ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΟΙΚΟΝΟΜΙΚΗ ΤΩΝ ΤΗΛΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

5G και IoT και σύγχρονες εφαρμογές

Νικόλαος Σ. Τριανταφυλλόπουλος

Επιβλέπων: **Σαράντης Πασκαλής** , ΕΔΙΠ

ΑΘΗΝΑ

ΑΥΓΟΥΣΤΟΣ 2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

5G και IoT και σύγχρονες εφαρμογές

Νικόλαος Σ. Τριανταφυλλόπουλος

Α.Μ.:ΜΟΠ504

ΕΠΙΒΛΕΠΩΝ: **Σαράντης Πασκαλής ,** ΕΔΙΠ

ΑΥΓΟΥΣΤΟΣ 2022

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία ασχολείται με το IoT με δυνατότητα 5G. Αρχικά στην εργασία γίνεται αναφορά στην ιστορική εξέλιξη του 5G. Ακολουθεί αναφορά στην τεχνολογία 5G, όπου αναφέρονται τα χαρακτηριστικά του 5G, τα οφέλη της τεχνολογίας 5G και παρουσιάζονται αναλυτικά οι τεχνολογίες για αλληλεπίδραση με IoT. Επίσης, γίνεται περιγραφή της τεχνολογίας IoT, όπου αποτυπώνονται οι προκλήσεις και τα χαρακτηριστικά του IoT, οι τεχνολογίες IoT και οι τεχνολογίες για αλληλεπίδραση με 5G. Ακολουθεί εκτενής αναφορά στην αρχιτεκτονική του συστήματος 5G - IoT, καθώς και στις απαιτήσεις ασφαλείας και τις πιθανές επιθέσεις σε επικοινωνία IoT με δυνατότητα. Στη συνέχεια, αναφέρονται τα υπάρχοντα πρωτόκολλα ασφαλείας σε περιβάλλον επικοινωνιών IoT με δυνατότητα 5G. Η εργασία ολοκληρώνεται με αναφορά στο υφιστάμενο εμπορικό πλαίσιο του 5G στην παγκόσμια βιομηχανία, αλλά και με ιδιαίτερη αναφορά στις μελλοντικές προκλήσεις της τεχνολογίας που μελετήθηκε.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: 5G δίκτυα , διαδίκτυο των πραγμάτων και εφαρμογές

ΛΕΞΕΙΣ-ΚΛΕΙΔΙΑ: Τεχνολογία πέμπτης γενιάς, Διαδίκτυο των Πραγμάτων, τεχνολογίες, προκλήσεις, εφαρμογές

ABSTRACT

The present work deals with IoT with 5G capability. Initially, the work refers to the historical development of 5G. The following is a reference to 5G technology, which mentions the features of 5G, the benefits of 5G technology and presents in detail the technologies for interaction with IoT. It also describes IoT technology, which captures the challenges and features of IoT, IoT technologies and technologies for 5G interaction. The following is an extensive reference to the 5G - IoT system architecture, as well as security requirements and possible attacks on IoT communication capabilities. The following is a list of existing security protocols in a 5G IoT communication environment. The work concludes with a reference to the current commercial context of 5G in the global industry, but also with a special reference to the future challenges of the technology studied.

SUBJECT AREA : 5G networks , Internet of Things and applications

KEYWORDS : 5G technology, Internet of Things, technologies, challenges, applications

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να εκφράσω τις βαθύτατες ευχαριστίες μου στον επιβλέποντα καθηγητή μου κύριο Σαράντη Πασκαλή , που μου προσέφερε την ευκαιρία να ασχοληθώ με ένα τόσο ενδιαφέρον και σύγχρονο θέμα. Επιπρόσθετα, θα ήθελα να ευχαριστήσω κάθε άτομο που στάθηκε δίπλα μου καθ' όλη τη διάρκεια των σπουδών μου και ιδιαίτερα τους γονείς μου χωρίς τον μόχθο των οποίων δεν θα ήταν δυνατή η ολοκλήρωση των σπουδών μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ **3**

ABSTRACT **4**

ΕΥΧΑΡΙΣΤΙΕΣ **5**

ΠΡΟΛΟΓΟΣ **11**

ΚΕΦΑΛΑΙΟ 1 : ΕΙΣΑΓΩΓΗ **12**

ΚΕΦΑΛΑΙΟ 2 : ΙΣΤΟΡΙΚΟ **14**

ΚΕΦΑΛΑΙΟ 3 : ΤΕΧΝΟΛΟΓΙΑ 5G **17**

3.1 Χαρακτηριστικά του 5G **17**

3.2 Οφέλη της τεχνολογίας 5G **19**

3.3 Τεχνολογίες για αλληλεπίδραση με IoT **20**

3.3.1 Επικοινωνίες από συσκευή σε συσκευή 20

3.3.2 Τεχνολογία κυμάτων χιλιοστών 21

3.3.3 Αναμετάδοση 21

3.3.4 Ασύρματο δίκτυο που καθορίζεται από λογισμικό (WSDN) 22

3.3.5 Οπτικοποίηση Λειτουργίας Δικτύου 22

ΚΕΦΑΛΑΙΟ 4 : ΤΕΧΝΟΛΟΓΙΑ IoT **24**

4.1 Προκλήσεις και χαρακτηριστικά του IoT **24**

4.1.1 Προκλήσεις IoT 24

4.1.2 Χαρακτηριστικά IoT 26

4.2 Τεχνολογίες IoT **26**

4.3 Τεχνολογίες για αλληλεπίδραση με 5G **27**

4.3.1 Nano - Chip 28

4.3.2 Κύμα χιλιοστών (mmWave) 28

4.3.3 Ετερογενή Δίκτυα (Het - Net) 28

4.3.4 Απευθείας επικοινωνία από συσκευή σε συσκευή (D2D) 29

4.3.5 Ασύρματα συστήματα πέμπτης γενιάς (5G) 29

4.3.6 Επικοινωνία τύπου μηχανής (MTC) 30

4.3.7 Ασύρματα δίκτυα καθορισμένα από λογισμικό (WSDN) 30

4.3.8 Προηγμένη διαχείριση κοινής χρήσης και παρεμβολών φάσματος (Advanced SSIM) 31

4.3.9 Mobile Edge Computing (MEC) 31

4.3.10 Εικονικοποίηση λειτουργιών ασύρματου δικτύου (WNFV) 32

4.3.11 Mobile Cloud Computing (MCC) 32

4.3.12 Data Analytics και Big Data 33

4.3.13 Ασφάλεια και Εγκληματολογία 34

ΚΕΦΑΛΑΙΟ 5 : ΣΥΝΕΡΓΑΣΙΑ 5G ΚΑΙ IoT 35

5.1 Αρχιτεκτονική συστήματος 5G - IoT 35

5.2 Απαιτήσεις ασφαλείας και πιθανές επιθέσεις σε επικοινωνία IoT με δυνατότητα 5G 38

5.2.1 Θεματα ασφαλείας και ιδιωτικότητας στις επικοινωνίες IoT - 5G 38

5.2.2 Απαιτήσεις ασφαλείας σε επικοινωνία IoT με δυνατότητα 5G 39

5.2.3 Πιθανές επιθέσεις σε επικοινωνία IoT με δυνατότητα 5G 40

5.3 Υπάρχοντα πρωτόκολλα ασφαλείας σε περιβάλλον επικοινωνιών IoT με δυνατότητα 5G 43

5.3.1 Υπάρχοντα πρωτόκολλα βασικής διαχείρισης στο περιβάλλον IoT 43

5.3.2 Υπάρχοντα πρωτόκολλα αυτονόμησης χρηστών στο περιβάλλον IoT 44

5.3.3 Υπάρχοντα πρωτόκολλα ελέγχου πρόσβασης στο περιβάλλον IoT 45

5.3.4 Υπάρχοντα πρωτόκολλα ανίχνευσης εισβολής στο περιβάλλον IoT 46

ΚΕΦΑΛΑΙΟ 6 : ΕΜΠΟΡΙΚΟ ΠΛΑΙΣΙΟ - ΤΟ 5G ΣΤΗΝ ΠΑΓΚΟΣΜΙΑ ΒΙΟΜΗΧΑΝΙΑ.....49

ΚΕΦΑΛΑΙΟ 7 : Μελλοντικές προκλήσεις 53

7.1 Ασφάλεια των υπαρχόντων πρωτοκόλλων..... 53

7.2 Αποτελεσματικός σχεδιασμός πρωτοκόλλων ασφαλείας 53

7.3 Επεκτασιμότητα πρωτοκόλλων ασφαλείας..... 54

7.4 Απόρρητο αποθηκευμένων δεδομένων 54

7.5 Ετερογένεια μεταχειρισμένων συσκευών..... 55

7.6 Σχεδιασμός πρωτοκόλλων ασφαλείας βασισμένων σε blockchain..... 55

ΣΥΜΠΕΡΑΣΜΑΤΑ.....57

ΒΙΒΛΙΟΓΡΑΦΙΑ.....58

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

Εικόνα 1 : Εξέλιξη/γενιές συστήματος κινητής επικοινωνίας ……..15

Εικόνα 2 : Αρχιτεκτονική συστήματος 5G – IoT ……....37

Εικόνα 3 : Περιπτώσεις χρήσης - απαιτήσεις καθυστέρησης και εύρους ζώνης……50

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

Πίνακας 1 :Βασικοί δείκτες απόδοσης για το 5G …….....16

ΠΡΟΛΟΓΟΣ

Η παρούσα Διπλωματική Εργασία εκπονήθηκε κατά την θερινή περίοδο του Ακαδημαϊκού Έτους 2021 - 2022, στα πλαίσια του Διατμηματικού Προγράμματος Μεταπτυχιακών Σπουδών “ Διοίκηση και Οικονομική των Τηλεπικοινωνιακών Δικτύων και Πληροφοριακών Συστημάτων ” του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών. Η εργασία πραγματοποιήθηκε υπό την επίβλεψη του κ. Σαράντη Πασκαλή, Μέλος ΕΔΙΠ του τμήματος Πληροφορικής και Τηλεπικοινωνιών .

ΚΕΦΑΛΑΙΟ 1 : ΕΙΣΑΓΩΓΗ

Το Industry 4.0 αντιπροσωπεύει την Τέταρτη Βιομηχανική Επανάσταση (4IR) στον αυτοματισμό και την ανταλλαγή δεδομένων. Αναφέρεται σε πολλές θεμελιώδεις νέες τεχνολογικές καινοτομίες όπως τα Cyber - Physical Systems (CPS), το Internet of Things (IoT) και το Data Analytics (Tseng et al., 2018). Το Industry 4.0 οργανώνει ειδικές συνδέσεις μεταξύ φυσικών συσκευών, πληροφοριών, ανθρώπων και βιολογικών σφαιρών για να τροποποιήσει τον παραδοσιακό τρόπο ζωής (Bassi, 2017). Το IoT ως ένα από τα πιο σημαντικά μέρη του κλάδου γίνεται ιδιαίτερα απαιτητικό και πιθανότατα θα αλλάξει τις κοινωνικές σχέσεις (Conti et al., 2018). Σύμφωνα με την έκθεση Statista, ο αριθμός των συνδεδεμένων συσκευών που θα είναι εγκατεστημένες παγκοσμίως το 2025 θα αυξηθεί σε περισσότερες από 75 δισεκατομμύρια συσκευές. Η Telefonica υπολόγισε ότι περισσότερο από το 90 τοις εκατό των αυτοκινήτων μέχρι το 2022 θα είναι συνδεδεμένα στα δίκτυα του Διαδικτύου (Rahimi et al., 2018).

Στο εγγύς μέλλον, ο αριθμός των νέων εφαρμογών IoT και τα δεδομένα που δημιουργούνται θα αυξηθούν εξαιρετικά. Επομένως, ο όγκος των δεδομένων και οι απαιτήσεις των πελατών θα αυξηθούν σημαντικά. Αυτή η περίσταση θα δημιουργήσει μια δύσκολη κατάσταση, επειδή οι εφαρμογές θα χρειάζονται πιο γρήγορη, πιο έξυπνη, πιο απλή, πιο αξιόπιστη και πιο επεκτάσιμη αρχιτεκτονική από πριν. Στην πραγματικότητα, η τρέχουσα αρχιτεκτονική IoT δεν θα είναι αξιόπιστη και δεν θα ανταποκρίνεται στις εφαρμογές IoT επόμενης γενιάς και στις επερχόμενες υπηρεσίες. Ως εκ τούτου, δεν θα μπορεί πλέον να υποστηρίζει τις συσκευές IoT λόγω του εξαιρετικά μεγάλου αριθμού συσκευών και αιτημάτων υπηρεσιών. Οι τεχνολογίες, που έχουν χρησιμοποιηθεί για τον σχεδιασμό των τρεχουσών αρχιτεκτονικών, δεν θα παρέχουν ομαλή συνδεσιμότητα σε μεγάλο αριθμό πραγμάτων λόγω των υψηλών αιτημάτων υπηρεσιών και των τιμών ανταλλαγής δεδομένων (Rahimi et al., 2018). Πρόσφατα, το τμήμα επικοινωνίας των συστημάτων IoT έχει αναπτυχθεί σημαντικά με τέτοιο τρόπο ώστε τα πράγματα και οι συσκευές συνδέονται με διάφορα πρωτόκολλα επικοινωνίας όπως ZigBee, Bluetooth Low Energy (BLE), Wi - Fi, GSM, Lora και Sigfox (Al - Fuqaha et al., 2015).

Κατά συνέπεια, η ανισορροπία των πρωτοκόλλων επικοινωνίας μπορεί να δημιουργήσει σοβαρά προβλήματα, όπως παρεμβολές ραδιοσυχνοτήτων (RFI). Ως εκ τούτου, απαιτείται μια νέα αρχιτεκτονική βασισμένη σε νέες τεχνολογίες για την αντιμετώπιση μελλοντικών προκλήσεων όπως το RFI. Επίσης, τα δίκτυα, οι διαδικασίες, οι εφαρμογές και οι αρχιτεκτονικές διαχείρισης δεδομένων απαιτούν διαφορετικό μοντέλο επικοινωνίας και επεξεργασίας. Κατά συνέπεια, πολλοί ερευνητές εργάζονται σε αυτήν την κατεύθυνση (Rahimi et al., 2018).

Οι ασύρματες επικοινωνίες και η συνδεσιμότητα δεδομένων υψηλής ταχύτητας είναι η ανάγκη του σήμερα και διαδραματίζει σημαντικό ρόλο στην ψηφιοποίηση και την ανάπτυξη σε όλο τον κόσμο (Rana et al., 2021). Η ερευνητική κοινότητα

προσανατολίζεται προς το IoT (Internet of Things) (Palattella et al., 2016) για να καλύψει τις τρέχουσες ανάγκες έξυπνων συσκευών σε τεράστια πεδία συνδέοντας τις συσκευές μεταξύ τους μέσω μιας κοινής πλατφόρμας. Οι τρέχουσες διαθέσιμες ασύρματες τεχνολογίες 3G και 4G είναι ανεπαρκείς για να ανταποκριθούν στις απαιτήσεις και το IoT στο 5G απαιτείται ουσιαστικά χωρίς ανθρώπινη παρέμβαση για τις επικοινωνίες μηχανής με μηχανή μέσω ετερογενών συσκευών (Gubbi et al., 2013). Το IoT φαντάζεται τόσο σε ατομικό όσο και σε επαγγελματικό επίπεδο. Σε ατομικό επίπεδο, το IoT είναι ένα κρίσιμο μέρος για την αύξηση του βιοτικού επιπέδου όσον αφορά την υγεία, το σπίτι και την έξυπνη μάθηση. Σε περίπτωση επαγγελματικού επιπέδου, η εφαρμογή των IoT's είναι η εφοδιαστική αλυσίδα, οι αυτοματισμοί, τα logistics, η μεταφορά και η παρακολούθηση μέσω τηλεχειρισμού. Στο IoT, η ασύρματη τεχνολογία 5G υποτίθεται ότι χρησιμοποιεί αχρησιμοποίητη και μη αδειοδοτημένη ζώνη φάσματος και μέσω δικτύου ευρείας περιοχής χαμηλής ισχύος θα είναι εύκολα προσβάσιμη όπως WiFi, SigFox και NB - IoT (Al - Falahy & Alani, 2017). Σε περίπτωση επαναχρησιμοποίησης φάσματος, η αυτόνομη λειτουργία είναι πολύ χρήσιμη. Ομοίως, σε περίπτωση σωστής χρήσης του φάσματος είναι χρήσιμη και για αχρησιμοποίητο μπλοκ πόρων η ζώνη προστασίας είναι χρήσιμη (Solomitckii et al., 2018).

Η τελευταία τεχνολογία 5G προστίθεται σε βελτιωμένη επικοινωνία τύπου μηχανής (eMTC), βελτιωμένη ευρυζωνική σύνδεση κινητής τηλεφωνίας (eMBB) και κρίσιμες επικοινωνίες (URLLC) (Bockelmann et al., 2016). Το IoT σίγουρα θα δημιουργήσει ατμόσφαιρα που θα βελτιώσει τους τρόπους της καθημερινής μας ζωής και θα είναι ένας διευκολυντής στην παγκόσμια οικονομία. Έχει τεράστιες δυνατότητες. μέσω των πολυάριθμων εφαρμογών του μπορεί να αξιολογηθούν (Rana et al., 2021).

ΚΕΦΑΛΑΙΟ 2 : ΙΣΤΟΡΙΚΟ

Το 5G είναι η πέμπτη γενιά συστημάτων κινητής επικοινωνίας που προωθεί το δίκτυο κινητής τηλεφωνίας όχι μόνο για τη διασύνδεση ατόμων, αλλά και για τη διασύνδεση και τον έλεγχο των μηχανών και άλλων συσκευών (δηλαδή, έξυπνες συσκευές). Βελτιώνει την απόδοση και την αποδοτικότητα που δυναμώνουν τις εμπειρίες των χρηστών. Το 5G παρέχει ταχύτητες αιχμής έως και 10 Gbps, «υπερ χαμηλή καθυστέρηση» και «μεγάλη χωρητικότητα» που παρέχει τη συνέπεια και την ομοιόμορφη εξυπηρέτηση στον χρήστη. Πρόκειται για μια αρχιτεκτονική ασύρματης δικτύωσης που χτίστηκε στο "802.11ac IEEE πρότυπο ασύρματης δικτύωσης" και στοχεύει να βελτιώσει τις ταχύτητες επικοινωνίας δεδομένων έως και τρεις φορές σε σύγκριση με το προηγούμενο "4G - IEEE 802.11n" (Ahad et al., 2019; Braeken et al., 2019; Khan et al., 2020).

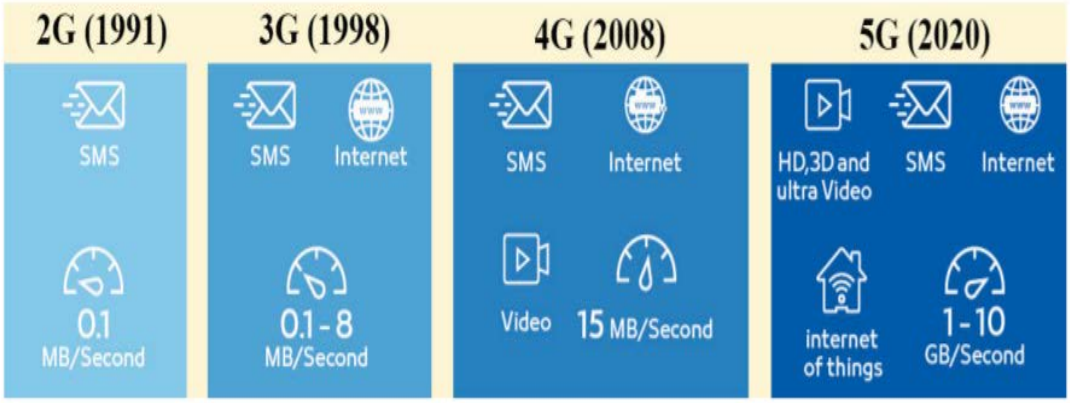
Η εξέλιξη του συστήματος κινητής επικοινωνίας ωστόσο ξεκίνησε πριν περίπου πέντε δεκαετίες (Wazid et al., 2021). Το 1G (Πρώτη Γενιά) εισήχθη στα τέλη της δεκαετίας του 1970. Δεν είχε ισχυρό μηχανισμό ασφαλείας, υπέφερε από προβλήματα πτώσης κλήσεων και η ταχύτητα μετάδοσης δεδομένων ήταν περίπου 2,4 Kbps. Το 2G (Δεύτερη γενιά) υποστήριζε υπηρεσίες δεδομένων όπως «υπηρεσία σύντομων μηνυμάτων (SMS)» και «υπηρεσία ανταλλαγής μηνυμάτων πολυμέσων (MMS)». Η ταχύτητα μετάδοσης δεδομένων μέσω της υπηρεσίας γενικής ραδιοφωνικής υπηρεσίας πακέτων (GPRS) ήταν μεταξύ 50 Kbps έως 1 Mbps. Το 3G (Τρίτη γενιά) παρείχε υπηρεσίες όπως περιήγηση στον ιστό, email, λήψη βίντεο, κοινή χρήση εικόνων και άλλες εφαρμογές smartphone. Η σταθερή ταχύτητα μετάδοσης δεδομένων του ήταν έως 2 Mbps και η ταχύτητα κινητής τηλεφωνίας έως 384 kbps. Η θεωρητική μέγιστη ταχύτητα για «πρόσβαση πακέτων υψηλής ταχύτητας (HSPA+)» ήταν 21,6 Mbps.

Επόμενο ήταν το 4G (τέταρτη γενιά). Το κίνητρο του 4G ήταν να παρέχει υπηρεσίες υψηλής ποιότητας, υψηλής χωρητικότητας και υψηλής ταχύτητας στους χρήστες. Παρέχει καλύτερη ασφάλεια μαζί με χαμηλό κόστος υπηρεσιών δεδομένων και φωνής και Internet μέσω IP. Υποστηρίζει διάφορες εφαρμογές όπως "βελτιωμένη πρόσβαση στο διαδίκτυο για κινητά", "gaming", "κινητή τηλεόραση υψηλής ευκρίνειας", "τηλεφωνία IP", "βίντεοδιάσκεψη", "3D τηλεόραση" και άλλο νέο υπολογιστικό περιβάλλον. Χρησιμοποιεί βασικές τεχνολογίες όπως «πολλαπλής εισόδου πολλαπλής εξόδου (MIMO)» και «πολυπλεξία ορθογώνιας διαίρεσης συχνότητας (OFDM)». Ορισμένα βασικά πρότυπα του 4G είναι η «μακροπρόθεσμη εξέλιξη (LTE)» και η «παγκόσμια διαλειτουργικότητα για πρόσβαση μικροκυμάτων (WiMAX)». Υποστηρίζεται ταχύτητα μεταφοράς δεδομένων έως 100 Mbps με κινητή συσκευή ή 1 Gbps για χαμηλή κινητικότητα.

Τέλος, έρχεται το 5G (πέμπτη γενιά). Το 5G εισήχθη για να βελτιώσει τους περιορισμούς και την απόδοση του 4G. Υποστηρίζει πολύ καλό ρυθμό μεταφοράς δεδομένων με χαμηλή καθυστέρηση και υψηλή πυκνότητα σύνδεσης. Υποστηρίζει επικοινωνία συσκευής με συσκευή με καλύτερη

κατανάλωση μπαταρίας μαζί με καλή ασύρματη κάλυψη. Η ταχύτητα μεταφοράς δεδομένων του 5G είναι περίπου 35 φορές ταχύτερη από το 4G, η οποία στοχεύει έως 35,46 Gbps. Οι τεχνολογίες που λειτουργούν στο παρασκήνιο είναι «μαζικές πολλαπλές εισόδους και πολλαπλές εξόδους (MIMO)» και «κινητές επικοινωνίες κυμάτων χιλιοστών». Τεχνικές και τεχνολογίες όπως "small cell", "masive MIMO", "millimeter wave" και "light fidelity (Li - Fi)" χρησιμοποιούνται για την παροχή 10Gbps με πολύ χαμηλή καθυστέρηση. Το 5G υποστηρίζει συνδέσεις περίπου για 100 δισεκατομμύρια συσκευές. Απαιτείται πλήρης υλοποίησή του άμεσα για να ικανοποιηθούν οι αυξημένες απαιτήσεις των καταναλωτών (Ahmad et al., 2018; Tian et al., 2019).

Η εξέλιξη του συστήματος κινητής επικοινωνίας τονίζεται επίσης στην Εικόνα 1 που δείχνει την πρόοδο τις τελευταίες δεκαετίες. Περιλαμβάνει επίσης τις λεπτομέρειες των λειτουργιών που υποστηρίζονται από διάφορες γενιές.



Εικόνα 1 : Εξέλιξη/γενιές συστήματος κινητής επικοινωνίας (Wazid et al., 2021)

Το 5G έχει σχεδιαστεί με τις προηγούμενες τέσσερις μεγάλες τάσεις (για παράδειγμα, αυξημένος αριθμός συσκευών, αύξηση επισκεψιμότητας, υψηλή εξάρτηση από το cloud και διαφορετικές υπηρεσίες σύγκλισης 5G). Ορισμένες προτάσεις δόθηκαν από ορισμένες ενδιαφερόμενες εταιρείες για την επιλογή των βασικών δεικτών απόδοσης που θα πρέπει να χρησιμοποιηθούν στο 5G. Με βάση αυτές τις προτάσεις, το International Telecommunication Union–Radiocommunication Sector (ITU - R) (Lee, 2015) επέλεξε μερικές από τις σημαντικές παραμέτρους που παρατίθενται στον Πίνακα 1.

Πίνακας 1 : Βασικοί δείκτες απόδοσης για το 5G (Wazid et al., 2021)

Key performance indicators	Target values
Data rate (user experience)	100 Mbps to 1 Gbps
Data rate (peak)	10 Gbps to 50 Gbps
Support for Mobility	Up to 500 Kmph
Latency	1 ms
Connection density	10^6 to 10^7 per Km^2
Traffic volume density	1TB to 10TB/s/Km^2

ΚΕΦΑΛΑΙΟ 3 : ΤΕΧΝΟΛΟΓΙΑ 5G

3.1 Χαρακτηριστικά του 5G

Προκειμένου να ενισχυθούν οι δυνατότητες του LTE, μια πέμπτη γενιά κυψελοειδούς δικτύου (5G) βρίσκεται στο προσκήνιο (Alsulami & Akkari, 2018). Επίσης, το 5G έχει ορισμένες απαιτήσεις και προκλήσεις που πρέπει να ικανοποιηθούν και να επιλυθούν χρησιμοποιώντας ποικιλία τεχνολογιών. Οι προκλήσεις που αντιμετώπισε το 5G αφορούν (Akyildiz et al., 2016) :

- Αύξηση χωρητικότητας,
- Υψηλός ρυθμός δεδομένων,
- Χαμηλή καθυστέρηση,
- Τεράστιος αριθμός συνδέσεων και
- Χαμηλό κόστος και ποιότητα υπηρεσιών (QoS)

Για την επίτευξη αυτών των απαιτήσεων, ή με άλλα λόγια, για την επίλυση αυτών των προκλήσεων, ορισμένες τεχνολογίες έχουν εμπλακεί ως τεχνολογίες ενεργοποίησης για το 5G. Αυτές οι τεχνολογίες είναι : μαζική MIMO, D2D, Εικονικοποίηση λειτουργιών δικτύου, Ασύρματο SDN, IoT, υπερπύκνωση, τεχνολογίες πρόσβασης ραδιοφώνου, πράσινη επικοινωνία και μεγάλα δεδομένα και φορητό υπολογιστικό νέφος. Το 5G αναμένεται να πληροί ορισμένες απαιτήσεις για να μπορεί να εξυπηρετεί τους διάφορους τύπους συσκευών και εφαρμογών. Κάθε μία από αυτές τις απαιτήσεις συζητείται παρακάτω (Alsulami & Akkari, 2018) :

1) Υψηλός ρυθμός μετάδοσης δεδομένων

Με την έκρηξη της χρήσης δικτύων σε εφαρμογές που απαιτούσαν γρήγορη επικοινωνία, η ανάγκη για υψηλό ρυθμό δεδομένων αυξάνεται ραγδαία. Με τα χρόνια, η επίτευξη υψηλού ρυθμού δεδομένων στα ασύρματα δίκτυα είναι ένας από τους πιο σημαντικούς παράγοντες για την αξιολόγηση της απόδοσης τέτοιων δικτύων. Ωστόσο, το LTE παρείχε ρυθμό δεδομένων που έφτασε τα 15 Mbps. Οι νέες εφαρμογές όπως η ροή βίντεο ultra - HD χρειάζονται υψηλότερους ρυθμούς δεδομένων (έως 25 Mbps) από αυτές που είναι διαθέσιμες αυτήν τη στιγμή (Akyildiz et al., 2016). Ο ρυθμός δεδομένων έχει δύο κύριες μετρήσεις που χαρακτήριζαν το δίκτυο : ρυθμός δεδομένων αιχμής κυψέλης και χωρητικότητα περιοχής. Ο ρυθμός δεδομένων ακμής κυψέλης υποδεικνύει τον ρυθμό των δεδομένων στην άκρη της κυψέλης όπου το σήμα σύνδεσης βρίσκεται στο πιο αδύναμο σημείο. Ο ρυθμός δεδομένων αιχμής κυψέλης θα πρέπει να βελτιωθεί για να επιτευχθεί υψηλός ρυθμός δεδομένων για το συνολικό σύστημα. Επιπλέον, όταν ένας χρήστης βρίσκεται κοντά στην άκρη κυψέλης σε ένα δίκτυο, η παρεμβολή θα είναι υψηλή, γεγονός που οδηγεί σε αδύναμο σήμα. Από την άλλη πλευρά, όταν ένας χρήστης βρίσκεται κοντά στο κέντρο της κυψέλης, η παρεμβολή θα είναι χαμηλή, γεγονός που οδηγεί σε ισχυρό σήμα. Ο στόχος είναι να βελτιωθεί ο ρυθμός δεδομένων στην άκρη του

κελιού για να βελτιωθεί η εμπειρία χρήστη. Ένας από τους πιο αποτελεσματικούς τρόπους για να γίνει αυτό είναι μέσω της χρήσης μικρών κυττάρων. Η χρήση μικρών κελιών βελτιώνει την κάλυψη των κυψελοειδών δικτύων καθώς και τη χωρητικότητα. Η δεύτερη μέτρηση που επηρεάζει αυτόν τον ρυθμό δεδομένων είναι η χωρητικότητα της περιοχής. Η χωρητικότητα περιοχής υποδεικνύει τον συνολικό ρυθμό δεδομένων που μπορεί να εξυπηρετήσει ένα δίκτυο ανά μονάδα επιφάνειας. Στο 5G, ο ρυθμός δεδομένων αναμένεται να φτάσει τα 10 Gbps με 100 Mbps για ρυθμό δεδομένων κυψέλης (Akyildiz et al., 2016). Οι λύσεις/τεχνολογίες ενεργοποίησης που έχουν χρησιμοποιηθεί για την απόκτηση υψηλού ρυθμού δεδομένων είναι οι εξής (Alsulami & Akkari, 2018) :

- MIMO
- Αναμεταδόσεις
- Μικρά κελιά
- Επικοινωνία χιλιοστών κυμάτων
- Ασύρματο SDN

2) Μειωμένη καθυστέρηση

Η καθυστέρηση είναι ο χρόνος που απαιτείται για τη μεταφορά δεδομένων από την πηγή στον προορισμό μέσω ενός δικτύου. Η σημασία της μείωσης του λανθάνοντος χρόνου ενός δικτύου προκύπτει από την εφαρμογή που επηρεάζεται σε μεγάλο βαθμό από καθυστερήσεις όπως το gaming. Στην πραγματικότητα, η καθυστέρηση RTT του LTE είναι περίπου 15 χιλιοστά του δευτερολέπτου και αναμένεται να μειωθεί στο 1 ms για να ικανοποιήσει τις απαιτήσεις του 5G. Ο λόγος μιας τέτοιας ανάγκης για μειωμένο λανθάνοντα χρόνο στο 5G είναι η αυξανόμενη χρήση αλληλεπιδράσεων σε πραγματικό χρόνο σε πολλές εφαρμογές, οι οποίες δεν απαιτούσαν καθυστέρηση για τη βελτίωση της εμπειρίας του χρήστη. Επίσης, η ιδέα του Διαδικτύου των πραγμάτων και της επικοινωνίας τύπου μηχανής όπου όλα είναι συνδεδεμένα και η καθυστέρηση δεν είναι αποδεκτή (Akyildiz et al., 2016). Οι τεχνολογίες ενεργοποίησης που έχουν χρησιμοποιηθεί για τη μείωση του λανθάνοντος χρόνου είναι :

- Επικοινωνία D2D
- Όλα τα οπτικά δίκτυα
- Big data και φορητό υπολογιστικό νέφος (Alsulami & Akkari, 2018).

3) Χαμηλή ενέργεια

Μία από τις τεχνολογίες ενεργοποίησης που υποστηρίζονται από το 5G είναι το IoT όπου οι συσκευές συνδέονται χρησιμοποιώντας αισθητήρες χωρίς να χρειάζεται να συνδέονται πάντα σε σταθμό βάσης. Αυτό το σενάριο υποδεικνύει ότι αυτές οι συσκευές θα ενεργοποιούνται μόνο όταν χρειάζονται. Αυτό σημαίνει

ότι το 5G απαιτεί μείωση της ενέργειας και δεν υποστηρίζει συγχρονισμούς (Alsulami & Akkari, 2018).

4) Υψηλή επεκτασιμότητα

Με το σχεδιασμό των ασύρματων δικτύων LTE και στη συνέχεια 5G, θα πρέπει να ληφθεί υπόψη ο αυξανόμενος αριθμός συσκευών κινητής τηλεφωνίας. Ο αριθμός των συσκευών που είναι συνδεδεμένες σε ένα κυψελοειδές δίκτυο αναμένεται να αυξηθεί. Η εξυπηρέτηση και ο χειρισμός αυτού του αριθμού συσκευών χρειάζεται ένα αποτελεσματικό επεκτάσιμο δίκτυο. Η παροχή υψηλής επεκτασιμότητας για δίκτυα κινητής τηλεφωνίας απαιτεί αρκετούς πόρους φάσματος συχνοτήτων και αποτελεσματικό έλεγχο μέσων (Alsulami & Akkari, 2018).

3.2 Οφέλη της τεχνολογίας 5G

Το σύστημα κινητής επικοινωνίας 5G παρέχει πολύ γρήγορη ταχύτητα και πιο αξιόπιστες συνδέσεις σε smartphone και άλλες κινητές συσκευές (δηλαδή, έξυπνα οχήματα) από ποτέ. Μερικά από τα βασικά οφέλη των δικτύων 5G είναι τα παρακάτω (Ahmad et al., 2018; Gandotra & Jha, 2017; Tian et al., 2019) :

- Παρέχει πολύ υψηλό ρυθμό μεταφοράς δεδομένων (1 - 20 Gbps) που διευκολύνει τους χρήστες να κατεβάζουν περιεχόμενο πολύ γρήγορα.
- Παρέχει εξαιρετικά χαμηλή καθυστέρηση (1 ms) που επιτρέπει στους χρήστες να αντιμετωπίζουν λιγότερη καθυστέρηση όταν ζητούν δεδομένα από το δίκτυο.
- Η χωρητικότητα αυξάνεται καθώς επεκτείνεται το δίκτυο.
- Διαχειρίσιμο με τις προηγούμενες γενιές τεχνολογιών κινητής επικοινωνίας.
- Αποτελεσματικό και υποστηρικτικό για ετερογενείς υπηρεσίες (δηλαδή, ιδιωτικό δίκτυο).
- Παρέχει ομοιόμορφη, αδιάλειπτη και συνεπή συνδεσιμότητα για τις διάφορες εφαρμογές (δηλαδή επικοινωνία έξυπνων οχημάτων) σε όλο τον κόσμο.

Το σύστημα επικοινωνίας πέμπτης γενιάς (5G) έχει μεγάλο αντίκτυπο στην επικοινωνία που συμβαίνει στο IoT. Το 5G ενεργοποιεί την καινοτομία σε πολλούς κλάδους (δηλαδή, τον τομέα της αυτοκινητοβιομηχανίας, τον τομέα της υγείας κ.α.) και παρέχει μια πλατφόρμα που επιτρέπει στις αναδυόμενες τεχνολογίες (για παράδειγμα, το IoT) να γίνουν ουσιαστικό μέρος της οικονομίας και της καθημερινής ζωής των ανθρώπων (Wazid et al., 2021).

3.3 Τεχνολογίες για αλληλεπίδραση με IoT

Ως αποτέλεσμα της εξέλιξης των συστημάτων IoT, πολλά χαρακτηριστικά και λειτουργίες πρέπει να εμπλακούν στο σχεδιασμό της επόμενης γενιάς κυψελοειδών δικτύων. Πολλές μελέτες δείχνουν ότι το 5G είναι ο βασικός μοχλός του IoT λόγω των τεχνολογιών του που λαμβάνουν υπόψη την ποικιλία των απαιτήσεων του IoT. Επιπλέον, η παροχή αξιόπιστης συνδεσιμότητας για συσκευές IoT είναι μια εργασία που περιλαμβάνει συντονισμό και ενοποίηση πολλών τεχνολογιών ενεργοποίησης.

Για να ικανοποιηθούν οι απαιτήσεις IoT όπως η μεγάλη κάλυψη, ο εξαιρετικά υψηλός ρυθμός δεδομένων, η επεκτασιμότητα και η χωρητικότητα, χρησιμοποιούνται διάφορες τεχνολογίες από σχέδια 5G για να επιτρέψουν τις επικοινωνίες IoT. Αυτές οι τεχνολογίες συζητούνται στις εισερχόμενες υποενότητες (Alsulami & Akkari, 2018).

3.3.1 Επικοινωνίες από συσκευή σε συσκευή

Η κύρια ιδέα της επικοινωνίας συσκευής με συσκευή (D2D) είναι να επιτρέπει σε δύο συσκευές να επικοινωνούν μεταξύ τους χωρίς έναν ενδιάμεσο σταθμό βάσης (BS) που ελέγχει την επικοινωνία. Επίσης, το κύριο πλεονέκτημα μιας τέτοιας τεχνολογίας είναι η χρήση αδειοδοτημένου φάσματος και όχι μη αδειοδοτημένου φάσματος που χρησιμοποιείται από τεχνολογίες όπως το Wi - Fi και το Bluetooth (Palattella et al., 2016). Αυτός ο τύπος επικοινωνίας παρέχει υψηλό ρυθμό δεδομένων και χαμηλό λανθάνοντα χρόνο λόγω της αποτελεσματικής και άμεσης επικοινωνίας μεταξύ των δύο συνδεδεμένων συσκευών. Φυσικά, για να επικοινωνήσουν δύο συσκευές μέσω κυψελοειδούς συστήματος, πρέπει να συνδεθούν μεταξύ τους μέσω ενός σταθμού βάσης (BS), το οποίο με τη σειρά του έχει ως αποτέλεσμα χαμηλό ρυθμό μετάδοσης δεδομένων και καθυστέρηση. Τα συστήματα 5G αναμένεται να επιτρέπουν στην άμεση επικοινωνία που απεικονίζεται στις επικοινωνίες D2D να υποστηρίζει πολλές εφαρμογές IoT που απαιτούσαν τέτοια επικοινωνία. Όπως αναφέρθηκε προηγουμένως, η χρήση αδειοδοτημένου φάσματος στην επικοινωνία D2D βελτιώνει την ποιότητα της υπηρεσίας (QoS) αυξάνοντας τον ρυθμό δεδομένων και μειώνοντας την καθυστέρηση. Επίσης, η επικοινωνία D2D επιτρέπει καλύτερη εμπειρία χρήστη, ειδικά όταν η χωρητικότητα ενός BS επιτυγχάνεται λόγω της κίνησης δεδομένων. Επιπλέον, οι επικοινωνίες D2D μπορούν να χρησιμοποιηθούν ως βάση για πολλές τεχνολογίες όπως η επικοινωνία τύπου μηχανής (MTC) και οι επικοινωνίες οχήματος με όχημα

(V2V). Υπάρχουν τέσσερις τύποι επικοινωνίας D2D (Alsulami & Akkari, 2018) :

1. Αναμετάδοση συσκευής με ελεγχόμενη σύνδεση BS.

2. Αναμετάδοση συσκευής με εγκατάσταση ζεύξης ελεγχόμενης συσκευής.

3. Άμεση επικοινωνία D2D με εγκατάσταση συνδέσμων ελεγχόμενης BS.

4. Απευθείας επικοινωνία D2D με εγκατάσταση σύνδεσης ελεγχόμενης συσκευής.

Η χρήση της επικοινωνίας D2D για την ενεργοποίηση εφαρμογών IoT έχει ένα πιθανό όφελος στις ομαδικές επικοινωνίες μέσω συσκευών IoT. Ωστόσο, πολλά ανοιχτά ζητήματα πρέπει να διερευνηθούν στην επικοινωνία D2D, όπως : ασφάλεια, ανακάλυψη πόρων και διαχείριση παρεμβολών (Palattella et al., 2016).

3.3.2 Τεχνολογία κυμάτων χιλιοστών

Μία από τις πολλά υποσχόμενες τεχνολογίες που παρουσιάζουν σημαντικό αντίκτυπο στη βελτίωση της χωρητικότητας και της απόδοσης των κινητών επικοινωνιών είναι η χρήση ζωνών συχνοτήτων χιλιοστών. Οι ζώνες συχνοτήτων στο κύμα mm είναι από 30 έως 300 GHz (Akyildiz et al., 2016). Επιπλέον, οι συχνότητες φέροντος κυμάτων mm αυξάνουν τους ρυθμούς δεδομένων επιτρέποντας μεγάλες εκχωρήσεις εύρους ζώνης (Palattella et al., 2016). Όσον αφορά τις εφαρμογές IoT, η χρήση mm wave θα μπορούσε να επιτρέψει υψηλούς ρυθμούς δεδομένων για τέτοιου είδους εφαρμογές με μεγάλη χωρητικότητα (Palattella et al., 2016). Όπως συζητήθηκε στο προηγούμενο σημείο, η επικοινωνία μικρής εμβέλειας που προσφέρεται από την τεχνολογία κυμάτων mm μπορεί να είναι ελκυστική για επικοινωνίες D2D (Agiwal et al., 2016).

3.3.3 Αναμετάδοση

Ένα δίκτυο αναμετάδοσης μπορεί να θεωρηθεί ως μια τοπολογία δικτύου που χρησιμοποιείται κυρίως στο ασύρματο δίκτυο για τη βελτίωση της απόδοσής του. Η ιδέα των αναμεταδόσεων είναι να υπάρχει ένας κόμβος αναμετάδοσης (RN) ανάμεσα σε UE και eNB. Επιπλέον, αυτά τα RN έχουν τη λειτουργικότητα τόσο των UE όσο και των eNB. Είναι υπεύθυνοι για τη λήψη και τη μεταφορά πληροφοριών μέσω ασύρματου δικτύου από UE/eNB σε eNB/UE. Υπάρχουν τέσσερα κύρια πλεονεκτήματα των κόμβων αναμετάδοσης. Πρώτον, παρέχουν προσωρινές αναπτύξεις δικτύου αφού τα RN είναι εύκολο να αναπτυχθούν και

να αφαιρεθούν περισσότερο από τα eNB. Δεύτερον, αυξάνουν τη διεκπεραίωση της ακμής κυψέλης επειδή ο εντοπισμός των RN κοντά στην άκρη της κυψέλης βελτιώνει την άκρη της κυψέλης σε όλη την έκταση. Τρίτον, το πιο σημαντικό πλεονέκτημα των RN είναι η αύξηση του ρυθμού δεδομένων με τον εντοπισμό των RN σε περιοχές χαμηλού επιπέδου σήματος. Τέλος, σε ορισμένες περιπτώσεις πολλοί χρήστες (UE) μετακινούνται μαζί από τη μια τοποθεσία στην άλλη και αυτό απαιτούσε μια δυνατότητα κινητικότητας, η οποία υποστηρίζεται από συντοποθετημένα RN (Akyildiz et al., 2014). Όσον αφορά τα συστήματα IoT, η αναμετάδοση είναι μια βασική τεχνολογία που παρέχει επεκτασιμότητα για εφαρμογές IoT. Σε περίπτωση που υπάρχει είδος κίνησης σε έναν σταθμό βάσης (BS), οι συσκευές IoT μπορούν να συνδεθούν σε πολλούς σταθμούς αναμετάδοσης (RS), οι οποίοι με τη σειρά τους επιτρέπουν καλύτερη συνδεσιμότητα και κάλυψη.

3.3.4 Ασύρματο δίκτυο που καθορίζεται από λογισμικό (WSDN)

Πολλές μελέτες έχουν θεωρήσει το SDN ως μία από τις τεχνολογίες ενεργοποίησης για κυψελωτά συστήματα 5G (Palattella et al., 2016). Το SDN είναι ένα αναδυόμενο παράδειγμα που βασίζεται στην ιδέα του διαχωρισμού των σχεδίων δεδομένων από το σχέδιο ελέγχου, τα οποία αυξάνουν την ευελιξία της απόδοσης του δικτύου (Agiwal et al., 2016). Διαχωρίζοντας τα σχέδια ελέγχου από τα σχέδια δεδομένων ή χρηστών, η χωρητικότητα και οι ρυθμοί δεδομένων μπορούν να αυξηθούν μειώνοντας τα γενικά έξοδα που μπορεί να προκύψουν από τα σχέδια ελέγχου. Επιπλέον, το SDN μπορεί να χρησιμοποιηθεί στην εξέλιξη των συστημάτων IoT για να τονίσει τις προκλήσεις ευελιξίας και διαλειτουργικότητας. Όσον αφορά την ευελιξία, το SDN επιτρέπει τη δυναμική αρχιτεκτονική IoT που μπορεί να αντιμετωπίσει τον αριθμό των συνδεδεμένων συσκευών και δεδομένων που ανταλλάσσονται (Agiwal et al., 2016). Όσον αφορά τη διαλειτουργικότητα, ο διαχωρισμός του ελέγχου από τα σχέδια δεδομένων επιτρέπει την ανεξάρτητη χρήση των πόρων. Στην πραγματικότητα, το SDN επιτρέπει σε πολλές διαφορετικές υπηρεσίες με διαφορετική ποιότητα υπηρεσίας QoS να υπάρχουν στον ίδιο τομέα (Palattella et al., 2016).

3.3.5 Οπτικοποίηση Λειτουργίας Δικτύου

Το NFV είναι μια συμπληρωματική έννοια του SDN. Η έννοια του NFV προέρχεται βασικά από την ιδέα της ύπαρξης αρκετών εικονικών μηχανών που λειτουργούν σε διαφορετικά λειτουργικά συστήματα που λειτουργούν σε διαφορετικό υλικό (Agiwal et al., 2016). Ο στόχος αυτής της τεχνολογίας είναι η

εικονικοποίηση πολλών λειτουργιών δικτύου. Αυτή η εικονικοποίηση μπορεί να αυξήσει την ευελιξία και την επεκτασιμότητα στις εφαρμογές IoT (Palattella et al., 2016).

ΚΕΦΑΛΑΙΟ 4 : ΤΕΧΝΟΛΟΓΙΑ IoT

4.1 Προκλήσεις και χαρακτηριστικά του IoT

Το Διαδίκτυο των πραγμάτων (IoT) μπορεί να οριστεί σύμφωνα ως μια δυναμική παγκόσμια υποδομή δικτύου με δυνατότητα αυτοδιαμόρφωσης. Έχει την ιδέα της σύνδεσης διαφόρων τύπων φυσικών ή εικονικών αντικειμένων (Alsulami & Akkari, 2018).

4.1.1 Προκλήσεις IoT

1) Ενεργειακή απόδοση

Μία από τις κύριες προκλήσεις που χαρακτηρίζει το IoT είναι η παροχή αποδοτικής κατανάλωσης ενέργειας. Η ιδέα είναι πώς να επιτευχθεί υψηλή ενεργειακή απόδοση μεταξύ των επικοινωνιών IoT. Στην πραγματικότητα, οι περισσότερες από τις ενεργειακές προκλήσεις στο IoT σχετίζονται με τις συνδεδεμένες συσκευές. Αυτές οι συνδεδεμένες συσκευές εξαρτώνται συνήθως από μπαταρίες ή από ενεργειακά συστήματα συγκομιδής. Επίσης, μερικές φορές ειδικά σε εφαρμογές που απαιτούσαν απομακρυσμένη επικοινωνία, η κατανάλωση ενέργειας μπορεί να είναι προβληματική σε περίπτωση που απαιτείται επαναφόρτιση ή αντικατάσταση ενεργειακών συστημάτων. Το IoT επιτυγχάνει την ενεργειακή απόδοση ή την κατανάλωση μέσω της άμεσης επικοινωνίας μεταξύ συνδεδεμένων συσκευών, η οποία επιτρέπει ένα είδος τοπικής συνδεσιμότητας μεταξύ συσκευών που συνήθως παρέχεται από ασύρματες τεχνολογίες (Militano et al., 2015).

2) Επεκτασιμότητα

Δεδομένου ότι οι αισθητήρες είναι φθηνοί και διαθέσιμοι, η ανάπτυξη πολλών από αυτούς για τη σύνδεση αντικειμένων σε διαφορετικά μέρη είναι εύκολη. Αυτή η αύξηση του αριθμού των συνδεδεμένων συσκευών εγείρει πολλές προκλήσεις όσον αφορά την παροχή κάλυψης σε όλες αυτές τις συνδεδεμένες συσκευές με αξιόπιστο τρόπο. Επιπλέον, πρέπει να μειωθεί η επιβάρυνση της ρύθμισης σήματος και σύνδεσης. Λόγω του αυξανόμενου αριθμού συνδεδεμένων συσκευών, η παράδοση μεταξύ των κυψελών αυξάνεται. Αυτά τα ζητήματα που σχετίζονται με τη δυνατότητα κλιμάκωσης του IoT μπορούν να αντιμετωπιστούν από τεχνολογίες όπως το SDN (Alsulami & Akkari, 2018).

3) Έξυπνη επεξεργασία και αποθήκευση

Όπως αναφέρθηκε προηγουμένως, η έννοια του IoT είναι να έχει αριθμό συνδεδεμένων συσκευών μέσω αρκετών αισθητήρων, οι οποίοι είναι υπεύθυνοι για την αποστολή πληροφοριών, αφού τις αντιληφθούν από αυτές τις συσκευές, σε απομακρυσμένο διακομιστή. Αυτός ο απομακρυσμένος διακομιστής είναι υπεύθυνος για τη μετάφραση και επεξεργασία αυτών των πληροφοριών σε γνώση που αντιπροσωπεύεται ως συγκεκριμένες ενέργειες ή συμπεριφορές. Συνήθως αυτοί οι απομακρυσμένοι διακομιστές φιλοξενούνται σε παρόχους cloud. Δεδομένου ότι η συλλογή και η επεξεργασία όλων των πληροφοριών από διαφορετικές συσκευές είναι πολύπλοκες διαδικασίες, οι πάροχοι cloud IoT πρέπει να έχουν ορισμένες δυνατότητες για να χειριστούν αυτές τις περίπλοκες εργασίες. Επιπλέον, οι πάροχοι cloud σε αυτό το πλαίσιο απαιτείται να παρέχουν υπολογιστική ικανότητα κατ' απαίτηση. Υπάρχουν δύο τρόποι ή προσεγγίσεις για τη διαχείριση της πολυπλοκότητας των παρόχων cloud IoT και του υπολογιστικού φόρτου που πρέπει να εκτελεστούν από την πλευρά των παρόχων διακομιστών. Πρώτον, πολλοί πάροχοι cloud μπορούν να χρησιμοποιηθούν για το ίδιο δίκτυο IoT. Δεύτερον, για να μειωθεί η καθυστέρηση που θα μπορούσε να προκύψει λόγω της πολυπλοκότητας της επεξεργασίας, η υπολογιστική υπηρεσία θα μπορούσε να μετακινηθεί στην άκρη του δικτύου (Alsulami & Akkari, 2018).

4) Ασφάλεια

Η πρόκληση ασφαλείας απεικονίζεται στην ιδέα της ύπαρξης ποικιλίας συνδεδεμένων συσκευών με διαφορετικό υλικό και πλατφόρμες. Η επικοινωνία μεταξύ αυτών των συσκευών μπορεί να παραβιαστεί, καθώς η παροχή ενός μηχανισμού ασφαλείας που είναι συμβατός με όλες αυτές τις διαφορετικές συσκευές είναι μια πολύπλοκη εργασία. Στην πραγματικότητα, οι απειλές θα μπορούσαν να προέρχονται από δύο πτυχές : μεταξύ της επικοινωνίας συσκευών ή στην επικοινωνία μεταξύ αυτών των συσκευών και των απομακρυσμένων διακομιστών (Gupta & Gupta, 2016).

5) Διαλειτουργικότητα

Μία από τις πιο προφανείς προκλήσεις που αντιμετωπίζει το IoT είναι η διαλειτουργικότητα. Λόγω του ποικίλου εύρους των συσκευών που πρέπει να συνδεθούν, η ανάγκη συντονισμού αυτών των διαφορετικών συσκευών αυξάνεται. Αυτές οι συσκευές χρησιμοποιούν διαφορετικό υλικό, τρέχουν σε διαφορετικές πλατφόρμες και κατασκευάζονται από διαφορετικούς προμηθευτές. Υπάρχουν πολλές συσκευές IoT στην αγορά σήμερα, αλλά καθεμία από αυτές χρησιμοποιεί τα δικά της πρότυπα και διεπαφές για να επικοινωνεί με άλλες συσκευές ή απομακρυσμένους διακομιστές. Αυτό θα μπορούσε να προκαλέσει διένεξη όταν χρησιμοποιούνται διαφορετικές συσκευές στον ίδιο τομέα. Η ασυμβατότητα μεταξύ συσκευών, αισθητήρων, ακόμη και διεπαφών απομακρυσμένων διακομιστών είναι ο κύριος λόγος που προκαλεί την πρόκληση διαλειτουργικότητας στο IoT (Alsulami & Akkari, 2018).

4.1.2 Χαρακτηριστικά IoT

Το IoT δεν είναι μόνο μια τεχνολογία. Είναι μια έννοια πολλών ολοκληρωμένων τεχνολογιών. Έχει πολλά χαρακτηριστικά που διαμορφώνουν τους σκοπούς και τις λειτουργίες του IoT. Αυτά τα χαρακτηριστικά ή χαρακτηριστικά αναλύονται ως εξής (Militano et al., 2015) :

1. Διασυνδεσιμότητα : Στο IoT, τα πάντα μπορούν να συνδεθούν, συμπεριλαμβανομένων οποιωνδήποτε εικονικών ή φυσικών αντικειμένων. Το χαρακτηριστικό διασυνδεσιμότητας απεικονίζεται από τη σύνδεση μεταξύ αυτών των διαφορετικών αντικειμένων και της υποδομής επικοινωνίας.

2. Υπηρεσίες που σχετίζονται με πράγματα : Η έννοια αυτού του χαρακτηριστικού είναι να παρέχει υπηρεσίες που μπορούν να εφαρμοστούν σε πολλά συνδεδεμένα πράγματα με βάση τους περιορισμούς αυτών των πραγμάτων. Για παράδειγμα, η προστασία της ιδιωτικής ζωής ως υπηρεσία μπορεί να εφαρμοστεί στα ίδια πράγματα με τους περιορισμούς τους.

3. Ετερογένεια : Η δυνατότητα ετερογένειας του IoT προέρχεται από την ιδέα της σύνδεσης διαφορετικών συσκευών που κατασκευάζονται χρησιμοποιώντας διαφορετικό υλικό και τρέχουν σε διαφορετικές πλατφόρμες.

4. Δυναμικές αλλαγές : Το IoT μπορεί να χειριστεί δυναμικές αλλαγές που απαιτούνται από εμπλεκόμενα διαφορετικά αντικείμενα. Θα μπορούσαν να προκύψουν αρκετές δυναμικές αλλαγές όσον αφορά τις αλλαγές κατάστασης, όπως η αδράνεια, η σύνδεση και η αποσύνδεση, ή όσον αφορά τις αλλαγές περιβάλλοντος, όπως η αλλαγή τοποθεσιών.

4.2 Τεχνολογίες IoT

Πολλές μελέτες έχουν επικεντρωθεί στις τεχνολογίες που χρησιμοποιούνται για να επιτρέψουν τις επικοινωνίες που απαιτούνται από το IoT. Διάφορες τεχνικές χρησιμοποιούνται για την παροχή επικοινωνίας μεταξύ συσκευών στο IoT. Για να συνδέσετε συσκευές, κάθε συσκευή πρέπει να αναγνωρίζεται από ένα μοναδικό αναγνωριστικό. Βασικά αυτές οι τεχνολογίες χρησιμοποιούνται για να υλοποιήσουν την πραγματική ιδέα του IoT και να κάνουν δυνατές τις αλληλεπιδράσεις μεταξύ διαφορετικών συσκευών. Παρακάτω παρατίθενται μερικές από αυτές τις τεχνολογίες και προσεγγίσεις (Shah & Yaqoob, 2016) :

1. Ταυτοποιήσεις ραδιοσυχνοτήτων (RFID) : Το RFID είναι ένα ασύρματο σύστημα που αποτελείται από δύο μέρη : ετικέτες και αναγνώστες. Οι ετικέτες είναι προσαρτημένες σε αντικείμενα ή συσκευές που στόχευαν να συνδεθούν και περιέχουν αποθηκευμένες πληροφορίες που συνήθως διαβάζονται από

τους αναγνώστες. Αυτές οι ετικέτες χρησιμοποιούν ραδιοκύματα με διαφορετικές συχνότητες από διαφορετικές κεραίες για να σχηματίσουν μια επικοινωνία μεταξύ συσκευών. Επίσης, αυτές οι ετικέτες μπορεί να είναι παθητικές όταν τροφοδοτούνται από αναγνώστη ή μπορεί να είναι ενεργές όπου τροφοδοτούνται από μπαταρίες.

2. Επικοινωνίες κοντινού πεδίου (NFC) : Το NFC βασίζεται στον ίδιο μηχανισμό της RFID, καθώς διαθέτει ετικέτες και αναγνώστες. Ωστόσο, η ιδέα είναι να ενσωματωθεί αυτή η ιδέα στα έξυπνα τηλέφωνα. Το NFC απεικονίζει την ιδέα των ασύρματων δικτύων μικρής εμβέλειας χαμηλής ισχύος όπου όλες οι συσκευές είναι συνδεδεμένες στον ίδιο τομέα άλλων κινητών τηλεφώνων. Επιτρέπει την αποστολή μικρού όγκου δεδομένων σε έναν συγκεκριμένο τομέα μεταξύ δύο συσκευών. Η τυπική εμβέλεια του NFC είναι 20 μέτρα. Το NFC μπορεί να θεωρηθεί ως μία από τις πιο σημαντικές ραδιοτεχνολογίες που επιτρέπουν στις ασύρματες επικοινωνίες να ενεργοποιήσουν το IoT. Στην πραγματικότητα, αυτή η τεχνολογία θα επιτρέψει τη χρήση έξυπνων τηλεφώνων ως άλλων αντικειμένων που συνδέονται με αυτό.

3. Επικοινωνίες από μηχανή με μηχανή (M2M) : Η έννοια του M2M είναι πολύ παρόμοια με την έννοια του IoT. Στο IoT, η ποικιλομορφία των συνδεδεμένων αντικειμένων είναι ο βασικός οδηγός ενώ στις επικοινωνίες M2M. Η επικοινωνία γίνεται μεταξύ διαφορετικών μηχανημάτων όπως υπολογιστές, επεξεργαστές, αισθητήρες και έξυπνα τηλέφωνα. Το M2M είναι δομημένο σε πέντε μέρη : Συσκευή M2M, M2M Gateways, δίκτυο επικοινωνίας M2M, δίκτυο περιοχής M2M και εφαρμογές M2M. Όλες οι τεχνολογίες που χρησιμοποιούνται για την ενεργοποίηση των επικοινωνιών M2M μπορούν να χρησιμοποιηθούν για την ενεργοποίηση του IoT.

4. Επικοινωνίες οχήματος με όχημα (V2V) : Αυτό το είδος επικοινωνίας απαιτεί μια πολύπλοκη υποδομή δικτύου, καθώς περιλαμβάνει επικοινωνία μέσω οχημάτων. Τα οχήματα συνήθως μετακινούνται από το ένα μέρος στο άλλο, γεγονός που προκαλεί μια μη σταθερή τοπολογία. Για να περιγράψουμε την επικοινωνία V2V, εμπλέκονται δύο τύποι αλληλεπιδράσεων : η αλληλεπίδραση μεταξύ οχήματος και οχήματος και η αλληλεπίδραση μεταξύ οχήματος και οδικής υποδομής.

4.3 Τεχνολογίες για αλληλεπίδραση με 5G

Σε αυτή την ενότητα, παρουσιάζονται αρκετές νέες τεχνολογίες που αποτελούν εξέλιξη στο μέλλον των εφαρμογών IoT. Αυτές οι τεχνολογίες δεν έχουν σχεδιαστεί αρχικά για το IoT, αλλά μπορούν να περιλαμβάνουν εφαρμογές IoT επόμενης γενιάς, όπως νέες υπηρεσίες έξυπνων πόλεων και αυτόνομα οχήματα. Για να αντιμετωπιστούν τέτοιες επερχόμενες απαιτήσεις, αυτές οι

τεχνολογίες πρέπει να ενσωματωθούν στην προτεινόμενη αρχιτεκτονική η οποία περιλαμβάνει τη συνεργασία του IoT με το 5G (Rahimi et al., 2018).

4.3.1 Nano - Chip

Τις τελευταίες δύο δεκαετίες, συσκευές που βασίζονται σε Nano - Chip έχουν βρει γενικές εφαρμογές στην ανάλυση βιολογικών και χημικών δειγμάτων. Ένα μικροσκοπικό τσιπ, το οποίο βάζει κάτω από το δέρμα και μέσω ενός ηλεκτρικού πεδίου, επαναπρογραμματισμένα κύτταρα θα μπορούσε να είναι μια εφεύρεση με τη μορφή που θεραπεύουμε τον τραυματισμένο ή γηρασμένο ιστό. Οι ερευνητές λένε ότι το νανο - τσιπ θα μπορούσε να θεραπεύσει τραυματισμούς ή με ένα άγγιγμα, να αναπτύξει ξανά όργανα. Ωστόσο, η χρήση συσκευών που βασίζονται σε Nano - chip δεν θα περιοριστεί σε ιατρικές εφαρμογές. Για παράδειγμα, αυτή η τεχνολογία θα μπορούσε να χρησιμοποιηθεί σε στρατιωτικές και οικιακές εφαρμογές αυτοματισμού που θα καλύψουν το τεράστιο μέρος των εφαρμογών IoT (Rahimi et al., 2018).

4.3.2 Κύμα χιλιοστών (mmWave)

Την τελευταία δεκαετία, η προσβασιμότητα του φάσματος συχνοτήτων κάτω από τις ζώνες των 6 GHz μειώνεται και το αίτημα για υψηλότερο ρυθμό μετάδοσης δεδομένων αυξάνεται. Οι υψηλότερες συχνότητες, όπως το χιλιοστό κύμα (mmWave), στις οποίες οι ζώνες συχνοτήτων είναι πάνω από 24 GHz, έχουν προταθεί ως υποψήφιες για μελλοντικές εφαρμογές 5G IoT, επειδή θα μπορούσε να εξεταστεί το μεγαλύτερο εύρος ζώνης για να βελτιώσει την ικανότητα και να επιτρέψει στους χρήστες να χρησιμοποιούν πολύ υψηλούς ρυθμούς δεδομένων για εφαρμογές μικρής εμβέλειας. Η ζώνη συχνοτήτων των 24–28 GHz αξιοποιείται ως μία από τις εξεταζόμενες ζώνες για εφαρμογές 5G - IoT (Stanley et al., 2017).

4.3.3 Ετερογενή Δίκτυα (Het - Net)

Τα ετερογενή δίκτυα (HetNet) έχουν σχεδιαστεί για την ικανοποίηση της απαίτησης κατ' απαίτηση του 5G - IoT που οδηγεί σε υπηρεσίες. Αυτό το νέο μοντέλο δικτύωσης επιτρέπει στο 5G - IoT να παρέχει ρυθμό μετάδοσης δεδομένων κατόπιν αιτήματος. Πρόσφατα, ορισμένες λύσεις 5G HetNet έχουν

σχεδιαστεί, οι οποίες θα αναπτύξουν έναν τεράστιο αριθμό συσκευών με περιορισμένους πόρους (Rahimi et al., 2018).

4.3.4 Απευθείας επικοινωνία από συσκευή σε συσκευή (D2D)

H Direct Device - to - Device Communication (D2D) έχει σχεδιαστεί ως ένας νέος τρόπος για τη μετάδοση δεδομένων μικρής εμβέλειας, ο οποίος θα ωφελήσει το 5G - IoT με χαμηλότερη κατανάλωση ενέργειας, καλύτερη QoS για τους χρήστες και εξισορρόπηση φορτίου. Ο παραδοσιακός Σταθμός Βάσης Μακροκυψελών (MBS) θεωρείται ως BS χαμηλής τροφοδοσίας. Ωστόσο, το D2D επιτρέπει τη μετάδοση πληροφοριών μεταξύ εξοπλισμού αιχμής χρήστη χωρίς το BS και χρησιμεύει ως "Cell Tier" στο 5G - IoT (Rahimi et al., 2018).

4.3.5 Ασύρματα συστήματα πέμπτης γενιάς (5G)

Τα δίκτυα πέμπτης γενιάς (5G) γίνονται ο κύριος οδηγός για την ανάπτυξη των εφαρμογών IoT. Το 5G μπορεί να συνεισφέρει σημαντικά στην επόμενη γενιά του IoT συνδέοντας δισεκατομμύρια έξυπνα πράγματα για να δημιουργήσει πραγματικό μελλοντικό και τεράστιο IoT. Προς το παρόν, η αναγνώριση της ικανότητας των συσκευών IoT είναι πολύ δύσκολη, επειδή ο ετερογενής τομέας των εφαρμογών θα πρέπει να ικανοποιεί τις απαιτήσεις της εφαρμογής. Σύμφωνα με την έκθεση της International Data Corporation (IDC), οι υπηρεσίες του παγκόσμιου 5G θα υποστηρίξουν το 70% των εταιρειών να δαπανήσουν 1,2 δισεκατομμύρια δολάρια για τις λύσεις διαχείρισης συνδεσιμότητας. Τα τρέχοντα συστήματα IoT έχουν σχεδιαστεί ευρέως από συγκεκριμένο τομέα εφαρμογών, όπως BLE, ZigBee, άλλες τεχνολογίες, όπως δίκτυα Wi - Fi, LP - WA (Lora, Sixgfox) και κυψελοειδείς επικοινωνίες (3GPP, LTE) κ.λπ. Σήμερα, τα συστήματα IoT βελτιώνουν την ποιότητα των τρόπων ζωής που περιλαμβάνουν τη διασύνδεση μεταξύ έξυπνων οικιακών συσκευών και έξυπνων περιβαλλόντων. Το Industrial IoT (IIoT) εξελίσσει πολλές προκλήσεις, όπως νέες απαιτήσεις για προϊόντα και λύσεις και μετασχηματίζει τα επιχειρηματικά μοντέλα. Οι πιο δημοφιλείς τεχνικές επικοινωνίας στη συνδεσιμότητα του IoT είναι τα δίκτυα 3GPP και LTE (4G) (Astely et al., 2013), τα οποία προσφέρουν συστήματα IoT με αξιοπιστία, διαχρονική, στιβαρότητα σύνδεσης και με μεγάλη κάλυψη, χαμηλό κόστος ανάπτυξης, υψηλό επίπεδο ασφάλειας, πρόσβαση σε αποκλειστικό φάσμα και απλότητα διαχείρισης (Palattella et al., 2016). Ωστόσο, τα υπάρχοντα κυψελοειδή δίκτυα, για παράδειγμα. δεν είναι σε θέση να υποστηρίξουν τις επικοινωνίες MTC αλλά τα δίκτυα 5G - IoT θα μπορούσαν να το παρέχουν. Επιπλέον, το 5G - IoT παρέχει τον ταχύτερο ρυθμό δεδομένων δικτύου κινητής τηλεφωνίας με πολύ χαμηλό

λανθάνοντα χρόνο και βελτιωμένη κάλυψη για την επικοινωνία MTC. Τα τελευταία χρόνια έχουν γίνει διάφορες εργασίες στο 5G - IoT (Astely et al., 2013). Οι CISCO, Intel, Verizon, κ.λπ. έχουν κάνει ασύρματα ερευνητικά έργα στο 5G, τα οποία προσάρμοσαν την ποιότητα του βίντεο στις απαιτήσεις του ανθρώπινου ματιού. Το 5G - IoT παρέχει σε πραγματικό χρόνο, επαναδιαμορφώσιμες, διαδικτυακές εμπειρίες, κατ' απαίτηση και κοινωνικές εμπειρίες σε εφαρμογές IoT. Η αρχιτεκτονική 5G - IoT θα πρέπει να είναι αυτόματη και να μπορεί να συντονίζεται από άκρο σε άκρο και έξυπνα και γρήγορα σε κάθε φάση (Kaplan, 2018).Οι αρχιτεκτονικές 5G - IoT θα παρέχουν :

- Λογικά ανεξάρτητα δίκτυα για τις απαιτήσεις των εφαρμογών.
- Για την ανακατασκευή του δικτύου ραδιοπρόσβασης (RAN) δεσμεύστε το δίκτυο ραδιοπρόσβασης που βασίζεται σε σύννεφο (Cloud RAN) για την παροχή τεράστιων συνδέσεων σε πολλαπλά πρότυπα και την εφαρμογή της κατ' απαίτηση ανάπτυξης των λειτουργιών RAN που απαιτούνται από το 5G.
- Απλοποίηση της αρχιτεκτονικής του βασικού δικτύου για τη σχεδίαση κατά παραγγελία διαμόρφωσης λειτουργιών δικτύου.

4.3.6 Επικοινωνία τύπου μηχανής (MTC)

Οι επικοινωνίες τύπου μηχανής (MTC) ή οι επικοινωνίες από μηχανή σε μηχανή (M2M) αντιπροσωπεύουν αυτοματοποιημένες επικοινωνίες δεδομένων μεταξύ της βασικής υποδομής της μεταφοράς δεδομένων και των συσκευών. Οι επικοινωνίες δεδομένων αναπτύχθηκαν απευθείας μεταξύ δύο συσκευών MTC ή μεταξύ μιας συσκευής MTC και μιας βάσης δεδομένων (Shariatmadari et al., 2015). Η MTC δημιουργεί ένα ευρύ φάσμα εφαρμογών από μια μεγάλη ανάπτυξη αυτόνομων συσκευών έως υπηρεσίες κρίσιμες για την αποστολή. Τα κυψελοειδή συστήματα (ειδικά το 5G) έχουν θεωρηθεί ως σημαντικός υποψήφιος για την παροχή συνδεσιμότητας για συσκευές MTC. Οι συσκευές MTC γίνονται όλο και πιο ουσιαστικό μέρος του τρόπου ζωής μας. Η υψηλή υποστήριξη του ρυθμού δεδομένων και άλλα σημαντικά χαρακτηριστικά του MTC φαίνεται ότι η 5G - Plus - HetNet θεωρεί ως μια ισχυρή τεχνολογική λύση στο 5G - IoT στις αυξανόμενες απαιτήσεις μεταφοράς δεδομένων από συσκευές MTC (Ali et al., 2017).

4.3.7 Ασύρματα δίκτυα καθορισμένα από λογισμικό (WSDN)

Το Wireless Software - Defined Networking (WSDN) είναι μια νέα τεχνολογία που προσεγγίζει το φορητό υπολογιστικό νέφος που βοηθά στη διαχείριση του

δικτύου και επιτρέπει τη διαμόρφωση δικτύου αντί να βελτιώνει την απόδοση του δικτύου ή την παρακολούθηση δικτύου. Τα τρέχοντα δίκτυα απαιτούν μεγαλύτερη ευελιξία και εύκολη αντιμετώπιση προβλημάτων. Για να φτάσει σε αυτό το θέμα, το SDN σπάει την κάθετη αφομοίωση των παραδοσιακών δικτύων και μέσω του κεντρικού ελέγχου δικτύου παρέχει την ευελιξία προγραμματισμού του δικτύου. Το SDN είναι σε θέση να προσαρμόζει τις παραμέτρους του δικτύου του εν κινήσει με βάση τις συνθήκες λειτουργίας του (Rawat & Reddy, 2017). Τα δίκτυα 5G μπορούν να εφαρμοστούν μέσω του παραδείγματος WSDN για να παρέχουν ταχύτερα και επεκτάσιμα συστήματα 5G - IoT (Rahimi et al., 2018).

4.3.8 Προηγμένη διαχείριση κοινής χρήσης και παρεμβολών φάσματος (Advanced SSIM)

Ο χρησιμοποιούμενος πόρος φάσματος είναι περιορισμένος και γεμάτος. Μπορεί να χρειαστούν χρόνια για τον επαναπροσδιορισμό μιας ζώνης φάσματος για τις άλλες χρήσεις, π.χ. η τακτοποίηση ή η τυποποίηση αυτών δεν είναι εύκολη. Η αποτελεσματικότητα του φάσματος είναι μία από τις σημαντικές μετρήσεις απόδοσης στα δίκτυα επικοινωνίας 5G. Για τη βελτίωση της απόδοσης του φάσματος, χρησιμοποιούνται συνήθως προηγμένες τεχνικές κοινής χρήσης φάσματος. Ως εκ τούτου, τα δίκτυα επικοινωνίας 5G αναμένεται να λύσουν το πρόβλημα με διαφορετικές μεθόδους (Zhang et al, 2017).

4.3.9 Mobile Edge Computing (MEC)

Το Edge (Fog) computing είναι ένα κατανεμημένο υπολογιστικό παράδειγμα, το οποίο χρησιμεύει ως μεσαίο επίπεδο μεταξύ της βάσης δεδομένων Cloud και των συσκευών/αισθητήρων IoT. Το Mobile Edge Computing (MEC) πρότεινε να περιγράψει την εκτέλεση υπηρεσιών στην άκρη του δικτύου, η οποία στοχεύει να «παρέχει ένα περιβάλλον υπηρεσίας πληροφορικής και δυνατότητες υπολογιστικού νέφους στην άκρη του δικτύου κινητής τηλεφωνίας». Οι αρχιτεκτονικές και τα πλαίσια αναφοράς MEC διαθέτουν τα λειτουργικά στοιχεία που υποστηρίζουν υπηρεσίες όπως η αναγνώριση θέσης, οι πληροφορίες ραδιοφωνικού δικτύου και η εκτέλεση εφαρμογών. Τα πλεονεκτήματα της επέκτασης των υπηρεσιών cloud στην άκρη των δικτύων κινητής τηλεφωνίας, όπως το 5G, περιλαμβάνουν χαμηλό λανθάνοντα χρόνο, υψηλό εύρος ζώνης και πρόσβαση σε πληροφορίες δικτύου ραδιοφώνου και επίγνωση τοποθεσίας. Έτσι, θα είναι δυνατή η βελτιστοποίηση των τρεχουσών υπηρεσιών υποδομής κινητής τηλεφωνίας ή η εφαρμογή νέων. Το MEC είναι

ένα άλλο βασικό στοιχείο στο 5G - IoT, το οποίο θα επικεντρωθεί σε δύο πτυχές :

- Η επανάσταση της ανάλυσης, τα δίκτυα MEC και 5G θα είναι ο πυρήνας της επόμενης γενιάς IoT.
- Το MEC στο 5G - IoT θα αυξήσει σημαντικά τις εφαρμογές που σχετίζονται με υπολογισμούς που απαιτούν μαζική επεξεργασία, όπως η εικονική πραγματικότητα (VR) ή η επαυξημένη πραγματικότητα (AR).

Η προαναφερθείσα ανάπτυξη θα μειώσει το κόστος και θα παρέχει μια γενική υποδομή διαχείρισης για όλες τις εικονικές υπηρεσίες (Roman et al., 2018).

4.3.10 Εικονικοποίηση λειτουργιών ασύρματου δικτύου (WNFV)

Το Wireless Network Function Virtualization (WNFV) αναφέρεται σε υπηρεσίες και λειτουργίες δικτύου για την ασύρματη προβολή πόρων δικτύου, όπως βάσεις δεδομένων, δρομολογητές, συνδέσμους και δεδομένα, με τρόπο ξεχωριστό από τη γενική φυσική υποδομή και για χρήση αυτών των πόρων ως απαιτήσεις υπηρεσίας όπως χρειάζεται. Το WNFV διαχωρίζει ένα φυσικό δίκτυο σε διάφορα εικονικά δίκτυα, επομένως οι συσκευές μπορούν να διαμορφωθούν εκ νέου ώστε να οργανώνουν διάφορα δίκτυα σύμφωνα με τις απαιτήσεις των εφαρμογών. Το WNFV ως συμπληρωματικό των δικτύων 5G θα επιτρέψει την εικονικοποίηση του συνόλου των λειτουργιών του δικτύου για την απλούστευση της ανάπτυξης του 5G - IoT. Το WNFV παρέχει το επεκτάσιμο και ευέλικτο δίκτυο για εφαρμογές 5G - IoT, το οποίο θα επιτρέψει σε ένα προσαρμοσμένο δίκτυο να δημιουργήσει προγραμματιζόμενα δίκτυα για εφαρμογές 5G - IoT. Στην πραγματικότητα, το WNFV θα παρέχει 5G - IoT διαδικτυακή δυνατότητα επεξεργασίας βελτιστοποιώντας το ρυθμό, την ικανότητα και την κάλυψη στα δίκτυα ώστε να ταιριάζουν στις απαιτήσεις των εφαρμογών. Επιπλέον, το WNFV θα βελτιώσει σημαντικά τη βιωσιμότητα του δικτύου ασύρματης πρόσβασης (RAN). Στο HetNet 5G - IoT, η συμπίεση δικτύου μπορεί να συγκεντρώσει υποδομές 5G με δυνατότητα σύνδεσης πολλαπλών RAT για να ταιριάζει στις απαιτήσεις των υπηρεσιών εφαρμογών (van de Belt et al., 2017).

4.3.11 Mobile Cloud Computing (MCC)

Το cloud computing είναι ένα ενθαρρυντικό υπολογιστικό παράδειγμα στον ακαδημαϊκό χώρο και τη βιομηχανία, το οποίο αναφέρεται στις τεχνολογίες εικονικοποίησης μόχλευσης που παρέχουν μια ποικιλία μοντέλων ανάπτυξης και μοντέλων υπηρεσιών, από τα δημόσια σύννεφα σε ιδιωτικά και από την

Υποδομή ως μοντέλο υπηρεσίας στο λογισμικό. Επίσης, το cloud computing παρέχει υπολογιστικούς πόρους όπως επεξεργαστή, αποθήκευση και δίκτυα ως υπηρεσία. Τα οφέλη, όπως η αποτελεσματική ικανότητα, η αυτοεξυπηρέτηση κατά παραγγελία, η προσβασιμότητα και η επεκτασιμότητα καθιστούν το cloud computing μια ευκαιρία υπολογιστικού πόρου για φορητές συσκευές. Λόγω της φυσικής απόστασης, οι υπηρεσίες cloud δεν μπορούν να έχουν άμεση πρόσβαση σε τοπικές περιστασιακές πληροφορίες, όπως η ακριβής τοποθεσία του χρήστη, οι συνθήκες του τοπικού δικτύου ή η κατάσταση της κινητικότητας των χρηστών. Για εφαρμογές ευαίσθητες σε καθυστερήσεις, όπως το VR και το AR, αυτές οι απαιτήσεις (όπως η υποστήριξη κινητικότητας χαμηλής καθυστέρησης και η επίγνωση περιβάλλοντος) αναμένονται. Το Mobile Cloud Computing (MCC) εστιάζει ουσιαστικά στην έννοια της «εκχώρησης από κινητά» : λόγω των περιορισμένων διαθέσιμων πόρων των φορητών συσκευών, η αποθήκευση μαζικών δεδομένων και η εκτέλεση εργασιών υπολογιστικής έντασης θα πρέπει να ανατίθενται σε απομακρυσμένες οντότητες. Το MCC αναφέρεται σε ένα παράδειγμα, το οποίο αξιοποιεί τους πόρους του Cloud Computing για να βελτιώσει την απόδοση περιορισμένων πόρων. Επί του παρόντος, πολλές από τις υπηρεσίες που εφαρμόζονται σε ένα κεντρικό cloud ή στις ίδιες τις κινητές συσκευές. Υπάρχουν πολλές εφαρμογές (όπως εφαρμογές AR και επαυξημένης διεπαφής (AI)) όπου η παρουσία μιας πλατφόρμας απόδοσης που βρίσκεται στο περιβάλλον των φορητών συσκευών μπορεί να παρουσιάσει πολλά πλεονεκτήματα (όπως χαμηλότερη καθυστέρηση και πρόσβαση σε πληροφορίες περιβάλλοντος). Επιπλέον, καθώς οι κινητές συσκευές είναι εξοπλισμένες με πρακτικά εξαρτήματα (όπως αισθητήρες και κάμερες υψηλής ανάλυσης), είναι δυνατή η δημιουργία συλλογικών εφαρμογών ανίχνευσης ή καινοτόμων crowdsourcing που επιτυγχάνουν τις πληροφορίες τοποθεσίας (Roman et al., 2018).

4.3.12 Data Analytics και Big Data

Μια από τις σημαντικές πτυχές μιας επιτυχημένης εφαρμογής IoT είναι η Data Analytics. Οι εταιρείες ενδιαφέρονται για πληροφορίες που φέρνουν αξία από τεράστια δεδομένα. Η έννοια του Big Data είναι μια αφηρημένη έννοια, η οποία εξαρτάται τακτικά από τη διαμόρφωση του συστήματος (όπως RAM, χώρος σκληρού δίσκου κ.λπ.). Πρόσφατα, η αξία των Big Data έχει αναγνωριστεί, υπάρχουν διαφορετικές απόψεις σχετικά με τον ορισμό των Big Data. Στην πραγματικότητα, τα Big Data αναφέρονται στα σύνολα δεδομένων που δεν μπορούσαν να αναγνωριστούν, να αποκτηθούν, να διαχειριστούν και να επεξεργαστούν αποτελεσματικά από κοινά εργαλεία πληροφορικής και λογισμικού ή συσκευές υλικού. Τεχνολογίες όπως τα Big Data και Data Analytics αλλάζουν τον τρόπο που ζούμε και δημιουργούν πολλές νέες ευκαιρίες. Το έξυπνο εργοστάσιο είναι μια από τις ευκαιρίες, που μπορεί να περιέχει εκατοντάδες αισθητήρες που παράγουν τεράστιες ποσότητες

δεδομένων, Big Data. Οι ανάγκες των ανθρώπων θα μπορούσαν να ικανοποιηθούν περισσότερο με την ανάλυση των Μεγάλων Δεδομένων (Wang et al., 2018).

4.3.13 Ασφάλεια και Εγκληματολογία

Με την ενσωμάτωση του 5G και του IoT, ζητήματα ασφάλειας όπως το απόρρητο, ο έλεγχος πρόσβασης, η ασφαλής επικοινωνία και η ασφαλής αποθήκευση δεδομένων γίνονται σημαντικές προκλήσεις στις Εφαρμογές IoT. Επιπλέον, κάθε συσκευή που έχει κατασκευαστεί και κάθε μεμονωμένο δεδομένα που έχει συγχρονιστεί με μια εφαρμογή IoT τίθεται υπό διερεύνηση. Η μεγάλης κλίμακας διανομή των συσκευών IoT και η ιδιωτική φύση των δεδομένων που έχουν συσσωρευτεί και μεταφερθεί από κόμβους IoT καθιστούν την ασφάλεια πρωταρχική πρόκληση. Δεν θα χρειαστεί πολύς χρόνος για να δούμε ανθρώπους να μηνύουν ο ένας τον άλλον επειδή κακομεταχειρίζονται τα έξυπνα gadget τους, τα σκεπτόμενα οχήματα που έχουν ατύχημα και εγκληματίες που θέτουν σε κίνδυνο μεμονωμένους έξυπνους αισθητήρες. Το IoT έχει αναπτύξει ένα άχυρο, το οποίο περιλαμβάνει πολλά χρήσιμα εγκληματολογικά τεχνουργήματα, ενώ η ταυτοποίηση, η συλλογή, η διατήρηση και η αναφορά τεκμηρίων, όπως μια επίθεση, θα ήταν προκλητική σε αυτό το πλαίσιο (Conti et al., 2018).

Το IoT σύντομα θα διαπεράσει όλες τις πτυχές της ζωής μας, από τη διαχείριση της θερμοκρασίας του σπιτιού μας μέχρι τα έξυπνα αυτοκίνητα και την έξυπνη διαχείριση των πόλεων και οι νέες τεχνολογίες υποστηρίζουν αυτή τη διαδικασία. Οι ερευνητές χρειάζονται μια κοινή γλώσσα για να χρησιμοποιήσουν αυτές τις τεχνολογίες κατάλληλα. Μέχρι τώρα, αυτές οι τεχνολογίες όλες μαζί δεν είναι συμβατές με την τρέχουσα αρχιτεκτονική του IoT. Επομένως, απαιτείται ο σχεδιασμός μιας νέας αρχιτεκτονικής που βασίζεται σε αυτές τις τεχνολογίες. Στην επόμενη ενότητα, παρουσιάζεται η προτεινόμενη αρχιτεκτονική IoT με δυνατότητα 5G (Rahimi et al., 2018).

ΚΕΦΑΛΑΙΟ 5 : ΣΥΝΕΡΓΑΣΙΑ 5G ΚΑΙ IoT

5.1 Αρχιτεκτονική συστήματος 5G - IoT

Η λεγόμενη αρχιτεκτονική 5G - IoT (Rahimi et al., 2018) είναι μια νέα αρχιτεκτονική που χρησιμοποιεί νέες τεχνολογίες για την επίτευξη μιας πιο βιώσιμης και επεκτάσιμης αρχιτεκτονικής IoT από τις υπάρχουσες. Οι νέες τεχνολογίες που χρησιμοποιούνται στην ανάπτυξη της αρχιτεκτονικής 5G - IoT το καθιστούν απλό και βολικό για επεκτασιμότητα, ανάλυση και αρθρωτότητα. Τα χαρακτηριστικά αυτής της αρχιτεκτονικής περιλαμβάνουν αποτελεσματικότητα, ευελιξία, επεκτασιμότητα, απλότητα και προσβασιμότητα για υπηρεσίες υψηλής ζήτησης. Η αρχιτεκτονική 5G - IoT, η οποία φαίνεται στην Εικόνα 2, έχει σχεδιαστεί σε οκτώ διασυνδεδεμένα επίπεδα με δυνατότητα αμφίδρομης ανταλλαγής δεδομένων. Αυτά τα στρώματα εξηγούνται εν συντομία ως εξής (Rahimi et al., 2018).

L.1 Επίπεδο φυσικής συσκευής. Αυτό το επίπεδο αποτελείται από ασύρματους αισθητήρες, ενεργοποιητές και ελεγκτές που είναι τα πράγματα του IoT. Το επίπεδο φυσικής συσκευής είναι ένα γενικό επίπεδο μεταξύ όλων των αρχιτεκτονικών.

L.2 Επίπεδο επικοινωνίας. Αυτό το στρώμα αποτελείται από δύο υποστρώματα. Επίπεδα επικοινωνίας και συνδεσιμότητας D2D, τα οποία επεξηγούνται ως εξής.

- Direct Device To Device (D2D) Communication SubLayer. Σε αυτό το υποεπίπεδο, το 5G είναι σε θέση να βελτιώσει την επικοινωνία D2D, η οποία είναι σημαντικός υποψήφιος για την παροχή συνδεσιμότητας για συσκευές Επικοινωνίας Τύπου Μηχανής (MTC).
- Υποστρώμα συνδεσιμότητας. Στο υποεπίπεδο συνδεσιμότητας, οι συσκευές (π.χ. κινητά τηλέφωνα και ταμπλέτες) συνδέονται με κέντρα επικοινωνίας, όπως τα BS. Η ανάλυση δεδομένων γίνεται από αυτές τις συσκευές και αποστέλλεται μέσω κέντρων με σύνδεση Intranet στη μονάδα αποθήκευσης. Αυτό το υποεπίπεδο του 5G - IoT καθορίζεται με υψηλή αξιοπιστία, απόδοση και ευελιξία.

L.3 Edge (Fog) Computing Layer. Σε αυτό το επίπεδο, τα δεδομένα υποβάλλονται σε επεξεργασία από τους κόμβους ή τους ηγέτες τους προκειμένου να ληφθούν αποφάσεις σε επίπεδο Edge.

L.4 Επίπεδο αποθήκευσης δεδομένων. Οι μονάδες αποθήκευσης δεδομένων σε αυτό το επίπεδο λαμβάνουν τις πληροφορίες της επεξεργασίας ακμών από τις φυσικές συσκευές. Είναι υπεύθυνο για το χειρισμό τεράστιου όγκου δεδομένων και κίνησης μελλοντικών εφαρμογών. Σε αυτό το επίπεδο, η ασφάλεια των δεδομένων είναι απαραίτητη προϋπόθεση.

L.5 Επίπεδο υπηρεσίας διαχείρισης. Αυτό το επίπεδο αποτελείται από τρία υποεπίπεδα, συμπεριλαμβανομένων 1) Υποστρώματος Διαχείρισης Δικτύου,

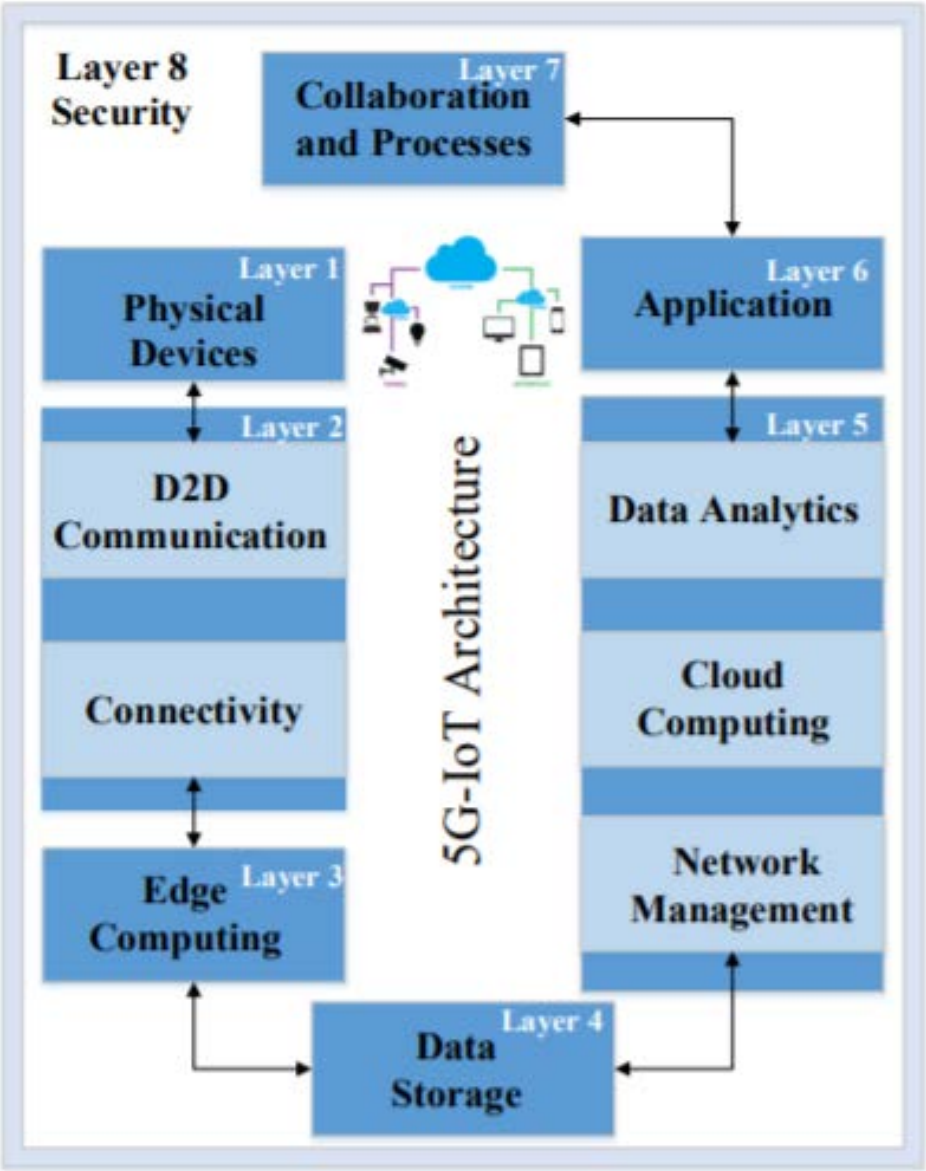
2) Υποστρώματος Υπολογιστικού Νέφους και 3) Υποστρώματος Αναλύσεων Δεδομένων ως εξής.

- Υποεπίπεδο διαχείρισης δικτύου. Το υποεπίπεδο διαχείρισης δικτύου ενεργεί για την επικοινωνία μεταξύ των συσκευών και των κέντρων δεδομένων. Η τεχνολογία Wireless Network Functionality Virtualization (WNFV) σε αυτό το επίπεδο είναι συνεπής με το δίκτυο και τον τύπο των πρωτοκόλλων επικοινωνίας, όπως το 5G - IoT ή το ZigBee. Το Wireless Software Defined Network (WSDN) είναι μια άλλη τεχνολογία που χρησιμοποιείται σε αυτό το υποεπίπεδο που διαχειρίζεται το δίκτυο IoT και επιτρέπει την αναδιαμόρφωση δικτύου αντί της παραδοσιακής παρακολούθησης δικτύου για βελτίωση της απόδοσης.
- Υποεπίπεδο υπολογιστικού νέφους. Σε αυτό το υπο - στρώμα, τα δεδομένα από το επίπεδο L. 3 μπορούν να υποβληθούν σε επανεπεξεργασία. Στη συνέχεια, μπορούν να δημιουργηθούν οι τελικές επεξεργασμένες πληροφορίες. Η τεχνολογία 5G επιτρέπει στις κινητές συσκευές να εκτελούν το Mobile Cloud Computing (MCC) σε πραγματικό χρόνο. Αυτό κάνει την αρχιτεκτονική πιο αποτελεσματική, βιώσιμη, επεκτάσιμη και ταχύτερη.
- Υποεπίπεδο ανάλυσης δεδομένων. Σε αυτό το υποεπίπεδο, οι νέοι αλγόριθμοι μάθησης της ανάλυσης δεδομένων μπορούν να εφαρμοστούν σε πληροφορίες του τελευταίου υποστρώματος για τη δημιουργία τιμών για τη λήψη αποφάσεων, την ταξινόμηση κ.λπ. Καθώς ο όγκος των πληροφοριών που συλλέγονται από ένα δίκτυο IoT είναι εξαιρετικά αυξημένος στο εγγύς μέλλον, ο ρόλος αυτού του υποστρώματος γίνεται πιο κυρίαρχος.

L.6 Επίπεδο Εφαρμογής. Αυτό το επίπεδο είναι χρήσιμο για επιχειρηματίες που ελπίζουν να κάνουν το σωστό πράγμα την κατάλληλη στιγμή με τα σωστά δεδομένα. «Οι εφαρμογές αυτού του επιπέδου φέρνουν επανάσταση στις κάθετες αγορές και τις επιχειρηματικές ανάγκες μέσω εφαρμογών ελέγχου, κάθετων και φορητών εφαρμογών και επιχειρηματικής ευφυΐας και ανάλυσης».

L.7 Επίπεδο συνεργασίας και διαδικασιών. Στην αρχιτεκτονική 5G - IoT, αυτό το επίπεδο επιτρέπει στα άτομα να συνεργάζονται και να επικοινωνούν σε υπηρεσίες IoT, καθώς οι πληροφορίες που προέρχονται από τα προηγούμενα επίπεδα δεν πρόκειται να χρησιμοποιηθούν από μία μόνο οντότητα.

L.8 Επίπεδο Ασφαλείας. Αυτό το επίπεδο είναι ένα μεμονωμένο επίπεδο που προστατεύει όλα τα προηγούμενα επίπεδα χωρίς να διαταράσσει άλλες λειτουργίες του επιπέδου. Αυτό το επίπεδο παρέχει μια ταξινόμηση ασφάλειας για τον αποκλεισμό και την πρόβλεψη των κινδύνων και των κυβερνοεπιθέσεων. Ωστόσο, δεν είναι ακόμη σαφές πώς το επίπεδο ασφαλείας μπορεί να χειριστεί ή να νικήσει τις γνωστές επιθέσεις και τους κινδύνους ασφαλείας.



Εικόνα 2 : Αρχιτεκτονική συστήματος 5G - IoT (Rahimi et al., 2018)

5.2 Απαιτήσεις ασφαλείας και πιθανές επιθέσεις σε επικοινωνία IoT με δυνατότητα 5G

Στη συνέχεια, συζητούνται διάφορα θέματα «ασφάλειας και απορρήτου» της επικοινωνίας IoT με δυνατότητα 5G. Εκτός από αυτό συζητούνται οι απαιτήσεις ασφαλείας και οι πιθανές επιθέσεις.

5.2.1 Θεματα ασφαλείας και ιδιωτικότητας στις επικοινωνίες IoT - 5G

Παρόλο που το IoT αναπτύσσεται ταχέως και οι ερευνητές ανακάλυψαν τις νέες τεχνικές για να διορθώσουν τα προβλήματα στην επικοινωνία IoT, ωστόσο, εξακολουθεί να αντιμετωπίζει ζητήματα ασφάλειας και απορρήτου (Assiri & Almagwashi, 2018; Hou et al., 2019; Al - Garadi et al., 2020).

Έλλειψη ισχυρών σχημάτων ασφαλείας : Οι συσκευές IoT συνδέονται με το σύστημα, π.χ. επιτραπέζιους υπολογιστές ή smartphone. Σε ένα τέτοιο περιβάλλον η έλλειψη μηχανισμού ασφαλείας βελτιώνει την απειλή διαρροής προσωπικών δεδομένων. Τα δεδομένα που συλλέγονται και μεταδίδονται των συσκευών IoT ενδέχεται να αποκαλυφθούν (δηλαδή, δεδομένα υγείας που συλλέγονται μέσω έξυπνων συσκευών υγειονομικής περίθαλψης).

Ανοιχτότητα δικτύου : Είναι απαραίτητη η σύνδεση συσκευών IoT με δίκτυο καταναλωτών που έχουν σύνδεση με τα άλλα συστήματα. Είναι επίσης πιθανό οι συσκευές IoT να κατανοούν ορισμένες ευπάθειες ασφαλείας, οι οποίες μπορεί να είναι επιβλαβείς για το δίκτυο των καταναλωτών. Επειδή μπορεί να γίνει το σημείο εισόδου για τον εισβολέα για να εισέλθει στο σύστημα.

Απόρρητο ευαίσθητων δεδομένων : Το περιβάλλον IoT αποτελείται από διαφορετικούς τύπους συσκευών, οι οποίες διαθέτουν διάφορους τύπους υλικού και λογισμικού. Ορισμένα από αυτά μπορεί να είναι ευάλωτα σε διαφορετικές επιθέσεις, π.χ. επανάληψη, MITM, πλαστοπροσωπία, εικασία κωδικού πρόσβασης κ.λπ. Επομένως, τα ευαίσθητα δεδομένα ενδέχεται να διαρρεύσουν μέσω μη εξουσιοδοτημένης πρόσβασης και χειρισμών. Ορισμένες από αυτές τις συσκευές μεταδίδουν τα προσωπικά στοιχεία του χρήστη, όπως όνομα, διεύθυνση, αριθμό επικοινωνίας, ημερομηνία γέννησης, δεδομένα υγείας και πιστωτική κάρτα. Ως εκ τούτου, απαιτείται πάντα η προστασία της επικοινωνίας του IoT από πιθανές επιθέσεις.

5.2.2 Απαιτήσεις ασφαλείας σε επικοινωνία IoT με δυνατότητα 5G

Οι βασικές απαιτήσεις ασφάλειας σε περιβάλλον IoT με δυνατότητα 5G μαζί με τις «γενικές απαιτήσεις ασφάλειας» είναι οι εξής (Stallings, 2010; Wazid et al., 2021) :

- Διαδικασία ελέγχου ταυτότητας : Αυτή η διαδικασία χρησιμοποιείται για την επικύρωση των ταυτοτήτων των συσκευών που επικοινωνούν (δηλαδή της συσκευής IoT). Η αμοιβαία επαλήθευση ταυτοτήτων είναι υποχρεωτική για την έναρξη μιας ασφαλούς επικοινωνίας και θα πρέπει να διεξάγεται εκ των προτέρων. Σε ένα περιβάλλον IoT με δυνατότητα 5G, ο έλεγχος ταυτότητας μπορεί να πραγματοποιηθεί μεταξύ των έξυπνων συσκευών IoT, διαφόρων ειδών διακομιστών (δηλαδή διακομιστών cloud, fog, edge), διαφόρων ειδών χρηστών, παρόχων υπηρεσιών και κόμβων πύλης.
- Ιδιότητα ακεραιότητας : Παρέχει διασφάλιση πραγματικών και ακριβών δεδομένων. Η σύνθεση του ληφθέντος μηνύματος δεν πρέπει να περιλαμβάνει παράνομη ένεση, μη εγκεκριμένη τροποποίηση και αφαίρεση. Τα δεδομένα θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη τροποποίηση.
- Ιδιότητα εμπιστευτικότητας : Αυτή η ιδιότητα παρέχει προστασία πληροφοριών από κάθε είδους μη εξουσιοδοτημένη πρόσβαση. Με άλλο τρόπο, είναι γνωστό ως «απόρρητο» που προστατεύει τα ανταλλασσόμενα μηνύματα από κάθε είδους επιθέσεις αποκάλυψης.
- Ιδιότητα μη απόρριψης : Διαβεβαιώνει ότι οποιαδήποτε οντότητα δεν πρέπει να αρνηθεί την εγκυρότητα κάτι, για παράδειγμα, ενός μηνύματος. Είναι μια από τις σημαντικές υπηρεσίες στην «ασφάλεια πληροφοριών» που παρέχει αποδείξεις σχετικά με την «προέλευση του μηνύματος» και «την ακεραιότητα των δεδομένων» σε αυτό το μήνυμα.

  Επομένως, είναι πολύ δύσκολο για τις παράνομες οντότητες να αρνηθούν την «προέλευση του μηνύματος» και «την αυθεντικότητα του μηνύματος». Οι μέθοδοι ψηφιακών υπογραφών είναι χρήσιμες για «μη απόρριψη». Για παράδειγμα, σε περίπτωση διαδικτυακών συναλλαγών, όπου είναι σημαντικό να διασφαλιστεί ότι ένα μέρος στο οποίο συνήφθη η σύμβαση (ανακοινωθέν μέρος) δεν θα πρέπει να αρνηθεί την πρωτοτυπία της υπογραφής του/της στην αναφορά. Έχει τις εξής κατηγορίες :

  – Μη απόρριψη πηγής : Παρέχει διαβεβαίωση γνησιότητας του αποστολέα. Αυτό καταλήγει στο συμπέρασμα ότι το μήνυμα μεταδόθηκε από την αυθεντική πηγή.

  – Μη αποκήρυξη προορισμού : Παρέχει διαβεβαίωση γνησιότητας του παραλήπτη. Αυτό καταλήγει στο συμπέρασμα ότι το μήνυμα ελήφθη από τον γνήσιο δέκτη.

- Διαδικασία εξουσιοδότησης : Η διαδικασία εξουσιοδότησης χρησιμοποιείται για τη ρύθμιση των προνομίων συσκευής ή χρήστη (δηλαδή, περιορισμοί πρόσβασης) για πόρους δικτύου ή συστήματος (δηλαδή αρχεία, εφαρμογές δεδομένων και υπηρεσίες). Γενικά, προβλέπεται μέσω διαδικασίας ελέγχου ταυτότητας για την επαλήθευση των ταυτοτήτων της συσκευής ή του χρήστη. Γενικά, μια αρχή (για παράδειγμα, ένας διαχειριστής) σχεδιάζει και εφαρμόζει τους κανόνες πρόσβασης για όλους τους διαθέσιμους πόρους.
- Ιδιότητα ανανέωσης δεδομένων : Αυτή η ιδιότητα παρέχει διασφάλιση «ανανέωσης δεδομένων». Ως εκ τούτου, η παράνομη οντότητα δεν θα μπορεί να μεταδώσει εκ νέου τα μηνύματα που ανταλλάχθηκαν προηγουμένως.
- Ιδιότητα διαθεσιμότητας : Παρέχει διαβεβαίωση ότι οι πληροφορίες είναι διαθέσιμες μόνο σε αυθεντικές οντότητες. Εάν ένας αντίπαλος δεν είναι σε θέση να προκαλέσει την επίθεση κατά της εμπιστευτικότητας και της ακεραιότητας, τότε μπορεί να αντιμετωπίσει άλλες επικίνδυνες επιθέσεις, όπως επίθεση κατανεμημένης άρνησης υπηρεσίας (DDoS) σε διακομιστή ιστού που καταστρέφει τους συσχετιζόμενους ιστότοπους.
- Ιδιότητα προώθησης μυστικότητας : Εάν μια οντότητα (για παράδειγμα, έξυπνος οικιακός χρήστης, έξυπνη συσκευή IoT) εγκαταλείψει το δίκτυο επικοινωνίας, τότε δεν πρέπει να έχει καμία δυνατότητα πρόσβασης στα μελλοντικά μηνύματα.
- Ιδιότητα Backward Secrecy : Εάν μια οντότητα (για παράδειγμα, έξυπνος οικιακός χρήστης, έξυπνη συσκευή IoT) έχει μόλις αναπτυχθεί στο δίκτυο επικοινωνίας, τότε αυτή η οντότητα δεν θα πρέπει να έχει πρόσβαση στα μηνύματα που έχουν ανταλλάξει προηγουμένως.

5.2.3 Πιθανές επιθέσεις σε επικοινωνία IoT με δυνατότητα 5G

Μια επικοινωνία IoT με δυνατότητα 5G μπορεί να έχει τις ακόλουθες πιθανές επιθέσεις που μπορεί να εκτελεστούν από έναν παθητικό ή έναν ενεργό αντίπαλο (Das & Zeadally, 2019; Wazid et al., 2021) :

- Υποκλοπή : Ονομάζεται επίσης ως εισπνοή ή επίθεση. Συμβαίνει σε περίπτωση που ο εισβολέας κρυφακούει τα μηνύματα που ανταλλάσσονται μεταξύ των μερών που επικοινωνούν. Είναι μία από τις πιθανές επιθέσεις στην επικοινωνία IoT με δυνατότητα 5G, καθώς αυτό θα βοηθήσει τον εισβολέα να εξαπολύσει περαιτέρω επιθέσεις.
- Ανάλυση κυκλοφορίας : Είναι μια άλλη μορφή παθητικής επίθεσης κατά την οποία ο εισβολέας κάνει την υποκλοπή και εξετάζει τα μηνύματα που ανταλλάσσονται για να καταλάβει τι συμβαίνει εκεί.

- Επίθεση επανάληψης : Συμβαίνει όταν ένας εισβολέας παρεμποδίζει τα μηνύματα που ανταλλάσσονται και στη συνέχεια καθυστερεί ή τα εκπέμπει με δόλο για να μπερδέψει την οντότητα που λαμβάνει.
- Man - in - the - middle attack (MITM) : Σε αυτήν την κακοήθη δραστηριότητα, ο εισβολέας απαλλοτριώνει πρώτα τα μεταδιδόμενα μηνύματα και στη συνέχεια επιχειρεί να ενημερώσει ή να διαγράψει τα μηνύματα προτού τα προωθήσει στον δέκτη.
- Επίθεση πλαστοπροσωπίας : Σε αυτήν την κακόβουλη δραστηριότητα, ένας επιτιθέμενος προσδιορίζει επιτυχώς την ταυτότητα ενός γνήσιου μέρους επικοινωνίας και στη συνέχεια δημιουργεί ένα μήνυμα και το στέλνει στον παραλήπτη εξ ονόματος του ‘’ γνήσιου μέρους επικοινωνίας ’’.
- Επίθεση Denial - of - Service : Σε αυτήν την κακοήθη δραστηριότητα, ένας αντίπαλος εκτελεί ορισμένες εκδικητικές εργασίες για να αποτρέψει την πρόσβαση των νόμιμων μερών στους πόρους του δικτύου ή του συστήματος (για παράδειγμα, κάποιος πόρος δεδομένων ή κάποια συσκευή IoT). Υπάρχει επίσης μια παραλλαγή DoS επίθεσης, που ονομάζεται επίθεση «Distributed DoS (DDoS)», η οποία διεξάγεται μέσω των πολλαπλών συστημάτων εισβολέων ταυτόχρονα. Μερικά από τα παραδείγματα είναι οι επιθέσεις πλημμύρας UDP, HTTP, TCP SYN. Τα πλημμυρισμένα πακέτα κάτω από αυτές τις επιθέσεις καταναλώνουν τους πόρους (για παράδειγμα, εύρος ζώνης) του στοχευμένου συστήματος (δηλαδή, διακομιστές ιστού) πολύ γρήγορα. Σε μια επικοινωνία IoT με δυνατότητα 5G, η επίθεση DoS μπορεί επίσης να εκτελεστεί μέσω άλλων τύπων επιθέσεων δρομολόγησης, για παράδειγμα, επιθέσεις καταβόθρα, σκουληκότρυπα, γκρίζο τρύπα, μαύρη τρύπα και επιθέσεις λανθασμένης κατεύθυνσης. Σε τέτοιες επιθέσεις, οι φυσικώς αναπτυσσόμενοι κόμβοι εισβολέα διαταράσσουν τη συνεχιζόμενη διαδικασία δρομολόγησης για απόρριψη, καθυστέρηση ή τροποποίηση των πακέτων που ανταλλάσσονται. Παρουσία τέτοιων επιθέσεων, τα μηνύματα δεδομένων (πακέτα) ενδέχεται να τροποποιηθούν, να καθυστερήσουν ή να απορριφθούν πριν φτάσουν στον προβλεπόμενο παραλήπτη. Αυτό προκαλεί αύξηση της «καθυστέρησης από άκρο σε άκρο», μείωση της «απόδοσης» και επηρεάζει επίσης τις άλλες παραμέτρους απόδοσης δικτύου.
- Επίθεση βάσης δεδομένων : Σε μια επικοινωνία IoT με δυνατότητα 5G, οι επιθέσεις που σχετίζονται με τη βάση δεδομένων είναι επίσης εφικτές στη βάση δεδομένων που διαχειρίζεται μέσω διαφορετικών διακομιστών, π.χ. διακομιστή ομίχλης, διακομιστή cloud. Τα παραδείγματα είναι «Επίθεση δομημένης γλώσσας ερωτήματος (SQL), «Επίθεση δέσμης ενεργειών μεταξύ ιστότοπων (XSS)» και «Πλαστογραφία αιτημάτων μεταξύ ιστότοπων (CSRF)». Ο υπάρχων αντίπαλος εξαπολύει αυτές τις επιθέσεις για να βλάψει τα χρηματοοικονομικά περιουσιακά στοιχεία, για παράδειγμα, μπορεί να πραγματοποιήσει παράνομη μεταφορά χρημάτων από λογαριασμό

εξουσιοδοτημένου χρήστη ή να αλλάξει τον κωδικό πρόσβασης ενός λογαριασμού γνήσιου χρήστη.

- Επίθεση κακόβουλου λογισμικού : Μερικές φορές ένας αντίπαλος εκτελεί κακόβουλο σενάριο σε απομακρυσμένο σύστημα για να εκτελέσει διάφορες μη εξουσιοδοτημένες δραστηριότητες, για παράδειγμα, κλοπή, διαγραφή, ενημέρωση και κρυπτογράφηση σημαντικών πληροφοριών. Το κακόβουλο λογισμικό μπορεί να είναι διαφορετικών τύπων, για παράδειγμα, ιοί, σκουλήκια, keylogger, spyware, ransomware και δούρειοι ίπποι. Χρησιμοποιούνται επίσης για την παρακολούθηση των δραστηριοτήτων των χρηστών χωρίς τη συγκατάθεσή του/της. Για τη διάδοση κακόβουλου λογισμικού σε περιβάλλον IoT, ο αντίπαλος μπορεί να χρησιμοποιήσει botnet (συσχετισμένα και συνεργαζόμενα συστήματα εισβολέων). Τα botnets όπως τα Mirai, Reaper, Echobot και Necurs είναι ενεργά αυτές τις μέρες. Αυτές οι επιθέσεις μπορεί επίσης να βλάψουν τη λειτουργία του περιβάλλοντος IoT με δυνατότητα 5G. Μια έξυπνη συσκευή IoT μπορεί να παραβιαστεί (ελεγχθεί) εξ αποστάσεως χρησιμοποιώντας κακόβουλο λογισμικό. Μερικές φορές είναι πολύ επικίνδυνο για τους ανθρώπους (για παράδειγμα, ο έξυπνος βηματοδότης πιθανότατα ενεργοποιεί μη απαραίτητους ηλεκτρικούς παλμούς για έναν ασθενή και υπό τέτοιες συνθήκες ο ασθενής μπορεί να πεθάνει).
- Επίθεση Insider : Σε αυτήν την κακόβουλη δραστηριότητα, «ένας privilegedinsider user» της αξιόπιστης αρχής εκμεταλλεύεται τις αποθηκευμένες πληροφορίες για να εισάγει άλλες σοβαρές επιθέσεις, όπως υπολογισμό κλειδιού συνεδρίας, επίθεση εικασίας κωδικού πρόσβασης.
- Φυσική καταγραφή αναπτυγμένων συσκευών : Η φυσική παρακολούθηση συσκευών IoT δεν είναι δυνατή για 24 × 7 ώρες. Ως εκ τούτου, μερικές φορές ο αντίπαλος παίρνει ευκαιρία να συλλάβει αυτές τις συσκευές φυσικά και στη συνέχεια προσπαθεί να εξαγάγει τις ευαίσθητες πληροφορίες (δηλαδή ταυτότητες, μυστικά κλειδιά κ.λπ.) από τις μνήμες αυτών των συσκευών.

Περαιτέρω, ο αντίπαλος μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για τη διεξαγωγή άλλων ανεπιθύμητων δραστηριοτήτων (για παράδειγμα, πλαστοπροσωπία, εικασία κωδικού πρόσβασης, υπολογισμός κλειδιού συνεδρίας και επιθέσεις man - in - the - middle (MITM)) σε περιβάλλον IoT με δυνατότητα 5G (Wazid et al., 2021).

5.3 Υπάρχοντα πρωτόκολλα ασφαλείας σε περιβάλλον επικοινωνιών IoT με δυνατότητα 5G

Τα πρωτόκολλα ασφαλείας σε περιβάλλον επικοινωνιών IoT με δυνατότητα 5G μπορούν να χωριστούν σε τέσσερις κατηγορίες. Στη συνέχεια, παρέχονται οι λεπτομέρειες ορισμένων από τα υπάρχοντα πρωτόκολλα που ανήκουν σε αυτές τις κατηγορίες.

5.3.1 Υπάρχοντα πρωτόκολλα βασικής διαχείρισης στο περιβάλλον IoT

Οι λεπτομέρειες των σχημάτων ελέγχου ταυτότητας και διαχείρισης κλειδιών παρουσιάζονται στο επόμενο μέρος αυτής της ενότητας. Οι Li et al. (2009) παρουσίασαν ένα ιεραρχικό μοντέλο βασισμένο σε ταυτότητα για το cloud computing. Το μοντέλο αυτό έχει συσχετίσει τεχνικές κρυπτογράφησης και υπογραφής που χρησιμοποιήθηκαν στο σχεδιασμό συστημάτων ελέγχου ταυτότητας βάσει υπηρεσιών ταυτότητας για υπηρεσίες cloud computing. Αποδείχθηκε ότι η παρουσιαζόμενη μέθοδος ήταν αποτελεσματική από το «πρωτόκολλο ελέγχου ταυτότητας στρώματος ασφαλούς υποδοχής (SSL)».

Οι Li et al. (2015) χρησιμοποίησαν την «κρυπτογραφία ελλειπτικής καμπύλης (ECC)» για το σχεδιασμό ενός πρωτοκόλλου ελέγχου ταυτότητας κατάλληλου για περιβάλλον υπολογιστικού νέφους.

Οι Hu et al. (2017) πρότειναν μεθόδους για έλεγχο ταυτότητας, κρυπτογράφηση δεδομένων και έλεγχο ακεραιότητας δεδομένων. Οι μέθοδοι προτάθηκαν για την επίτευξη ιδιοτήτων εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας.

Οι Mishra et al. (2018) πρότειναν επίσης ένα σύστημα ελέγχου ταυτότητας και διαχείρισης κλειδιών για ασφαλείς επικοινωνίες πολυμέσων σε WSN με δυνατότητα IoT. Αργότερα, παρατηρήθηκε ότι ορισμένα από τα υπάρχοντα σχήματα στερούνται χαρακτηριστικά ασφάλειας και λειτουργικότητας, όπως διάφορες επιθέσεις όπως "κλοπή έξυπνης κάρτας", "πλαστοπροσωπία", "μάντευση κωδικού πρόσβασης", "επανάληψη" και οι επιθέσεις ήταν δυνατές (Wazid et al., 2016).

Οι Sharif et al. (2019) πρότειναν «ένα ελαφρύ σύστημα ελέγχου ταυτότητας και συμφωνίας κλειδιού» για WSN που βασίζονται στο IoT. Η επίσημη επαλήθευση ασφαλείας με τη χρήση του αυτοματοποιημένου επίσημου λογισμικού επαλήθευσης ασφαλείας που ονομάζεται «Αυτόματη επικύρωση πρωτοκόλλων και εφαρμογών ασφάλειας Διαδικτύου» (AVISPA, 2019) παρέχεται επίσης (Sharif et al., 2019).

Τέλος, οι Wazid et al. (2019) πρότειναν μια τεχνική «διαχείρισης κλειδιών και ελέγχου ταυτότητας» για την ασφαλή επικοινωνία σε περιβάλλον υπολογιστών ομίχλης. Η διαδικασία διαχείρισης κλειδιών χρησιμοποιήθηκε για τις «έξυπνες

συσκευές και διακομιστές ομίχλης» και «διακομιστές ομίχλης και διακομιστές cloud», «δημιουργία κλειδιών κατά ζεύγη» για την ασφαλή επικοινωνία.

5.3.2 Υπάρχοντα πρωτόκολλα αυτονόμησης χρηστών στο περιβάλλον IoT

Οι λεπτομέρειες των πρωτοκόλλων ελέγχου ταυτότητας χρήστη σε περιβάλλον IoT δίνονται ως εξής. Αρχικά, οι Porambage et al. (2014) πρότειναν ένα «σχήμα ελέγχου ταυτότητας που βασίζεται σε πιστοποιητικά» σε WSN για κατανεμημένες εφαρμογές IoT. Το αναπτυγμένο σχήμα είχε «πρωτόκολλο ελέγχου ταυτότητας δύο φάσεων» που επέτρεπε στους κόμβους αισθητήρων και στους τελικούς χρήστες να ελέγχουν ο ένας τον άλλον και να διατηρούν μια ασφαλή σύνδεση.

Οι Porambage et al. (2015) παρουσίασαν δύο πρωτόκολλα δημιουργίας ομάδας κλειδιών για ασφαλή επικοινωνία IoT. Οι συνθήκες ανάπτυξης και οι απαιτήσεις των πρωτοκόλλων περιγράφηκαν επίσης από την άποψη των σεναρίων εφαρμογών IoT. Τα προτεινόμενα πρωτόκολλα αναλύθηκαν και αιτιολογήθηκαν επίσης όσον αφορά την ανάλυση των επιδόσεων, την επεκτασιμότητα και την ασφάλεια.

Οι Turkanovic et al. (2014) πρότειναν «ένα σύστημα ελέγχου ταυτότητας χρήστη και συμφωνίας κλειδιού» για ετερογενή WSN που εφαρμόζονται στο IoT. Το παρουσιαζόμενο σχήμα βοήθησε τον απομακρυσμένο χρήστη να δημιουργήσει ένα ασφαλές κλειδί συνεδρίας με έναν κόμβο αισθητήρα με τη βοήθεια ενός ελαφρού μηχανισμού συμφωνίας κλειδιού. Η παρουσιαζόμενη μέθοδος εξασφάλισε επίσης τον «αμοιβαίο έλεγχο ταυτότητας» μεταξύ του χρήστη, του κόμβου αισθητήρα και του κόμβου πύλης. Το παρουσιαζόμενο σχήμα τους θα μπορούσε να προσαρμοστεί για το περιορισμένο σε πόρους WSN, καθώς χρησιμοποιούσε μόνο «απλό κατακερματισμό» και «υπολογισμούς XOR».

Οι Farash et al. (2016) πρότειναν ένα πρωτόκολλο για «έλεγχο ταυτότητας χρήστη και συμφωνία κλειδιού» για ετερογενή WSN που ισχύει για περιβάλλον IoT.

Οι Challa et al. (2017) παρουσίασαν ένα πρωτόκολλο ελέγχου ταυτότητας χρήστη για εφαρμογές IoT. Το παρουσιαζόμενο σχήμα βασίστηκε στην «κρυπτογραφία ελλειπτικής καμπύλης (ECC)» και εξαρτιόταν από την «ψηφιακή υπογραφή που βασίζεται σε ECC». Το παρουσιαζόμενο σχήμα υποστήριζε ιδιότητες ανωνυμίας χρήστη και μη ιχνηλασιμότητας. Ωστόσο, αυτό το σύστημα χρειαζόταν περισσότερο κόστος υπολογισμού και επικοινωνίας.

Οι Wazid et al. (2020) πρότειναν «ένα ελαφρύ πρωτόκολλο ελέγχου ταυτότητας» σε περιβάλλον IoT που βασίζεται στο cloud (LAM - CIoT). Μέσω

του LAM - CIoT, ένας πιστοποιημένος χρήστης μπορούσε να έχει πρόσβαση στα δεδομένα ενός απομακρυσμένου αισθητήρα IoT με ασφάλεια. Το LAM - CIoT χρησιμοποίησε αποτελεσματικές «μονόδρομες κρυπτογραφικές συναρτήσεις κατακερματισμού» μαζί με «λειτουργίες XOR κατά bitwise». Το LAM - CIoT αναλύθηκε επίσης ως προς την ασφάλεια με τη βοήθεια επίσημης ανάλυσης ασφαλείας χρησιμοποιώντας το ευρέως χρησιμοποιούμενο μοντέλο "Real - Or - Random (ROR)", επίσημη επαλήθευση ασφάλειας μέσω " Automated Validation of Internet Security Protocols and Applications (AVISPA) " καθώς και άτυπη ανάλυση ασφάλειας. Τελικά αποδείχτηκε η ανθεκτικότητα του παρουσιαζόμενου πρωτοκόλλου έναντι πιθανών επιθέσεων.

5.3.3 Υπάρχοντα πρωτόκολλα ελέγχου πρόσβασης στο περιβάλλον IoT

Τα γεγονότα των πρωτοκόλλων ελέγχου πρόσβασης σε περιβάλλον IoT παρουσιάζονται στο ακόλουθο μέρος αυτής της ενότητας. Οι Li et al. (2016) πρότειναν μια τεχνική ελέγχου πρόσβασης για ασύρματα δίκτυα αισθητήρων που να εφαρμόζεται στο περιβάλλον IoT. Έχουν χρησιμοποιήσει ένα ετερογενές σχήμα κρυπτογράφησης που επέτρεπε στο μέρος να στείλει ένα μήνυμα σε άλλο μέρος σε ένα περιβάλλον κρυπτογράφησης που βασίζεται σε ταυτότητα. Το πρωτόκολλό τους είναι δαπανηρό όσον αφορά το κόστος υπολογισμού λόγω της χρήσης κρυπτογραφίας με βάση την ταυτότητα (IBC) και μηχανισμών διγραμμικής σύζευξης.

Οι Braeken et al. (2016) πρότειναν ένα αποτελεσματικό και κατανεμημένο πρωτόκολλο ελέγχου ταυτότητας (eDAAAS) για την πρόσβαση σε τερματικούς κόμβους σε περιβάλλον IoT έξυπνου σπιτιού. Το πρωτόκολλό τους βασίστηκε σε συμμετρική κρυπτογραφική τεχνική κλειδιού και μονόδρομη κρυπτογραφική λειτουργία κατακερματισμού. Αν και αυτό το πρωτόκολλο είχε χαμηλό υπολογιστικό κόστος αλλά είχε υψηλό κόστος επικοινωνίας. Επιπλέον, αυτό το πρωτόκολλο περιλάμβανε κόμβο πύλης στον μηχανισμό ελέγχου πρόσβασης μεταξύ των δύο συσκευών IoT.

Οι Luo et al. (2018) παρουσίασαν ένα πρωτόκολλο ελέγχου πρόσβασης για WSN που ισχύει για περιβάλλον IoT. Διευκόλυνε την επικοινωνία των χρηστών του Διαδικτύου σε περιβάλλον κρυπτογραφίας με πιστοποιητικό λιγότερο κρυπτογραφίας με την έξυπνη συσκευή σε περιβάλλον IBC. Ωστόσο, το πρωτόκολλό τους ήταν δαπανηρό όσον αφορά το κόστος υπολογισμού λόγω της χρήσης μηχανισμών IBC και διγραμμικής σύζευξης.

Οι Ding et al. (2019) παρουσίασαν έναν μηχανισμό ελέγχου πρόσβασης βάσει χαρακτηριστικών για περιβάλλον IoT. Η τεχνολογία blockchain χρησιμοποιήθηκε για την καταγραφή της κατανομής των χαρακτηριστικών για να αποφευχθεί η αποτυχία του ενός σημείου και για την ασφάλεια των δεδομένων.

Οι Riad et al. (2019) πρότειναν πρωτόκολλο ελέγχου πρόσβασης για τη διαχείριση και την ασφάλεια των ηλεκτρονικών αρχείων υγείας που φιλοξενούνται στο cloud. Το πρωτόκολλό τους εξασφάλιζε το απόρρητο των δεδομένων των ασθενών στα οποία μόνο εξουσιοδοτημένοι χρήστες μπορούσαν να επεξεργαστούν ή να ελέγξουν τα δεδομένα υγείας των ασθενών.

Οι Fan et al. (2019) παρουσίασαν ένα πρωτόκολλο ελέγχου πρόσβασης πολλαπλών εξουσιών που διατηρεί το απόρρητο για περιβάλλον IoT που βασίζεται σε ομίχλη. Στο πρωτόκολλό τους χρησιμοποιήθηκε επαληθεύσιμη αποκρυπτογράφηση με εξωτερική ανάθεση για τη μείωση του κόστους υπολογισμού για τις συσκευές τελικού χρήστη. Σχεδιάστηκε επίσης μια ασφαλής μέθοδος ανάκλησης χρηστών.

Οι Das et al. (2019) παρουσίασαν ένα ελαφρύ έλεγχο πρόσβασης βασισμένο σε πιστοποιητικό και βασικό πρωτόκολλο συμφωνίας για περιβάλλον IoT. Χρησιμοποίησε μηχανισμούς όπως η κρυπτογράφηση ελλειπτικής καμπύλης (ECC) και η μονόδρομη κρυπτογραφική λειτουργία κατακερματισμού ανθεκτική σε σύγκρουση. Διάφορες αναλύσεις, π.χ., επίσημη ανάλυση ασφαλείας υπό το μοντέλο "RealOr - Random (ROR)", ανεπίσημη (μη μαθηματική) ανάλυση ασφαλείας και επίσημη επαλήθευση ασφάλειας μέσω του εργαλείου "Αυτόματη επικύρωση πρωτοκόλλων και εφαρμογών ασφάλειας Διαδικτύου (AVISPA)" υπό την προϋπόθεση. Η ανάλυση που διεξήχθη απέδειξε την ανθεκτικότητα του πρωτοκόλλου τους έναντι πιθανών επιθέσεων.

5.3.4 Υπάρχοντα πρωτόκολλα ανίχνευσης εισβολής στο περιβάλλον IoT

Στη συνέχεια, παρουσιάζονται οι λεπτομέρειες των διαφορετικών πρωτοκόλλων ανίχνευσης εισβολής σε περιβάλλον IoT. Οι Wazid & Das (2016) σχεδίασαν έναν μηχανισμό ανίχνευσης εισβολής για την ανίχνευση και την πρόληψη κόμβων εισβολέα καταβόθρα σε ένα ασύρματο δίκτυο αισθητήρων που βασίζεται σε συμπλέγματα. Οι εργασίες διεξήχθησαν σε δύο φάσεις, στην πρώτη φάση ανακάλυψε την ύπαρξη άτακτων κόμβων μέσω διαφόρων παραμέτρων απόδοσης δικτύου. Εάν ένας κόμβος περιλαμβανόταν σε ύποπτη κατηγορία, τότε τα βήματα της δεύτερης φάσης επιβεβαίωσαν τον κόμβο ως τον κόμβο εισβολέα καταβόθρα μαζί με τους τύπους του, π.χ. "κόμβος τροποποίησης μηνύματος καταβόθρα", "κόμβος απόρριψης μηνύματος καταβόθρα" και "καθυστέρηση μηνύματος καταβόθρα". κόμβος".

Οι Selvakumar et al. (2019) παρουσίασαν ένα πρωτόκολλο ανίχνευσης εισβολής με βάση τη μέθοδο χρονικής συλλογιστικής. Είχε χρησιμοποιήσει «ταξινόμηση πολλαπλών κλάσεων» μέσω αυτοσχεδιασμένου μηχανισμού που ονομάζεται «αλγόριθμος πλησιέστερης γειτονιάς με βάση το ασαφές και τραχύ σύνολο (FRNN)».

Οι Wazid & Das (2017) παρουσίασαν μια μέθοδο ανίχνευσης εισβολής για τον εντοπισμό κόμβων εισβολής μαύρης τρύπας και για την «υβριδική ανωμαλία» σε ένα ασύρματο δίκτυο αισθητήρων που βασίζεται σε συμπλέγματα. Ανίχνευσαν κόμβους εισβολέα με τη βοήθεια κόμβων κεφαλής συμπλέγματος πλούσιων πόρων. Αυτά τα προτεινόμενα πρωτόκολλα ισχύουν επίσης για τον εντοπισμό εισβολών σε περιβάλλον IoT.

Οι Jan et al. (2019) σχεδίασε μια τεχνική ανίχνευσης εισβολής ελαφρού βάρους για τον μετριασμό κοινών τύπων επιθέσεων DOS στο IoT. Από τον ρυθμό μετάδοσης πακέτων, εξήχθησαν δύο - τρία χαρακτηριστικά τα οποία χρησιμοποιήθηκαν για τη μείωση του συνολικού χρόνου που απαιτείται για την ταξινόμηση των διαφόρων ροών κίνησης. Υπήρξε μείωση της πολυπλοκότητας και του χρόνου που απαιτούνται από τη «μηχανή διανύσματος υποστήριξης (SVM)» για την ταξινόμηση που οδηγεί σε μια αποτελεσματική επίθεση DOS μετριασμού.

Οι Sharma et al. (2019) σχεδίασαν μια τεχνική ανίχνευσης μικρού βάρους με βάση τις προδιαγραφές κανόνων συμπεριφοράς για «ενσωματωμένα στο Διαδίκτυο Κυβερνοφυσικά συστήματα». Η ύπαρξη εισβολέα εντοπίστηκε μέσω του χαρακτηριστικού κακής συμπεριφοράς ενός υπάρχοντος κόμβου. Στον σχεδιασμένο μηχανισμό χρησιμοποίησαν ένα «προφίλ» που διαβάζει τη μονάδα και προωθεί αυτά τα δεδομένα στο τμήμα ασαφούς ανάλυσης για να επαληθεύσει την εγκυρότητα των κανόνων συμπεριφοράς.

Οι Pajouh et al. (2019) παρουσίασαν έναν μηχανισμό ανίχνευσης εισβολής για διαφορετικές επιθέσεις που συνέβησαν σε περιβάλλον IoT. Τα πρωτόκολλα που παρουσιάστηκαν χρησιμοποιούσαν δύο μηχανισμούς για τη μείωση των διαστάσεων και την ελαχιστοποίηση του αριθμού των απαιτούμενων χαρακτηριστικών. Ο αλγόριθμος ταξινόμησης, για παράδειγμα, «KNN» και «Nive Bayes» χρησιμοποιήθηκαν για την ανίχνευση κακοήθων κόμβων.

Οι Mudgerikar et al. (2019) παρουσίασαν ένα πρωτόκολλο ανίχνευσης εισβολής βασισμένο σε σύστημα πελάτη το οποίο χρησιμοποιούσε μέθοδο ανίχνευσης με βάση ανωμαλίες. Αναπτύχθηκε με τρία επίπεδα ασφάλειας. Ωστόσο, υπήρχαν ορισμένα μειονεκτήματα, καθώς με το αυξανόμενο επίπεδο ασφάλειας σημειώθηκε η αύξηση των γενικών εξόδων, δηλαδή το κόστος υπολογισμού και επικοινωνίας. Στο πρώτο στοιχείο της μονάδας ανίχνευσης ετοιμάστηκε μια λευκή λίστα κατά τη διαδικασία εκμάθησης. Διαχώρισε τις νόμιμες διαδικασίες από τις κακόβουλες διαδικασίες. Οι συγκρίσεις έγιναν με βάση τα αναγνωριστικά των διεργασιών. Στη δεύτερη ενότητα, ο ταξινομητής εκπαιδεύτηκε χρησιμοποιώντας τα δημιουργημένα αρχεία καταγραφής που ελήφθησαν κατά τη φάση εκμάθησης. Ωστόσο, ήταν πολύ δαπανηρή διαδικασία λόγω της χρήσης αλγορίθμων μηχανικής μάθησης στις συσκευές με περιορισμένους πόρους.

Οι Saeed et al. (2016) παρουσίασαν μια τεχνική ανίχνευσης εισβολής αποτελούμενη από δύο φάσεις για τη διατήρηση της ασφάλειας στο σύστημα. Το νευρωνικό δίκτυο χρησιμοποιήθηκε στην πρώτη φάση για τον σκοπό

ανίχνευσης ανωμαλιών. Αν και στη δεύτερη φάση αναπτύχθηκε ένα σύστημα ετικετών για την ανίχνευση ανωμαλιών. Στη συνέχεια, η ανίχνευση ανωμαλίας πραγματοποιήθηκε μέσω της μεθόδου ελέγχου ετικετών.

Τέλος, οι Wazid et al. (2019) σχεδίασαν μια μέθοδο ανίχνευσης εισβολής για τον μετριασμό των επιθέσεων δρομολόγησης σε περιβάλλον IoT βασισμένο σε αιχμή. Σε αυτή την τεχνική έχουν χρησιμοποιήσει έναν κόμβο ακμής πλούσιο σε πόρους για τον εντοπισμό εισβολής στο δίκτυο.

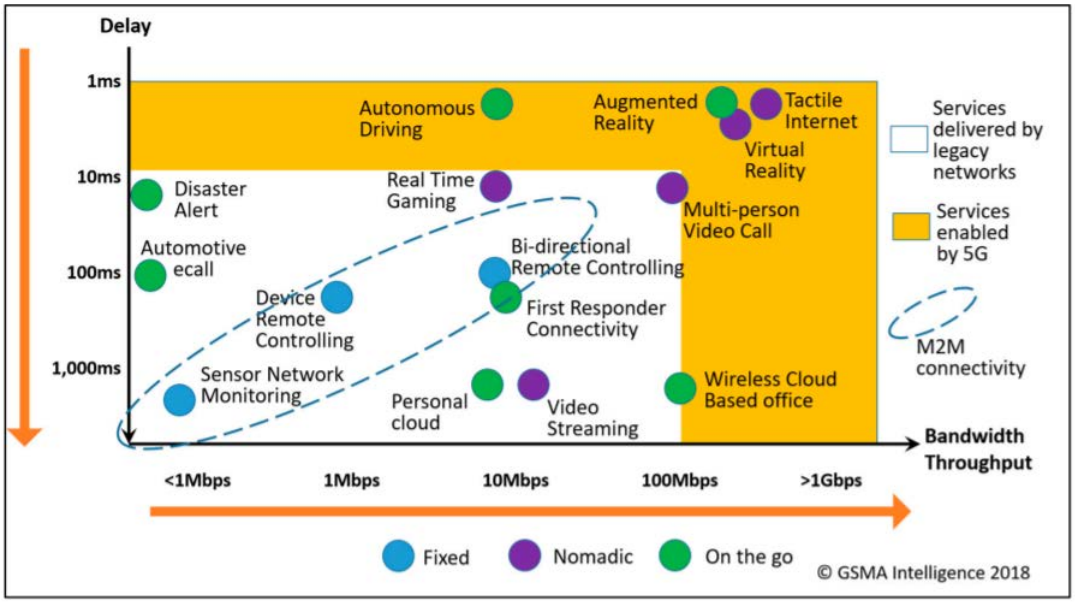
ΚΕΦΑΛΑΙΟ 6 : ΕΜΠΟΡΙΚΟ ΠΛΑΙΣΙΟ - ΤΟ 5G ΣΤΗΝ ΠΑΓΚΟΣΜΙΑ ΒΙΟΜΗΧΑΝΙΑ

Το 5G έχει τη δυνατότητα να γίνει το υποκείμενο ψηφιακό υλικό που συνδέει όλα τα στοιχεία του κατασκευαστικού κόσμου. Το 5G υπόσχεται γρήγορη συνδεσιμότητα, περισσότερο εύρος ζώνης από το Wi - Fi και το 4G LTE, αλλά και χαμηλή καθυστέρηση με υποστήριξη για χιλιάδες συσκευές σε μια μικρή τοποθεσία, τα οποία αποτελούν ελκυστικές προοπτικές για τις εγκαταστάσεις παραγωγής. Η ικανότητα ενσωμάτωσης του 5G με δικτύωση ευαίσθητη στον χρόνο (TSN) καθιστά τα έξυπνα εργοστάσια εφικτό στόχο. Η δυνατότητα TSN θα βοηθήσει το 5G να αξιοποιήσει τις βελτιώσεις στο ethernet για να το κάνει πιο αντιδραστικό στη ζήτηση ή «ντετερμινιστικό», καθιστώντας ουσιαστικά το 5G διαθέσιμο έγκαιρα με χαμηλή καθυστέρηση, χαμηλό jitter και υψηλή αξιοπιστία. Προκειμένου αυτή η διεπαφή να επιτύχει χαμηλό λανθάνοντα χρόνο, όλες οι συσκευές πρέπει να συγχρονιστούν στην ίδια βάση χρόνου, στην πραγματικότητα πρέπει να έχουν «συνειδητοποίηση χρόνου» (O'Connell et al., 2020).

Η ευρεία διάδοση του 5G είναι πλέον πραγματικότητα. Οι κατασκευαστές συσκευών έχουν ήδη ξεκινήσει την ανάπτυξη εξοπλισμού δικτύου 5G, ενώ οι εταιρείες κινητής τηλεφωνίας δικτύων βρίσκονται στα πρόθυρα της εμπορευματοποίησης των δικτύων 5G σε νέους κλάδους όπως η κατασκευή (Cheng et al., 2018). Ενώ εξακολουθούν να υπάρχουν πολλά εμπόδια που εμποδίζουν την καθολική ανάπτυξη των δικτύων 5G, υπάρχουν επίσης ατελείωτες εφαρμογές και πιθανά οφέλη.

Το 5G έχει τη δυνατότητα να φέρει επανάσταση σε διάφορους κρίσιμους τομείς όπως το IoT, η ψυχαγωγία, η αυτοματοποίηση, η πληροφορική και πολλά άλλα. Τα ιδιωτικά δίκτυα 5G, τα οποία προσφέρουν πολλά πλεονεκτήματα, θα ενισχύσουν τη δύναμη του Industrial IoT (IIoT), καθώς το 5G προσφέρει περισσότερα από αυξημένες ταχύτητες δικτύου και εύρος ζώνης. Η ασύρματη τεχνολογία 5G και η σχετική ανάπτυξή της υλοποιείται σε μια εποχή που πολλές βιομηχανίες μεταμορφώνονται οι ίδιες μέσω μεγαλύτερης αυτοματοποίησης, χρησιμοποιώντας τεχνικές όπως το IoT, η μηχανική όραση, η μηχανική μάθηση και η ρομποτική. Οι συνδέσεις 5G θα υπερβούν τις ανάγκες ανθρώπινης επικοινωνίας και αναμένεται να ενεργοποιήσουν το έξυπνο διαδίκτυο των πραγμάτων. Η επόμενη γενιά (NextGen) τηλεπικοινωνιακών τεχνολογιών θα υιοθετηθεί από ένα ευρύτερο φάσμα βιομηχανιών και τομέων με μεγάλο όφελος την ψηφιακή παραγωγή. Ο ασύρματος έλεγχος της NextGen πολύ εξελιγμένων κινητών μηχανών γίνεται εφικτός και θα επιτρέψει στις μηχανές να επωφεληθούν από την τεράστια υπολογιστική ισχύ και τις διαθέσιμες επιλογές αποθήκευσης cloud, χωρίς να συνδέονται με φυσικά καλώδια. Ένας πρώιμος τομέας ενδιαφέροντος για το 5G στο IIoT είναι η διευκόλυνση της εργοστασιακής παρακολούθησης, όπου είναι εγκατεστημένοι αισθητήρες στο εργοστάσιο για την παρακολούθηση των συνθηκών του εξοπλισμού και την επίβλεψη ότι όλα λειτουργούν όπως θα έπρεπε και για τον εντοπισμό πιθανών

προβλημάτων πριν προκύψουν. Αυτοί οι αισθητήρες θα ερωτηθούν και τα τελικά δεδομένα θα χρησιμοποιηθούν για τη δημιουργία πληροφοριών σχετικά με τα τελικά προϊόντα και τα παραδοτέα, παρέχοντας βελτιώσεις στον ποιοτικό έλεγχο και την κατά παραγγελία κατασκευή. Το 5G έχει ενσωματώσει πολλά αιτήματα για τη βελτίωση του 4G και τώρα είναι σε θέση να παρέχει νέες υπηρεσίες που μπορούν να προσαρμοστούν στις απαιτήσεις των επιχειρηματικών μοντέλων των πελατών (Εικόνα 3) (Orlosky et al., 2017).



Εικόνα 3 : Περιπτώσεις χρήσης - απαιτήσεις καθυστέρησης και εύρους ζώνης (O'Connell et al., 2020)

Οι ρυθμοί δεδομένων των 10 Gbps είναι ευρέως αποδεκτοί ως μια εφικτή προσδοκία για το 5G όταν είναι πλήρως διαθέσιμο στο εμπόριο, αλλά οι πρώιμες υπηρεσίες 5G φαίνεται να μεγιστοποιούνται σε περίπου 1 Gbps. Καθώς οι αναπτύξεις αυξάνονται, όλα τα δεδομένα που δημιουργούνται θα συλλέγονται και θα αναλύονται για να δώσουν λεπτομερείς πληροφορίες για κάθε πτυχή της λειτουργίας ενός εργοστασίου. Τα έξυπνα ρομπότ με δυνατότητα μηχανικής εκμάθησης θα κατασκευάσουν προϊόντα και θα τους δοθεί η δυνατότητα να μετακινούν αγαθά και να αναπτύσσουν εξοπλισμό μέσα και γύρω από το εργοστάσιο, δημιουργώντας ακόμη περισσότερα δεδομένα. Η κατασκευή αναμένεται να στραφεί από μια γραμμή συναρμολόγησης στην παραγωγή προϊόντων υψηλής προσαρμογής που θα επιτρέπουν ουσιαστικά τη μαζική παραγωγή προϊόντων κατά παραγγελία, με τους εργαζόμενους να

μεταδίδουν βίντεο εικονικής/επαυξημένης πραγματικότητας ή να εργάζονται σε εικονικά περιβάλλοντα (Atanasovski et al., 2015). Αυτές οι ιδέες μπορούν να διευκολυνθούν από το πρότυπο 5G NR.

Ενώ το εύρος των πλεονεκτημάτων του 5G είναι εντυπωσιακό, υπάρχουν εγγενείς περιορισμοί στην ανάπτυξη του 5G. Το φάσμα που εκχωρείται είναι σε υψηλότερη συχνότητα και αναλογικά το μήκος κύματος αυτών των σημάτων είναι μικρότερο, γεγονός που περιορίζει την ικανότητα διείσδυσης σήματος. Το 5G θα εκχωρηθεί αρχικά σε φάσμα 3 έως 6 GHz (ανάλογα με τους εθνικούς κανονισμούς). Μέσα σε ένα βαρύ περιβάλλον μηχανικής, με πυκνά, γενικά μεταλλικά μηχανήματα, η διείσδυση του σήματος θα πρέπει να λαμβάνεται υπόψη στη σχεδίαση.

Για να αναπτυχθεί με επιτυχία το 5G σε ένα βιομηχανικό περιβάλλον, πρέπει να υπάρχει στενή συνεργασία μεταξύ όλων των συστημάτων, που να εκτείνονται σε όλες τις εταιρικές τεχνολογίες πληροφοριών και επικοινωνιών (IT) και τις επιχειρησιακές τεχνολογίες κατασκευής (OT) για να μεγιστοποιηθούν οι εγγενείς δυνατότητες του 5G. Το όραμα είναι ότι η βιομηχανία θα είναι σε θέση να κατασκευάσει κυβερνοφυσικά συστήματα που επιτρέπουν τον έλεγχο ακριβείας σε σχεδόν πραγματικό χρόνο, σχεδόν από οπουδήποτε στον κόσμο. Τυπικά σενάρια ανάπτυξης, δίνονται παρακάτω (O'Connell et al., 2020) :

- Δυνατότητα απομακρυσμένης λειτουργίας εξοπλισμού, π.χ. ρομποτικής γραμμής παραγωγής στο πάτωμα του εργοστασίου. Τυπικές εφαρμογές είναι συγκόλληση, βαφή και συναρμολόγηση.
- Τηλεχειρισμός του εξοπλισμού της αλυσίδας εφοδιασμού, π.χ., ο χειριστής μπορεί να τηλεχειριστεί τον εξοπλισμό, όπως τα μη συνδεδεμένα ρομπότ, οι τυπικές εφαρμογές περιλαμβάνουν, αυτόνομα οχήματα εδάφους (AGV) ή περονοφόρα ανυψωτικά.
- Απομακρυσμένη παρακολούθηση του εξοπλισμού, π.χ., η μετάδοση διαγνωστικών πληροφοριών, ώστε οι τεχνικοί σέρβις να φτάνουν προετοιμασμένοι για επιτυχείς επισκευές και ενημερώσεις όταν χρειάζεται.
- Επικοινωνία από μηχανή σε μηχανή : επικοινωνίες κλειστού βρόχου μεταξύ μηχανών για τη βελτιστοποίηση των διαδικασιών παραγωγής.
- Επικοινωνία εντός και μεταξύ επιχειρήσεων : για την παρακολούθηση των περιουσιακών στοιχείων που διανέμονται σε ευρύτερες γεωγραφικές περιοχές σε όλη την αλυσίδα αξίας.
- Υποστήριξη επαυξημένης πραγματικότητας στο σχεδιασμό, τη συντήρηση και την επισκευή : χρήση επαυξημένης πραγματικότητας για βοήθεια στην εκτέλεση διαδικαστικών εργασιών στον τομέα σχεδιασμού, συντήρησης και επισκευής (μέσω προσομοιώσεων).

Κάθε ανάπτυξη του κλάδου πρέπει να εξετάσει πολλαπλούς περιορισμούς και να εντοπίσει μια λύση που θα προσφέρει τη βέλτιστη λύση για την κάλυψη των επιχειρηματικών απαιτήσεων του τελικού χρήστη ή της εταιρικής ανάγκης.

Οι κύριες προκλήσεις για την υιοθέτηση του 5G από τη βιομηχανία είναι (O'Connell et al., 2020) :

- Κόστος : η μεταποιητική βιομηχανία έχει απαιτήσεις μείωσης υψηλού κόστους και θα εφαρμόσει νέες εφαρμογές μόνο εάν αυτές έχουν αποδειχθεί ότι μειώνουν τελικά το κόστος.
- Ασφάλεια : εκατοντάδες συνδεδεμένες αυτοματοποιημένες συσκευές σε ένα εργοστασιακό δάπεδο μπορούν να δημιουργήσουν ένα επικίνδυνο περιβάλλον για τον άνθρωπο.
- Γνώσεις ανάπτυξης : πολλές μικρές και μεσαίες επιχειρήσεις (ΜΜΕ) δεν έχουν την ικανότητα να προμηθεύουν τις απαιτήσεις μάθησης ή την τεχνική ικανότητα να αξιοποιήσουν τις δυνατότητες του 5G.
- Παρεμβολή ραδιοσυχνοτήτων : πολλά αντικείμενα στο εργοστασιακό δάπεδο χρησιμοποιούν ήδη ραδιοεπικοινωνίες.

Ένα άλλο ζήτημα για την κατασκευή είναι ο αυξημένος πολλαπλασιασμός πιο εξελιγμένων συνεργατικών ρομπότ (cobots). Αυτά τα μικρότερα, ελαφριά, έξυπνα ρομπότ μπορούν να ανιχνεύσουν πότε ένας άνθρωπος βρίσκεται κοντά, επιτρέποντας σε αυτό το άτομο να εργάζεται με μεγαλύτερη ασφάλεια δίπλα στο μηχάνημα. Ένα τυπικό σενάριο χρήσης για ένα cobot μπορεί να είναι η φροντίδα τέτοιων εργασιών όπως η μετακίνηση βαρέων εξαρτημάτων ή η εκτέλεση επαναλαμβανόμενων εργασιών, ενώ ένας ανθρώπινος συνεργάτης χειρίζεται τις πιο προηγμένες εργασίες. Τα Cobots είναι ήδη στην αγορά, αλλά τα δίκτυα 5G θα πρέπει να βοηθήσουν να γίνουν πιο χρήσιμα. Ένα παράδειγμα προστιθέμενης αξίας είναι η αξιοποίηση της χαμηλότερης καθυστέρησης του 5G, η οποία θα επιτρέψει μια πιο στιγμιαία επίγνωση παρουσίας σε πραγματικό χρόνο που θα επέτρεπε στο ρομπότ να εργάζεται με μεγαλύτερες ταχύτητες δίπλα σε έναν άνθρωπο με μειωμένο κίνδυνο (σχεδόν μηδέν) τραυματισμού (Rampa et al., 2019; Wdowik et al., 2019).

ΚΕΦΑΛΑΙΟ 7 : ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΚΛΗΣΕΙΣ

Το περιβάλλον επικοινωνιών IoT με δυνατότητα 5G υποστηρίζει διάφορους τύπους εφαρμογών, όπως έξυπνο σπίτι, έξυπνες μεταφορές, έξυπνη υγειονομική περίθαλψη, έξυπνο δίκτυο και έξυπνη κατασκευή. Αυτό το περιβάλλον απαιτεί μοναχικές απαιτήσεις, για παράδειγμα, ζωντανή επεξεργασία και πρόσβαση σε δεδομένα (δηλαδή, περιβαλλοντική παρακολούθηση μιας βιομηχανικής μονάδας σε πραγματικό χρόνο). Ένα τέτοιο περιβάλλον δημιουργεί πολύ τεράστια δεδομένα (δηλαδή μεγάλα δεδομένα), επομένως η διαδικασία ανάλυσης μεγάλων δεδομένων θα πρέπει να χρησιμοποιηθεί σε αυτά τα δεδομένα για να εντοπιστούν ορισμένα συγκεκριμένα μοτίβα από αυτό (π.χ. πιθανότητες ατυχήματος σε ένα εργοτάξιο). Σε αυτό το περιβάλλον όλες οι συσκευές και οι χρήστες επικοινωνούν μέσω του Διαδικτύου. Ως εκ τούτου, αντιμετωπίζει ορισμένες παραδοσιακές προκλήσεις ασφάλειας, ιδιωτικότητας και άλλου είδους. Στη συνέχεια, συζητούνται ορισμένες από τις τρέχουσες προκλήσεις αυτού του τομέα και επισημαίνονται περαιτέρω ορισμένες κατευθύνσεις για ερευνητικές εργασίες (Wazid et al., 2021).

7.1 Ασφάλεια των υπαρχόντων πρωτοκόλλων

Τα περισσότερα από τα πρωτόκολλα ασφαλείας που προτείνονται για το περιβάλλον IoT δεν είναι ασφαλή καθώς δεν παρέχουν την πλήρη ασφάλεια έναντι των πιθανών επιθέσεων. Επιπλέον, ορισμένα από τα υπάρχοντα πρωτόκολλα λειτουργούν για μια συγκεκριμένη επίθεση και δεν λειτουργούν ταυτόχρονα για πολλαπλές επιθέσεις. Ως εκ τούτου, είναι υποχρεωτικός ο σχεδιασμός ορισμένων πρωτοκόλλων ασφαλείας που θα πρέπει ταυτόχρονα να προστατεύουν πολλαπλές επιθέσεις. Επομένως, ο σχεδιασμός τέτοιου είδους πρωτοκόλλων για αυτόν τον τομέα είναι μια πρόκληση που θα πρέπει να επιλυθεί από τους μελλοντικούς ερευνητές (Wazid et al., 2019).

7.2 Αποτελεσματικός σχεδιασμός πρωτοκόλλων ασφαλείας

Το περιβάλλον IoT με δυνατότητα 5G περιέχει συσκευές με περιορισμένους πόρους, δηλαδή αισθητήρες IoT που έχουν περιορισμένη ικανότητα υπολογισμού, περιορισμένο μέγεθος αποθήκευσης και μικρή μονάδα μπαταρίας. Αυτές οι συσκευές δεν είναι σε θέση να εκτελέσουν απαιτητικές

εργασίες επικοινωνίας, υπολογισμού και αποθήκευσης που απαιτούν περισσότερη ισχύ από αυτές τις παραμέτρους. Ως εκ τούτου, είναι επιθυμητό να σχεδιάζονται πρωτόκολλα ασφαλείας σε τέτοιο βαθμό ώστε να χρειάζονται χαμηλή υπολογιστική ισχύ, χαμηλό κόστος επικοινωνίας και μικρό μέγεθος αποθήκευσης χωρίς να διαπραγματεύονται την ασφάλεια του συστήματος (Wazid et al., 2019; Wazid & Das, 2016, 2017).

7.3 Επεκτασιμότητα πρωτοκόλλων ασφαλείας

Το περιβάλλον IoT με δυνατότητα 5G είναι ένας συνδυασμός ετερογενών δικτύων διαφορετικών μηχανισμών επικοινωνίας και εφαρμογών. Αυτές οι εφαρμογές έχουν τις δικές τους ικανότητες και ανησυχίες. Σε τέτοιες καταστάσεις, ο σχεδιασμός ενός πρωτοκόλλου ασφαλείας για αυτό το είδος επικοινωνιακού περιβάλλοντος θα είναι πολύπλοκο έργο. Για παράδειγμα, σε ένα έξυπνο περιβάλλον επικοινωνίας υγειονομικής περίθαλψης, τα ηλεκτρονικά αρχεία υγείας του ασθενούς που πρέπει να αποθηκευτούν σε έναν διακομιστή cloud για περαιτέρω επεξεργασία και λήψη αποφάσεων. Σε ένα δίκτυο περιοχής σώματος (BAN), υπάρχουν διαφορετικοί τύποι συσκευών που δημιουργούν δεδομένα και στη συνέχεια τα προωθούν στον διακομιστή cloud. Αυτό αποτελεί ένα «ετερογενές δίκτυο» διαφορετικών τύπων συσκευών επικοινωνίας. Συνεπώς, θα πρέπει να σχεδιαστούν ορισμένοι ειδικοί τύποι πρωτοκόλλων ασφαλείας που μπορούν να χρησιμοποιηθούν για την προστασία διαφόρων τύπων συσκευών περιβάλλοντος IoT με δυνατότητα 5G. Ως εκ τούτου, απαιτείται περισσότερη έρευνα στον τομέα αυτό.

7.4 Απόρρητο αποθηκευμένων δεδομένων

Το απόρρητο των δεδομένων αφορά τον σωστό χειρισμό των πληροφοριών σχετικά με τους διάφορους πόρους, δηλαδή τη συγκατάθεση, την ειδοποίηση και τις κανονιστικές υποχρεώσεις. Το περιβάλλον IoT με δυνατότητα 5G χρησιμοποιείται επίσης σε «ευαίσθητες πληροφορίες» λειτουργίες (όπως η έξυπνη υγειονομική περίθαλψη). Σε αυτό το περιβάλλον που απαιτεί απόρρητο, οι έξυπνες συσκευές παρακολούθησης της υγείας χρησιμοποιούνται γύρω/μέσα στο σώμα ενός ασθενούς για την παρακολούθηση της κατάστασης της υγείας του/της. Στη συνέχεια, τα δεδομένα υγείας που ανιχνεύονται και συλλέγονται αποστέλλονται σε διακομιστές cloud για περαιτέρω αποθήκευση και επεξεργασία. Συνήθως, αυτός ο τύπος περιβάλλοντος επικοινωνίας μπορεί να επηρεαστεί από διαφορετικούς πιθανούς εισβολείς (Wazid & Das, 2016, 2017). Αυτό μπορεί να προκαλέσει τη διαρροή δεδομένων κατά τη μεταφορά και των δεδομένων που διατηρούνται στους διακομιστές.

Κατά συνέπεια, είναι σημαντικό να διατηρηθεί το απόρρητο των δεδομένων κατά τη μεταφορά καθώς και των αποθηκευμένων δεδομένων. Ως εκ τούτου, νέα αποτελεσματικά πρωτόκολλα χρειάζονται πολύ για τη διατήρηση της ιδιωτικής ζωής των δεδομένων. Στο εξής απαιτείται περισσότερη ερευνητική εργασία προς αυτή την κατεύθυνση.

7.5 Ετερογένεια μεταχειρισμένων συσκευών

Το περιβάλλον IoT με δυνατότητα 5G αποτελείται από διάφορους τύπους συσκευών από ισχυρούς διακομιστές, φορητούς υπολογιστές, προσωπικούς ψηφιακούς βοηθούς, επιτραπέζιους υπολογιστές έως ετικέτες RFID περιορισμένων πόρων και συσκευές ανίχνευσης. Επιπλέον, αυτές οι συσκευές λειτουργούν με διάφορους τύπους τεχνικών επικοινωνίας. Οι συσκευές έχουν επίσης αντίθεση ως προς την ισχύ επικοινωνίας, την υπολογιστική τους ικανότητα, το μέγεθος αποθήκευσης και το αναπτυγμένο λογισμικό συστήματος (π.χ. λειτουργικό σύστημα). Επομένως, τα πρωτόκολλα ασφαλείας πρέπει να σχεδιάζονται με τέτοιο τρόπο ώστε να παρέχουν προστασία σε διάφορες ποικιλίες συσκευών και σχετικές τεχνολογίες και μηχανισμούς. Έκτοτε, απαιτείται περισσότερη ερευνητική εργασία σε αυτόν τον τομέα (Wazid et al., 2019; Wazid & Das, 2017).

7.6 Σχεδιασμός πρωτοκόλλων ασφαλείας βασισμένων σε blockchain

Οι λειτουργίες του blockchain μπορούν επίσης να χρησιμοποιηθούν για την ασφάλεια του περιβάλλοντος IoT με δυνατότητα 5G. Επειδή οι λειτουργίες blockchain είναι αποκεντρωμένες, αποτελεσματικές και διαφανείς σε όλες τις οντότητες του περιβάλλοντος επικοινωνίας. Για να επινοηθούν πρωτόκολλα ασφάλειας σε περιβάλλον IoT με δυνατότητα 5G «λειτουργίες blockchain» είναι

επίσης ισχύει. Για να εκτελέσετε την απαιτούμενη εργασία, ένα μπλοκ αποτελείται από τα δεδομένα σχετικά με την απαιτούμενη λειτουργικότητα, π.χ., μήνυμα ελέγχου ταυτότητας, μήνυμα δεδομένων μπορεί να δημιουργηθεί και να προστεθεί στην αλυσίδα μπλοκ. Δεδομένου ότι το blockchain παρέχεται σε νομικές οντότητες δικτύου, τότε αυτές οι οντότητες μπορούν να έχουν πρόσβαση στα δεδομένα χρησιμοποιώντας τα μπλοκ του blockchain. Αυτό το έργο μπορεί να επιτευχθεί με αποτελεσματικό τρόπο χρησιμοποιώντας τη

λειτουργία του blockchain. Αντίστοιχα, ο σχεδιασμός «πρωτόκολλων ασφαλείας που βασίζονται σε blockchain» φαίνεται να είναι ένα καλό πρόβλημα για τους μελλοντικούς ερευνητές (Kumar et al., 2019; Wu et al., 2019).

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το IoT είναι η πολύ κοντινή μελλοντική ιδέα που διαμορφώνει τη ζωή μας. Είναι μια από τις τεχνολογίες που επιτρέπουν την εφαρμογή κινητών συστημάτων 5G. Για να ενεργοποιηθούν οι εφαρμογές IoT, πρέπει να ικανοποιούνται αρκετές απαιτήσεις, καθεμία από αυτές χρησιμοποιώντας ορισμένες τεχνολογίες. Αυτές οι τεχνολογίες θεωρούνται ως τεχνολογίες ενεργοποίησης του IoT, οι οποίες χρησιμοποιούνται κυρίως για να ενεργοποιήσουν και τα κυψελοειδή συστήματα 5G. Το περιβάλλον IoT με δυνατότητα 5G παρέχει υπηρεσίες με μηδενική καθυστέρηση. Διαθέτει μεγάλη ποικιλία εφαρμογών, όπως υγειονομική περίθαλψη, οικιακό αυτοματισμό, χειρουργική εξ αποστάσεως, αυτόνομο όχημα (AV), εικονική πραγματικότητα (VR), ιπτάμενα drones IoT και ασφάλεια και επιτήρηση. Αυτό το περιβάλλον επικοινωνίας διευκολύνει τις καθημερινές δραστηριότητες των ανθρώπων. Ωστόσο, ταλανίζεται επίσης από διάφορα θέματα «ασφάλειας και απορρήτου». Για να αντιμετωπιστεί αυτό, οι ερευνητές που εργάζονται σε αυτόν τον τομέα πρότειναν διάφορους τύπους πρωτοκόλλων ασφαλείας σε διαφορετικές κατηγορίες, όπως "πρωτόκολλα διαχείρισης κλειδιών", "πρωτόκολλα ελέγχου ταυτότητας/ ελέγχου ταυτότητας χρήστη", "πρωτόκολλα ελέγχου πρόσβασης/ελέγχου πρόσβασης χρήστη" και "ανίχνευση εισβολής". Τα πρωτόκολλα ανίχνευσης εισβολής είναι τριών τύπων όπως «ανίχνευση βάσει κακής χρήσης», «ανίχνευση βάσει ανωμαλίας» και «ανίχνευση βάσει προδιαγραφών». Το σύστημα «ανίχνευσης βάσει προδιαγραφών» χρειάζεται ορισμένους περιορισμούς και προδιαγραφές για την ανάπτυξή του. Χρησιμοποιεί τα πλεονεκτήματα των άλλων δύο σχημάτων. Ο ψευδώς θετικός ρυθμός του είναι επίσης μικρότερος σε σύγκριση με τα άλλα συστήματα ανίχνευσης.

Συνολικά, προκύπτει ότι το περιβάλλον IoT με δυνατότητα 5G πάσχει από διάφορους τύπους ζητημάτων «ασφάλειας και απορρήτου», καθώς είναι επιρρεπές σε διάφορους τύπους επιθέσεων. Είναι απαραίτητο να προστατεύσουμε την υποδομή του περιβάλλοντος IoT με δυνατότητα 5G από αυτές τις επιθέσεις. Επομένως, προέκυψαν διαφορετικοί τύποι πρωτοκόλλων ασφαλείας σε διαφορετικές κατηγορίες (για παράδειγμα, "διαχείριση κλειδιών", "έλεγχος ταυτότητας χρήστη/έλεγχος συσκευής", "έλεγχος πρόσβασης/έλεγχος πρόσβασης χρήστη" και "ανίχνευση εισβολής") σε εικόνα. Στην παρούσα εργασία παρουσιάστηκαν οι λεπτομέρειες διαφόρων μοντέλων συστημάτων (για παράδειγμα, μοντέλο δικτύου και μοντέλο απειλής) για περιβάλλον IoT με δυνατότητα 5G. Περιγράφηκαν επίσης διάφορες απαιτήσεις ασφάλειας και πιθανές επιθέσεις σε αυτό το περιβάλλον επικοινωνίας. Στη συνέχεια οργανώθηκαν διάφοροι τύποι ανάλυσης των υφιστάμενων πρωτοκόλλων ασφαλείας σε περιβάλλον IoT με δυνατότητα 5G. Τέλος, αποτυπώθηκαν τα περισσότερο προκλητικά προβλήματα του μέλλοντος στην ασφάλεια του περιβάλλοντος IoT με δυνατότητα 5G με σκοπό να βοηθήσουν τους ερευνητές που εργάζονται στον ίδιο τομέα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Agiwal, M., Roy, A., & Saxena, N. (2016). Next Generation 5G Wireless Networks : A Comprehensive Survey. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 18 (3).

[2] Ahad, A. , M. Tahir, and K. - L. - A. Yau, ‘‘5G - based smart healthcare network : Architecture, taxonomy, challenges and future research directions,’’ IEEE Access, vol. 7, pp. 100747–100762, 2019.

[3] Ahmad, I., T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, ‘‘Overview of 5G security challenges and solutions,’’ IEEE Commun. Standards Mag., vol. 2, no. 1, pp. 36–43, Mar. 2018.

[4] Ahmad, I., T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, ‘‘Overview of 5G security challenges and solutions,’’ IEEE Commun. Standards Mag., vol. 2, no. 1, pp. 36–43, Mar. 2018.

[5] Akyildiz, Ian F., David M. Gutierrez - Estevez, Ravikumar Balakrishnan, and Elias Chavarria - Reyes. "LTE - Advanced and the evolution to Beyond 4G (B4G) systems." eLSERVIER, vol. 10, 2014, pp. 31 - 60.

[6] Akyildiz, Ian F., Shuai Nie, Shih - Chun Lin, and Manoj Chandrasekaran. "5G roadmap : 10 key enabling technologies." ELSERVIER, vol. 106, 2016, pp. 17 - 48.

[7] Al - Falahy, N., Alani, O.Y., Technologies for 5G networks : Challenges and opportunities, IT Professional 19 (1) (2017) 12–20.

[8] Al - Fuqaha, A., M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things : A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[9] Al - Garadi, M. A. , A. Mohamed, A. K. Al - Ali, X. Du, I. Ali, and M. Guizani, ‘‘A survey of machine and deep learning methods for Internet of Things (IoT) security,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1646–1685, 3rd Quart., 2020.

[10] Ali, K. T. , S. Ben Rejeb, and Z. Choukair, “A congestion control approach based on dynamic ACB of differentiated M2M services in 5G/HetNet,” in Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International, 2017, pp. 1126–1131.

[11] Alsulami, M. M., & Akkari, N. (2018). The role of 5G wireless networks in the internet - of - things (IoT). 2018 1st International Conference on Computer Applications & Information Security (ICCAIS). doi : 10.1109/cais.2018.8471687

[12] Assiri, A. and H. Almagwashi, ‘‘IoT security and privacy issues,’’ in Proc. 1st Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS), Riyadh, Saudi Arabia, Apr. 2018, pp. 1–5.

[13] Astely, D., E. Dahlman, G. Fodor, S. Parkvall, and J. Sachs, “LTE release 12 and beyond [accepted from open call],” IEEE Commun. Mag., vol. 51, no. 7, pp. 154–160, 2013.

[14] Atanasovski, V.; Leon - Garcia, A. Future Access Enablers for Ubiquitous and Intelligent Infrastructures; Springer : Berlin, Germany, 2015.

[15] AVISPA. (2019). Automated Validation of Internet Security Protocols and Applications. [Online]. Available : http : //www.avispa - project.org/

[16] Bassi, L., “Industry 4.0 : Hope, hype or revolution?,” in Research and Technologies for Society and Industry (RTSI), IEEE 3rd International Forum on, 2017, pp. 1–6.

[17] Bockelmann, C., PratasN., H. Nikopour, K. Au, T. Svensson, C. Stefanovic, P. Popovski, A. Dekorsy, Massive Machine - Type Communications in 5G : Physical and MAC - Layer Solutions, IEEE communications magazine 54 (9) (2016) 59–65.

[18] Braeken A., P. Porambage, M. Stojmenovic, and L. Lambrinos, ‘‘eDAAAS : Efficient distributed anonymous authentication and access in smart homes,’’ Int. J. Distrib. Sensor Netw., vol. 12, no. 12, pp. 1–11, Dec. 2016.

[19] Braeken, A., M. Liyanage, P. Kumar, and J. Murphy, ‘‘Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks,’’ IEEE Access, vol. 7, pp. 64040–64052, 2019.

[20] Challa S., Wazid M., A. K. Das, N. Kumar, A. G. Reddy, E. - J. Yoon, and K. - Y. Yoo, ‘‘Secure signature - based authenticated key establishment scheme for future IoT applications,’’ IEEE Access, vol. 5, pp. 3028–3043, 2017.

[21] Cheng, J.; Chen, W.; Tao, F.; Lin, C. - L.; Da Xu, L. Industrial IoT in 5G environment towards smart manufacturing. J. Ind. Inf. Integr. 2018, 10, 10–19.

[22] Conti, M. , A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics : Challenges and opportunities.” Elsevier, 2018.

[23] Conti, M., A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics : Challenges and opportunities.” Elsevier, 2018.

[24] Das , A. K. & Zeadally, S. (2019). ‘‘Data security in the smart grid environment,’’ in Pathways to a Smarter Power System, A. Tascikaraoglu and O. Erdinc, Eds. New York, NY, USA : Academic, 2019, ch. 13, pp. 371–395.

[25] Das A. K., M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, ‘‘Provably secure ECC - based device access control and key agreement protocol for IoT environment,’’ IEEE Access, vol. 7, pp. 55382–55397, 2019.

[26] Ding S., J. Cao, C. Li, K. Fan, and H. Li, ‘‘A novel attribute - based access control scheme using blockchain for IoT,’’ IEEE Access, vol. 7, pp. 38431–38441, 2019.

[27] Fan K., H. Xu, L. Gao, H. Li, and Y. Yang, ‘‘Efficient and privacy preserving access control scheme for fog - enabled IoT,’’ Future Gener. Comput. Syst., vol. 99, pp. 134–142, Oct. 2019.

[28] Farash M. S., M. Turkanović, S. Kumari, and M. Hölbl, ‘‘An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,’’ Ad Hoc Netw., vol. 36, pp. 152–176, Jan. 2016.

[29] Gandotra, P., & Jha, R. K., ‘‘A survey on green communication and security challenges in 5G wireless communication networks,’’ J. Netw. Comput. Appl., vol. 96, pp. 39–61, Oct. 2017.

[30] Gubbi, J., B. Rajkumar, M. Slaven, P. Marimuthu, Internet of Things (IoT) : A vision, architectural elements, and future directions, Future generation computer systems 29 (7) (2013) 1645–1660.

[31] Gupta, R., & Gupta, R. (2016). ABC of Internet of Things : Advancements, Benefits, Challenges, Enablers and Facilities of IoT. Symposium on Colossal Data Analysis and Networking.

[32] Hou, J. , L. Qu, and W. Shi, ‘‘A survey on Internet of Things security from data perspectives,’’ Comput. Netw., vol. 148, pp. 295–306, Jan. 2019.

[33] Hu P., H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, ‘‘Security and privacy preservation scheme of face identification and resolution framework using fog computing in Internet of Things,’’ IEEE Internet Things J., vol. 4, no. 5, pp. 1143–1155, Oct. 2017.

[34] Jan S. U., S. Ahmed, V. Shakhov, and I. Koo, ‘‘Toward a lightweight intrusion detection system for the Internet of Things,’’ IEEE Access, vol. 7, pp. 42450–42471, 2019.

[35] Kaplan, K. (2018). “Will 5G wireless networks make every internet thing faster and smarter?” [Online]. Available : https : //qz.com/179794/will - 5g - wireless - networks - make - every - internetthing - faster - and - smarter/.

[36] Khan, R. , P. Kumar, D. N. K. Jayakody, and M. Liyanage, ‘‘A survey on security and privacy of 5G technologies : Potential solutions, recent advancements, and future directions,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 196–248, 1st Quart., 2020, doi : 10.1109/COMST.2019.2933899.

[37] Kumar, R. , X. Zhang, W. Wang, R. U. Khan, J. Kumar, and A. Sharif, ‘‘A multimodal malware detection technique for Android IoT devices using various features,’’ IEEE Access, vol. 7, pp. 64411–64430, 2019.

[38] Lee, H. (2015). Concept and Characteristics of 5G Mobile Communication Systems. [Online]. Available : https : [39]//www.netmanias.com/en/post/blog/7109/5g-iot/concept - andcharacteristics - of - 5g - mobile - communication - systems - 1

[40] Li F., Y. Han, and C. Jin, ‘‘Practical access control for sensor networks in the context of the Internet of Things,’’ Comput. Commun., vols. 89–90, pp. 154–164, Sep. 2016.

[41] Li H., F. Li, C. Song, and Y. Yan, ‘‘Towards smart card based mutual authentication schemes in cloud computing,’’ KSII Trans. Internet Inf. Syst., vol. 9, no. 7, pp. 2719–2735, 2015.

[42] Li H., Y. Dai, L. Tian, and H. Yang, ‘‘Identity - based authentication for cloud computing,’’ in Cloud Computing. Berlin, Germany : Springer, 2009, pp. 157–166.

[43] Luo M., Y. Luo, Y. Wan, and Z. Wang, ‘‘Secure and efficient access control scheme for wireless sensor networks in the cross - domain context of the IoT,’’ Secur. Commun. Netw., vol. 2018, pp. 1–10, Feb. 2018, doi : 10.1155/2018/6140978.

[44] Militano, L., Araniti, G., Condoluci, M., Farris, I., & era, A. (2015). Device - to - device communications for 5G The internet of things. EAI Approved Internet Transactions Things, 1 (1).

[45] Mishra D., P. Vijayakumar, V. Sureshkumar, R. Amin, S. H. Islam, and P. Gope, ‘‘Efficient authentication protocol for secure multimedia communications in IoT - enabled wireless sensor networks,’’ Multimedia Tools Appl., vol. 77, no. 14, pp. 18295–18325, Jul. 2018.

[46] Mudgerikar A., P. Sharma, and E. Bertino, ‘‘E - spion : A system - level intrusion detection system for IoT devices,’’ in Proc. ACM Asia Conf. Comput. Commun. Secur. (Asia CCS), Auckland, New Zealand, 2019, pp. 493–500.

[47] O’Connell, E., Moore, D., & Newe, T. (2020). Challenges Associated with Implementing 5G in Manufacturing. Telecom, 1(1), 48–67. doi : 10.3390/telecom1010005

[48] Orlosky, J.; Kiyokawa, K.; Takemura, H. Virtual and Augmented Reality on the 5G Highway. J. Inf. Process. 2017, 25, 133–141.

[49] Ostad - Sharif A., H. Arshad, M. Nikooghadam, and D. Abbasinezhad - Mood, ‘‘Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme,’’ Future Gener. Comput. Syst., vol. 100, pp. 882–892, Nov. 2019.

[50] Pajouh H. H., R. Javidan, R. Khayami, A. Dehghantanha, and K. - K. - R. Choo, ‘‘A two - layer dimension reduction and two - tier classification model for anomaly - based intrusion detection in IoT backbone networks,’’ IEEE Trans. Emerg. Topics Comput., vol. 7, no. 2, pp. 314–323, Apr. 2019.

[51] Palattella, M. R. et al., “Internet of things in the 5G era : Enablers, architecture, and business models,” IEEE J. Sel. Areas Commun., vol. 34, no. 3, pp. 510–527, 2016.

[52] Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., & Engel, T. (2016). Internet of Things in the 5G Era : Enablers, Architecture, and Business Models. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, 34 (3).

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

[54] Porambage P., A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, ‘‘Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications,’’ IEEE Access, vol. 3, pp. 1503–1511, 2015.

[55] Porambage P., C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, ‘‘Two - phase authentication protocol for wireless sensor networks in distributed IoT applications,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Istanbul, Turkey, Apr. 2014, pp. 2728–2733.

[56] Rahimi, H., Zibaeenejad, A., & Safavi, A. A. (2018). A Novel IoT Architecture based on 5G - IoT and Next Generation Technologies. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). doi : 10.1109/iemcon.2018.8614777

[57] Rampa, V.; Savazzi, S.; Malandrino, F. Opportunistic sensing in beyond - 5G networks : The opportunities of transformative computing. In 5G Italy Book 2019 : A Multiperspective View of 5G; CNIT : Parma, Italy, 2019; pp. 461–476. ISBN 9788832170030.

[58] Rana, A., Taneja, A., & Saluja, N. (2021). Accelerating IoT applications new wave with 5G : A review. Materials Today : Proceedings. doi : 10.1016/j.matpr.2021.03.292

[59] Rawat , D. B., Reddy, S. R. (2017). “Software defined networking architecture, security and energy efficiency : A survey,” IEEE Commun. Surv. Tutorials, vol. 19, no. 1, pp. 325–346, 2017.

[60] Riad K., R. Hamza, and H. Yan, ‘‘Sensitive and energetic IoT access control for managing cloud electronic health records,’’ IEEE Access, vol. 7, pp. 86384–86393, 2019.

[61] Roman, R., J. Lopez, and M. Mambo, “Mobile edge computing, fog et al. : A survey and analysis of security threats and challenges,” Futur. Gener. Comput. Syst., vol. 78, pp. 680–698, 2018.

[62] Saeed A., A. Ahmadinia, A. Javed, and H. Larikani, ‘‘Intelligent intrusion detection in low - power IoTs,’’ ACM Trans. Internet Technol., vol. 16, no. 4, pp. 27 : 1–27 : 25, 2016.

[63] Selvakumar K., M. Karuppiah, L. SaiRamesh, S. H. Islam, M. M. Hassan, G. Fortino, and K. - K. - R. Choo, ‘‘Intelligent temporal classification and fuzzy rough set - based feature selection algorithm for intrusion detection system in WSNs,’’ Inf. Sci., vol. 497, pp. 77–90, Sep. 2019.

[64] Shah, S. H., & Yaqoob, I. (2016). A Survey : Internet of Things (IOT) Technologies, Applications and Challenges. The 4th IEEE International Conference on Smart Energy Grid Engineering.

[65] Shariatmadari , H. et al. (2015). “Machine - type communications : current status and future perspectives toward 5G systems,” IEEE Commun. Mag., vol. 53, no. 9, pp. 10–17, 2015.

[66] Sharma V., I. You, K. Yim, I. - R. Chen, and J. - H. Cho, ‘‘BRIoT : Behavior rule specification - based misbehavior detection for IoT - embedded Cyberphysical systems,’’ IEEE Access, vol. 7, pp. 118556–118580, 2019.

[67] Solomitckii, D., M. Gapeyenko, V. Semkin, S. Andreev, Y. Koucheryavy, Technologies for Efficient Amateur Drone Detection in 5G, Millimeter - Wave Cellular Infrastructure, IEEE Communication magazine 56 (1) (2018) 43–50.

[68] Stallings, W. (2010). Cryptography and Network Security : Principles and Practice, 5th ed. Upper Saddle River, NJ, USA : Prentice - Hall, 2010.

[69] Stanley, M., Y. Huang, H. Wang, H. Zhou, A. Alieldin, and S. Joseph, “A novel mm - Wave phased array antenna with 360° coverage for 5G smartphone applications,” in Millimetre Waves and Terahertz Technologies (UCMMT), 2017 10th UK - Europe - China Workshop on, 2017, pp. 1–3.

[70] Tian, Z. , Y. Sun, S. Su, M. Li, X. Du, and M. Guizani, ‘‘Automated attack and defense framework for 5G security on physical and logical layers,’’ 2019, arXiv : 1902.04009. [Online]. Available : http : //arxiv.org/abs/1902.04009

[71] Tian, Z. , Y. Sun, S. Su, M. Li, X. Du, and M. Guizani, ‘‘Automated attack and defense framework for 5G security on physical and logical layers,’’ 2019, arXiv : 1902.04009. [Online]. Available : http : //arxiv.org/abs/1902.04009

[72] Tseng, M. - L., Tan, R. R., Chiu, A. S. F., Chien, C. - F., & Kuo, T. C. (2018). Circular economy meets industry 4.0 : Can big data drive industrial symbiosis? Resources, Conservation and Recycling, 131, 146–147. doi : 10.1016/j.resconrec.2017.12.0

[73] Turkanović M., B. Brumen, and M. Hölbl, ‘‘A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,’’ Ad Hoc Netw., vol. 20, pp. 96–112, Sep. 2014.

[74] van de Belt, J., H. Ahmadi, and L. E. Doyle, “Defining and surveying wireless link virtualization and wireless network virtualization,” IEEE Commun. Surv. Tutorials, vol. 19, no. 3, pp. 1603–1627, 2017.

[75] Wang, Y. , L. Kung, W. Y. C. Wang, and C. G. Cegielski, “An integrated big data analytics - enabled transformation model : Application to health care,” Inf. Manag., vol. 55, no. 1, pp. 64–79, 2018.

[76] Wazid M. and A. K. Das, ‘‘A secure group - based blackhole node detection scheme for hierarchical wireless sensor networks,’’ Wireless Pers. Commun., vol. 94, no. 3, pp. 1165–1191, Jun. 2017.

[77] Wazid M., A. K. Das, S. Kumari, X. Li, and F. Wu, ‘‘Provably secure biometric - based user authentication and key agreement scheme in cloud computing,’’ Secur. Commun. Netw., vol. 9, no. 17, pp. 4103–4119, Nov. 2016.

[78] Wazid M., A. K. Das, V. Bhat K, and A. V. Vasilakos, ‘‘LAM - CIoT : Lightweight authentication mechanism in cloud - based IoT environment,’’ J. Netw. Comput. Appl., vol. 150, Jan. 2020, Art. no. 102496, doi : 10.1016/j.jnca.2019.102496.

[79] Wazid M., Das A. K., S. Kumari, and M. K. Khan, ‘‘Design of sinkhole node detection mechanism for hierarchical wireless sensor networks,’’ Secur. Commun. Netw., vol. 9, no. 17, pp. 4596–4614, Nov. 2016.

[80] Wazid M., P. R. Dsouza, A. K. Das, V. K. Bhat, N. Kumar, and J. J. P. C. Rodrigues, ‘‘RAD - EI : A routing attack detection scheme for edge - based [81]Internet of Things environment,’’ Int. J. Commun. Syst., vol. 32, no. 15, p. e4024, Oct. 2019, doi : 10.1002/dac.4024.

[82] Wazid, M. , A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, ‘‘Authentication in cloud - driven IoT - based big data environment : Survey and outlook,’’ J. Syst. Archit., vol. 97, pp. 185–196, Aug. 2019.

[83] Wazid, M., Das, A. K. N. Kumar, and A. V. Vasilakos, (2019). ‘‘Design of secure key management and user authentication scheme for fog computing services,’’ Future Gener. Comput. Syst., vol. 91, pp. 475–492, Feb. 2019.

[84] Wazid, M., Das, A.K., Shetty, S. et al. (2021) Security in 5G - enabled Internet of Things communication : issues, challenges, and future research roadmap. IEEE Access, 9. pp. 4466 - 4489. https : //doi.org/10.1109/access.2020.3047895

[85] Wdowik, R.; Ratnayake, R.C. Collaborative Technological Process Planning with 5G Mobile Networks and Digital Tools : Manufacturing Environments’ Perspective. In Proceedings

of the 2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Macau, China, 15–18 December 2019; pp. 349–353.

[86] Wu, B., K. Xu, Q. Li, Z. Liu, Y. - C. Hu, Z. Zhang, X. Du, B. Liu, and S. Ren, ‘‘SmartCrowd : Decentralized and automated incentives for distributed IoT system detection,’’ in Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS), Dallas, TX, USA, Jul. 2019, pp. 1106–1116.

[87] Zhang, L., M. Xiao, G. Wu, M. Alam, Y. - C. Liang, and S. Li, “A Survey of Advanced Techniques for Spectrum Sharing in 5G Networks,” IEEE Wirel. Commun., vol. 24, no. 5, pp. 44–51, 2017.