα με τη μελέτη των Guo και συν. (2016), για έλεγχο πρόσβασης ή έλεγχο ταυτότητας συσκευών IoT [150].

Οι έξυπνες οικιακές συσκευές IoT είναι πιθανώς οι πιο δημοφιλείς συσκευές στην αγορά. Αυτό οφείλεται στο ότι αυτή η κατηγορία συσκευών IoT εξυπηρετεί άμεσα έναν τεράστιο όγκο καταναλωτών που δεν έχουν τεχνική κατάρτιση και απαιτούν αξιοπιστία και ευκολία χρήσης. Οι έξυπνοι μετρητές είναι ένα σημαντικό στοιχείο των έξυπνων σπιτιών, δεδομένου ότι μετρούν με ακρίβεια τον ηλεκτρισμό και το φυσικό αέριο, παρέχουν καλύτερη κατανόηση της χρήσης της ενέργειας και έχουν τη δυνατότητα να αποστέλλουν τις πληροφορίες αυτές στον εκάστοτε πάροχο υπηρεσιών [151]. Εκτός από τους έξυπνους μετρητές, ένα έξυπνο σπίτι περιλαμβάνει έξυπνες οικιακές συσκευές οι οποίες καταγράφουν δεδομένα τα οποία αποστέλλονται στους κατασκευαστές τους. Έξυπνες οικιακές συσκευές μπορούν να θεωρηθούν αισθητήρες, ενεργοποιητές, δίαυλοι ή και απλές κοινές συσκευές με ενσωματωμένους αισθητήρες και ενεργοποιητές [152]. Οι έξυπνες πρίζες είναι ένα επιπλέον αναπόσπαστο στοιχείο των έξυπνων σπιτιών. Ο Fernández-Caramés (2015) παρουσίασε ένα δοκιμασμένο έξυπνο πολύπριζο που στοχεύει να κάνει τα σπίτια ασφαλέστερα και πιο έξυπνα. Η λύση του χρησιμοποιεί το Zigbee με χαρακτηριστικά που παρέχουν τηλεχειριστήριο, παρακολούθηση της κατανάλωσης, αποφυγή υπερβολικής κατανάλωσης και πρόληψη ηλεκτροπληξίας [153].

Μια έξυπνη πόλη θα πρέπει να παρέχει αξιόπιστα συστήματα μεταφοράς στους πολίτες της. Το IoT εδώ παίζει σημαντικότατο ρόλο και χρησιμοποιώντας πολλές ασύρματες τεχνολογίες επικοινωνίας και ανταλλαγής πληροφοριών μπορεί να υιοθετηθεί για τη δημιουργία συστημάτων μεταφορών που να έχουν τη δυνατότητα ανταλλαγής δεδομένων. Οι Masek και συν. (2016) παρουσίασαν μια μελέτη που ασχολείται με το ρόλο του IoT σε συστήματα διαχείρισης της οδικής κυκλοφορίας, εστιάζοντας στη χρήση τεχνολογιών επικοινωνίας

μεγάλου εύρους κάλυψης, όπως οι 3G, 4G (LTE) και πρωτοκόλλων δρομολόγησης όπως το VANET (Vehicular Adhoc NETwork), το οποίο είναι ένα σύστημα που βοηθά στη μεταφορά δεδομένων μεταξύ οχημάτων [154]. Η επικοινωνία μεταξύ των οχημάτων είναι επίσης ένα ακόμα στοιχείο των συστημάτων μεταφοράς στο οποίο το IoT παίζει μεγάλο ρόλο. Οι Parrado & Donoso (2015) εξέτασαν μια λύση δρομολόγησης που βασίζεται στις επικοινωνίες V2I (Vehicle-to-Infrastrucrure) και V2V (Vehicle-to-Vehicle), η οποία μειώνει την κυκλοφοριακή συμφόρηση, εξισορροπώντας τη ροή των οχημάτων στους δρόμους [155].

Οι Montori, Bedogni & Bononi (2017) πρότειναν την αρχιτεκτονική δομή SenSquare η οποία είναι σε θέση να διαχειρίζεται την ετερογένεια των πηγών δεδομένων που υπάρχει σε ένα σύστημα IoT αλλά και την έννοια του crowdsensing, η οποία χρησιμοποιείται σε μεγάλο βαθμό στις έξυπνες πόλεις, για να παρουσιάσει μια ενοποιημένη πρόσβαση στους χρήστες. Το crowdsensing, γνωστό και ως mobile crowdsensing, είναι μια τεχνική σύμφωνα με την οποία μια μεγάλη ομάδα ατόμων που έχουν κινητές συσκευές ικανές να ανιχνεύουν και να υπολογίζουν συλλογικά, μοιράζονται δεδομένα και εξάγουν πληροφορίες. Οι συγγραφείς εξέτασαν όλες τις πτυχές ενός τόσο περίπλοκου συστήματος, όπως την ετερογενή ταξινόμηση των δεδομένων, τη διαχείριση του crowdsensing για περιβαλλοντικά δεδομένα, την ενοποίηση και αναπαράσταση των πληροφοριών και τη σύνθεση και δημιουργία υπηρεσιών IoT. Στην προτεινόμενη αρχιτεκτονική δομή χρησιμοποιήθηκε κατηγοριοποίηση διαδικασιών μέσω της τεχνικής της εξόρυξης δεδομένων, με σκοπό την αξιολόγηση της αποδοτικότητάς της. Ωστόσο, δεν εξετάστηκαν τα ζητήματα της ποιότητας των δεδομένων και της διατήρησης του απορρήτου των χρηστών [156].

Πίνακας 4-3: Σύνοψη εφαρμογών IoT στο πλαίσιο των έξυπνων πόλεων

Μελέτη	Εφαρμογή	Πρωτόκολλο / Τεχνική	Συσκευή
Guo και συν. (2016)	Έλεγχος πρόσβασης έξυπνων οικιακών συσκευών IoT με χρήση βιομετρικών μεθόδων	Βιομετρία	–
Fernández-Caramés (2015)	Έξυπνο πολύπριζο	ZigBee RFID	Αισθητήρες ρεύματος

Masek και συν. (2016)	Σύστημα διαχείρισης οδικής κυκλοφορίας	3G / 4G (LTE) VANET	Ενσωματωμένα συστήματα χαμηλής ισχύος
Parrado & Donoso (2015)	Μείωση κυκλοφοριακής συμφόρησης	Επικοινωνίες V2I/V2V	Έξυπνες συσκευές σε οχήματα & οδικές υποδομές
Montori, Bedogni & Bononi (2017)	Σύστημα ενοποίησης πληροφοριών για τη δημιουργία υπηρεσιών στο πλαίσιο των έξυπνων πόλεων	Κυψελοειδής επικοινωνία	Smartphone
Lin και συν. (2017)	Σύστημα εντοπισμού θέσης εσωτ./εξωτ. χώρων για παρακολούθηση σκύλων	LoRa	Αισθητήρες θέσης

Οι Lin και συν. (2017) παρουσίασαν διάφορες εφαρμογές που έχουν αναπτυχθεί και εφαρμοστεί βάσει του IoTtalk, μια πλατφόρμα διαχείρισης συσκευών IoT που χρησιμοποιείται σε αρκετές εφαρμογές IoT τοπικής εμβέλειας. Οι εφαρμογές περιλαμβάνουν παρακολούθηση σκύλων, κουμπιά έκτακτης ανάγκης και παρακολούθηση των περιβαλλοντικών συνθηκών εσωτερικού / εξωτερικού χώρου (θερμοκρασία, επίπεδα διοξειδίου του άνθρακα, κλπ.). Ορισμένες από τις συσκευές IoT που χρησιμοποιούνται σε αυτές τις εφαρμογές δεν είναι εξοπλισμένες με αισθητήρες εντοπισμού θέσης (π.χ. GPS ή iBeacon) επειδή δεν διαθέτουν επαρκείς πόρους για εξοικονόμηση ενέργειας. Οι συγγραφείς ανέπτυξαν έναν μηχανισμό εύρεσης τοποθεσίας στο IoTtalk, με σκοπό την υποστήριξη της διαχείρισης της κινητικότητας για αυτές τις απλές συσκευές IoT. Στη μελέτη περιγράφεται ο τρόπος ανάπτυξης της εφαρμογής του εντοπισμού θέσης και ο τρόπος διαμόρφωσης του μηχανισμού της μέσω του IoTtalk GUI. Οι συγγραφείς διεξήγαγαν ανάλυση και προσομοίωση για να διερευνήσουν την ακρίβεια του εντοπισμού θέσης και της κατανάλωσης ισχύος για την εφαρμογή παρακολούθησης σκύλου [157].

Στον πίνακα 4-3 παρουσιάζεται μια σύνοψη των μελετών που αφορούν τις εφαρμογές του IoT στο πλαίσιο των έξυπνων πόλεων. Στον πίνακα αυτόν αναφέρονται η εφαρμογή που μελετήθηκε, το πρωτόκολλο, η τεχνολογία ή η τεχνική που χρησιμοποιήθηκε, καθώς και οι συσκευές άντλησης των δεδομένων / πληροφοριών.

4.5 Εμπορικές εφαρμογές

Οι εμπορικές εφαρμογές του IoT έχουν ως στόχο τη βελτίωση της καθημερινότητας των ατόμων εκτός σπιτιού. Ως επί το πλείστο αφορούν τις καταναλωτικές συνήθειες των ατόμων. Οι εμπορικές εφαρμογές IoT μπορούν να αναπτυχθούν σε μέρη που οι καταναλωτές επισκέπτονται συχνά, όπως εμπορικά καταστήματα, σουπερμάρκετ, ξενοδοχεία ή χώρους ψυχαγωγίας. Η ποικιλία τους μπορεί να καλύψει ένα ευρύ φάσμα δραστηριοτήτων, όπως έλεγχος του προσωπικού προγραμματισμού ή πρόσβαση σε καταστήματα, αλλά και εφαρμογές παρακολούθησης ή επιτήρησης που σχετίζονται άμεσα ή έμμεσα με τους καταναλωτές, όπως η παρακολούθηση των περιβαλλοντικών συνθηκών, η παρακολούθηση / επιτήρηση περιουσιακών στοιχείων, κλπ.. Αυτοί οι τύποι εφαρμογών παρέχουν καλύτερη εμπειρία στους επισκέπτες σε μέρη, όπως ξενοδοχεία και εστιατόρια, μέσω αποτελεσματικότερης παρακολούθησης σε έξυπνα κτίρια και έξυπνα γραφεία [106].

Στη βιβλιογραφία το θέμα των εμπορικών εφαρμογών του IoT έχει μελετηθεί πολύ τα τελευταία χρόνια. Οι Han & Crespi (2017) παρουσίασαν μια σημασιολογική αρχιτεκτονική παροχής υπηρεσιών από έξυπνα αντικείμενα, με σκοπό την ενσωμάτωση εφαρμογών IoT στον Ιστό. Στόχος των συγγραφέων ήταν η παροχή υπηρεσιών Ιστού από έξυπνα αντικείμενα, τα οποία μπορεί να είναι προσπελάσιμα μέσω πολλών συμβατικών διεπαφών API, λαμβάνοντας υπόψη υφιστάμενους περιορισμούς, όπως οι περιορισμένοι πόροι των αντικειμένων (μνήμες ROM, RAM και CPU), οι επικοινωνίες χαμηλής ταχύτητας και οι μικροελεγκτές χαμηλής ισχύος. Η αξιολόγηση της μελέτης απέδειξε τη βελτίωση των εφαρμογών IoT στον Ιστό και την ανάδειξη των παραμέτρων της ασφάλειας, της αξιοπιστίας και της επεκτασιμότητας στις παρεχόμενες υπηρεσίες [158].

Οι Huo και συν. (2018) πρότειναν ένα μοντέλο σύνθεσης υπηρεσιών λαμβάνοντας υπόψη τη βελτιστοποίηση χαρακτηριστικών ποιότητας QoS των υπηρεσιών, όπως ο χρόνος απόκρισης, η διαθεσιμότητα, η ταχύτητα και η απόδοση. Με στόχο τη μεγιστοποίηση των χαρακτηριστικών ποιότητας QoS και την ελαχιστοποίηση του κόστους ανάπτυξης, το προτεινόμενο μοντέλο σύνθεσης υπηρεσιών βασίστηκε στη χρήση αλγόριθμου ABC. Η

αξιολόγηση του μοντέλου σύνθεσης υπηρεσιών έγινε μέσω χρήσης δύο συνόλων δεδομένων. Τα αποτελέσματα της αξιολόγησης απέδειξαν τη βελτίωση της αποτελεσματικότητας και της ποιότητας του προτεινόμενου μοντέλου σε σύγκριση με άλλες λύσεις. Παρόλα αυτά, το προτεινόμενο μοντέλο δεν μπορεί να υποστηρίξει περιβάλλοντα, όπως τα cloud με ταχεία ροή δεδομένων η οποία δημιουργεί εξαιρετικά σοβαρές ανάγκες [159].

Οι Temglit και συν. (2017) πρότειναν μια μέθοδο επιλογής και σύνθεσης διαδικτυακών υπηρεσιών με γνώμονα την ποιότητα QoS, χρησιμοποιώντας προσέγγιση πολλαπλών αντιπροσώπων στα στρώματα των συσκευών IoT. Η προτεινόμενη μέθοδος βασίζεται σε μια προσέγγιση κατανεμημένης βελτιστοποίησης με γνώμονα το πλαίσιο της διαχείρισης των υπηρεσιών. Οι συγγραφείς χρησιμοποίησαν τη μέθοδο απλής πρόσθετης στάθμισης (Simple Additive Weighting - SAW) για να επιτύχουν τους απαιτούμενους παράγοντες της ποιότητας QoS, στην επιλογή και τη σύνθεση υπηρεσιών από τις ήδη υπάρχουσες στο IoT. Η εφαρμογή της θεωρίας γραφημάτων είχε ως αποτέλεσμα χαμηλούς χρόνους απόκρισης και καλύτερη σύνθεση υπηρεσιών σε σύγκριση με άλλες προσεγγίσεις σύνθεσης [160].

Οι Cao και συν. (2019) παρουσίασαν μια λύση σύστασης υπηρεσιών με γνώμονα την ποιότητα QoS για IoT εφαρμογές Ιστού mashup. Στην προτεινόμενη λύση, η σχέση των εφαρμογών mashup και των υπηρεσιών μπορεί να χαρακτηριστεί μέσω χρήσης μοντέλου RTM (Relational Topic Model). Επίσης, η λύση περιλαμβάνει χρήση μηχανών FM (Factorization Machines) με σκοπό την κατανόηση και μοντελοποίηση των επικοινωνιών μεταξύ ορισμένων μεταβλητών τεράστιας έλλειψης, αλλά και την πρόβλεψη της σχέσης μεταξύ των εφαρμογών mashup και των υπηρεσιών. Τα πειραματικά αποτελέσματα έδειξαν ότι η προτεινόμενη μέθοδος αυξάνει ουσιαστικά την ακρίβεια των συστάσεων υπηρεσιών [161].

Οι Cuomo, Di Somma & Sica (2018) παρουσίασαν τη χρήση του μοντέλου Hull White σε μια οικονομική εφαρμογή IoT που περιλαμβάνει τρεις φάσεις: (1) εξαγωγή πληροφοριών από διάφορες βάσεις δεδομένων, (2) έρευνα και έλεγχο και (3) υποβολή εκθέσεων. Σε αυτήν την εφαρμογή, τα χρηματοπιστωτικά ιδρύματα μπορούν να προσφέρουν στους εμπόρους

περισσότερες δυνατότητες χάρη στη γνώση των διαφόρων μεταβλητών της αγοράς. Ειδικότερα, στην συγκεκριμένη περίπτωση τα δεδομένα χρησιμοποιούνται για τον προσδιορισμό της αξίας ενός ομολόγου μέσω της χρήσης του μοντέλου Hull-White. Η διάσταση των συνόλων δεδομένων επιτρέπει την εφαρμογή παράλληλων τεχνικών σε ένα στατιστικό λογισμικό. Η προτεινόμενη προσέγγιση επιτυγχάνει μείωση του χρόνου υπολογισμού της αξίας του ομολόγου σε σύγκριση με άλλες τεχνικές [162].

Οι Pustišek & Kos (2018) πρότειναν τρεις πιθανές αρχιτεκτονικές για front-end εφαρμογές Blockchain σε περιβάλλον IoT. Οι προτεινόμενες αρχιτεκτονικές διαφέρουν στον τρόπο τοποθέτησης των πελατών Blockchain Ethereum, όπως τοπικά αντικείμενα ή απομακρυσμένους διακομιστές, και της βασικής αποθήκευσης που απαιτείται για τη διαχείριση των εξερχόμενων συναλλαγών. Οι περιορισμοί των προτεινόμενων αρχιτεκτονικών αφορούν τον όγκο των δεδομένων, την τοποθέτηση και την οργάνωση των κόμβων blockchain και την θέση και πρόσβαση του χώρου αποθήκευσης του Ethereum. Οι συγγραφείς μελέτησαν επίσης τη δυνατότητα εφαρμογής των προτεινόμενων αρχιτεκτονικών σε μια αποκλειστική επικοινωνία μεταξύ του απομακρυσμένου πελάτη Blockchain και της συσκευής IoT, με σκοπό τη βελτίωση της ασφάλειας και τη μείωση της κίνησης του δικτύου. Οι προτεινόμενες αρχιτεκτονικές μπορούν να εφαρμοστούν μόνο σε περιπτώσεις χαμηλού ρυθμού μετάδοσης δεομένων και περιορισμένη ισχύ σε ασύρματες τεχνολογίες [163].

Πίνακας 4-4: Σύνοψη εμπορικών εφαρμογών IoT

Μελέτη	**Εφαρμογή**	**Πρωτόκολλο / Τεχνική**	**Συσκευή**
Han & Crespi (2017)	Σημασιολογική αρχιτεκτονική παροχής υπηρεσιών από έξυπνα αντικείμενα IoT στον Ιστό.	6LoWPAN CoAP	Έξυπνα αντικείμενα
Huo και συν. (2018).	Μοντέλο σύνθεσης υπηρεσιών με γνώμονα την ποιότητα QoS	Αλγόριθμος Artificial Bee Colony (ABC)	-
Temglit και συν. (2017)	Μέθοδος επιλογής και σύνθεσης διαδικτυακών υπηρεσιών με γνώμονα την ποιότητα QoS χρησιμοποιώντας προσέγγιση πολλαπλών αντιπροσώπων	XMPP	-

Cao και συν. (2019)	Σύσταση υπηρεσιών με γνώμονα την ποιότητα QoS για IoT εφαρμογές Ιστού mashup	Μοντέλο RTM Μηχανές FM	Αισθητήρες IoT
Cuomo, Di Somma & Sica (2018)	Οικονιμική εφαρμογή IoT υπολογισμού της αξίας ομολόγων	Μοντέλο Hull-White	-
Pustišek & Kos (2018)	Αρχιτεκτονικές front-end εφαρμογών Blockchain σε περιβάλλον IoT	Blockchain	-

Στον πίνακα 4-4 παρουσιάζεται μια σύνοψη των μελετών που αφορούν τις εφαρμογές του IoT στο πλαίσιο των έξυπνων πόλεων. Στον πίνακα αυτόν αναφέρονται η εφαρμογή που μελετήθηκε, το πρωτόκολλο, η τεχνολογία ή η τεχνική που χρησιμοποιήθηκε, καθώς και οι συσκευές άντλησης των δεδομένων / πληροφοριών.

4.6 Βιομηχανικές εφαρμογές

Η εφαρμογή του IoT στον βιομηχανικό κλάδο ουσιαστικά ενσωματώνει στοιχεία που χρησιμοποιούνται στη βιομηχανία εδώ και χρόνια, όπως η μηχανική μάθηση και η τεχνολογία των Big Data, τα δεδομένα αισθητήρων και οι επικοινωνίες M2M. Μια τέτοιας φύσης εφαρμογή αποσκοπεί στη δημιουργία ενός κόσμου στον οποίο άνθρωποι και επιχειρήσεις μπορούν να διαχειρίζονται τα περιουσιακά τους στοιχεία και να λαμβάνουν πιο κατάλληλες αποφάσεις, με βάση την καλύτερη πληροφόρηση και ενημέρωση που τους παρέχεται. Παρά το γεγονός ότι πολλές προηγμένες βιομηχανικές εφαρμογές IoT έχουν ήδη υλοποιηθεί με επιτυχία στην καθημερινή ζωή, εξακολουθούν να υπάρχουν ακόμα πολλά πρακτικά προβλήματα που αντιμετωπίζονται με παραδοσιακές μεθόδους, κάτι που αποτελεί ένα μεγάλο εμπόδιο όσον αφορά την πλήρη υιοθέτηση του IoT από τον βιομηχανικό κλάδο [164].

Τα τελευταία χρόνια δεν είναι λίγες οι μελέτες που έχουν ασχοληθεί διεξοδικά σχετικά με τη χρήση του IoT στον βιομηχανικό τομέα. Οι Venticinque & Amato (2019) παρουσίασαν μια προσέγγιση αντιμετώπισης του ζητήματος της τοποθέτησης των υπηρεσιών Fog, το οποίο αφορά την εύρεση της βέλτιστης χαρτογράφησης μεταξύ των υπολογιστικών πόρων και των εφαρμογών IoT. Οι συγγραφείς αξιοποίησαν και επέκτειναν ένα μοντέλο εφαρμογών Fog με

σκοπό την εφαρμογή της προτεινόμενης προσέγγισης στη διερεύνηση της βέλτιστης ανάπτυξης εφαρμογών IoT. Ως μελέτη περίπτωσης χρησιμοποιήθηκε μια εφαρμογή IoT στον τομέα της παροχής έξυπνης ενέργειας. Πιο συγκεκριμένα, επέκτειναν μια πλατφόρμα λογισμικού, με σκοπό την αυτόματη εκμάθηση των ενεργειακών προφίλ και τη βελτίωση της λειτουργίας της πλατφόρμας από τους χρήστες, μέσω παρουσίασης διαφορετικών υπολογιστικών πόρων. Τα πειραματικά αποτελέσματα απέδειξαν την αποτελεσματικότητα της προτεινόμενης μεθοδολογίας στο στάδιο ανάπτυξης [165].

Οι Jin και συν. (2017) πρότειναν μια προσέγγιση προγραμματισμού πολλαπλών στρωμάτων με γνώμονα το περιεχόμενο, την CONCISE, για βιομηχανικές εφαρμογές IoT. Η συγκεκριμένη προσέγγιση παρουσιάζει ένα νέο μοντέλο επίβλεψης και συλλογής δεδομένων μέσω προγραμματισμού TSCH (Time Synchronized Channel Hopping). Τα πειραματικά αποτελέσματα της προσέγγισης έδειξαν μείωση της κυκλοφοριακής συμφόρησης του δικτύου, βελτίωση της αξιοπιστίας επικοινωνίας και μείωση της καθυστέρησης από άκρο σε άκρο [166].

Οι Kiran & Rajalakshmi (2018) παρουσίασαν μια προσέγγιση ανάλυσης της απόδοσης του στρώματος MAC IEEE 802.15.4-2015 των δικτύων PAN σε βιομηχανικές εφαρμογές IoT, στις οποίες χρησιμοποιείται επικοινωνία μεταξύ beacon. Οι συγγραφείς ανέπτυξαν ένα μαθηματικό μοντέλο με χρήση αλυσίδας Markov με σκοπό την εύρεση της καθυστέρησης της επιτυχημένης μετάδοσης πακέτων, της αξιοπιστίας και της τροφοδοσίας των κόμβων. Τα πειραματικά αποτελέσματα απέδειξαν βελτίωση της λειτουργικής αποτελεσματικότητας του δικτύου [167].

Οι Kwon και συν. (2016) παρουσίασαν ένα σύστημα διαχείρισης της υγείας για βιομηχανικές εφαρμογές. Το προτεινόμενο σύστημα εισάγει την έννοια της προγνωστικής διαχείρισης της υγείας (Prognostics and Systems Health Management – PHM), βασικοί άξονες της οποίας είναι οι εξής: η ανίχνευση, η διάγνωση, η πρόγνωση και η διαχείριση. Η μελέτη κατέληξε στο συμπέρασμα ότι η έννοια της διαχείρισης PHM είναι πιθανό να επηρεάσει σημαντικά την

ανάπτυξη, την πρόβλεψη, τη διαχείριση κινδύνων, την αξιολόγηση και τη δημιουργία νέων επιχειρηματικών ευκαιριών [168].

Πίνακας 4-5: Σύνοψη βιομηχανικών εφαρμογών IoT

Μελέτη	Εφαρμογή	Πρωτόκολλο / Τεχνική	Συσκευή
Venticinque & Amato (2019)	Αυτόματη εκμάθηση ενεργειακών προφίλ και βελτίωση λειτουργικότητας πλατφόρμας ενσωμάτωσης σφαρμογών IoT στο Fog	–	–
Jin και συν. (2017)	Προσέγγιση προγραμματισμού πολλαπλών στρωμάτων με γνώμονα το περιεχόμενο	IEEE 802.15.4-2015 TSCH MAC	–
Kiran & Rajalakshmi (2018)	Βιομηχανική εφαρμογή IoT σε δίκτυα PAN με χρήση επικοινωνίας μεταξύ beacon	IEEE 802.15.4-2015	–
Kwon και συν. (2016)	Σύστημα διαχείρισης υγείας PHM	–	Έξυπνα αντικείμενα
Luvisotto και συν. (2018)	Χρήση δικτύων LPWAN στον τομέα του IIoT	LoRaWAN IEEE 802.15.4	Βιομηχανικοί αισθητήρες
Mazzei και συν. (2020)	Εκτέλεση IBT σε βιομηχανικές εφαρμογές	Adhoc Haye	Αισθητήρες

Οι Luvisotto και συν. (2018) ασχολήθηκαν με την ιδέα του βιομηχανικού IoT (Industrial IoT – IIoT), εστιάζοντας στα δίκτυα LPWAN. Η ιδέα των συγγραφέων ήταν να σχεδιάσουν ένα ρεαλιστικό μοντέλο προσομοίωσης του LoRaWAN που επέτρεπε την εξέταση της απόδοσης δικτύων που συνήθως χρησιμοποιούνται σε εφαρμογές παρακολούθησης στον τομέα της βιομηχανίας. Η σύγκριση του μοντέλου με άλλα δίκτυα WPAN, όπως το IEEE 802.15.4, άφησε πολλά υποσχόμενα αποτελέσματα για το μέλλον [169].

Οι Mazzei και συν. (2020) όρισαν την εκτέλεση ενός μεταβιβάσιμου και αξιόπιστου IBT (Industrial Blockchain Tokenizer) για εφαρμογές IoT. Η λειτουργία του είναι να συλλέγει βιομηχανικά δεδομένα και πληροφορίες από νέα αλλά και από συμβατικά συστήματα, ενώ ταυτόχρονα επικοινωνεί με αισθητήρες [170].

Στον πίνακα 4-5 παρουσιάζεται μια σύνοψη των μελετών που αφορούν τις βιομηχανικές εφαρμογές του IoT. Στον πίνακα αυτόν αναφέρονται η εφαρμογή που μελετήθηκε, το πρωτόκολλο, η τεχνολογία ή η τεχνική που χρησιμοποιήθηκε, καθώς και οι συσκευές άντλησης των δεδομένων / πληροφοριών.

5 Ζητήματα & Προκλήσεις IoT

5.1 Ταξινόμηση των προκλήσεων

Τα συστήματα IoT είναι συνήθως περίπλοκα λόγω της τεράστιας γκάμας εφαρμογών στις οποίες μπορούν να χρησιμοποιηθούν και των διαφορετικών τεχνολογιών που αναπτύσσονται σε αυτά, με σκοπό την αυτόνομη ανταλλαγή δεδομένων μεταξύ των συσκευών τους. Λόγω αυτής της πολυπλοκότητας, τα ζητήματα και οι προκλήσεις που σχετίζονται με το IoT θα πρέπει να εξεταστούν από διάφορες πλευρές, όπως οι χρησιμοποιούμενες τεχνολογίες, οι υπηρεσίες και οι εφαρμογές, τα επιχειρηματικά μοντέλα καθώς και οι κοινωνικές και περιβαλλοντικές επιπτώσεις [107].

Η ανάλυση των πρόσφατων μελετών που έχουν εμφανιστεί στη βιβλιογραφία έδειξε ότι τα περισσότερα από τα ανοιχτά ζητήματα του IoT προκύπτουν από τον αυξανόμενο αριθμό συνδεδεμένων συσκευών, κάτι που δημιουργεί αυξημένες απαιτήσεις ανεμπόδιστης κυκλοφορίας των δεδομένων και επομένως το σχεδιασμό νέων μοντέλων που θα μπορούν να αντιμετωπίσουν αυτό το ζήτημα [171]. Άλλα ζητήματα σχετίζονται με την ενσωμάτωση διάφορων τεχνολογιών, την ύπαρξη ενός ετερογενούς περιβάλλοντος, τις αυξημένες απαιτήσεις αποθήκευσης και επεξεργασίας των δεδομένων, τους κινδύνους που προκύπτουν από την διατήρηση του απορρήτου, κλπ. [172]. Εκτός από τα ζητήματα αυτά, για τη σωστή εφαρμογή και υλοποίηση του IoT απαιτείται επίσης η αντιμετώπιση κάποιων προκλήσεων, όπως είναι η παροχή ασφάλειας, η επεκτασιμότητα, η διαχείριση των δεδομένων, κλπ. [43].

Λόγω της μεγάλης έκτασης των ζητημάτων και των προκλήσεων που καλείται να αντιμετωπίσει το IoT, στα πλαίσια της παρούσας εργασίας, θεωρήθηκε σωστότερο να γίνει μια ταξινόμηση των μελετών που παρουσιάζονται στη βιβλιογραφία την τελευταία πενταετία με σκοπό την ομαδοποίηση των θεμάτων που παρουσιάζονται ως επί το πλείστο σε αυτές. Από αυτήν την ταξινόμηση προέκυψαν τα ζητήματα και οι προκλήσεις που σχετίζονται με το IoT, που θα εξεταστούν στις επόμενες ενότητες. Από την εξέταση της βιβλιογραφίας προέκυψε το συμπέρασμα ότι οι πλήρεις δυνατότητες του IoT μπορεί να αξιοποιηθούν μόνο

μέσα από την ανάπτυξη μιας ενιαίας αρχιτεκτονικής δομής, με την ενσωμάτωση των αντίστοιχων τεχνολογιών. Επομένως, η αντιμετώπιση όλων των ζητημάτων και των προκλήσεων που θα αναφερθούν στη συνέχεια, είναι υψίστης σημασίας για την ανάπτυξη μιας τέτοιας αρχιτεκτονικής δομής.

5.2 Τυποποίηση

Η διαφορετικότητα που παρουσιάζουν οι τεχνολογίες και τα πρότυπα που χρησιμοποιούνται στο πλαίσιο του IoT θεωρούνται ως μία από τις σημαντικότερες προκλήσεις στην ανάπτυξη των εφαρμογών του. Η τυποποίηση της αρχιτεκτονικής δομής του IoT και των τεχνολογιών επικοινωνίας θεωρούνται ως η ραχοκοκαλιά για την μελλοντική εξέλιξη της τεχνολογίας [60]. Από τις παραπάνω παρατηρήσεις προκύπτει το συμπέρασμα ότι τα ανοιχτά πρότυπα αποτελούν έναν πολύ βασικό παράγοντα όσον αφορά την επιτυχή ανάπτυξη του IoT. Αυτός ο τύπος προτύπων αποτελεί σημαντικό στοιχείο για τη δημιουργία καινοτομιών, λόγω της διαθεσιμότητάς τους στο ευρύ κοινό. Τα ανοιχτά πρότυπα αναπτύσσονται, εγκρίνονται και συντηρούνται από μια συλλογική διαδικασία λήψης αποφάσεων βάσει συναίνεσης για την παροχή καλύτερης διαλειτουργικότητας σε συστήματα που χρησιμοποιούν διαφορετικές τεχνολογίες. Επίσης, τα ανοιχτά πρότυπα δίνουν τη δυνατότητα εξάλειψης της ανάγκης εξάρτησης από συγκεκριμένους κατασκευαστές συσκευών ή χρήσης συγκεκριμένων τεχνολογιών, παράγοντες από τους πλέον σημαντικούς στην ανάπτυξη του IoT.

Οι κύριοι φορείς τυποποίησης, όπως οι ITU, ETSI, IETF, IEEE, W3C, OneM2M, OASIS, NIST, κ.λπ. συμμετέχουν στην προσπάθεια δημιουργίας ενός πλαισίου προτύπων IoT. Τα πεδία των δραστηριοτήτων τυποποίησης είναι τέτοια ώστε να παρέχουν ανοιχτά πρότυπα και αρχιτεκτονικές, απρόσκοπτη συνδεσιμότητα, διαλειτουργικότητα, κ.λπ. Ωστόσο, παρά τις τεράστιες προσπάθειες από φορείς και συμμαχίες τυποποίησης, δεν έχει δημιουργηθεί ακόμη κάποιο πρότυπο αναφοράς για την πλατφόρμα του IoT [173]. Μια τέτοια έλλειψη δημιουργεί ζητήματα όσον αφορά την ενσωμάτωση των διαφόρων υπαρχόντων προτύπων, τα οποία σύμφωνα με έκδοση του ETSI σχετικά με την επίτευξη της τεχνικής διαλειτουργικότητας, αφορούν τη δημιουργία ατελών και μη επαρκών διεπαφών, τον κακό χειρισμό των επιλογών,

την έλλειψη σαφήνειας και την κακή συντήρηση [107]. Όλα αυτά τα ανοιχτά ζητήματα και οι προκλήσεις πρέπει να εξεταστούν στο μέλλον για να επιτρέψουν την απρόσκοπτη συνδεσιμότητα, καθώς και την ύπαρξη διαλειτουργικότητας μεταξύ των διαφόρων τεχνολογιών που χρησιμοποιούνται στο πλαίσιο του IoT.

5.3 Αρχιτεκτονική δομή

Το πλαίσιο της αρχιτεκτονικής δομής των συστημάτων IoT θα πρέπει να περιλαμβάνει ένα σύνολο ανοιχτών προτύπων που θα επιτρέπουν την υποστήριξη διαφόρων τεχνολογιών και την πλήρη διαλειτουργικότητα καθώς και την πλήρη κινητικότητα, ώστε να διασφαλίζεται η αδιάλειπτη παροχή υπηρεσιών. Κατά συνέπεια, μία από τις κύριες προκλήσεις για τα συστήματα IoT είναι η χρήση μιας ανοιχτής, ολοκληρωμένης και τυποποιημένης αρχιτεκτονικής με ξεχωριστή λογική εφαρμογών και υποδομή hardware υλικού. Η αρχιτεκτονική αυτή πρέπει να υποστηρίζει την ετερογενή φύση πραγμάτων, δικτύων, δεδομένων και εφαρμογών, έχοντας τη δυνατότητα με αυτόν τον τρόπο να υποστηρίξει την πλήρη διαλειτουργικότητα.

Βασικές απαιτήσεις σχεδιασμού της αρχιτεκτονικής του IoT είναι η δυνατότητα κλιμάκωσης, η διαλειτουργικότητα και η αρθρωτότητα σε ένα ετερογενές περιβάλλον. Μια τέτοια αρχιτεκτονική IoT θα πρέπει να επιτρέπει την ενσωμάτωση πολλαπλών συστημάτων, τις αλληλεπιδράσεις μεταξύ τομέων, τις απλές και επεκτάσιμες λειτουργίες διαχείρισης, την ανάλυση δεδομένων και τις φιλικές προς το χρήστη εφαρμογές, καθώς και τη δυνατότητα να συμπεριληφθεί η ευφυΐα και ο αυτοματισμός σε ολόκληρο το σύστημα IoT. Έτσι δημιουργείται ένα σύστημα IoT που μπορεί να περιλαμβάνει φυσικά αντικείμενα (π.χ. αισθητήρες, ενεργοποιητές), εικονικά αντικείμενα (π.χ. υπηρεσίες fog / cloud, επίπεδα επικοινωνίας και πρωτόκολλα) ή ένα συνδυασμό και των δύο [174]. Έχοντας όλα αυτά τα στοιχεία υπόψη, προκύπτει το συμπέρασμα ότι οι αρχιτεκτονικές δομές των συστημάτων IoT μπορούν να ταξινομηθούν σε δύο βασικά είδη [106]: (α) τις αρχιτεκτονικές hardware υλικού και δικτύου και (β) τις αρχιτεκτονικές λογισμικού.

5.3.1 Αρχιτεκτονικές hardware υλικού και δικτύου

Όπως έχει ήδη αναφερθεί, στη βιβλιογραφία έχουν παρουσιαστεί πολλά προτεινόμενα μοντέλα αναφοράς του IoT, αλλά ακόμα, καμιά αρχιτεκτονική δομή δεν έχει γίνει κοινά αποδεκτή, ώστε να παρέχει πλήρη διαλειτουργικότητα. Οι υπάρχουσες προσεγγίσεις και προσπάθειες για επίλυση αυτού του ζητήματος βασίζονται σε αρχιτεκτονικές δομές πολλών στρωμάτων [175]. Οι αρχιτεκτονικές hardware υλικού και δικτύου πρέπει να επιτρέπουν τη διαλειτουργικότητα μεταξύ των διαφόρων δικτύων και τεχνολογιών επικοινωνίας για την παροχή πλήρους συνδεσιμότητας μεταξύ των αντικειμένων IoT. Οι συσκευές IoT μπορούν να ομαδοποιηθούν σε δύο ομάδες με βάση την υποστήριξη της σουίτας πρωτοκόλλων TCP/IP. Προκειμένου να επιλυθεί το ζήτημα που σχετίζεται με την ετερογένεια, έχουν προταθεί διάφορες προσεγγίσεις και λύσεις, όπως [176]: προσεγγίσεις διεπαφών API, λύσεις πύλης, λύσεις που βασίζονται στην τεχνολογία δικτύωσης που καθορίζεται από λογισμικό (Software Defined Networking – SDN), λύσεις που βασίζονται στη χρήση εικονικοποίησης δικτυακών λειτουργιών (Network Functions Virtualization – NFV), λύσεις που βασίζονται στη δικτύωση με κέντρο το περιεχόμενο (Content-Centric Networking - CCN), κλπ. Επίσης, υπάρχουν και κάποιες άλλες προτάσεις, όπως η wearable αρχιτεκτονική IoT που παρουσιάζει την ικανότητα παροχής ιχνηλασιμότητας των ροών δεδομένων που μεταδίδονται μεταξύ των συσκευών [177]. Άλλες προκλήσεις σχετίζονται με τις διάφορες τεχνολογίες που αναπτύσσονται σε διαφορετικά δίκτυα, συμπεριλαμβανομένων των διεπαφών επικοινωνίας και των ελέγχων πρόσβασης. Όλα αυτά τα ζητήματα πρέπει να ληφθούν υπόψη στις αρχιτεκτονικές hardware υλικού και δικτύου.

Το μοντέλο αναφοράς και η αρχιτεκτονική που βασίζεται στη στοίβα πρωτοκόλλων επικοινωνίας IoT που παρουσιάστηκε στο project IoT-A της ΕΕ [7], μπορεί να αποτελέσει μια καλή επιλογή για διάφορες περιπτώσεις, αλλά για ορισμένους τομείς εφαρμογών θα πρέπει να διερευνηθούν άλλες αρχιτεκτονικές, όπως η αρχιτεκτονική που βασίζεται στο cloud, η οποία χρησιμοποιείται σε περιπτώσεις παροχής υπηρεσιών που απαιτούν αποδοτικότητα κόστους [68]. Παραδείγματα άλλων IoT αρχιτεκτονικών hardware υλικού και δικτύου αποτελούν [107]: η αρχιτεκτονική EPCglobal με βάση τις τεχνολογίες RFID και

EPC, η αρχιτεκτονική με αισθητήρες και δίκτυα WSN, η αρχιτεκτονική P2P και η αυτόνομη αρχιτεκτονική. Παρά τις τεράστιες προσπάθειες που έχουν καταβάλει οι οργανισμοί και οι συμμαχίες τυποποίησης, οι επιχειρήσεις και η ακαδημαϊκή κοινότητα, εξακολουθούν να υπάρχουν πολλά ανοιχτά ζητήματα που σχετίζονται με αυτές τις αρχιτεκτονικές.

5.3.2 Αρχιτεκτονικές λογισμικού

Οι αρχιτεκτονικές λογισμικού θα πρέπει να παρέχουν ένα κοινό σύνολο υπηρεσιών που θα επιτρέπουν την επεξεργασία του μεγάλου όγκου δεδομένων που δημιουργούνται σε οποιαδήποτε εφαρμογή IoT. Θα πρέπει επίσης να χαρακτηρίζονται από ένα ολοκληρωμένο περιβάλλον ανάπτυξης, όπως τα Java και HTML5. Οι σύγχρονες εφαρμογές IoT εξειδικεύονται ως επί το πλείστο σε συγκεκριμένους τομείς και χαρακτηρίζονται από κατακερματισμένες αρχιτεκτονικές που δεν μπορούν να ενσωματώσουν τα δεδομένα από διαφορετικές πηγές [178]. Προκειμένου να καταστεί δυνατή η ενσωμάτωση διαφόρων υπηρεσιών με άλλες υποδομές (π.χ. fog ή / και cloud) μπορεί να χρησιμοποιηθούν οι προσεγγίσεις και λύσεις που αναφέρθηκαν στην προηγούμενη υποενότητα ως προτάσεις επίλυσης του ζητήματος της ετερογένειας.

Στη βιβλιογραφία έχουν εμφανιστεί επίσης διάφορες προσεγγίσεις πλαισίου εφαρμογών και υπηρεσιών για το IoT, όπως η αρχιτεκτονική SOA, η αρχιτεκτονική RESTful, αρχιτεκτονικές που βασίζονται στο fog και στο cloud computing, πλαίσια εφαρμογών Ιστού που βασίζονται στο Google Toolkit, κλπ [107]. Αυτές οι αρχιτεκτονικές καλύπτουν λειτουργικά συστήματα, μεσαίο λογισμικό IoT, διεπαφές API, διαχείριση δεδομένων, Big data κ.λπ. Οι μελλοντικές έρευνες θα πρέπει να επικεντρωθούν στις βελτιώσεις των λειτουργικών συστημάτων πραγματικού χρόνου (RTOS), τις διεπαφές API και άλλων στοιχείων εντός των αρχιτεκτονικών IoT, για την προσαρμογή αυτών των συστημάτων στο IoT.

Η ομάδα εργασίας IETF CoRE (Internet Engineering Task Force Constrained Restful Environments) έχει καθορίσει το υποσύνολο των προδιαγραφών RESTful για την κάλυψη απαιτήσεων των εφαρμογών IoT, όπως η διαλειτουργικότητα με το πρωτόκολλο HTTP, η μικρή κεφαλίδα, και το multicast [107]. Αυτή η αρχιτεκτονική μπορεί να εφαρμοστεί σε

εφαρμογές smartphone, καθώς απαιτεί μόνο μια βιβλιοθήκη HTTP. Παρόλα αυτά, οι περιορισμοί των δικτύων LLN καθιστούν αδύνατη την απευθείας εφαρμογή της αρχιτεκτονικής RESTful. Τα SmartM2M και oneM2M είναι project του οργανισμού ETSI που βασίζονται στο σχεδιασμό RESTful και δημιουργήθηκαν με σκοπό την επίλυση διαφόρων ζητημάτων κατακερματισμού και την ενεργοποίηση της διαλειτουργικότητας, αλλά εξακολουθούν να μην μπορούν να επιλύσουν ορισμένα ζητήματα όπως η επεκτασιμότητα και η κινητικότητα, καθώς και η ενσωμάτωση των υπηρεσιών RESTful στην επιχειρηματική διαδικασία. Παρά την ύπαρξη αυτών των ζητημάτων, η αρχιτεκτονική RESTful θεωρείται σήμερα ως μια από τις καλύτερες λύσεις, επειδή ορισμένα χαρακτηριστικά της, όπως ο έλεγχος ταυτότητας και η προσωρινή αποθήκευση μπορούν να υποστηριχθούν από όλες τις πλατφόρμες cloud [179].

Η αρχιτεκτονική SOA θεωρείται ως μια καλή λύση για το μεσαίο λογισμικό IoT. Ο σχεδιασμός της αρχιτεκτονικής SOA για το IoT αποτελεί μεγάλη πρόκληση, καθώς θα πρέπει να δίνεται η δυνατότητα διαχείρισης πολλών συσκευών που συνδέονται στο σύστημα, κάτι που συνεπάγεται ζητήματα κλιμάκωσης και δυσκολία επέκτασης της αρχιτεκτονικής [176]. Ορισμένες συγκεκριμένες μελέτες περιπτώσεων IoT χρησιμοποιούν την αρχιτεκτονική SOA με διαφορετικούς τρόπους. Για παράδειγμα, το στρώμα μεσαίου λογισμικού μπορεί να έχει σκοπό να αναπτύξει και να χειριστεί μια υποδομή για την επεξεργασία και τη μετάδοση δεδομένων σε μια πύλη ή κόμβο ενεργοποίησης, ενώ άλλες λειτουργίες της αρχιτεκτονικής SOA μπορούν να χρησιμοποιούνται σε άλλα στρώματα [12].

5.4 Διαλειτουργικότητα

Η ποικιλία των προτύπων και των τεχνολογιών που χρησιμοποιούνται στο IoT καθώς και τα διαφορετικά πρωτόκολλα που χρησιμοποιούν οι κατασκευαστές συσκευών IoT, οδηγούν στη δημιουργία ενός περιβάλλοντος τεράστιας ετερογένειας που προκαλεί ζητήματα διαλειτουργικότητας. Το ζήτημα της διαλειτουργικότητας του IoT αφορά όλα τα στρώματα της αρχιτεκτονικής του δομής. Όπως αναφέρθηκε στην προηγούμενη ενότητα, η επίλυση του

ζητήματος της διαλειτουργικότητας είναι άρρηκτα συνδεδεμένη με την εύρεση μίας και μόνο κοινά αποδεκτής τυποποιημένης αρχιτεκτονικής δομής IoT.

Η έκδοση του ETSI σχετικά με την επίτευξη της τεχνικής διαλειτουργικότητας παρουσιάζει τέσσερα διαφορετικά επίπεδα διαλειτουργικότητας [180]: (α) την τεχνική, (β) την συντακτική, (γ) την σημασιολογική και (δ) την οργανωτική.

5.4.1 Τεχνική διαλειτουργικότητα

Η τεχνική διαλειτουργικότητα (technical interoperability) συνδέεται συνήθως με την υποδομή και τα πρωτόκολλα επικοινωνίας. Τα συστήματα IoT πρέπει να παρέχουν διαλειτουργικότητα στην ετερογένεια που παρουσιάζουν οι συσκευές, τα δίκτυα και τα πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Η υπάρχουσα αρχιτεκτονική του Διαδικτύου δεν υποστηρίζει την πλήρη συνδεσιμότητα των ετερογενών συσκευών, με αποτέλεσμα να είναι δύσκολη η ενσωμάτωση διαφορετικών συστημάτων [90]. Μια τέτοια ενσωμάτωση θα μπορούσε να επιτρέψει τη συνύπαρξη διαφορετικών πρωτοκόλλων επικοινωνίας και την ενίσχυση της απρόσκοπτης επικοινωνίας, από τη στιγμή που το IoT υποστηρίζει και τεχνολογίες που δεν βασίζονται στο πρωτόκολλο IP. Επομένως, η πανταχού παρούσα συνδεσιμότητα θα μπορούσε να υποστηριχθεί από την ανάπτυξη ενός προτύπου ετερογενούς δικτύωσης HetNet (Heterogeneous Networking), που να υποστηρίζει διαφορετικά πρωτόκολλα MAC και PHY και να περιλαμβάνει μηχανισμούς διαχείρισης και συντονισμού [181]. Το πρότυπο IEEE 1905.1 σχεδιάστηκε με σκοπό την υποστήριξη της διαλειτουργικότητας και παρέχει μια κοινή διεπαφή που χρησιμοποιείται ευρέως στις τεχνολογίες οικιακού δικτύου. Παρέχει διαλειτουργικότητα, καθώς και ασφαλείς συνδέσεις, διαχείριση δικτύου, επιλογή διαδρομής, αυτόματη διαμόρφωση, επέκταση της κάλυψης του δικτύου και ποιότητα QoS από άκρο σε άκρο [182].

Στη βιβλιογραφία έχουν παρουσιαστεί πολλές και διαφορετικές λύσεις στα προβλήματα της διαλειτουργικότητας. Οι λύσεις αυτές βασίζονται: (α) στις διεπαφές API, (β) στην εφαρμογή πυλών, (γ) στην ενσωμάτωση έξυπνων αντικειμένων περιορισμένων πόρων στο Διαδίκτυο χρησιμοποιώντας εικονικά δίκτυα, (δ) στη χρήση της τεχνολογίας δικτύωσης SDN, κ.λπ.

Οι λύσεις στο πρόβλημα της διαλειτουργικότητας που βασίζονται στις διεπαφές API μπορούν να χρησιμοποιηθούν για την αυτόματη μετατροπή των πρωτοκόλλων εφαρμογών. Κάποιες εφαρμογές IoT χρησιμοποιούν τα πρωτόκολλα εφαρμογών CoAP, MQTT, MQTT-SN, AMQP, REST, αλλά υπάρχουν και εφαρμογές που δεν υποστηρίζουν αντίστοιχα TCP/IP πρωτόκολλα, γεγονός που δημιουργεί ζήτημα διαλειτουργικότητας. Οι Al-Fuqaha και συν. (2015) υπογραμμίζουν την ανάγκη δημιουργίας νέων πρωτοκόλλων για συμβατότητα επικοινωνίας σε ετερογενές περιβάλλον. Οι διεπαφές API μπορούν να εφαρμοστούν σε διαφορετικές πλατφόρμες λογισμικού και cloud. Ορισμένα λειτουργικά συστήματα όπως τα Contiki, Riot OS, Android, TinyOS, LiteOS, κ.λπ., επιτρέπουν αρθρωτό σχεδιασμό και παρέχουν ανοιχτές διεπαφές API που είναι απαραίτητες για τη διαλειτουργικότητα της εφαρμογής [60]. Επίσης, οι Di Martino και συν. (2018) μελέτησαν τη επίτευξη διαλειτουργικότητας με χρήση διεπαφών API και κατέληξαν στο συμπέρασμα ότι η παροχή αξιόπιστης διαλειτουργικότητας στο IoT μπορεί να επιτευχθεί μέσω χρήσης ενός πλαισίου μεσολάβησης (proxy framework) διαλειτουργικότητας API [183].

Οι πύλες παρέχουν διάφορες λύσεις, όπως μετατροπή πρωτοκόλλου, κεντρική απομακρυσμένη συνδεσιμότητα, κεντρικό έλεγχο, κλπ., ανάλογα με το σκοπό και το στρώμα όπου υλοποιούνται. Οι διαλειτουργικές πύλες στο στρώμα αντικειμένων υποστηρίζουν πολλαπλές διεπαφές και επιτρέπουν τη σύνδεση συσκευών μέσω διαφορετικών τύπων δικτύων πρόσβασης, ενώ η εφαρμογή τους στο στρώμα δικτύου επιτρέπει τη συνδεσιμότητα μεταξύ διαφόρων τεχνολογιών δικτύου [107]. Σύμφωνα με μελέτη των Aguzzi και συν. (2015) η αποφυγή χρήσης των πυλών ως αρχιτεκτονικών στοιχείων στο στρώμα αντικειμένων μπορεί να υποστηρίξει ολοκληρωμένες λύσεις σύνδεσης και δικτύωσης P2P, ενώ οι ρόλοι των πυλών μπορούν να αντιμετωπιστούν από τα ειδικά χαρακτηριστικά των έξυπνων συσκευών του δικτύου, όπως τα smartphone. Αυτή η λύση επιτρέπει στις συσκευές να συνδέονται άμεσα με οποιαδήποτε άλλη συσκευή ή σημείο στο Διαδίκτυο, κάτι που αποτελεί το πραγματικό όραμα του IoT. Η πρόκληση που δημιουργείται όμως με αυτόν τον τρόπο αφορά την ενίσχυση των δυνατοτήτων των έξυπνων συσκευών, όπως η υπολογιστική ικανότητα, η αποθήκευση, οι διεπαφές επικοινωνίας, η χαμηλή κατανάλωση ενέργειας, κ.λπ.

[184]. Για την αντιμετώπιση αυτής της πρόκλησης, στη βιβλιογραφία έχουν παρουσιαστεί πολλές μελέτες. Οι Aloi και συν. (2017) πρότειναν τη χρήση των smartphone ως κινητές πύλες [173]. Οι Santos και συν. (2016) πρότειναν τη βελτίωση των δυνατοτήτων των smartphone με σκοπό την ανάπτυξη μιας αρχιτεκτονικής λογισμικού κινητής πύλης, που να υποστηρίζει την πλήρη διαλειτουργικότητα [185]. Παρόλα αυτά, στις μελέτες αυτές δεν παρουσιάζονται λύσεις που αφορούν τις περιορισμένες δυνατότητες αποθήκευσης και υπολογισμού και την αποδοτικότητα στην κατανάλωση μπαταρίας, ειδικά όταν αναπτύσσονται ταυτόχρονες διεπαφές επικοινωνίας [107].

Οι πλατφόρμες IoT βελτιώνουν τη διαλειτουργικότητα σε ένα ετερογενές περιβάλλον και παρέχουν λειτουργίες όπως συνδεσιμότητα διαφόρων αντικειμένων χρησιμοποιώντας τεχνολογίες επικοινωνίας, διαχείριση συσκευών, επεξεργασία δεδομένων, οπτικοποίηση δεδομένων, κλπ. [186]. Σύμφωνα με τις λειτουργίες τους, οι πλατφόρμες IoT μπορούν να ομαδοποιηθούν ως [187]: α) πλατφόρμες hardware υλικού, β) πλατφόρμες λογισμικού και γ) πλατφόρμες cloud. Η χρήση αυτών των πλατφορμών ως λύση του ζητήματος της διαλειτουργικότητας μπορεί να περιλαμβάνει διάφορες προσεγγίσεις, όπως διαφορετικές διεπαφές δικτύου, πύλες, διεπαφές API, κλπ. Οι πλατφόρμες IoT hardware υλικού παρέχουν τεχνική διαλειτουργικότητα και επιτρέπουν τη σύνδεση συσκευών καθώς και την επεξεργασία δεδομένων εκτός του κέντρου δεδομένων. Παρέχουν επίσης πύλες για τη δυνατότητα σύνδεσης συσκευών με διάφορες τεχνολογίες δικτύου. Παραδείγματα πλατφορμών hardware υλικού αποτελούν τα Arduino, Raspberry Pi, Gadgeteer, BeagleBoard, pcDuino, κ.λπ. Παρά την ευρεία χρήση τους, δεν έχουν καταφέρει να αντιμετωπίσουν σε μέγιστο βαθμό την πρόκληση ανάπτυξης μιας πλατφόρμας ικανής να αλληλοεπιδράσει με όλες τις τεχνολογίες που χρησιμοποιούνται στο πλαίσιο του IoT. Ένα άλλο σημαντικό ζήτημα είναι να καταστεί δυνατή η διασύνδεση μεταξύ διαφόρων πλατφορμών για την ενδυνάμωση των ικανοτήτων τους. Άλλα ζητήματα σχετίζονται με την τροφοδοσία τους, την ενεργειακή τους απόδοση, την ασφάλεια που παρέχουν, την απρόσκοπτη συνδεσιμότητα, την κινητικότητα που παρουσιάζουν, κλπ. [107]. Οι πλατφόρμες IoT λογισμικού επιτρέπουν την ενσωμάτωση των αντικειμένων IoT σε τεχνολογίες δικτύου χρησιμοποιώντας διάφορα

πρωτόκολλα επικοινωνίας. Αυτές οι πλατφόρμες ενσωματώνουν περιβάλλοντα ανάπτυξης (HTML5, Java, κ.λπ.) και παρέχουν διεπαφές API, που επιτρέπουν στους προγραμματιστές να επικοινωνούν με συσκευές IoT μέσω διαφόρων τεχνολογιών δικτύου [107]. Οι πλατφόρμες cloud επιτρέπουν την ανάπτυξη λύσεων IoT με βάση τα τρία μοντέλα υπηρεσιών που παρέχουν (SaaS, PaaS και IaaS). Τα βασικά ζητήματα που παρουσιάζουν όλες οι πλατφόρμες IoT σχετίζονται με υποστηρικτικές τεχνολογίες, όπως οι επεξεργαστές, οι αισθητήρες, το hardware υλικό και τα πρωτόκολλα επικοινωνίας, τα λειτουργικά συστήματα, τα εργαλεία προγραμματισμού, τα εργαλεία ανάλυσης, κλπ. Ένα άλλο βασικό ζήτημα αυτών των πλατφορμών σχετίζεται με την ασφάλεια (έλεγχος ταυτότητας, εξουσιοδότηση, έλεγχος πρόσβασης, ανίχνευση εισβολής, μηχανισμοί ανάκτησης, κλπ.) [187].

Κάποιες άλλες λύσεις του ζητήματος της τεχνικής διαλειτουργικότητας αφορούν προσεγγίσεις που εφαρμόζονται σε διαφορετικά στρώματα της αρχιτεκτονικής δομής του IoT και παρέχουν δυναμική, ευέλικτη και αυτόματη διαχείριση και αναδιάρθρωση του δικτύου [90]. Στόχος τους είναι η απλοποίηση του σχεδιασμού και της διαχείρισης του δικτύου που θα συνεισφέρει στην επίλυση ορισμένων τεχνικών ζητημάτων διαλειτουργικότητας. Οι Talavera και συν. (2015) παρουσίασαν μια προσέγγιση που βασίζεται στη χρήση hub, η οποία παρέχει επεκτάσιμη και αξιόπιστη επικοινωνία και βελτιώνει ορισμένα προβλήματα διαλειτουργικότητας [188]. Επίσης, οι αρχιτεκτονικές λογισμικού, όπως η αρχιτεκτονική SOA, μειώνουν τα προβλήματα ενσωμάτωσης ετερογενών συσκευών IoT σε ένα σύστημα και βελτιώνουν τη διαλειτουργικότητα τους. Κάτι τέτοιο μπορεί να επιτευχθεί μέσω της παροχής ενός ισχυρού πλαισίου που υποστηρίζει τη συνδεσιμότητα και την ενσωμάτωση στοιχείων σε συστήματα IoT [189]. Ωστόσο, παρά την ευελιξία που προσφέρει αυτό το πλαίσιο, υπάρχουν ορισμένα ζητήματα που σχετίζονται με την αρχιτεκτονική SOA, όπως η έλλειψη ενός ευφυούς πλαισίου με γνώμονα τη σύνδεση, που δεν μπορεί να υποστηρίξει τη διαλειτουργικότητα [107].

5.4.2 Συντακτική διαλειτουργικότητα

Η συντακτική διαλειτουργικότητα (syntactical interoperability) σχετίζεται με την κατανόηση του περιεχομένου (πληροφορίες) και αναφέρεται στη μορφή, τη σύνταξη και την κωδικοποίηση των δεδομένων. Καθώς ιι εφαρμογές IoT πρέπει να ενσωματώνουν δεδομένα από διαφορετικές πηγές, η αρχιτεκτονική λογισμικού θα πρέπει να επιτρέπει την αναζήτηση, τη συγκέντρωση και την επεξεργασία των δεδομένων αυτών. Κάτι τέτοιο μπορεί να επιτευχθεί μέσω τυποποιημένης μορφής, σύνταξης και κωδικοποίησης των δεδομένων. Το μεσαίο λογισμικό του IoT πρέπει επίσης να περιλαμβάνει μηχανισμούς, όπως λύσεις διεπαφών API, για υποστήριξη της διαλειτουργικότητας μεταξύ διαφορετικών εφαρμογών, υπηρεσιών και μορφών δεδομένων [190].

5.4.3 Σημασιολογική διαλειτουργικότητα

Η σημασιολογική διαλειτουργικότητα (semantic interoperability) επιτρέπει την κοινή χρήση της ερμηνείας του περιεχομένου (έννοια των πληροφοριών) μεταξύ των μερών που επικοινωνούν [191]. Ο όρος "σημασιολογικός" στο πλαίσιο του IoT αναφέρεται στη δυνατότητα εξαγωγής γνώσεων από ακατέργαστα δεδομένα που συλλέγονται από τους αισθητήρες. Αυτή η "γνώση" επιτρέπει την παροχή χρήσιμων υπηρεσιών και αναφορών βάσει των δεδομένων που έχουν υποστεί ανάλυση και επεξεργασία [192]. Η εξέλιξη των σημασιολογικών τεχνολογιών επιτρέπει κάποιο επίπεδο διαλειτουργικότητας δεδομένων, καθώς και προηγμένη λήψη αποφάσεων. Η σημασιολογική διαλειτουργικότητα επιτρέπει στα αντικείμενα IoT να μαθαίνουν, να σκέφτονται και να κατανοούν στοιχεία του φυσικού κόσμου. Η ύπαρξη ενός κοινού πλαισίου υψηλού επιπέδου με επαρκή αρχιτεκτονική και ο συνδυασμός του με νέες τεχνικές, όπως η εξόρυξη δεδομένων, θα μπορούσε να συμβάλλει στην εξαγωγή μετα-δεδομένων. Για παράδειγμα, οι Cimmino και συν. (2020) παρουσίασαν μια αρχιτεκτονική διαλειτουργικότητας σημασιολογικού επιπέδου διάχυτου υπολογισμού (pervasive computing) και IoT [193].

Οι Ganzha και συν. (2016) παρουσίασαν κάποιες από τις σημασιολογικές τεχνολογίες που χρησιμοποιούνται στο IoT, όπως οι JSON, W3C, OWL, RDF, EXI (Efficient XML

Interchange) και WSDL (Web Services Description Language) [194]. Η χρήση τόσο πολλών και διαφορετικών τεχνολογιών οδηγεί στην ύπαρξη ετερογένειας σε σημασιολογικό επίπεδο, κάτι που αποτελεί σημαντικό ερευνητικό πεδίο. Παρά τη χρήση μερικών χρήσιμων προτύπων δεδομένων, όπως τα IOTDB, SensorML, Semantic Sensor Net Ontology - W3C, Wolfram Language, RAML (RESTful API Modeling Language), SENML (Sensor Markup Language), LsDL (Lemon-beat smart Device Language), κλπ., ο σχεδιασμός ενός σημασιολογικού πλαισίου IoT και ανοικτών προτύπων δεδομένων για την υποστήριξη της πλήρους διαλειτουργικότητας, εξακολουθεί να αποτελεί ανοιχτό ζήτημα προς επίλυση [107].

5.4.4 Οργανωτική διαλειτουργικότητα

Η οργανωτική διαλειτουργικότητα (organizational interoperability) συνδέεται συνήθως με την ικανότητα ανταλλαγής δεδομένων παρά τη χρήση διαφορετικών συστημάτων πληροφοριών και υποδομών. Η επίτευξή της καθορίζεται αποκλειστικά από την επιτυχημένη επίτευξη των άλλων τριών ειδών διαλειτουργικότητας [180].

5.5 Διαθεσιμότητα και αξιοπιστία

Η διαθεσιμότητα των υπηρεσιών αποτελεί ένα ακόμα κρίσιμο ζήτημα της τεχνολογίας του IoT, η αντιμετώπιση του οποίου θα βελτιώσει τη δυνατότητα σωστής διαχείρισης της δυναμικής των συστημάτων IoT. Με τον όρο διαθεσιμότητα εννοείται ότι οι εφαρμογές IoT πρέπει να είναι διαθέσιμες οπουδήποτε και οποτεδήποτε για κάθε εξουσιοδοτημένο αντικείμενο. Τα αντικείμενα που πρόκειται να συνδεθούν πρέπει να είναι προσαρμοστικά και ευφυή, ώστε να υποστηρίζουν απρόσκοπτη συνδεσιμότητα και επιθυμητή διαθεσιμότητα [195].

Η διαθεσιμότητα του δικτύου και η περιοχή κάλυψης του πρέπει να επιτρέπουν τη συνέχεια της χρήσης των υπηρεσιών, ανεξάρτητα από την κινητικότητα, τη δυναμική αλλαγή της τοπολογίας του δικτύου ή τις χρησιμοποιούμενες τεχνολογίες. Όλα αυτά απαιτούν μηχανισμούς υποστήριξης της διαλειτουργικότητας, της παράδοσης δεδομένων και της ανάκτησης σε περίπτωση σφαλμάτων ή δυσλειτουργιών. Για το λόγο αυτό, η ανάπτυξη

κατάλληλου συστήματος παρακολούθησης, πρωτοκόλλων και μηχανισμών αυτοθεραπείας θα συμβάλλει στην επίτευξη στιβαρότητας του συστήματος [107]. Ορισμένες τεχνολογίες επικοινωνίας υποφέρουν από διαλείπουσα διαθεσιμότητα η οποία μπορεί να προκαλέσει διακοπή της υπηρεσίας, όπως για παράδειγμα οι δορυφορικές επικοινωνίες που παρουσιάζουν διακυμάνσεις ποιότητας [196]. Στα συστήματα IoT, οι διαδικασίες συλλογής, επεξεργασίας, ελέγχου, κλπ. των δεδομένων θα πρέπει να είναι πάντα διαθέσιμες, ανεξάρτητα από το δίκτυο μεταφοράς τους (Διαδίκτυο ή άλλα δίκτυα). Η χρήση MCC, MEC, Cloudlet και Fog computing θα μπορούσαν να αποτελέσουν λύσεις αντιμετώπισης ορισμένων από αυτά τα ζητήματα [107]. Ωστόσο, μια τέτοια χρήση δημιουργεί νέες προκλήσεις όπως αναφέρθηκε σε προηγούμενη ενότητα.

Η κινητικότητα των συσκευών IoT δημιουργεί μια συχνή μεταβολή της τοπολογίας του δικτύου, γεγονός που αποτελεί μια ακόμα σημαντική πρόκληση όσον αφορά την διαθεσιμότητα και την αξιοπιστία των υπηρεσιών που παρέχονται σε χρήστες κινητών συσκευών. Λύση θα μπορούσε να αποτελέσει η δημιουργία ενός ανθεκτικού συστήματος που θα μπορεί να αντιμετωπίσει αυτές τις δυναμικές αλλαγές. Με άλλα λόγια, δημιουργείται η απαίτηση για αποτελεσματικούς μηχανισμούς διαχείρισης της κινητικότητας [197]. Το MIPv6 (Mobile IPv6) είναι ένα πρωτόκολλο που αναπτύχθηκε για την υποστήριξη της κινητικότητας σε δίκτυα IPv6. Επιπλέον, το IPSec (Internet Protocol Security) είναι υποχρεωτικό για το MIPv6 προκειμένου να υποστηρίζει την εμπιστοσύνη μεταξύ των οικιακών πρακτόρων και των κινητών συσκευών. Ορισμένες αναπτύξεις συστημάτων IoT θεωρούν ότι οι συσκευές πρέπει να γνωρίζουν την τοποθεσία τους αλλά και τις θέσεις των γειτονικών τους συσκευών [198]. Αυτό αποτελεί μια ακόμα σημαντική πρόκληση για μελλοντική έρευνα, ιδίως στις περιπτώσεις ανάπτυξης εφαρμογών πραγματικού χρόνου που απαιτούν επίγνωση θέσης [107].

Τα ζητήματα δρομολόγησης είναι πολύ σημαντικά για την αξιοπιστία κυρίως στις περιπτώσεις τοπολογίας πλέγματος πολλαπλών αλμάτων. Οι διαδικασίες δρομολόγησης πρέπει να υποστηρίζουν τις δυναμικές αλλαγές της τοπολογίας, δρομολόγηση πολλαπλών αλμάτων, επεκτασιμότητα, μηχανισμούς ασφάλειας με γνώμονα το πλαίσιο, ποιότητα QoS,

κλπ. [199]. Το ζήτημα της δρομολόγησης στα συστήματα IoT είναι ένα από τα πλέον σημαντικά για ακαδημαϊκή μελέτη. Οι Huang και συν. (2016) παρουσίασαν μια σειρά από αλγόριθμους για τη δημιουργία ενός δέντρου δρομολόγησης multicast σε περιβάλλον IoT [200]. Τα πρωτόκολλα RSVP (Resource Reservation Protocol) και MPLS (Multi-Protocol Label Switching) επιλύουν πολλά προβλήματα δρομολόγησης [201]. Επίσης, η ανάπτυξη πρωτοκόλλου δρομολόγησης RPL παρέχει ορισμένες λύσεις στα ζητήματα δρομολόγησης σύνδεσης των δικτύων LLN με το Διαδίκτυο [67]. Αυτό το πρωτόκολλο επιτρέπει την προσαρμογή της τοπολογίας και παρέχει αποτελεσματικές λειτουργίες δρομολόγησης. Ωστόσο, παρουσιάζει κάποιες αδυναμίες και όρια όπως μεγάλη κεφαλίδα, μεγάλη απώλεια πακέτων και καθυστέρηση στις περιπτώσεις κινητών εφαρμογών [202]. Μια άλλη πρόκληση αποτελεί η ύπαρξη αντιστάθμισης μεταξύ της αξιοπιστίας και της κατανάλωσης ενέργειας. Αυτός είναι ο λόγος για τον οποίο πολλά συστήματα IoT χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς, ενώ οι μηχανισμοί ελέγχου αναμετάδοσης εφαρμόζονται στο στρώμα εφαρμογών [90]. Επομένως, η παροχή αξιοπιστίας από άκρο σε άκρο απαιτεί την ανάπτυξη αποτελεσματικών πρωτοκόλλων ανώτερου στρώματος (μεταφοράς και εφαρμογών). Μια άλλη λύση για την αντιμετώπιση του ζητήματος της αξιοπιστίας είναι η ανάπτυξη μιας νέας επέκτασης πρωτοκόλλου, όπως το νέο στρώμα υποστήριξης κινητικότητας (MoMoRo) για ασύρματα δίκτυα LPWSN [202].

5.6 Αποθήκευση, επεξεργασία και οπτικοποίηση δεδομένων

Με την τεράστια αύξηση των συνδεδεμένων αντικειμένων και του όγκου των δεδομένων, έχει δημιουργηθεί η απαίτηση για νέες τεχνικές ανάλυσης. Τα συστήματα IoT χρειάζονται μια κοινή πλατφόρμα ανάλυσης, με σκοπό την υποστήριξη των Big Data που πρέπει να παραδοθούν ως υπηρεσία σε εφαρμογές IoT. Διάφορες μέθοδοι εξόρυξης δεδομένων, όπως η τεχνητή νοημοσύνη (AI), η μηχανική μάθηση και άλλοι έξυπνοι αλγόριθμοι λήψης αποφάσεων, επιτρέπουν την οργάνωση, την εξερεύνηση και την ανάλυση του τεράστιου όγκου πρωτογενών δεδομένων με στόχο την ανακάλυψη μοτίβων σε αυτά, τα οποία με τη

σειρά τους θα οδηγήσουν στην εξαγωγή χρήσιμων πληροφοριών, με μόνο περιορισμό το κόστος [203].

Από τις νέες αναδυόμενες τεχνολογίες, μόνο αυτή του cloud φαίνεται ότι μπορεί να ικανοποιήσεις αποτελεσματικά τις απαιτήσεις που δημιουργούνται για τη σωστή διαχείριση της συνεχώς αυξανόμενης ποσότητας δεδομένων. Οι διάφορες πλατφόρμες cloud που υπάρχουν στην αγορά, παρουσιάζουν δυνατότητες αποθήκευσης και υπολογιστικής, τέτοιες ώστε να είναι σε θέση να υποστηρίξουν πρωτόκολλα εφαρμογών, διαλειτουργικότητα, πύλες, μοντέλα χρέωσης, κλπ. [204]. Ωστόσο, η μεταφορά των Big Data από τις συσκευές παρυφών (π.χ. αισθητήρες, smartphone, κλπ.) στην υποδομή cloud δημιουργεί διάφορα ζητήματα, όπως ζητήματα στις επιδόσεις του δικτύου (π.χ. καθυστερήσεις, εύρος ζώνης, κίνηση, αξιοπιστία, διαθεσιμότητα, κλπ.), μεγαλύτερο κόστος μετακίνησης των δεδομένων μέσω του Διαδικτύου, μεγαλύτερο κόστος αποθήκευσης των δεδομένων σε διακομιστές cloud, ζητήματα ασφάλειας των δεδομένων κατά τη μετάδοση και αποθήκευση, ζητήματα απορρήτου, κλπ [205]. Η επίλυση των ζητημάτων αυτών δημιουργεί την ανάγκη για ανάπτυξη μιας υβριδικής πλατφόρμας cloud με δυνατότητες κλιμάκωσης και υψηλής απόδοσης, όπως επίσης και νέων αλγορίθμων φιλτραρίσματος, επιλογής, αφαίρεσης και συγκέντρωσης των ακατέργαστων δεδομένων [206].

Στις περιπτώσεις στις οποίες οι τοπικοί πόροι της υποδομής του IoT επαρκούν για αποθήκευση και επεξεργασία των δεδομένων, δεν υπάρχει ανάγκη χρήσης της τεχνολογίας του cloud computing. Η επεξεργασία ανεπεξέργαστων δεδομένων σε τοπικά αναπτυγμένους κόμβους μπορεί να μειώσει την ποσότητα των δεδομένων που απαιτείται να μεταφερθούν μέσω του Διαδικτύου. Κάτι τέτοιο μειώνει τη συμφόρηση δεδομένων, τον λανθάνοντα χρόνο, το κόστος και βελτιώνει κάποιες άλλες επιδόσεις του δικτύου. Στις περιπτώσεις αυτές, υπολογιστικές τεχνολογίες, όπως οι MCC, MEC, Cloudlet και Fog computing, μπορούν να χρησιμοποιηθούν σε τοπικό επίπεδο ως επεκτάσεις του cloud computing [207]. Αυτά τα συστήματα βελτιώνουν κάποιες από τις επιδόσεις του IoT, όπως η ποιότητα QoS, η αξιοπιστία, η κινητικότητα, η ασφάλεια και η διατήρηση του απορρήτου [208]. Για παράδειγμα, το fog computing επιτρέπει την ανάπτυξη έξυπνων συσκευών, όπως έξυπνα

τηλέφωνα και οικιακές πύλες, για την προεπεξεργασία και τον υπολογισμό των δεδομένων με γνώμονα το πλαίσιο. Ωστόσο, αυτές οι πλατφόρμες δεν μπορούν να προσαρμοστούν σε όλες τις περιπτώσεις χρήσης, λόγω έλλειψης δυνατοτήτων σύνθετης ανάλυσης και αποθήκευσης τεράστιου όγκου δεδομένων. Αυτές οι λειτουργίες συμπληρώνονται από το cloud computing. Ως εκ τούτου, σε τοπικό επίπεδο και κυρίως στις παρυφές ενός συστήματος IoT, είναι δυνατή η πραγματοποίηση μόνο ορισμένων βασικών υπολογιστικών διεργασιών. Για να ξεπεραστούν οι περιορισμοί πόρων της τοπικής υποδομής, τα δεδομένα πρέπει να προωθηθούν σε ένα cloud. Η χρήση της τεχνολογίας MEC στα συστήματα IoT, προκειμένου να υποστηριχθεί η κινητικότητα, θα πρέπει να αντιμετωπίσει το ζήτημα της δυναμικότητας των συσκευών IoT. Το ζήτημα αυτό σε συνδυασμό με την ύπαρξη της απαίτησης χαμηλής κατανάλωσης ενέργειας από τις συσκευές, οδηγεί στη δημιουργία νέων ζητημάτων, όπως η δυνατότητα μετεγκατάστασης των υπηρεσιών και η δυνατότητα υπολογισμών. Ένα άλλο σημαντικό ζήτημα που σχετίζεται με την κινητικότητα είναι η συνεργασία και ο συγχρονισμός μεταξύ των κόμβων edge. Ένας μηχανισμός συγκέντρωσης δεδομένων θα μπορούσε να εφαρμοστεί στην πύλη για τη διαχείριση των ροών δεδομένων, αλλά αυτή η λύση συνεπάγεται την ανάπτυξη επαρκούς λογισμικού. Επομένως, η ενσωμάτωση του MEC στο IoT δεν μπορεί να επιλύσει ζητήματα όπως η κινητικότητα, η πολύπλοκη ανάλυση, η ασφάλεια και το απόρρητο των δεδομένων στις συσκευές edge [209].

Η οπτικοποίηση των δεδομένων αντιμετωπίζει εξίσου σημαντικές προκλήσεις που αφορούν την ανάπτυξη εργαλείων για την αλληλεπίδραση του χρήστη με το περιβάλλον IoT, την οπτικοποίηση των ανεπεξέργαστων δεδομένων με ουσιαστικό τρόπο και σύμφωνα με τις ανάγκες του τελικού χρήστη, κλπ. [210]. Οι εφαρμογές IoT απαιτούν σύνδεση με υποδομή (π.χ. cloud και δίκτυο) και πρέπει να υποστηρίζουν φιλικές προς το χρήστη διεπαφές για να επιτρέπουν τον ασφαλή απομακρυσμένο έλεγχο των συσκευών. Η εξάλειψη της ανάγκης φυσικών ελέγχων στο ίδιο το αντικείμενο χρησιμοποιώντας νέες ψηφιακές διεπαφές χρήστη είναι λιγότερο δαπανηρή και έχει περισσότερες δυνατότητες προσαρμογής. Οι εφαρμογές IoT μπορούν να είναι αυτόνομες ή να ελέγχονται από τον άνθρωπο (άμεσα, παθητικά ή υβριδικά). Ο έλεγχος των συσκευών αποτελεί μια πολύ ενδιαφέρουσα ερευνητική περιοχή λόγω των

πολλών προκλήσεων που αντιμετωπίζει, όπως η κατανόηση των διαφορετικών τύπων ελέγχων, ο τρόπος υλοποίησης της ανατροφοδότησης ελέγχου, κλπ. [107]. Η οπτικοποίηση των δεδομένων που συλλέγονται από τους αισθητήρες περιλαμβάνει τη χρήση διαγραμμάτων, χαρτογράφησης, παρακολούθηση τοποθεσίας σε χάρτες, κλπ. Το γραφικό περιβάλλον χρήστη GUI (Graphic User Interface) παρέχει οπτικοποίηση των εκτελούμενων μετρήσεων και επιτρέπει την εκτέλεση διαφορετικών ενεργειών ελέγχου. Η οπτικοποίηση των δεδομένων παρουσιάζει κάποια ζητήματα τα οποία αφορούν προβλήματα κατά την εξαγωγή πληροφοριών από τα ανεπεξέργαστα δεδομένα, όπως η υπεραπλούστευση των δεδομένων ή η υπερβολική εμπιστοσύνη στην οπτικοποίησή τους. Η απλοποίηση των δεδομένων, ιδιαίτερα στην περίπτωση των Big Data, θα μπορούσε να οδηγήσει στην εξαγωγή αβάσιμων συμπερασμάτων. Οι τεχνολογίες Ιστού, όπως το HTML 5, παρέχουν λύσεις για ορισμένα από αυτά τα ζητήματα [211]. Αναδυόμενες τεχνολογίες, όπως οι τεχνολογίες αφής ή οι τρισδιάστατες οθόνες μπορούν επίσης να προσφέρουν έναν αποτελεσματικό τρόπο παρουσίασης των δεδομένων, αλλά και να βοηθήσουν στην εξαγωγή χρήσιμων πληροφοριών από ανεπεξέργαστα δεδομένα [107].

5.7 Επεκτασιμότητα

Μια βασική πρόκληση που σχετίζεται με την επεκτασιμότητα είναι η δυνατότητα ενός συστήματος IoT να υποστηρίξει ένα μεγάλο αριθμό διαφόρων συσκευών με περιορισμούς μνήμης, δυνατότητας επεξεργασίας, εύρους ζώνης και άλλων πόρων [212]. Οι μηχανισμοί επεκτασιμότητας χρησιμοποιούνται με σκοπό την αποτελεσματική ανακάλυψη συσκευών, αλλά και για να καταστεί δυνατή η διαλειτουργικότητά τους. Για να καταστεί δυνατή η επεκτασιμότητα καθώς και η διαλειτουργικότητα ενός συστήματος IoT, η δημιουργία ενός πλαισίου και μιας αρχιτεκτονικής στρωμάτων θα αποτελούσε ιδανική λύση [213].

Μία από τις πιθανές λύσεις του ζητήματος της επεκτασιμότητας είναι η χρήση πλατφορμών cloud υψηλής κλιμάκωσης με δυνατότητα αποθήκευσης τεράστιας ποσότητας δεδομένων. Με τον τρόπο αυτό δημιουργείται ένας νέος όρος ο οποίος απαντάει στο όνομα Σύννεφο των Πραγμάτων (Cloud of Things), που μπορεί να χρησιμοποιηθεί ως παγκόσμια αρχιτεκτονική

που κλιμακώνει το cloud computing [206]. Μια άλλη λύση είναι η χρήση συστημάτων edge computing, τα οποία επεκτείνουν τις υπηρεσίες cloud στις συσκευές παρυφών. Αυτή η τεχνολογία παρέχει δυνατότητες αποθήκευσης, υπολογισμού και μερικές υπηρεσίες δικτύωσης μεταξύ των συσκευών και της υποδομής cloud. Το πρόβλημα όμως είναι ότι τα συστήματα edge computing δεν μπορούν να παρέχουν λειτουργίες, όπως σύνθετη ανάλυση, πρόσβαση δεδομένων σε μεγάλο αριθμό χρηστών και αποθήκευση δεδομένων ιστορικού, οι οποίες συμπληρώνονται με τη χρήση του cloud computing [181].

Μια άλλη πρόκληση αποτελεί η δυνατότητα υπολογισμού με γνώμονα το πλαίσιο με παράλληλη υποστήριξη επεκτασιμότητας. Αυτό το πρόβλημα τονίζει τα ζητήματα των επιδόσεων των αντικειμένων, όπως οι δυνατότητες αποθήκευσης και επεξεργασίας, αλλά και η κατανάλωση ενέργειας [214]. Ένα σημαντικό πρόβλημα που σχετίζεται με την επεκτασιμότητα είναι η παροχή απρόσκοπτης συνδεσιμότητας με σκοπό τη διευκόλυνση της προσθήκης νέων στοιχείων και αντικειμένων στο σύστημα IoT, καθώς και την υποστήριξη αλλαγών της τοπολογίας του. Η δικτύωση CCN στην επόμενη γενιά αρχιτεκτονικής δικτύου θα μπορούσε να αποτελέσει λυση των προβλημάτων αυτών, εστιάζοντας στα θέματα της επεκτασιμότητας, της κινητικότητας και της ασφάλειας [215].

5.8 Ποιότητα QoS

Τα χαρακτηριστικά της ποιότητας QoS, όπως η καθυστέρηση, το jitter, η απώλεια πακέτων και η αξιοπιστία, πρέπει να λαμβάνονται υπόψη σε όλα τα στρώματα της αρχιτεκτονικής του δικτύου. Η βελτιστοποίηση της κατανομής πόρων ενός δικτύου οδηγεί στη βελτίωση της ποιότητας QoS. Όσον αφορά τις εφαρμογές IoT που παρουσιάζουν ευαισθησία στις καθυστερήσεις, θα πρέπει να λαμβάνεται υπόψη ότι τα δίκτυα υποδομής cloud παρουσιάζουν ζητήματα όσον αφορά τις επιδόσεις τους (π.χ. καθυστερήσεις, εύρος ζώνης, συμφόρηση, αξιοπιστία), τα οποία, όπως έχει ήδη αναφερθεί, προκαλούνται από τη μεταφορά του τεράστιου όγκου δεδομένων που έχουν συλλεχθεί από τις συσκευές παρυφών στο cloud [216].

Το cloud computing δεν επαρκεί για τη διαχείριση περιπτώσεων υποστήριξης της κινητικότητας, της γεωγραφικής κατανομής και της επίγνωσης της τοποθεσίας σε πραγματικό χρόνο [217]. Η χρήση τεχνολογιών, όπως οι edge computing, MCC, MEC, Cloudlet και fog computing θα μπορούσε να αποτελέσει τρόπος αντιμετώπισης αυτών των περιορισμών του cloud. Η αρχιτεκτονική σε επίπεδο συστήματος όλων αυτών των τεχνολογιών επιτρέπει τη διανομή πόρων, διαδικασιών και υπηρεσιών σε κέντρα δεδομένων που βρίσκονται πιο κοντά στις παρυφές του δικτύου. Με τον τρόπο αυτό επιτυγχάνουν την ύπαρξη μικρού λανθάνοντα χρόνου σε εφαρμογές IoT πραγματικού χρόνου, για τις οποίες η καθυστέρηση είναι ζωτικής σημασίας. Οι τεχνολογίες edge computing παρέχουν επίσης καλύτερη ποιότητα QoS με γνώμονα τον καλύτερο χρόνο απόκρισης, το jitter, την απόδοση και τη δυναμική προσαρμογή στους διαθέσιμους πόρους [218]. Παρόλα αυτά, το ζήτημα των υπολογιστικών περιορισμών που παρουσιάζουν, δεν επιτρέπει τη χρήση τους σε όλες τις περιπτώσεις. Για να ξεπεραστεί ο περιορισμός αυτός, προτείνεται η αρχιτεκτονική IFCIoT (Integrated Fog Cloud IoT). Η ενσωμάτωση του IoT με τις τεχνολογίες fog / cloud δημιουργεί νέα ζητήματα, τα οποία εξακολουθούν να είναι ανοιχτά, όπως η μέτρηση υπολογισμού (π.χ. κατανομή πόρων και λειτουργιών) και η ανάπτυξη δυναμικών αλγορίθμων κατανομής πόρων [219].

5.9 Κατανάλωση ενέργειας

Οι τεχνολογίες αποθήκευσης ενέργειας πρέπει να πληρούν διάφορες απαιτήσεις των συστημάτων IoT, όπως η παροχή πηγών ενέργειας για τις συσκευές. Η παροχή αξιόπιστης ισχύος στους αισθητήρες και τις συσκευές, καθώς και η ανάπτυξη chipset χαμηλής ισχύος θεωρείται ως μία πολύ σημαντική πρόκληση [220]. Μια πολλά υποσχόμενη λύση σε αυτό το ζήτημα αποτελεί η χρήση ασύρματων τεχνολογιών ισχύος, οι οποίες μπορούν να μεταδώσουν ισχύ σε κάποια απόσταση, αλλά βρίσκονται ακόμη στην αρχική φάση ανάπτυξής τους.

Μια άλλη σημαντική πρόκληση όσον αφορά την κατανάλωση ενέργειας αποτελεί η ενσωμάτωση δυνατοτήτων υπολογισμού στις συσκευές μικρής κατανάλωσης ενέργειας, ιδίως στην περίπτωση εφαρμογών που βασίζονται στην επεξεργασία εικόνας και βίντεο. Ένα από τα κύρια ζητήματα αφορά τη βελτίωση των δυνατοτήτων των συσκευών με ταυτόχρονη

μείωση της ενέργειας που καταναλώνουν, αλλά και του κόστους κατασκευής τους. Επίσης, η δημιουργία μιας στοίβας επικοινωνίας χαμηλής ισχύος αποτελεί μία ακόμα πρόκληση, όσον αφορά την ενεργειακή απόδοση των συστημάτων IoT [90].

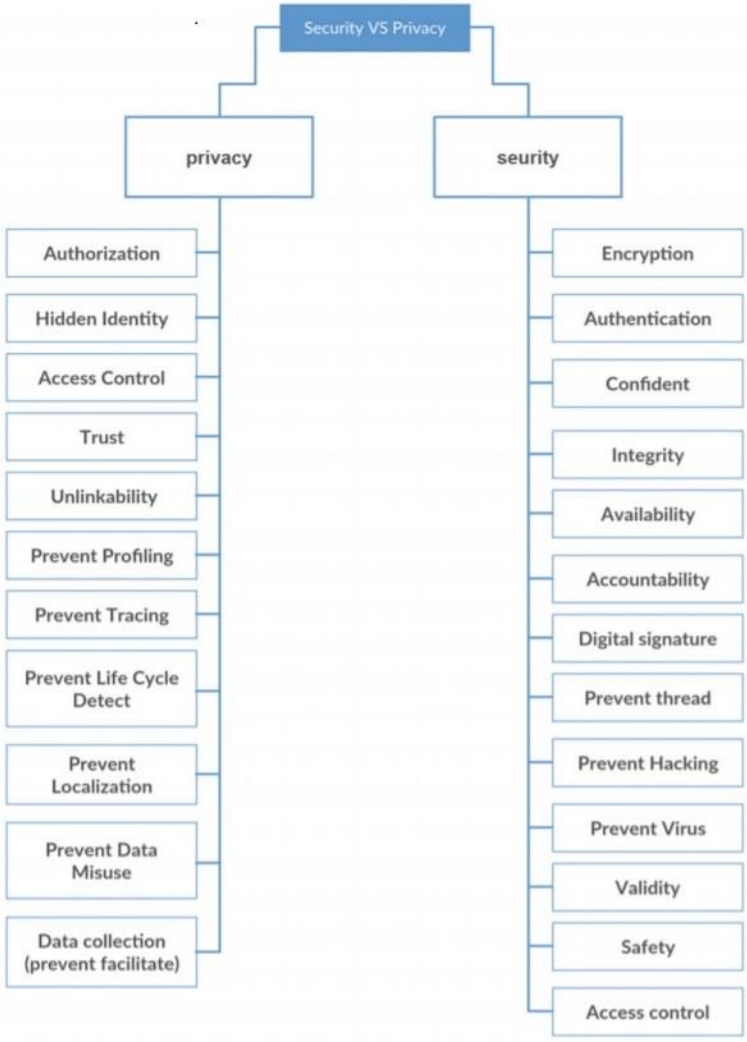
Η χρήση πρωτοκόλλων επικοινωνίας στο IoT, όπως τα HTTP και TCP, δεν μπορεί να θεωρηθεί βέλτιστη, καθώς η φιλοσοφία τέτοιων πρωτοκόλλων δεν αφορά τα συστήματα χαμηλής ισχύος. Η ενεργειακή απόδοση του πρωτοκόλλου MAC και ο σχεδιασμός ενός κατάλληλου πρωτοκόλλου δρομολόγησης θεωρούνται ως κρίσιμοι παράγοντες για την ενεργειακή αποτελεσματικότητα ενός συστήματος [221]. Οι οργανισμοί τυποποίησης, όπως οι ITU-T, IETF, ISO, IEEE, κλπ., έχουν ορίσει αρκετά πρωτόκολλα και διεπαφές στο στρώμα επικοινωνίας των συστημάτων χαμηλής ισχύος, αλλά οι πρακτικές εφαρμογές τους εξακολουθούν να μην είναι ικανοποιητικές. Μία από τις προτεινόμενες λύσεις αφορά το IEEE 802.15.4 και τις βελτιώσεις του, όπως το IEEE 802.15.4e. Το συγκεκριμένο πρότυπο καθορίζει τα επίπεδα PHY και MAC για τη χαμηλή ισχύ, αλλά εξακολουθεί να είναι ακατάλληλο για δίκτυα χαμηλής ισχύος πολλαπλών αλμάτων [90].

Ένας άλλος τομέας έρευνας περιλαμβάνει τη βελτιστοποίηση των τεχνικών δρομολόγησης για τη μείωση των ενεργειακών απαιτήσεων και τη βελτιστοποίηση της κατανάλωσης ενέργειας. Για παράδειγμα, η εξάλειψη του πλεονασμού δεδομένων θα μειώσει τις ενεργειακές απαιτήσεις όσον αφορά τη δρομολόγηση των δεδομένων. Κάποιες νέες τεχνολογίες, όπως το παράδειγμα δικτύωσης γνωστό ως IoNT (Internet of Nano-Things), μπορούν να μειώσουν την κατανάλωση ενέργειας, αλλά βρίσκονται ακόμη σε φάση ανάπτυξης [220].

5.10 Ασφάλεια και προστασία της ιδιωτικότητας

Τα ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας αναγνωρίζονται ως οι βασικότερες προκλήσεις της ανάπτυξης λύσεων IoT, καθώς το IoT ως τεχνολογία αντιμετωπίζει πολλές μορφές απειλών, ευπαθειών και κινδύνων [181]. Σύμφωνα με μελέτη των Abi Sen και συν. (2018), ζητήματα όπως, ο ανεπαρκής έλεγχος ταυτότητας και

εξουσιοδότησης, η έλλειψη κρυπτογράφησης μεταφοράς, η μη ασφαλής διασύνδεση του Ιστού, η χρήση μη ασφαλούς λογισμικού και υλικολογισμικού, κλπ., είναι οι λόγοι για τους οποίους δημιουργούνται ανησυχίες σχετικά με τη διατήρηση της ιδιωτικότητας των συσκευών IoT [222]. Το θέμα των μοντέλων ασφάλειας και της ταξινόμησης των απειλών που καλούνται να αντιμετωπίσουν τα συστήματα IoT είναι ιδιαίτερα δημοφιλές στην ακαδημαϊκή και ερευνητική κοινότητα. Στην εικόνα 5-1 παρουσιάζονται τα πιο συνηθισμένα θέματα ασφάλειας και διατήρησης της ιδιωτικότητας του IoT [222].



Εικόνα 5-1: Ζητήματα ασφάλειας και ιδιωτικότητας IoT [222]

Η ασφάλεια και η προστασία της ιδιωτικότητας βασίζεται σε μια σειρά κανόνων, όπως η ασφάλεια των πληροφοριών (εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) ή οι βασικοί πυλώνες διασφάλισης των πληροφοριών (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα, αυθεντικότητα και μη αποκήρυξη) [223]. Σε κάθε στρώμα της αρχιτεκτονικής του IoT θα πρέπει να υπάρχουν λειτουργίες που να επιτρέπουν την αποτελεσματική διαχείριση των παραπάνω κανόνων [224]. Η επίτευξη κάτι τέτοιου προκύπτει από την ανάπτυξη και εξέλιξη διαφόρων μηχανισμών ασφάλειας και προστασίας της ιδιωτικότητας, η χρήση των οποίων μεταβάλει και εξελίσσει ταυτόχρονα ολόκληρη την αρχιτεκτονική ασφάλειας του IoT [225]. Οι μηχανισμοί ασφάλειας θα πρέπει να παρέχουν έλεγχο ταυτότητας, έλεγχο πρόσβασης, ακεραιότητα δεδομένων, διατήρηση απορρήτου, κρυπτογράφηση και άλλες δυνατότητες, επιτρέποντας ταυτόχρονα την αυτόματη επεξεργασία των δεδομένων, με βάση τις πολιτικές και τους κανόνες που έχουν διαμορφωθεί από τους χρήστες. Αυτοί οι μηχανισμοί πρέπει να λειτουργούν σε πραγματικό χρόνο και πρέπει να είναι οικονομικά αποδοτικοί και επεκτάσιμοι για την ελαχιστοποίηση της πολυπλοκότητας και τη μεγιστοποίηση της χρηστικότητας.

Ένα βασικό ζήτημα είναι η έλλειψη λύσης για το πρόβλημα της προστασίας κλοπής ταυτότητας στο IoT (Identity Theft Prevention - ITP), κάτι που σημαίνει ότι το σύστημα εξουσιοδότησης του IoT θα πρέπει να ενημερώνεται συνεχώς με γνώμονα το πλαίσιο [226]. Για παράδειγμα, τα αντικείμενα IoT θα πρέπει να γνωρίζουν την τοποθεσία για να παρέχουν ισχυρή ασφάλεια. Τα ζητήματα ασφάλειας είναι περισσότερο εμφανή σε ετερογενή περιβάλλοντα και λόγω της προοπτικής τυποποίησης της ανταλλαγής δεδομένων [227]. Τα περισσότερα ζητήματα ασφαλείας σχετίζονται με απειλές κατά της επικοινωνίας, οι οποίες εκφράζονται με τη μορφή επιθέσεων, όπως: επιθέσεις κακόβουλου κώδικα, επιθέσεις υποκλοπής (sniffing attacks), επιθέσεις ηλεκτρονικού ψαρέματος τύπου spear (spear-phishing attacks), επιθέσεις άρνησης υπηρεσίας (Denial-of-Service attacks - DoS), σιβυλλικές επιθέσεις (Sybil attacks), επιθέσεις ενδιάμεσου (proxy attacks), επιθέσεις εξάντλησης πόρων (sleep deprivation attacks), κλπ. Λόγω της ύπαρξης τέτοιου είδους επιθέσεων απαιτείται η ανάπτυξη διάφορων μηχανισμών ασφάλειας, όπως εξουσιοδότηση, έλεγχος ταυτότητας, κρυπτογράφηση, προστασία κατά των ιών, κλπ.

Τα συστήματα IoT απαιτούν αξιόπιστα και ασφαλή πρωτόκολλα επικοινωνίας σε όλα τα στρώματα της στοίβας πρωτοκόλλων. Η καλύτερη λύση για την παροχή ασφάλειας με ιδιαίτερα χαρακτηριστικά, αφορά την ανάπτυξη ενός προσαρμοσμένου πρωτοκόλλου ασφαλείας στο στρώμα εφαρμογών, αλλά ο σχεδιασμός ενός τέτοιου πρωτοκόλλου είναι πολύ περίπλοκος [228]. Ορισμένα πρότυπα και πρωτόκολλα, όπως το OTrP (Open Trust Protocol) χρησιμοποιούνται από τις εφαρμογές για τη διαχείριση της διαμόρφωσης της ασφάλειας [229]. Μια άλλη λύση για τη βελτίωση της ασφάλειας είναι η χρήση του πρωτοκόλλου IPSec, το οποίο όμως δεν είναι κατάλληλο για όλες τις εφαρμογές IoT. Παρόλα αυτά, η εκτέλεσή του πάνω από το TLS (Transport Layer Security) είναι πολύ εύκολη [230]. Ορισμένα πρωτόκολλα εφαρμογών IoT χρησιμοποιούν άλλες μεθόδους για την ενίσχυση της ασφάλειας, αλλά οι περισσότερες λύσεις βασίζονται σε πρωτόκολλα κρυπτογράφησης, όπως το SSL (Secure Sockets Layer) και το DTLS (Datagram Transport Layer Security). Αυτά τα πρωτόκολλα εφαρμόζονται μεταξύ των στρωμάτων εφαρμογών και μεταφοράς της στοίβας πρωτοκόλλων TCP/IP. Το TLS πρέπει να εκτελείται πάνω από ένα αξιόπιστο κανάλι μεταφοράς (συνήθως TCP), αλλά επειδή ορισμένες εφαρμογές IoT προτιμούν να χρησιμοποιούν το UDP, απαιτείται η χρήση μιας συμβατής με datagram παραλλαγής του TLS, όπως το DTLS. Το DTLS είναι ένα πρωτόκολλο που βασίζεται στο TLS και παρέχει ισοδύναμες εγγυήσεις ασφαλείας για πρωτόκολλα datagram [231]. Τα πρωτόκολλα ασφαλείας χρησιμοποιούν διάφορους μηχανισμούς και πρότυπα, όπως το X.509 που χρησιμοποιείται για τη διαχείριση ψηφιακών πιστοποιητικών και κρυπτογράφησης δημόσιου κλειδιού στο TLS. Το CoAP χρησιμοποιεί το DTLS ενώ μια συμπιεσμένη έκδοση του DTLS χρησιμοποιείται στο Lightweight Secure CoAP για το IoT. Τα XMPP και AMQP χρησιμοποιούν τα TLS και SASL (Simple Authentication and Security Layer) ως πρωτόκολλα ασφάλειας. Το πρωτόκολλο MQTT βασίζεται κυρίως στη χρήση του TLS/SSL [60], αλλά κάποιες παραλλαγές του, όπως το OASIS MQTT, χρησιμοποιούν πλαίσιο κυβερνοασφάλειας ή το νέο μηχανισμό ασφάλειας MQTT, που ονομάζεται AUPS (AUthenticated Publish & Subscribe) [232].

Ο κίνδυνος ασφάλειας γίνεται περισσότερο εμφανής όταν το σύστημα IoT χρησιμοποιεί τεχνολογίες ασύρματων επικοινωνιών. Στην περίπτωση αυτή, απαιτείται η ανάπτυξη μηχανισμών ανίχνευσης κακόβουλων δραστηριοτήτων και μηχανισμών ανάκτησης (αυτοθεραπείας). Το IPSec παρέχει ασφάλεια από άκρο σε άκρο στο στρώμα δικτύου και μπορεί να χρησιμοποιηθεί με διάφορα πρωτόκολλα μεταφοράς. Η ασφάλεια του στρώματος σύνδεσης περιορίζεται στην παροχή ασφαλούς επικοινωνίας μεταξύ των συσκευών και επιτυγχάνεται με χρήση αποτελεσματικών αλγόριθμων κρυπτογράφησης [226]. Η κρυπτογράφηση είναι ένα από τα βασικά στοιχεία της διασφάλισης της ασφάλειας των πληροφοριών, αλλά στη περίπτωση μεγάλου όγκου δεδομένων που πρέπει να μεταφερθούν σε πραγματικό χρόνο, τότε η κρυπτογράφησή τους αποτελεί πραγματική πρόκληση. Οι αλγόριθμοι κρυπτογράφησης πρέπει επίσης να είναι ενεργειακά αποδοτικοί. Το χαρακτηριστικό αυτό αποτελεί πρόκληση, όσον αφορά την εφαρμογή πολύπλοκων σχημάτων βελτίωσης της ασφάλειας, σε περιβάλλοντα όπου τα συστατικά IoT πρέπει να καταναλώνουν μικρά ποσά ενέργειας.

Συμπεράσματα

Το Διαδίκτυο των Πραγμάτων (IoT) αποτελεί μια συμβολή πολλών τεχνολογιών που επιτρέπουν την παροχή διαδικτυακών υπηρεσιών και εφαρμογών, οι οποίες υποστηρίζονται από ηλεκτρονικές συσκευές που συνδέονται με φυσικά πράγματα για τη συλλογή δεδομένων και την πραγματοποίηση διαδικασιών ελέγχου. Στη βιβλιογραφία έχει παρουσιαστεί μια ποικιλία ορισμών που έχουν προσπαθήσει να ορίσουν αυτή την πολύπλοκη τεχνολογία. Αν και αυτοί οι ορισμοί ενδέχεται να εμφανίζουν μια απόκλιση, συνήθως εστιάζονται γύρω από τα πέντε βασικά στοιχεία του IoT: τη δικτύωση, τις υπηρεσίες, τις επικοινωνίες, τα δεδομένα και τα πράγματα. Οι αρχικοί ορισμοί του IoT επικεντρώνονταν στο στοιχείο της δικτύωσης, ενώ οι πιο πρόσφατοι τείνουν να είναι πιο περιεκτικοί, καθώς η τεχνολογία βρίσκεται στο στάδιο της ωρίμανσης και το εύρος χρήσης της αρχίζει να διευρύνεται, αποκαλύπτοντας συνεχώς περισσότερες δυνατότητες.

Σκοπός της παρούσας εργασίας, ήταν η παρουσίαση μιας όσο το δυνατόν πιο ολοκληρωμένης βιβλιογραφικής ανασκόπησης του IoT, με βάση τις πλέον πρόσφατες εξελίξεις σε διάφορες πτυχές του, όπως είναι οι χρησιμοποιούμενες τεχνολογίες, οι εφαρμογές και οι προκλήσεις που αντιμετωπίζει. Το IoT πρέπει να επιτρέπει την απρόσκοπτη συνδεσιμότητα ανά πάσα στιγμή, οπουδήποτε, από οποιονδήποτε και οτιδήποτε, με σκοπό την παροχή έξυπνων υπηρεσιών, όπως δυνατότητες αναγνώρισης, ανίχνευσης, δικτύωσης, επεξεργασίας και οπτικοποίησης. Η ιδέα του δημιούργησε πολλές νέες δυνατότητες για υπηρεσίες μεγάλης κλίμακας και ανάπτυξη προϊόντων που προκάλεσαν τεράστιες καινοτομίες και νέες επιχειρηματικές ευκαιρίες.

Το IoT έχει τόσες πολλές δυνατότητες ώστε η πλήρης υιοθέτησή του μπορεί να έχει τεράστιο κοινωνικό, περιβαλλοντικό και οικονομικό αντίκτυπο. Συνδέοντας δισεκατομμύρια πράγματα στο Διαδίκτυο, το IoT δημιούργησε μια πληθώρα εφαρμογών που αγγίζουν κάθε πτυχή της ανθρώπινης ζωής, όπως τα wearable και η παρακολούθηση της κατάστασης των ασθενών, οι στρατιωτικές εφαρμογές ανίχνευσης εισβολέων, η περιβαλλοντική παρακολούθηση, τα έξυπνα σπίτια, οι έξυπνες πόλεις, τα έξυπνα δίκτυα παροχής ενέργειας και πολλές άλλες.

Μέσα από την παρουσίαση κάποιων από αυτές τις εφαρμογές, προκύπτει το συμπέρασμα ότι το IoT έχει να αντιμετωπίσει διάφορες προκλήσεις, όπως η διατήρηση του απορρήτου των δεδομένων και η κλιμάκωση στις εφαρμογές υγειονομικής περίθαλψης, η εξουσιοδότηση και το υψηλό κόστος υλοποίησης στις περιβαλλοντικές εφαρμογές, η κινητικότητα και η αρχιτεκτονική δομή στις εφαρμογές έξυπνης πόλης, το κόστος και οι δυσκολίες υλοποίησης στις εμπορικές εφαρμογές και τα προβλήματα παραγωγής στις βιομηχανικές εφαρμογές. Σε πολλές από τις εφαρμογές αυτές θα μπορούσαν να αξιοποιηθούν περισσότερο κάποιες από τις αναδυόμενες τεχνολογίες, όπως το blockchain, προκειμένου να ενισχυθεί η υπάρχουσα απόδοση της δομής ή να αναπτυχθούν πιο εξελιγμένα συστήματα. Κάτι τέτοιο θα μπορούσε να βοηθήσει στην επίτευξη επιπλέον ασφάλειας, στην αυτοματοποίηση της διαχείρισης των επιχειρήσεων, στη δημιουργία κατανεμημένων πλατφορμών και σε πολλά άλλα.

Η ύπαρξη όμως διαφόρων προσεγγίσεων, καθώς και η έλλειψη συντονισμού μεταξύ των προτύπων και των τεχνολογιών που ενσωματώνονται στο πλαίσιο του IoT, δημιουργούν μια σειρά νέων προκλήσεων για μελλοντική έρευνα. Οι λύσεις που βασίζονται σε IoT έχουν γίνει πιο προηγμένες και εξελιγμένες, ενώ δεν υπάρχει ένα ολοκληρωμένο πλαίσιο που να ενσωματώνει όλα τα πρότυπα και τις τεχνολογίες. Κάτι τέτοιο δημιουργεί πολλά θέματα, που προκύπτουν λόγω του αυξανόμενου αριθμού των συνδεδεμένων συσκευών, της ενσωμάτωσης διαφόρων τεχνολογιών, των αυξημένων απαιτήσεων κυκλοφορίας, των απαιτήσεων αποθήκευσης και επεξεργασίας των πρωτογενών δεδομένων, των κινδύνων διατήρησης του απορρήτου και ασφάλειας κλπ.

Οι συνεχώς δημιουργούμενες εφαρμογές IoT και οι αναδυόμενες τεχνολογίες δημιουργούν νέες προκλήσεις που απαιτούν προσοχή από την ερευνητική κοινότητα. Ένα από τα πιο ελκυστικά μελλοντικά ερευνητικά θέματα σχετίζεται με την ενσωμάτωση του IoT με αναδυόμενες τεχνολογίες, όπως οι υβριδικές πλατφόρμες cloud, καθώς και οι MCC, MEC, fog computing, cloudlet, νανοτεχνολογίες κλπ. Αυτές οι λύσεις μπορούν να δημιουργήσουν μια πρωτοποριακή μελλοντική ανάπτυξη του IoT με νέες αρχιτεκτονικές δομές, όπως το Cloud of Things ή το Διαδίκτυο των νανο-πραγμάτων (IoNT). Επίσης, η ενοποίηση του IoT με τις υπάρχουσες τεχνολογίες ιστού δημιουργεί μια νέα έννοια που ακούει στο όνομα Ιστός

των Πραγμάτων (Web of Things - WoT), μια έννοια που θα μπορούσε να παρέχει ακόμη ευρύτερο φάσμα νέων δυνατοτήτων και λειτουργιών.

Ωστόσο, παρά τις τεράστιες ερευνητικές προσπάθειες πολλά ζητήματα και προκλήσεις παραμένουν ακόμα ανοιχτά. Τα ζητήματα ασφάλειας και διατήρησης του απορρήτου αποτελούν σημαντικά θέματα, η επίλυση των οποίων θα μπορούσε να οδηγήσει στην εξέλιξη του IoT ως μια παγκόσμια εφαρμοζόμενη τεχνολογία του μέλλοντος. Επί του παρόντος πάντως, η φύση του IoT το καθιστά ευαίσθητο σε πολλούς κινδύνους και απειλές που μπορεί να επιτρέψουν υποκλοπές ή πρόσβαση στα προσωπικά δεδομένα των χρηστών και επομένως να προκαλέσουν πιθανή οικονομική, και όχι μόνο, ζημία. Επομένως, απαιτείται η δημιουργία προηγμένων και βελτιστοποιημένων αλγορίθμων και πρωτοκόλλων προστασίας του απορρήτου αυτών των δεδομένων.

Ως γενικό συμπέρασμα μπορεί να θεωρηθεί ότι ο σχεδιασμός ενός ενεργειακού και οικονομικά αποδοτικού έξυπνου δικτύου με πιθανή επιχειρηματική ανάπτυξη για συστήματα IoT, μπορεί να οδηγήσει στη δημιουργία ενός ενοποιημένου μοντέλου ανάπτυξης που θα χρησιμοποιηθεί ως πλατφόρμα χρήσης της τεχνολογίας σε όλους ανεξαιρέτως τους τομείς που καθορίζουν την καθημερινότητα των ανθρώπων και θα μπορούσαν να βελτιώσουν σε μέγιστο βαθμό τις συνθήκες διαβίωσης.

Βιβλιογραφία

[1] Pawar, A. B., & Ghumbre, S. (2016, December). A survey on IoT applications, security challenges and counter measures. In 2016 International Conference on Computing, Analytics and Security Trends (CAST) (pp. 294-299). IEEE.

[2] Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. Sensors, 20(9), 2495.

[3] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

[4] Alansari, Z., Anuar, N. B., Kamsin, A., Belgaum, M. R., Alshaer, J., Soomro, S., & Miraz, M. H. (2018, August). Internet of things: infrastructure, architecture, security and privacy. In 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE) (pp. 150-155). IEEE.

[5] Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer networks, 54(15), 2787-2805.

[6] Dorsemaine, B., Gaulier, J. P., Wary, J. P., Kheir, N., & Urien, P. (2015, September). Internet of things: a definition & taxonomy. In 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies (pp. 72-77). IEEE.

[7] Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, 1(1), 1-86.

[8] Thaler, D., Tschofenig, H., & Barnes, M. (2015). Architectural considerations in smart object networking.

[9] Nepali, S. (2020). The Secure and Energy Efficient Data Routing in the IoT based Network. MSc thesis, Master's Programme in Computer Science. Faculty of Science University of Helsinki.

[10] Miller, M. (2015). The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world. Pearson Education.

[11] Suryadevara, N. K., & Mukhopadhyay, S. C. (2015). Smart Homes. Berlin, Germany: Springer.

[12] Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2015). Middleware for internet of things: a survey. IEEE Internet of things journal, 3(1), 70-95.

[13] Dash, A., Pal, S., & Hegde, C. (2018). Ransomware Auto-Detection in IoT Devices using Machine Learning. no. December, 0-10.

[14] Gupta, B. B., & Quamara, M. (2020). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience, 32(21), e4946.

[15] Khanna, A., & Kaur, S. (2019). Evolution of Internet of Things (IoT) and its significant impact in the field of Precision Agriculture. Computers and Electronics in Agriculture, 157, 218–231.

[16] Holst, A. (2021, January). Internet of Things - active connections worldwide 2015-2025. Statista. https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ (Προσπελάστηκε την 19 ΙΑΝ 2021).

[17] Holst, A. (2021, January). Global IoT end-user spending worldwide 2017-2025. Statista. https://www.statista.com/statistics/976313/global-iot-market-size/ (Προσπελάστηκε την 19 ΙΑΝ 2021).

[18] Linden, A., & Fenn, J. (2003). Understanding Gartner's hype cycles. Strategic Analysis Report Nº R-20-1971. Gartner, Inc, 88.

[19] Gartner. (2020, September). Gartner's Hype Cycle: IoT in "trough" but transformational stage on the way. Gartner. https://www.mmh.com/article/gartners_hype_cycle_iot_in_trough_but_transformational_stage_on_the_way (Προσπελάστηκε την 19 ΙΑΝ 2021).

[20] Stead, M. (2017). Spimes and speculative design: Sustainable product futures today. Strategic Design Research Journal, 10(1), 12-22.

[21] Silverio-Fernández, M., Renukappa, S., & Suresh, S. (2018). What is a smart device?-a conceptualisation within the paradigm of the internet of things. Visualization in Engineering, 6(1), 3.

[22] Khan, A. (2017). Microservices in context: Internet of Things: Infrastructure and Architecture. Master Thesis Project. Computer Science. Linnaeus University.

[23] Ibarra-Esquer, J. E., González-Navarro, F. F., Flores-Rios, B. L., Burtseva, L., & Astorga-Vargas, M. A. (2017). Tracking the evolution of the internet of things concept across different application domains. Sensors, 17(6), 1379.

[24] de Souza-Leão, A. L. M., & da Nóbrega Costa, F. Z. (2018). Assemblaged by desire: potterheads' productive consumption. RAE, 58(1).

[25] Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2018). How can heterogeneous Internet of Things build our future: A survey. IEEE Communications Surveys & Tutorials, 20(3), 2011-2027.

[26] Abane, A., Daoui, M., Bouzefrane, S., Banerjee, S., & Muhlethaler, P. (2020). A Realistic Deployment of Named Data Networking in the Internet of Things. Journal of Cyber Security and Mobility, 1-46.

[27] Thoelen, K. (2016). An Application Platform for Multi-purpose Sensor Systems. Dissertation for the degree of Doctor in Computer Science. Universiteit Antwerpen.

[28] Pal, A., Rath, H. K., Shailendra, S., & Bhattacharyya, A. (2018). IoT standardization: the road ahead. In Internet of Things-Technology, Applications and Standardization (pp. 53-74). IntechOpen.

[29] Gomes, T., Salgado, F., Pinto, S., Cabral, J., & Tavares, A. (2017). A 6LoWPAN accelerator for Internet of Things endpoint devices. IEEE Internet of Things Journal, 5(1), 371-377.

[30] Singh, D., Tripathi, G., & Jara, A. J. (2014, March). A survey of Internet-of-Things: Future vision, architecture, challenges and services. In 2014 IEEE world forum on Internet of Things (WF-IoT) (pp. 287-292). IEEE.

[31] Maarala, A. I., Su, X., & Riekki, J. (2016). Semantic reasoning for context-aware Internet of Things applications. IEEE Internet of Things Journal, 4(2), 461-473.

[32] Chaqfeh, M. A., & Mohamed, N. (2012, May). Challenges in middleware solutions for the internet of things. In 2012 international conference on collaboration technologies and systems (CTS) (pp. 21-26). IEEE.

[33] De, S., Zhou, Y., & Moessner, K. (2017). Ontologies and context modeling for the Web of Things. In Managing the Web of Things (pp. 3-36). Morgan Kaufmann.

[34] Alrae, R., Nasir, Q., & Abu Talib, M. (2020). Developing House of Information Quality framework for IoT systems. International Journal of System Assurance Engineering and Management.

[35] Zikria, Y. B., Yu, H., Afzal, M. K., Rehmani, M. H., & Hahm, O. (2018). Internet of things (IoT): Operating system, applications and protocols design, and validation techniques.

[36] Rashid, M., Nazeer, I., Gupta, S. K., & Khanam, Z. (2020). Internet of Things: Architecture, Challenges, and Future Directions. In Emerging Trends and Impacts of the Internet of Things in Libraries (pp. 87-104). IGI Global.

[37] Imani, M., Qiyasi, A., Zarif, N., Ali, M., Noshiri, O., Faramarzi, K., ... & Joudaki, M. (2020). A survey on subjecting electronic product code and non-ID objects to IP identification. Engineering Reports, 2(6), e12171.

[38] Sparber, T., Boano, C. A., Kanhere, S. S., & Römer, K. (2017). Mitigating radio interference in large iot networks through dynamic cca adjustment. Open Journal of Internet Of Things (OJIOT), 3(1), 103-113.

[39] Bilal, M. (2017). A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3D printers. arXiv preprint arXiv:1708.04560.

[40] Sharma, V., Sharma, V., & Mishra, N. (2018). Internet of Things: Concepts, Applications, and Challenges. In Exploring the Convergence of Big Data and the Internet of Things (pp. 73-95). IGI Global.

[41] Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1–31.

[42] Chandrashekhar, K. (2016, September). Internet of Things (IoT) Characteristics. Linkedin. https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c (Προσπελάστηκε την 22 IAN 2021).

[43] Muntjir, M., Rahul, M., & Alhumyani, H. A. (2017). An analysis of Internet of Things (IoT): novel architectures, modern applications, security aspects and future scope with latest case studies. Int. J. Eng. Res. Technol, 6(6), 422-447.

[44] Trakadas, P., Simoens, P., Gkonis, P., Sarakis, L., Angelopoulos, A., Ramallo-González, A. P., ... & Karkazis, P. (2020). An Artificial Intelligence-Based Collaboration Approach in Industrial IoT Manufacturing: Key Concepts, Architectural Extensions and Potential Applications. Sensors, 20(19), 5480.

[45] Comark. Internet of Things. https://comarkcorp.com/internet-of-things/ Προσπελάστηκε την 22 IAN 2021).

[46] Madakam, S., Lake, V., Lake, V., & Lake, V. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.

[47] Tohanean, D., & Vasilescu, A. (2019, May). Business Models and Internet of Things. In Proceedings of the International Conference on Business Excellence (Vol. 13, No. 1, pp. 1192-1203). Sciendo.

[48] Narendra, M. (2019, September). Research reveals the most vulnerable IoT devices. PrivSec Report. https://gdpr.report/news/2019/06/12/research-reveals-the-most-vulnerable-iot-devices/ (Προσπελάστηκε την 24 IAN 2021).

[49] Arpita, R., Saxena, K. & Bhadra, A.A. (2015, April). Internet of Things. International Journal of Engineering Studies and Technical Approach (IJESTA), Volume 01, No4., pp 36-42.

[50] Banafa, A. (2017). IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things.

[51] Light, D. (2014). The Internet of Things and Property/Casualty Insurance. Celent. https://www.celent.com/insights/877355504 (Προσπελάστηκε την 26 IAN 2021).

[52] Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. Procedia computer science, 132, 109-117.

[53] Calihman, A. (2019, January). Architectures in the IoT Civilization. NetBurner. https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/ (Προσπελάστηκε την 27 IAN 2021).

[54] Lv, W., Meng, F., Zhang, C., Lv, Y., Cao, N., & Jiang, J. (2017). A General Architecture of IoT System. 22017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC).

[55] Hammoudi, S., Aliouat, Z., & Harous, S. (2018). Challenges and research directions for Internet of Things. Telecommunication Systems, 67(2), 367-385.

[56] Fremantle, P. (2015). A reference architecture for the internet of things. WSO2 White paper.

[57] Aman, A. H. M., Yadegaridehkordi, E., Attarbashi, Z. S., Hassan, R., & Park, Y. J. (2020). A survey on trend and classification of internet of things reviews. IEEE Access, 8, 111763-111782.

[58] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. IEEE wireless communications, 24(3), 10-16.

[59] Aman, A. H. M., Yadegaridehkordi, E., Attarbashi, Z. S., Hassan, R., & Park, Y. J. (2020). A survey on trend and classification of internet of things reviews. IEEE Access, 8, 111763-111782.

[60] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). "Internet of things: A survey on enabling technologies, protocols, and applications". IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[61] Ali, I., Sabir, S., & Ullah, Z. (2019). Internet of things security, device authentication and access control: a review. arXiv preprint arXiv:1901.07309.

[62] Alshohoumi, F., Sarrab, M., AlHamadani, A., & Al-Abri, D. (2019). Systematic review of existing iot architectures security and privacy issues and concerns. Int. J. Adv. Comput. Sci. Appl, 10(7), 232-251.

[63] Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. Sensors, 18(9), 2796.

[64] Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), 2233-2243.

[65] Ghirardello, K., Maple, C., Ng, D., & Kearney, P. (2018). Cyber security of smart homes: Development of a reference architecture for attack surface analysis.

[66] Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018). Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. Journal of Hardware and Systems Security, 2(2), 97-110.

[67] Sobral, J. V., Rodrigues, J. J., Rabêlo, R. A., Al-Muhtadi, J., & Korotaev, V. (2019). Routing protocols for low power and lossy networks in internet of things applications. Sensors, 19(9), 2144.

[68] Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.

[69] Sabella, A., Irons-Mclean, R., & Yannuzzi, M. (2018). Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT. Cisco Press.

[70] Ahmadi, H., Arji, G., Shahmoradi, L., Safdari, R., Nilashi, M., & Alizadeh, M. (2019). The application of internet of things in healthcare: a systematic literature review and classification. Universal Access in the Information Society, 18(4), 837-869.

[71] Chaudhari, B. S., Zennaro, M., & Borkar, S. (2020). LPWAN technologies: Emerging application characteristics, requirements, and design considerations. Future Internet, 12(3), 46.

[72] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

[73] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80, 1-50.

[74] Bhushan, D., & Agrawal, R. (2020). Security challenges for designing wearable and IoT solutions. In A handbook of internet of things in biomedical and cyber physical system (pp. 109-138). Springer, Cham.

[75] Sakovich, N. (2018). Internet of Things (IoT) protocols and connectivity options: an overview.

[76] Leal Nadal, R. (2020). Smart City of Lappeenranta (Bachelor's thesis, Universitat Politècnica de Catalunya).

[77] Merenda, M., Porcaro, C., & Iero, D. (2020). Edge Machine Learning for AI-enabled IoT devices: a review. Sensors, 20(9), 2533.

[78] Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). The Internet of Things: Mapping the value beyond the hype. McKinsey & Company.

[79] Elahi, H., Munir, K., Eugeni, M., Atek, S., & Gaudenzi, P. (2020). Energy Harvesting towards Self-Powered IoT Devices. Energies, 13(21), 5528.

[80] Cook, S., Mathieu, B., Truong, P., & Hamchaoui, I. (2017, May). QUIC: Better for what and for whom?. In 2017 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[81] Doering, G., SpaceNet, A. G., Kumari, W., Huston, G., & Liu, W. (2021). IPv6 Operations Working Group (v6ops) F. Gont Internet-Draft SI6 Networks Intended status: Informational N. Hilliard Expires: July 6, 2021 INEX.

[82] Choi, Y., Choi, Y., Kim, D., & Park, J. (2017, February). Scheme to guarantee IP continuity for NFC-based IoT networking. In 2017 19th International Conference on Advanced Communication Technology (ICACT) (pp. 695-698). IEEE.

[83] Merenda, M., Iero, D., & G Della Corte, F. (2019). Cmos rf transmitters with on-chip antenna for passive RFID and iot nodes. Electronics, 8(12), 1448.

[84] Lazaro, A., Villarino, R., & Girbau, D. (2018). A survey of NFC sensors based on energy harvesting for IoT applications. Sensors, 18(11), 3746.

[85] Dekimpe, R., Xu, P., Schramme, M., Flandre, D., & Bol, D. (2018, July). A battery-less BLE IoT motion detector supplied by 2.45-GHz wireless power transfer. In 2018 28th International Symposium on Power and Timing Modeling, Optimization and Simulation (PATMOS) (pp. 68-75). IEEE.

[86] Bluetooth Special Interest Group (SIG). (2019). Bluetooth Core Specification Version 5.0. In Bluetooth Core Specif. Version 5.2; Bluetooth Special Interest Group (SIG): Kirkland, WA, USA, 2019. https://www.bluetooth.com/wp-content/uploads/2020/01/Bluetooth_5.2_Feature_Overview.pdf (Προσπελάστηκε την 31 ΙΑΝ 2021).

[87] Buthelezi, B. E., Mathonsi, T. E., Maswikaneng, S., & Mphahlele, M. (2017). Routing Schemes for ZigBee Low-Rate Power Personal Area Network: A Survey. In 11th International Conference on Data Mining, Computers, Communication and Industrial Applications (DMCCIA-2017).

[88] Yassein, M. B., Mardini, W., & Khalil, A. (2016, September). Smart homes automation using Z-wave protocol. In 2016 International Conference on Engineering & MIS (ICEMIS) (pp. 1-6). IEEE.

[89] Prisantama, A., Widyawan, & Mustika, I. W. (2016, July). Tunneling 6LoWPAN protocol stack in IPv6 network. In AIP Conference Proceedings (Vol. 1755, No. 1, p. 070006). AIP Publishing LLC.

[90] Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, 34(3), 510-527.

[91] Qiao, L., Zheng, Z., Cui, W., & Wang, L. (2018, October). A survey on Wi-Fi HaLow technology for Internet of Things. In 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2) (pp. 1-5). IEEE.

[92] Khorov, E., Krotov, A., & Lyakhov, A. (2015, June). Modelling machine type communication in IEEE 802.11 ah networks. In 2015 IEEE international conference on communication workshop (ICCW) (pp. 1149-1154). IEEE.

[93] Chiani, M., & Elzanaty, A. (2019). On the LoRa modulation for IoT: Waveform properties and spectral analysis. IEEE Internet of Things Journal, 6(5), 8463-8470.

[94] Augustin, A., Yi, J., Clausen, T., & Townsley, W. M. (2016). A study of LoRa: Long range & low power networks for the internet of things. Sensors, 16(9), 1466.

[95] Suresh, V. M., Sidhu, R., Karkare, P., Patil, A., Lei, Z., & Basu, A. (2018, February). Powering the IoT through embedded machine learning and LoRa. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 349-354). IEEE.

[96] Suresh, V. M., Sidhu, R., Karkare, P., Patil, A., Lei, Z., & Basu, A. (2018, February). Powering the IoT through embedded machine learning and LoRa. In 2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (pp. 349-354). IEEE.

[97] Coman, F. L., Malarski, K. M., Petersen, M. N., & Ruepp, S. (2019, June). Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT. In 2019 Global IoT Summit (GIoTS) (pp. 1-6). IEEE.

[98] GSMA, N. (2020). Programme,"Unlocking Commercial Opportunities–From 4G Evolution to 5G," 02/2016.

[99] Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE access, 6, 3619-3647.

[100] Fattah, H. (2018). 5G LTE Narrowband Internet of Things (NB-IoT). CRC Press.

[101] Ratasuk, R., Mangalvedhe, N., Zhang, Y., Robert, M., & Koskinen, J. P. (2016, October). Overview of narrowband IoT in LTE Rel-13. In 2016 IEEE conference on standards for communications and networking (CSCN) (pp. 1-7). IEEE.

[102] Borkar, S. R. (2020). Long-term evolution for machines (LTE-M). In LPWAN Technologies for IoT and M2M Applications (pp. 145-166). Academic Press.

[103] Wang, D., Chen, D., Song, B., Guizani, N., Yu, X., & Du, X. (2018). From IoT to 5G I-IoT: The next generation IoT-based intelligent algorithms and 5G technologies. IEEE Communications Magazine, 56(10), 114-120.

[104] Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9.

[105] Morocho-Cayamcela, M. E., Lee, H., & Lim, W. (2019). Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions. IEEE Access, 7, 137184-137206.

[106] Hassan, R., Qamar, F., Hasan, M. K., Aman, A. H. M., & Ahmed, A. S. (2020). Internet of Things and Its Applications: A Comprehensive Survey. Symmetry, 12(10), 1674.

[107] Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, 144, 17-39.

[108] Hassan, R., Jubair, A. M., Azmi, K., & Bakar, A. (2016, December). Adaptive congestion control mechanism in CoAP application protocol for internet of things (IoT). In 2016 International Conference on Signal Processing and Communication (ICSC) (pp. 121-125). IEEE.

[109] Tukade, T. M., & Banakar, R. (2018). Data transfer protocols in IoT—An overview. Int. J. Pure Appl. Math, 118, 121-138.

[110] Järvinen, I., Daniel, L., & Kojo, M. (2015, December). Experimental evaluation of alternative congestion control algorithms for Constrained Application Protocol (CoAP). In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 453-458). IEEE.

[111] Jaikar, S. P., & Iyer, K. R. (2018). A survey of messaging protocols for IOT systems. International Journal of Advanced in Management, Technology and Engineering Sciences, 8(II), 510-514.

[112] Bhattacharjya, A., Zhong, X., Wang, J., & Li, X. (2020). CoAP—application layer connection-less lightweight protocol for the Internet of Things (IoT) and CoAP-IPSEC Security with DTLS Supporting CoAP. In Digital Twin Technologies and Smart Cities (pp. 151-175). Springer, Cham.

[113] Akpakwu, G. A., Hancke, G. P., & Abu-Mahfouz, A. M. (2020). CACC: Context-aware congestion control approach for lightweight CoAP/UDP-based Internet of Things traffic. Transactions on Emerging Telecommunications Technologies, 31(2), e3822.

[114] Luzuriaga, J. E., Cano, J. C., Calafate, C., Manzoni, P., Perez, M., & Boronat, P. (2015, September). Handling mobility in IoT applications using the MQTT protocol. In 2015 Internet Technologies and Applications (ITA) (pp. 245-250). IEEE.

[115] Hwang, H. C., Park, J., & Shon, J. G. (2016). Design and implementation of a reliable message transmission system based on MQTT protocol in IoT. Wireless Personal Communications, 91(4), 1765-1777.

[116] Soni, D., & Makwana, A. (2017, April). A survey on mqtt: a protocol of internet of things (iot). In International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017) (Vol. 20).

[117] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

[118] Chen, Y., & Kunz, T. (2016, April). Performance evaluation of IoT protocols under a constrained wireless access network. In 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT) (pp. 1-7). IEEE.

[119] Babu, B. S., Srikanth, K., Ramanjaneyulu, T., & Narayana, I. L. (2016). IoT for healthcare. International Journal of Science and Research, 5(2), 322-326.

[120] Chien, H. Y., Chen, Y. J., Qiu, G. H., Liao, J. F., Hung, R. W., Lin, P. C., ... & Su, C. (2020). A MQTT-API-compatible IoT security-enhanced platform. International Journal of Sensor Networks, 32(1), 54-68.

[121] Joe, M. M., & Ramakrishnan, B. (2016). Review of vehicular ad hoc network communication models including WVANET (Web VANET) model and WVANET future research directions. Wireless networks, 22(7), 2369-2386.

[122] Yassein, M. B., & Shatnawi, M. Q. (2016, September). Application layer protocols for the Internet of Things: A survey. In 2016 International Conference on Engineering & MIS (ICEMIS) (pp. 1-4). IEEE.

[123] Dizdarević, J., Carpio, F., Jukan, A., & Masip-Bruin, X. (2019). A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration. ACM Computing Surveys (CSUR), 51(6), 1-29.

[124] Hakiri, A., Berthou, P., Gokhale, A., & Abdellatif, S. (2015). Publish/subscribe-enabled software defined networking for efficient and scalable IoT communications. IEEE communications magazine, 53(9), 48-54.

[125] Foster, A. (2015). Messaging technologies for the industrial internet and the internet of things. PrismTech Whitepaper, 21.

[126] Khanna, A., & Kaur, S. (2020). Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. Wireless Personal Communications, 114, 1687-1762.

[127] Chettri, L., & Bera, R. (2019). A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems. IEEE Internet of Things Journal, 7(1), 16-32.

[128] Tun, S. Y. Y., Madanian, S., & Mirza, F. (2020). Internet of things (IoT) applications for elderly care: a reflective review. Aging clinical and experimental research, 1-13.

[129] de Almeida, I. B. F., Mendes, L. L., Rodrigues, J. J., & da Cruz, M. A. (2019). 5G waveforms for IoT applications. IEEE Communications Surveys & Tutorials, 21(3), 2554-2567.

[130] Bhatia, H., Panda, S. N., & Nagpal, D. (2020, June). Internet of Things and its Applications in Healthcare-A Survey. In 2020 8th International Conference on

Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 305-310). IEEE.

[131] Mehrotra, P. (2016). Biosensors and their applications–A review. Journal of oral biology and craniofacial research, 6(2), 153-159.

[132] Uganya, G., Radhika, & Vijayaraj, N. (2020). A survey on internet of things: Applications, recent issues, attacks, and security mechanisms. Journal of Circuits, Systems and Computers, 2130006.

[133] Fafoutis, X., Clare, L., Grabham, N., Beeby, S., Stark, B., Piechocki, R., & Craddock, I. (2016, June). Energy neutral activity monitoring: Wearables powered by smart inductive charging surfaces. In 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON) (pp. 1-9). IEEE.

[134] Kim, S., & Kim, S. (2018). User preference for an IoT healthcare application for lifestyle disease management. Telecommunications Policy, 42(4), 304-314.

[135] Subrahmanyam, V., Zubair, M. A., Kumar, A., & Rajalakshmi, P. (2018). A low power minimal error IEEE 802.15. 4 Transceiver for heart monitoring in IoT applications. Wireless Personal Communications, 100(2), 611-629.

[136] Damis, H. A., Khalid, N., Mirzavand, R., Chung, H. J., & Mousavi, P. (2018). Investigation of epidermal loop antennas for biotelemetry IoT applications. IEEE Access, 6, 15806-15815.

[137] Malik, H., Alam, M. M., Le Moullec, Y., & Kuusik, A. (2018). NarrowBand-IoT performance analysis for healthcare applications. Procedia computer science, 130, 1077-1083.

[138] Dauwed, M., A., Yahaya, J., Mansor, Z., & Hamdan, R., A. (2018). Human factors for IoT services utilization for health information exchange. J. Theor. Appl. Inf. Technol, 96, 2095-2105.

[139] Shahidul Islam, M., Islam, M. T., Almutairi, A. F., Beng, G. K., Misran, N., & Amin, N. (2019). Monitoring of the human body signal through the Internet of Things (IoT) based LoRa wireless network system. Applied Sciences, 9(9), 1884.

[140] Ullo, S. L., & Sinha, G. R. (2020). Advances in smart environment monitoring systems using iot and sensors. Sensors, 20(11), 3113.

[141] Park, J., Kim, K. T., & Lee, W. H. (2020). Recent Advances in Information and Communications Technology (ICT) and Sensor Technology for Monitoring Water Quality. Water, 12(2), 510.

[142] Kumar, K., Mohd, Q., Mohd, A., & Mohd, Z. A. (2019). IoT based autonomous floor cleaning robot. Bachelor of Technology in Electrical Engineering. Electrical Engineering Department, Moradabad Institute of Technology.

[143] Madushanki, A. R., Halgamuge, M. N., Wirasagoda, W. S., & Syed, A. (2019). Adoption of the Internet of Things (IoT) in agriculture and smart farming towards urban greening: A review.

[144] Kim, N. S., Lee, K., & Ryu, J. H. (2015, July). Study on IoT based wild vegetation community ecological monitoring system. In 2015 Seventh International Conference on Ubiquitous and Future Networks (pp. 311-316). IEEE.

[145] Suparta, W., Alhasa, K. M., & Singh, M. S. J. (2017). Preliminary Development of Greenhouse Gases System Data Logger Using Microcontroller Netduino. Advanced Science Letters, 23(2), 1398-1402.

[146] Nordin, R., Mohamad, H., Behjati, M., Kelechi, A. H., Ramli, N., Ishizu, K., ... & Idris, M. (2017, November). The world-first deployment of narrowband IoT for rural hydrological monitoring in UNESCO biosphere environment. In 2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA) (pp. 1-5). IEEE.

[147] Ahamad, F., Latif, M. T., Yusoff, M. F., Khan, M. F., & Juneng, L. (2019). So near yet so different: Surface ozone at three sites in Malaysia. In IOP Conference Series: Earth and Environmental Science (Vol. 228, No. 1, p. 012024). IOP Publishing.

[148] Lee, S. K., Kwon, H. R., Cho, H., Kim, J., & Lee, D. (2016). International case studies of smart cities. Orlando, United States of America: Inter-American Bank.

[149] King, J., & Perry, C. (2017). Smart buildings: Using smart technology to save energy in existing buildings. Amercian Council for an Energy-Efficient Economy.

[150] Guo, Z., Karimian, N., Tehranipoor, M. M., & Forte, D. (2016, May). Hardware security meets biometrics for the age of IoT. In 2016 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1318-1321). IEEE.

[151] Zhou, B., Li, W., Chan, K. W., Cao, Y., Kuang, Y., Liu, X., & Wang, X. (2016). Smart home energy management systems: Concept, configurations, and scheduling strategies. Renewable and Sustainable Energy Reviews, 61, 30-40.

[152] Takenaka, T., Yamamoto, Y., Fukuda, K., Kimura, A., & Ueda, K. (2016). Enhancing products and services using smart appliance networks. CIRP Annals, 65(1), 397-400.

[153] Fernández-Caramés, T. M. (2015). An intelligent power outlet system for the smart home of the Internet of Things. International Journal of Distributed Sensor Networks, 11(11), 214805.

[154] Masek, P., Masek, J., Frantik, P., Fujdiak, R., Ometov, A., Hosek, J., ... & Misurec, J. (2016). A harmonized perspective on transportation management in smart cities: The novel IoT-driven environment for road traffic modeling. Sensors, 16(11), 1872.

[155] Parrado, N., & Donoso, Y. (2015). Congestion based mechanism for route discovery in a V2I-V2V system applying smart devices and IoT. Sensors, 15(4), 7768-7806.

[156] Montori, F., Bedogni, L., & Bononi, L. (2017). A collaborative internet of things architecture for smart cities and environmental monitoring. IEEE Internet of Things Journal, 5(2), 592-605.

[157] Lin, Y. B., Lin, Y. W., Hsiao, C. Y., & Wang, S. Y. (2017). Location-based IoT applications on campus: The IoTtalk approach. Pervasive and mobile computing, 40, 660-673.

[158] Han, S. N., & Crespi, N. (2017). Semantic service provisioning for smart objects: Integrating IoT applications into the web. Future Generation Computer Systems, 76, 180-197.

[159] Huo, Y., Qiu, P., Zhai, J., Fan, D., & Peng, H. (2018). Multi-objective service composition model based on cost-effective optimization. Applied Intelligence, 48(3), 651-669.

[160] Temglit, N., Chibani, A., Djouani, K., & Nacer, M. A. (2017). A distributed agent-based approach for optimal QoS selection in web of object choreography. IEEE Systems Journal, 12(2), 1655-1666.

[161] Cao, B., Liu, J., Wen, Y., Li, H., Xiao, Q., & Chen, J. (2019). QoS-aware service recommendation based on relational topic model and factorization machines for IoT Mashup applications. Journal of parallel and distributed computing, 132, 177-189.

[162] Cuomo, S., Di Somma, V., & Sica, F. (2018). An application of the one-factor HullWhite model in an IoT financial scenario. Sustainable cities and society, 38, 18-20.

[163] Pustišek, M., & Kos, A. (2018). Approaches to front-end IoT application development for the ethereum blockchain. Procedia Computer Science, 129, 410-419.

[164] Park, J. H. (2019). Advances in future Internet and the industrial Internet of Things.

[165] Venticinque, S., & Amato, A. (2019). A methodology for deployment of IoT application in fog. Journal of Ambient Intelligence and Humanized Computing, 10(5), 1955-1976.

[166] Jin, Y., Raza, U., Aijaz, A., Sooriyabandara, M., & Gormus, S. (2017). Content centric cross-layer scheduling for industrial IoT applications using 6TiSCH. IEEE Access, 6, 234-244.

[167] Kiran, M. S., & Rajalakshmi, P. (2018). Performance analysis of CSMA/CA and PCA for time critical industrial IoT applications. IEEE Transactions on Industrial Informatics, 14(5), 2281-2293.

[168] Kwon, D., Hodkiewicz, M. R., Fan, J., Shibutani, T., & Pecht, M. G. (2016). IoT-based prognostics and systems health management for industrial applications. IEEE Access, 4, 3659-3670.

[169] Luvisotto, M., Tramarin, F., Vangelista, L., & Vitturi, S. (2018). On the use of LoRaWAN for indoor industrial IoT applications. Wireless Communications and Mobile Computing, 2018.

[170] Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., & Rizzello, L. (2020). A Blockchain Tokenizer for Industrial IOT trustless applications. Future Generation Computer Systems, 105, 432-445.

[171] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.

[172] Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The internet of things: new interoperability, management and security challenges. arXiv preprint arXiv:1604.04824.

[173] Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W., & Savaglio, C. (2017). Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. Journal of Network and Computer Applications, 81, 74-84.

[174] Ray, P. P. (2018). A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences, 30(3), 291–319.

[175] Kiani, F. (2018). A survey on management frameworks and open challenges in IoT. Wireless Communications and Mobile Computing, 2018.

[176] Ray, P. P., & Kumar, N. (2021). SDN/NFV architectures for edge-cloud oriented IoT: A systematic review. Computer Communications.

[177] Lomotey, R. K., Pry, J., & Sriramoju, S. (2017). Wearable IoT data stream traceability in a distributed health information system. Pervasive and Mobile Computing, 40, 692-707.

[178] Ali, D. H. (2015). A social Internet of Things application architecture: applying semantic web technologies for achieving interoperability and automation between the cyber, physical and social worlds (Doctoral dissertation, Institut National des Télécommunications).

[179] Alaya, M. B. (2015). Towards interoperability, self-management, and scalability for machine-tomachine systems. Networking and Internet Architecture [cs.

[180] Hagman, A. (2016). The Knowledge-and Adoption Level of Standards for Technical Interoperability among Providers of Healthcare Information Systems.

[181] Babovic, Z. B., Protic, J., & Milutinovic, V. (2016). Web performance evaluation for internet of things applications. IEEE Access, 4, 6974-6992.

[182] Schneiderman, R. (2015). Modern standardization: case studies at the crossroads of technology, economics, and politics. John Wiley & Sons.

[183] Di Martino, B., Rak, M., Ficco, M., Esposito, A., Maisto, S. A., & Nacchia, S. (2018). Internet of things reference architectures, security and interoperability: A survey. Internet of Things, 1, 99-112.

[184] Aguzzi, S., Bradshaw, D., Canning, M., Cansfield, M., Carter, P., Cattaneo, G., ... & Stevens, R. (2015). Definition of a research and innovation policy leveraging cloud computing and IoT combination. Final Report, European Commission, SMART, 37, 2015.

[185] Santos, J., Rodrigues, J. J., Silva, B. M., Casal, J., Saleem, K., & Denisov, V. (2016). An IoT-based mobile gateway for intelligent personal assistants on mobile health environments. Journal of Network and Computer Applications, 71, 194-204.

[186] Mocnej, J., Pekar, A., Seah, W. K., Papcun, P., Kajati, E., Cupkova, D., ... & Zolotova, I. (2021). Quality-enabled decentralized IoT architecture with efficient resources utilization. Robotics and Computer-Integrated Manufacturing, 67, 102001.

[187] Zdravković, M., Trajanović, M., Sarraipa, J., Jardim-Gonçalves, R., Lezoche, M., Aubry, A., & Panetto, H. (2016, February). Survey of Internet-of-Things platforms. In 6th International Conference on Information Society and Techology, ICIST 2016 (Vol. 1, pp. 216-220).

[188] Talavera, L. E., Endler, M., Vasconcelos, I., Vasconcelos, R., Cunha, M., & e Silva, F. J. D. S. (2015, March). The mobile hub concept: Enabling applications for the internet of mobile things. In 2015 IEEE International conference on pervasive computing and communication workshops (percom workshops) (pp. 123-128). IEEE.

[189] Chen, R., Guo, J., & Bao, F. (2016). Trust management for SOA-based IoT and its application to service composition. IEEE Transactions on Services Computing, 9(3), 482-495.

[190] Pourghebleh, B., & Navimipour, N. J. (2017). Data aggregation mechanisms in the Internet of things: A systematic review of the literature and recommendations for future research. Journal of Network and Computer Applications, 97, 23-34.

[191] Jabbar, S., Ullah, F., Khalid, S., Khan, M., & Han, K. (2017). Semantic interoperability in heterogeneous IoT infrastructure for healthcare. Wireless Communications and Mobile Computing, 2017.

[192] Zgheib, R. (2017). SeMoM, a semantic middleware for IoT healthcare applications (Doctoral dissertation, Université Paul Sabatier-Toulouse III).

[193] Cimmino, A., Poveda-Villalón, M., & García-Castro, R. (2020). ewot: A semantic interoperability approach for heterogeneous iot ecosystems based on the web of things. Sensors, 20(3), 822.

[194] Ganzha, M., Paprzycki, M., Pawlowski, W., Szmeja, P., & Wasielewska, K. (2016, April). Semantic technologies for the IoT-an inter-IoT perspective. In 2016 IEEE First

International Conference on Internet-of-Things Design and Implementation (IoTDI) (pp. 271-276). IEEE.

[195] Friess, P. (2016). Digitising the industry-internet of things connecting the physical, digital and virtual worlds. River Publishers.

[196] Fraire, J. A., Céspedes, S., & Accettura, N. (2019, October). Direct-To-Satellite IoT-A Survey of the State of the Art and Future Research Perspectives. In International Conference on Ad-Hoc Networks and Wireless (pp. 241-258). Springer, Cham.

[197] Choi, S. I., & Koh, S. J. (2016). Use of proxy mobile IPv6 for mobility management in CoAP-Based internet-of-things networks. IEEE Communications Letters, 20(11), 2284-2287.

[198] Moore, S. J., Nugent, C. D., Zhang, S., & Cleland, I. (2020). IoT reliability: a review leading to 5 key research directions. CCF Transactions on Pervasive Computing and Interaction, 1-17.

[199] Dhumane, A., Prasad, R., & Prasad, J. (2016, March). Routing issues in internet of things: a survey. In Proceedings of the international multiconference of engineers and computer scientists (Vol. 1, pp. 16-18).

[200] Huang, J., Duan, Q., Zhao, Y., Zheng, Z., & Wang, W. (2016). Multicast routing for multimedia communications in the Internet of Things. IEEE Internet of Things Journal, 4(1), 215-224.

[201] Chakravarthy, C. S., Rao, Y. L., & NarayanaRao, C. (2015). RSVP-A Fault Tolerant Mechanism in MPLS Networks. International Journal of Science Engineering and Advance Technology,IJSEAT, Vol 3, Issue 4.

[202] Lamaazi, H., Benamar, N., & Jara, A. J. (2018). RPL-based networks in static and mobile environment: A performance assessment analysis. Journal of King Saud University-Computer and Information Sciences, 30(3), 320-333.

[203] Zain, M. S. I. M., & Rahman, S. A. (2017). Challenges of Applying Data Mining in Knowledge Management towards Organization. International Journal of Academic Research in Business and Social Sciences, 7(12), 405-412.

[204] Bouzerzour, N. E. H., Ghazouani, S., & Slimani, Y. (2020). A survey on the service interoperability in cloud computing: Client-centric and provider-centric perspectives. Software: Practice and Experience, 50(7), 1025-1060.

[205] Bittencourt, L., Immich, R., Sakellariou, R., Fonseca, N., Madeira, E., Curado, M., ... & Rana, O. (2018). The internet of things, fog and cloud continuum: Integration and challenges. Internet of Things, 3, 134-155.

[206] Roopaei, M., Rad, P., & Choo, K. K. R. (2017). Cloud of things in smart agriculture: Intelligent irrigation monitoring by thermal imaging. IEEE Cloud computing, 4(1), 10-15.

[207] Yousefpour, A., Fung, C., Nguyen, T., Kadiyala, K., Jalali, F., Niakanlahiji, A., ... & Jue, J. P. (2019). All one needs to know about fog computing and related edge computing paradigms: A complete survey. Journal of Systems Architecture, 98, 289-330.

[208] Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-Computing Architectures for Internet of Things Applications: A Survey. Sensors, 20(22), 6441.

[209] Chiang, M., & Zhang, T. (2016). Fog and IoT: An overview of research opportunities. IEEE Internet of things journal, 3(6), 854-864.

[210] Xu, K., Ottley, A., Walchshofer, C., Streit, M., Chang, R., & Wenskovitch, J. (2020, June). Survey on the analysis of user interactions and visualization provenance. In Computer Graphics Forum (Vol. 39, No. 3, pp. 757-783).

[211] Díaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer applications, 67, 99-117.

[212] Hussain, M. I. (2017). Internet of Things: challenges and research opportunities. CSI transactions on ICT, 5(1), 87-95.

[213] Aly, M., Khomh, F., Guéhéneuc, Y. G., Washizaki, H., & Yacout, S. (2018). Is Fragmentation a Threat to the Success of the Internet of Things?. IEEE Internet of Things Journal, 6(1), 472-487.

[214] Sezer, O. B., Dogdu, E., & Ozbayoglu, A. M. (2017). Context-aware computing, learning, and big data in internet of things: a survey. IEEE Internet of Things Journal, 5(1), 1-27.

[215] Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1), 1-21.

[216] Subash, K., Ramya, D. J., & Arockiam, L. (2019). Quality of Service in the Internet of Things (IoT)–A Survey. TIRUCHIRAPPALLI-620 002, TAMIL NADU, INDIA.

[217] Sharma, S. K., & Wang, X. (2017). Live data analytics with collaborative edge and cloud processing in wireless IoT networks. IEEE Access, 5, 4621-4635.

[218] Lai, P., He, Q., Cui, G., Xia, X., Abdelrazek, M., Chen, F., ... & Yang, Y. (2020). QoE-aware user allocation in edge computing systems with dynamic QoS. Future Generation Computer Systems, 112, 684-694.

[219] Munir, A., Kansakar, P., & Khan, S. U. (2017). IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things. IEEE Consumer Electronics Magazine, 6(3), 74-82.

[220] Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015, September). A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). In 2015 Internet Technologies and Applications (ITA) (pp. 219-224). IEEE.

[221] Elrefaei, J. H., Kunber, H., Shaat, M. K., Madian, A. H., & Saad, M. H. (2019). Energy-efficient wireless sensor network for nuclear radiation detection. Journal of Radiation Research and Applied Sciences, 12(1), 1-9.

[222] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. International Journal of Information Technology, 10(2), 189-200.

[223] Maple, C. (2017). Security and privacy in the internet of things. Journal of Cyber Policy, 2(2), 155-184.

[224] Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. Journal of Computer Networks and Communications, 2019.

[225] Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., & Coen-Porisini, A. (2016). A secure and quality-aware prototypical architecture for the Internet of Things. Information Systems, 58, 43-55.

[226] Singh, D., Tripathi, G., & Jara, A. (2015, December). Secure layers based architecture for Internet of Things. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 321-326). IEEE.

[227] El Khaddar, M. A., & Boulmalf, M. (2017). Smartphone: the ultimate IoT and IoE device. Smartphones from an applied research perspective, 137.

[228] Nebbione, G., & Calzarossa, M. C. (2020). Security of IoT application layer protocols: Challenges and findings. Future Internet, 12(3), 55.

[229] Ray, P. P., Mukherjee, M., & Shu, L. (2017). Internet of things for disaster management: State-of-the-art and prospects. IEEE access, 5, 18818-18835.

[230] Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. IEEE Access, 8, 167123-167163.

[231] Ismail, M. A., & Schmidt, T. C. (2019). A DTLS Abstraction Layer for the Recursive Networking Architecture in RIOT. arXiv preprint arXiv:1906.12143.

[232] Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2016). AUPS: An open source AUthenticated Publish/Subscribe system for the Internet of Things. Information Systems, 62, 29-41.

Συντομογραφίες

6LoPWPAN	IPv6 over Low -Power Wireless Personal Area Networks
AI	Artificial Intelligence
AMQP	Advanced Message Queuing Protocol
AOMDV-IoT	Ad-hoc on De-mand Multipath Distance Vector
API	Application Programming Interface
AUPS	AUthenticated Publish & Subscribe
BAN	Body Area Network
BLE	Bluetooth Low Energy
CAN	Campus / Corporate Area Network
CCN	Content-Centric Networking
CoAP	Constrained Application Protocol
DDS	Data Distribution Service
DoS	Denial-of-Service
DTLS	Datagram Transport Layer Security
EARA	Energy Aware Ant Routing Algorithm
EPC	Electronic Product Code
ETSI	European Telecommunications Standards Institute
EXI	Efficient XML Interchange
FPGA	Field Programmable Gate Array
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GUI	Graphic User Interface
HetNet	Heterogeneous Networking
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service

IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IERC	IoT European Research Cluster
IETF	Internet Engineering Task Force
IETF CoRE	Internet Engineering Task Force Constrained Restful Environments
IFCIoT	Integrated Fog Cloud IoT
IoNT	Internet of Nano-Things
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IPSO	Internet Protocol for Smart Objects
ISM	Industrial, Scientific and Medical
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ITP	Identity Theft Prevention
ITU	International Telecommunication Union
JMS	Java Message Service
JSON	JavaScript Object Notation
LAN	Local Area Network
LLN	Low-power and Lossy Network
LNMP	LoWPAN Network Management Protocol
LoRa	Long Range
LPWAN	Low Power Wide Area Network
LsDL	Lemon-beat smart Device Language
LTE	Long Term Evolution

LWM2M	Light-Weight M2M
MAC	Media Access Control
MAN	Metropolitan Area Network
MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing
MIMO	Multiple Input Multiple Output
MIT	Massachusetts Institute of Technology
MOM	Middle Oriented Middleware
MPLS	Multi-Protocol Label Switching
MQTT	Message Queuing Telemetry Transport
NanoIP	Nano Internet Protocol
NB-IoT	Narrow Band IoT
NFC	Near Field Communication
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
OneM2M	One Machine-to-Machine
OSI	Open Systems Interconnection
OTrP	Open Trust Protocol
OWL	Web Ontology Language
PaaS	Platform as a Service
PAIR	Pruned Adaptive IoT Routing
PAN	Personal Area Network
QoS	Quality of Service
QUIC	Quick UDP Internet Connections

RAML	RESTful API Modeling Language
RANaaS	Radio Access Network as a Service
RDF	Resource Description Framework
REL	Routing Protocol based on Energy and Link Quality
RFID	Radio-Frequency Identification
ROLL	Routing Over Low power and Lossy
RPL	Routing Protocol for LLNs
RSVP	Resource Reservation Protocol
RTOS	Real-Time Operating System
SaaS	Software as a Service
SASL	Simple Authentication and Security Layer
SBC	Single Board Computer
SDN	Software Defined Networking
SENML	Sensor Markup Language
SMRP	Secure Multihop Routing Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture
SOC	System On a Chip
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSMP	Time Synchronized Mesh Protocol
UDP	User Datagram Protocol
UNB	Ultra NarrowBand
W3C	World Wide Web Consortium
WAN	Wide Area Network

Wi-Fi	Wireless Fidelity
WSDL	Web Services Description Language
WSN	Wireless Sensor Network
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol