David Humam Al-Aani

Effect of 5G Internet on IoT Industry with Focus on Communication and Security Effects

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communication Technology

Bachelor's Thesis

22nd March 2021

Abstract

Author:	David Humam Al-Aani
Title:	Effect of 5G Internet on IoT Industry with Focus on Communication and Security Effects
Number of Pages:	42 pages
Date:	22nd March 2021
Degree:	Bachelor of Engineering
Degree Programme:	Information and Communication Technology
Professional Major:	IoT and Cloud Computing
Instructors:	Janne Salonen, Head of School

The aim of this thesis is to present the effect of the fifth-generation (5G) internet on the Internet of Things (IoT) industry. The thesis will focuses on the ease of communication brought about by the 5G network and the security aspects available, when the network is fully implemented, which will revolutionize the IoT to its full potential. With the evolution of the 5G wireless network, the IoT has become a revolutionary technique that allows a various range of options and applications. It will make a various quantity of devices ready to be connected so as to make one communication design. Because this field has increased considerably in recent years, it is important to review the technology well and take a detailed look at its applications within different domains.

The research has been completed by reading a number of different sources, such as books, online material, journals, publications, and previous theses, have published about IoT and 5G. The thesis presents the IoT, 5G and the security aspects, their evolution history, future prospects and potential market shares.

Based on of this study, it can be concluded, that the thesis shows what IoT and 5G are, how they will change the near future, what should be invested in the future, and what challenges new frontiers are facing in the world of modern technology. This study defines also what the IoT is and presents a summary of its main technologies and uses, giving a 5G protocol as an answer to the challenges.

Keywords: 5G, IoT industry, communication and security

Tiivistelmä

Tekijä:	David Humam Al-Aani
Otsikko:	5G-Internetin Vaikutus IoT-teollisuuteen Keskittyen Viestintä- ja Turvallisuusvaikutuksiin
Sivumäärä:	42 sivua
Aika:	22. maaliskuu 2021
Tutkinto:	Insinööri (AMK), Bachelor of Engineering
Tutkinto-ohjelma:	Tieto- ja viestintätekniikan
Ammatillinen pääaine:	Verkot ja Pilvipalvelut
Ohjaajat:	Janne Salonen

Tämän opinnäytetyön tarkoituksena on esittää 5G-internetin vaikutusta IoT-teollisuuteen. Työ keskittyy 5G-verkon tuoman viestinnän helppouteen ja turvallisuusnäkökohtiin. Viidennen sukupolven (5G) langattoman verkon kehityksen myötä esineiden internetistä (IoT) on tullut vallankumouksellinen tekniikka, joka mahdollistaa erilaisia vaihtoehtoja ja sovelluksia. Se valmistelee useita laitteita, jotka on kytketty, jotta voidaan tehdä yksi viestintäsuunnittelu. Koska laitteiden määrä on viime vuosina huomattavasti kasvanut, on tärkeää tutustua 5G-teknologiaan hyvin ja tarkastaa yksityiskohtaisesti sen sovelluksia täysin eri verkkotunnuksilla.

Valtavien laitteiden käyttöönotto internetissä, puettavat, älykkäät kaupungit ja älykodin laitteet sekä luotettavan 5G-viestintäalustan ja pilvipalvelujen kaltaisten teknologioiden käyttöönotto on laajentanut kyberturvallisuushyökkäysten spektriä. Verkolle tai liitetylle järjestelmälle suojaus on valtava haaste, sillä IoT:ssä valtava valikoima laitteita voi muodostaa yhteyden ja kommunikoida, jotta turvallisuushaaste voidaan ratkaista ositetulla tasolla. 5G:ssä tämä haaste ratkaistaan turvallisuusvarmistuksilla ja standardoinneilla. Pilven turvallisuus on suoritettu eristämällä ja viipaloimalla, ja radioyhteysverkko on suojattu kryptografialla.

Tärkeimmät ominaisuudet laajamittaiselle IoT:lle ovat edulliset anturit, nopea ja virheensietävä tietoviestintä, älykäs laskenta sekä erilaiset sovellukset. Tämä tutkimustyö on esitetty osissa, joita ovat yleiskatsaus IoT-teknologiaan, katsaus kaikkiin IoT-sovelluksiin ja paikallisuus IoT:n haasteissa.

Tutkimuksen tavoitteena on kattaa kokonaan IoT:n sovellukset sekä kiinnittää huomiota ympäristöön sekä kaupallisiin, teollisiin ja älykkäisiin kaupunkeihin ja infrastruktuurisovelluksiin. Tämä tutkimus selvittää IoT:n ajatusta ja määrittelee ja tiivistää sen tärkeimmät teknologiat ja käyttötarkoitukset. Työ vastaa 5G-protokollan haasteisiin.

Avainsanat: 5G, IoT-teollisuus, viestintä ja turvallisuus

Table of Contents

List of Abbreviations

1G:	First Generation
2G:	Second Generation
3G:	Third Generation
4G:	Fourth Generation
5G:	Fifth Generation
AES:	Advanced Encryption Standard
API:	Application Programming Interface
BLE:	Bluetooth Low Energy
CCN:	Content Centric Network
CDMA:	Code Division Multiple Access
CRC:	Cyclic Redundancy Check
DDoS:	Disturbed Denial of Service
DoS:	Denial of Service
EOT:	Extranet of Things
FDMA:	Frequency Division Multiplexing Access
GPS:	Global Positioning System
GSM:	Global System for Mobile
HDFS:	Hadoop File System
HTML:	Hypertext Markup Language
HTTP:	Hypertext Transport Protocol
ICT:	Information and Communication Technology
IEEE:	Institute of Electrical and Electronics Engineers
IMSI:	International Mobile Subscriber Identifier
IoT:	Internet of Things
IP:	Internet Protocol
IPv6:	Internet of Protocol version 6
JMS:	Java Message Service
ITU:	International Telecommunication Union
LPWAN:	Low Power Wide Area Network
LTE:	Long Term Evolution
MAN:	Metropolitan Area Network
NB-IoT:	Narrow Band Internet of Things
NFC:	Near Filed Communication
OSI:	Open System Interconnection
PAN:	Personal Area Network
PNF:	Physical Network Function
RAN:	Radio Access Network
RFID:	Radio Frequency Identification
SDN:	Software Defined Network
TCP:	Transmission Control Protocol
UDP:	User Datagram Protocol
UMTS:	Universal Mobile Telecommunication System
URI:	Uniform Resource Identifier
WAP2:	Wi-fi Protected Access 2
WebOS:	Web Operating System
VNF:	Virtual Network Function

XMPP:	Extensible Messaging and Presence Protocol
M2M:	Machine to Machine

1 Introduction

The effects of the 5G internet on the Internet of Things (IoT) industry are fueled by the exponential demand growth by customers needing faster data and fast networks for gathering, transmitting and processing; thus, 5G is irresistible. From an optimistic view the 5G technology poses a huge business opportunity in terms of both the concepts and the underlying applications. In contrast, the venture brings causes security vulnerabilities and points of exploitation.

According to Niklas Heuveldop, it is estimated that 29 billion subscribers will be connected to the internet by the year 2022. The utilities and the components have opened up research on the impact of connecting different devices, which enables communicating over the internet simultaneously. 5G is the fifth generation of telecommunication data communication. It is an advancement of 4G LTE which has offered faster real time connections and supported high speed applications and wearable devices. 3G meant the birth of video conferencing and GPS oriented applications, while 2G was reliable in browsing with voice calls. 1G was the first generation of voice calls. [1.] Smart driven cars, TVs and industrial deployments of the IoT technology have received a warm welcome and are expected to be important for the future of mankind and human labor, bringing efficiency in how work is carried out rather than replacing the human labor. To help one understand the potential in business opportunities awaiting IoT and 5G deployment, the figures below indicate the numbers of subscribers reported in worldwide research, according to Mobility Report 2017 [1].

	2016	2022
Smartphone subscribers	3.9 B	6.8 B
LTE subscribers	1.9 B	5 B
Mobile subscribers	7.5 B	9 B
Broadband subscribers	4.4 B	8.3 B
Data Traffic per smartphone	3.9 B	6.8 B

Big data is one of the leading markets in the IT industry, harnessing a huge amount of data at a very fast speed. Analyzing the trends and insights that large amounts of data show, it is possible to increase understanding of business intelligence and market research. The Data analytics in the IT industry is targeted by hackers and malicious business competitors, with intentions to intercept or steal network data for business advantage.

The popularity of the 5G networks and the IoT industry dates back to the ages of telecommunication and gradual evolution of the internet. In 1926 Nikola Tesla predicted in the Colliers magazine that from a pocket device a man will be able to carry out amazing tasks, with the use of a wireless brain like a network. The concept of the internet of things was introduced in the year 1999 through the realization of the Radio Frequency Identification (RFID) technology. The International Telecommunication Union (ITU) published the first report on the dynamic network of networks, in the year 2005; the network is now the internet of things. In the late 20th century from 2006 to 2008, early technology adopting telecommunication giants like Ericsson, Sun and Intel, opened a forum for the study of IP networks on smart objects running on IoT. [2.]

The purpose of this thesis is to present the impact of the 5G internet on the IoT industry and its interactions with devices. The subject is hot these days as everyone needs to obtain information quickly and quicker devices are needed. The thesis will give detailed information on the 5G internet with a focus on security effects. This thesis helps others concerned about the IoT idea and its opportunities by doing business and 5G interactions.

2 5G Network Feature for IoT Communications

Sensors or devices are basic tracking, measurement and monitoring components of the IoT system. Connections are communication links between end devices, which may be direct or indirect, wireless or virtualized for effectiveness. The processing unit does the analyzing and decision making on data, while energy efficiency manages energy utilization by the devices by the

switches mode from active to passive, enabling the sleep mode. Quality and reliability are the last two characteristics of the IoT infrastructure that ensures ISO quality standards are adhered to from start to end. [3.]

Smart home sensors that automatically communicate to the security cameras, appliances, TVs, water and irrigation have enormous data to process for authentication, calibration, calculations and recognition with the cloud services. Sensor-oriented and self-driving cars require high throughput for smart decisions on real-time processing and analyzing of data they are collecting. E-healthcare has deployed applications for remote sensing, online monitoring, collecting and analyzing data using the IoT concept. This application requires sharp accuracy and ease of accessibility for correct prescription and medication of patients. [3.]

2.1 IoT Architecture Layers

The layers of the Internet of things architecture start to communicate with each other the communication takes layers network for communication. The internet of things has a basic four-layer design that is shown in Table 1 below. [4.] The design will give us the more better understanding for IoT that which layers and which components corresponds to them and their practicality:

Table 1. Layer architecture with components. Based on [4].

IoT Architecture Layer	Components
Application Layer	Environment, Energy, Healthcare, Transportation, People tracking, Surveillance, Supply Chain, Retail
Management Service Layer	Device Modelling, Configuration and Management
Network Layer	WAN (GSM, UMTS, 4G, LTE, LTE-A,5G)

Sensors connectivity	Sensors Networks

1 Application layer: The application layer gets the data from the network layer, where cloud computing, mega databases, intelligent processing and ubiquitous computing are involved.

2 Management service layer: This is the layer that offers device configuration, modelling and management.

3 Network layer: This layer governs the protocols on transfer and transmission of data.

4 Sensor networks: This layer is also known as the device layer, consisting of all sorts of sensors gathering information from machine-to-machine communications to the internal gateways as data.

2.2 IoT Applications

The applications and use of IoT within the totally different domains area unit what drive and justify the event of this new trend, resulting in the acceptance of IoT by the new world [5]. The mind map as shown in Figure 1 below, it is about internet of things applications [6]. In fact, IoT and 5G are like two sides of single coin. There are many standards related to internet of things defined by various standarisation bodies. These standards are for healthcare, smart home, smart city, manufacturing, sensors, robotics, sports and leisure, analytics, data management, standirization and security. IoT is also about many protocols used. The internet of things application uses database with specific set of features.

The study of IoT applications improves the understanding and improvement of IoT technology, and thus, the look of latest systems for recently developed cases. The thought of IoT is often summarized as generating daily data from AN object and transferring it to a different one. Therefore, sanctionative

communication between objects makes the vary of IoT applications intensive, variable, and unlimited. [7.]

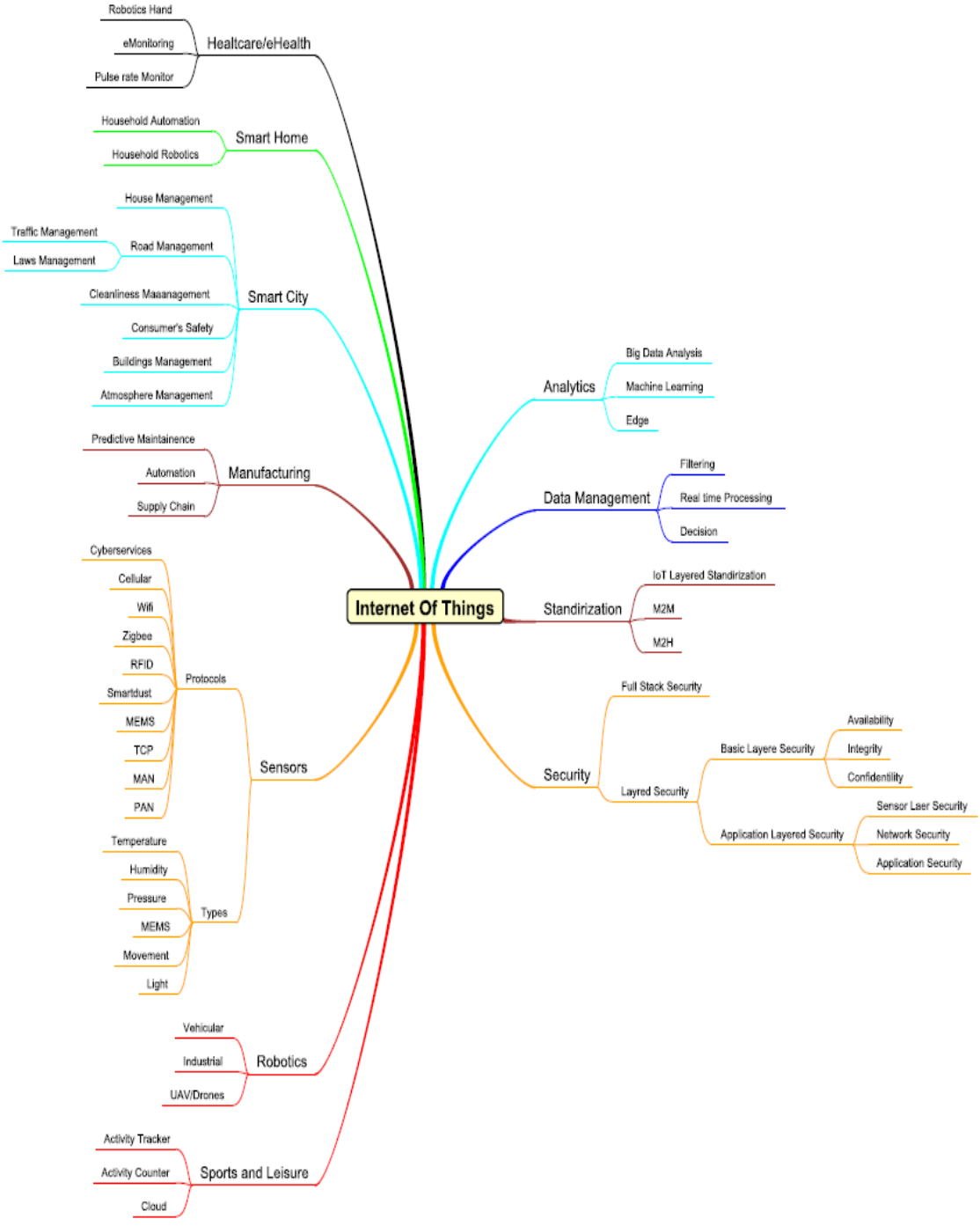

Figure 1. IoT mind map. Copied from [6].

2.3 5G Technologies

Figure 2 below is a mind map relating to some technologies associated with 5G [6]. In general, 5G involves many key technologies, and every technology is intended to handle specific demands in many completely different world and business eventualities. The 5G is wide believed because the missing link for the development of extremely advanced networked systems like IoT, self-driving cars, robotics, telemedicine, virtual reality. With additional capability within the networks, applications will run at the same time while not impacting different users' speeds. [8.]

Figure 2. 5G mind map. Copied from [6].

3 Security Concerns on Deployment of 5G Network for IoT Industry

Modern or new technologies are rolled out with a challenge to make them secure as a priority. Data confidentiality, integrity and availability are the pillars to security that should be maintained. The radio receiver's technology had eavesdropping as a security challenge on the mobile communication.

Radio network and cloud security, flexibility in scalable architecture, energy efficiency and security assurance are the core pillars of 5G security and identity management. These pillars are discussed in detail below. [9.]

3.1 Security Assurance

Adherence to international ISO standards will clear the usage of 5G for IoT industry. Here the 5G trust model is a complete loop advancement of 4G on User, Service, and Network.

3.2 5G Radio Network Security

The radio access network and radio protocol designs will be discussed as they add integrity protection in 5G.

3.3 Flexibility and Scalability in Architecture

From the virtualized and dynamic security management solutions in 5G, a replica security architecture of a more dynamic and flexible is mandatory.

3.4 Cloud Security

To provide efficient and secure data encryption, useful ecosystem and trusted computing tools and to secure virtualized and isolated networks, 5G is built with a similar security infrastructure.

3.5 IoT Privacy and Security

The IoT is facing a number of challenges, including inappropriate device updates, privacy, security, a lack of efficient and effective protocols for anti-botnet security, minimal user awareness, and lack of eminent active device monitoring. IoT brings users benefits; however, it comes along with a significant number of challenges. The primary concerns of the security experts discussed in this chapter are cyber security and privacy risks associated with the deployment of 5G. Many businesses and government agencies are in a difficult situation as a result of these two factors. The vulnerabilities of IoT technologies have been highlighted by recent high-profile cyber security attacks. [10.]

- Security assertion: The use of 5G for the IoT industry will be cleared if international ISO standards are followed. The 5G trust model is a full loop advancement of 4G on the user, service, and network levels.
- Radio network security in 5G: The designs of the radio access network and radio protocol will be discussed because they add integrity protection to 5G.
- Architectural flexibility and scalability: A replica security architecture that is more dynamic and flexible is required as a result of the virtualized and dynamic security management solutions in 5G.
- Security in the cloud: 5G is built with similar security infrastructure to provide efficient and secure data encryption, a useful ecosystem, and trusted computing tools, as well as to secure virtualized and isolated networks.

The Internet of Things presents a number of significant challenges, including privacy and security. These pillars are discussed below in detail.

3.5.1 Security for the Internet of Things

The highest profiled business asset protection concerning aspect of IoT is its security. As more devices connect to the internet or other networks, the volume and complexity of data grows. The risk of becoming vulnerable grows. The estimated number of IoT connected devices is around 50 billion, so securing them all is a major undertaking. [11.] The data collected by these devices must be stored securely by volume, while the user's or individual's integrity and confidentiality are maintained. Data confidentiality, data availability, and data integrity are the most basic IoT security requirements.

3.5.2 Privacy

The utility of the Internet of Things is measured by how well it can respect people's privacy preferences. Concerns about privacy and possible harms associated with IoT could be a significant factor in delaying IoT's complete acceptance. It is important to understand that user privacy rights and respect are critical in maintaining users' trust and confidence in the system. A considerable amount of work is put to ensure that the internet of things outweighs the privacy challenges around surveillance and monitoring. The omnipresent intelligence integrated artefacts where the sampling process and the information distribution in the IoT can be done early in any place are reasons for privacy concerns. The pervasive accessibility connectivity is also an important factor to understand this privacy because, unless a specific system is put in place, it will pose environment much more convenient to unauthorized access to personal information online. [12.]

3.5.3 Interoperability

A fragmented environment of proprietary IoT technical implementation is known to inhibit value for users. Even if complete interoperability across goods and services is not always possible, consumers may not like purchasing products and services that lack versatility and are subject to dealer lock-in. Poorly

planned IoT devices which have a negative effect on the networking services to which they link. [13.]

A single defence mechanism is not sustainable to detect, protect and remediate attacks, thus rendering traditional reliance on cryptography obsolete to time. As a result, different layers of protection are needed to overcome threats to IoT authentication. Hacks can be avoided by developing more sophisticated security features and incorporating them into goods. This evasion occurs because consumers would purchase goods that already have adequate security features in place to guard against vulnerabilities. Some of the steps suggested to ensure that IoT is safe include cyber security frameworks. [14.]

3.5.4 Security and Privacy Policies

Cloud-based platforms facilitating data collection, processing, and sharing have often been profiled as the critical infrastructure to IoT. IoT computing devices and nodes that are connected to the internet and that store or relay confidential data are being targeted by hackers and attackers. Patient data and electronic medical records, for example, make the healthcare system a lucrative target for hackers. Each layer of the IoT model poses security challenges as well as the ability to implement security and privacy requirements and protocols at the same time. In the system layer, for example, the sensor's data is sent to the edge, the fog, and then the cloud, necessitating authorization and certificates that trust specific servers in order to prevent the attacks. Firmware protection and hardware address authentication and more, but at the expense of power consumption, as certain wireless-enabled devices, such as wearables, are battery-powered. To achieve both security and power constraints, security steps must be revisited. On the cloud layer, protection measures must ensure the network protocol between the edge and fog nodes. Less data spying and logging is possible with the message passing protocol, point-to-point encryption, and certificates. It is important to ensure that long-term data storage and real-time data processing are safe from SQL injections, sniffing, and phishing scripting attacks at the data processing and end-user level. The long-term data

storage and real-time data processing are protected can be achieved by ensuring that the service certificate is modified and that it complies with the HIPPA standards (in health service). [14.]

4 Opportunities and Benefits for Enterprises

For telecom operators, the business market would be the primary source of additional 5G sales. The GSMA forecasts that by 2025, 5G will offer new technologies and flexibility to satisfy the unique needs of various business customers, potentially worth up to US$400 billion per year to operators. The importance of the enterprise segment to mobile operators is illustrated in two more GSMA surveys. In a global survey of 750 CEOs conducted in October 2016, nearly 70% of respondents said the enterprise segment is the most significant opportunity for the mobile industry in the 5G phase. According to a more recent survey from April 2018, the industry aspires to produce 40% of its revenue from businesses five years after 5G. When compared to previous cellular technology, such as 4G, 5G cellular connections would have a number of advantages for businesses. In a number of main areas, such as speed, power, and latency, it improves on 5G. Despite the fact that 4G is widely used around the world, it will not be able to match 5G speeds or accommodate large numbers of devices on the network. Latency is also a primary differentiator for 5G. [15.]

4.1 Opportunities and Benefits for Customers

Consumers' mobile broadband experiences will be transformed by early 5G networks that offer download speeds of over 1 Gbps, enabling a reliably high-quality mobile broadband experience with stable internet connectivity at home, in the workplace, and on the go. IoT devices and applications will be complemented by an improved, secure, and high-speed mobile broadband, facilitated by operators' Mobile IoT networks. Capturing the large quantities of data produced by consumer IoT devices would be one of 5G's ultimate tests. Edge computing, machine learning, and artificial intelligence can all be used to

capture, analyse, and respond to user demands in real time, and 5G can excel in this field due to its power, bandwidth, and low latency capabilities. As previously mentioned, one important area where users can benefit is transportation, with 5G-connected IoT devices offering a number of enhanced safety measures for drivers. Advanced alert capabilities, collision detection, prone user detection, the use of on-board IoT sensors, and enhanced infotainment facilities are only a few of them. [15.]

4.1.1 Enhanced Mobile Broadband (EMBB)

In its early implementations, the GSMA expects 5G to extend the consumer IoT market by providing high-speed, low-latency, reliable, and stable enhanced mobile broadband (eMBB)17. High-definition consumer video, immersive communications, such as video calling and augmented and virtual reality, and smart city facilities, such as IoT video cameras for surveillance, will all be supported by enhanced MBB. [16.]

The ability of 5G to accommodate large amounts of data traffic and large numbers of users, including IoT devices, would be the most important advantage. According to some figures, 5G would have at least 100 GB per month per customer. Furthermore, the cost per bit is expected to fall, theoretically allowing for “unlimited” data packages. [16.]

Consumers can benefit from low latency and high throughput IoT services provided by 5G. User use cases that would benefit from 5G's lower latency capabilities, which are expected to be as low as 1 ms between the system and base station. Fingertip monitoring of remote assets and "immersive interactions," such as high-definition video conferencing, are among the features of the device. [16.]

4.1.2 Fixed Wireless Access (FWA)

Fixed Wireless Access (FWA) networks use wireless technology rather than fixed lines to provide Internet access to homes.

5G FWA allows home broadband networks to be set up easily and cost-effectively in areas where fixed line home broadband is not accessible. Consumer 5G FWA is expected to have a significant impact in both emerging and developed markets, taking broadband to areas where fixed-line operators do not currently operate. The Consumers benefit most from FWA because of its performance. Furthermore, the cost per bit to connect a home to broadband via FWA can be 74% lower than wireline connections. Customers would benefit from faster speeds, power, and bandwidth to support their number of IoT devices, thanks to the introduction of 5G. [17.]

4.1.3 Economic Potential & Best Practices

Customers would expect high throughput and low latency connections anywhere, so both mobile and fixed networks would need to be densified to better support both user and business use cases.

FWA can be a cost-effective way to achieve network densification by introducing broadband access to areas where there is no wireline infrastructure or just copper wireline infrastructure. The emphasis of this GSMA document is FWA based on 3GPP standards, which includes 4G LTE and 5G NR. [18.]

4.1.4 Mobile IoT is Part of the 5G Story

Current 4G cellular networks, including those using LTE-M and NB-IoT technologies, will support a wide range of IoT applications. However, 5G will boost these IoT networks even further. As technology progresses, large IoT networking is set to cost less despite complexity, based on low-power wide-area networks, allowing for more IoT devices to be linked. A solid basis for energy-

saving smart services LTE-M and NB-IoT have been integrated into the 3GPP standard.5G requirements have been confirmed as being viable in the long term as part of future 5G requirements. As IoT becomes integrated within enterprise and consumer applications, many of which are built by small and medium-sized businesses, the large-scale rollout of 5G would accelerate. The case studies demonstrate how LTE-M and NB-IoT technologies are being used to deploy Mobile IoT applications to support a variety of use cases. [19.]

5 Impact of 5G on IoT

By 2021, the Internet of Things is expected to have 50 billion devices deployed and connected to the internet, ranging from wired temperature sensors to self-driving cars. The wide range of system types from various verticals correlates to a wide range of communication infrastructure requirements. Although battery-powered sensors necessitate a low-energy communication technology, industrial IoT applications necessitate ultra-reliable, low-latency connections. WLAN, Narrowband-IoT (NB-IoT), ZigBee, and LoRa Wide Area Network (LoRaWAN) are the wireless networking technologies that currently cover these complex criteria. [20.]

This is where the 5th Generation (5G) technology comes into play, with its extremely scalable architecture designed to adapt to almost every IoT use case using advanced techniques like network slicing and Network Function Virtualization (NFV). The 5G technology has the ability to be a catalyst for IoT development, providing a single communications network for the IoT – and vice versa.

In comparison to previous generations of mobile technology, 5G networks would expand mobile networking services past telephony services, the mobile broadband platform, and massive machine-to-machine communication into new vertical device domains, or and beyond.

5.1 IoT Requirements and Use Cases

There are use cases in the IoT vertical doman that are established in IoT based projects. They place basic constraints on the network infrastructure.

5.2 Smart Mobility

Smart mobility is becoming an increasingly present topic on sustainability agendas in a response to the impacts of urban transportation systems. The concept of smart mobility has mainly evolved from the convergence of the digital revolution with the transportation sector. Hence, new technologies have been used to increase the efficiency of the transport network, particularly those related to the IoT. The concept of smart mobility will be covered, which is intrinsically relevant to smart cities. [21.]

5.2.1 Automated Valet Parking (AVP)

Valet parking is a term that is commonly used around the world, for example, by high end restaurants and hotels, supermarkets, and shopping malls.

Upon arriving at the hotel with their vehicle, the customer exits the vehicle and hands over the keys to the hotel staff, who will then move the vehicle to its designated parking spot. Meanwhile, the customer will do things like sign in or go to a meeting. Upon exit, the car is returned to the onboarding spot by the hotel staff at the request of the client. With such and more advanced development of self-driving vehicle technology, it is a reasonable move to automate the valet parking concept, Automated Valet Parking (AVP). [22.]

Several stakeholders like, AVP application provider, IoT Devices maker, Communication Network providers, and IoT platform suppliers will participate in and benefit from the value chain by implementing this use case [22].

IoT plays a key role in this use case, as it is used to enhance the procedure of an autonomous driving vehicle in Valet Parking. After the driver has exited the vehicle, the autonomous vehicle can park itself in AVP. The self-driving car can locate an appropriate parking spot and drive and park itself. When the driver wants to exit the place, they will simply ask the autonomous vehicle to return to the collect point on its own using a smartphone application, for example.

5.2.2 Car Rebalancing

Car rebalancing service is designed to rebalance a driverless fleet of AD vehicles spread across a car sharing scheme with several collect points. The AD vehicles are able to drive themselves at a 10 km/h maximum speed, between dedicated collect points on specific areas like University campuses, using pre-defined and 3D-mapped tracks as well as IoT data to develop their world model, between several designated collect points in specific areas. This use case's scenario includes places like university campuses where there are no lane markers, traffic signals, pedestrian crossings, RSUs, or traffic lights, and cyclists in addition to several cars. This makes the urban environment a hard-hitting ground for automated driving vehicles. [23.]

The following are the main advantages of the car rebalancing use case:

- Boost protection by reducing the time it takes to detect and prevent VRU collisions.
- Increase of real-time vehicle availability, by reducing the time taken between request and delivery.
- Making better use of available parking lots.
- Reducing obstacle detection errors.
- Better prediction of unprecedented obstacles like blocked routes by use of VRU identification, resulting in less rerouting.
- Improving accuracy of localization by using, for example, localization offered by IoT-enabled smartphone applications.
- Improving demand prediction for requested vehicles by increasing dynamic obstacle motion accuracy.

5.2.3 Car Sharing

A car sharing service is designed to allow multiple customers to share a fleet of self-driving cars or human driven cars that are shared among them. Car sharing is a service that locates the nearest available car and assigns it to a single customer or drives it to the interested customer. Car sharing to some extent may also be referred to as ride sharing, in which several customers of varying sources and destinations get on board and share a portion of a ride in a single vehicle.

Customers' requests are input into the service, and out of these inputs, carsharing schedules are generated with a plan that caters for pick-up and drop-off locations, itineraries and times for each passenger, and so on.

IoT-enabled cars will be able to determine how much it will cost to pick up a particular customer based on time, adjustments to the current schedule in use, the best car-to-customer match, knowledge exchange between cars and journeys. This is in addition to the current car-sharing solutions deployed.

Car sharing is part of a growing movement to rethink the transportation system of major cities through mobility-on-demand. The fact that most vehicles around urban centres are underutilized is well known. With a standard urban driven car would be limited to speed of 20-30 km/h and would be spend 90% of its time parked. [24.]

5.2.4 Highway Pilot

Autonomous driving is expected to dramatically reshape global transportation networks by reduced congestion, minimal collisions, and reduced fuel consumption, as well as improvement in driving conditions, especially on the highways. Furthermore, autonomous driving in highway environments is projected to cut costs by up to 40 percent in the line-haul trucking industry.

The highway pilot feature automates driving by allowing the automatic driving system to manage steering and speed changes along the highways. The Highway Pilot, as its name suggests, is only intended for use on highways. This function's added benefit is its ability to raise driver and automated vehicle perception of possible road hazards along the route and help them adjust their driving accordingly. [11.]

According to the autopilot project, any autonomously driving vehicle would be intelligent enough to work and drive autonomously even though it is not connected to external sensors and sources. When an autonomously driven car uses communication network tools and data from sensors and sources externally, it can make improved and accurate decisions on what to do.

5.2.5 Platooning

Platooning is a scenario in which a vehicle follows another vehicle at a near distance automatically. To anticipate manoeuvres when driving in a platoon, vehicles must use intervehicle communications to and from other platoon vehicles. There are many goals and reasons for vehicular platooning, including increased traffic throughput and consistency and increased traffic safety caused by speed differences. Furthermore, in case of accidents it is possible to enhancing traffic safety for vehicle driver and passenger, experience low impact velocities, and reduced fuel consumption and pollution due to reduced air drag. Non-automated driving systems can already accomplish some of these goals to some degree. A human driver monitors the environment despite the high level of automation contribution, and to some extent the driver may execute the steering function. Automated driving, in which the device performs all of the driving aspects including the complex driving task, can provide comfort by relieving the drivers off the driving task. [25.]

5.2.6 Urban Driving

Commercial solutions that collect data from vehicles typically use cellular networks, but research in this area is focusing on Cooperative Intelligent Transportation Systems solutions that include On-Board Units and more advanced networking solutions, for instance “complex schemes incorporating IEEE 802.11p and various LTE cellular technologies”. The car, on the other hand, may be called a moving sensor composed of a number of sensors, bringing the IoT model into action. In this regard, the Low-Power Large Area Networks (LP-WAN) segment of IoT networking technologies could be considered for these vehicular scenarios. [26.]

Long-range access to on-board sensor data would be possible with LP-WAN technologies although the battery usage of sensors mounted in non-standard vehicles, such as bicycles or motorcycles, would be kept low. SigFox and LoRa can be supplemented with 5G-ready technologies like NB-IoT and mMTC. Narrowband-IoT Massive (NB-IoT) is the first step in the 3GPP requirements to shelter the LP-WAN segment while Massive Machine-Type Communications (mMTC) will be a key component in the IoT cellular support of the 5G field. Vehicle tracking using the IoT cellular technology particularly is useful in urban mobility scenarios, in acceleration towards adopting healthy transport practices, where cars, bikes, and any other mobile users is tracked to adjust traffic lights and prescribe data for safe riding. [26.]

5.3 Smart City

The basic thought of the smart cities aims to their future development towards IoT increase the standard of lifetime of its citizens through good technologies. The purpose of smart city is to provide efficient, standard and secure communication of emergency to citizens and vicinity, emergency bodies, governmental bodies and civil protection organization [27].

The enormous numbers of urbanization and burden of social services will produce a mayhem. The strain on the prevailing system will crumble the infrastructure. Because of that good, new and innovative solutions are required. In a smart city, there will be several tiny protocols that may gather data, then send it to a central information unit. [27.]

5.3.1 Public Warning System in Critical Infrastructures

The main objective is to provide reliable, normal, and safe emergency communication to a wide range of critical infrastructure stakeholders. Safe communication protocols with essential infrastructure such as 5G are needed to create an efficient emergency communication system.

5.3.2 In U-Space, UAS (Unmanned Aerial System) Operations

With a unique ecosystem of electronics, drones have emerged as one of the fastest growing trends in telecommuting markets. In 2014, the global commercial drone market was valued at USD 552 million, with a Compound Annual Growth Rate (CAGR) of 16.9% projected by 2022. One of the major barriers to the production of many commercial drone applications is safety issues. In the United States, for example, drone-provided logistics are also prohibited. The main factors are safety and the lack of a mature management scheme for the airspace. Alternatives, such as redundancies from other segments such as IoT protection and automotive, must be identified and enforced. A standardized communication system is needed for a real-time airspace management system that offers reliable and harmonized communication of drones, the surrounding environment, and the airspace controller. [28.]

Accidents are the primary target of Computer-to-all (D2X) contact. Drones must broadcast their UAV-ID, location, pace, heading, and surroundings, among other things. Information sharing amongst drones and the communication infrastructure through the established wireless communication has reduced

collision risks due to ease of detection and avoidance. The development of a drone communication protocol paves the way for the implementation of real-time management of the airspace and deployment of collision avoidance systems, expanding the possibilities and demand for the application of drones. [27.]

Example use case:

- Preparation of a drone mission: The drone operator uses U-Space services to get traffic and environment insights and prepare adequately for the mission.
- Submitting a flight request and awaiting reception of an acknowledgement: the flight request is send to the authorities for the regulatory guidance, on whether to approve it or recommend mission changes. While in the air, the drone collects data on local airspace conditions and broadcasts its own unique ID for monitoring purposes.
- Executing the flight: armed with a detect-and-avoid system, a flying drone can easily avoid unintended obstacles along its flight direction. Geo-fencing allows for adaptive airspace restrictions (for example, after incidents that result in temporary non-flying areas).
- Destination landing: the mission is complete on this step, and the drone is ready to move on to the next mission.

5.4 Smart Energy

Future energy grids: technological advancements, which are often supplied by prosumers at the network's edge, are remodelling the energy network from a closed, monolithic and extremely predictable infrastructure to an open, multi-ownership system [29]. The internet of things (IoT) and 5G technologies will provide the technological capabilities needed to support the vision of the smart energy grid.

The stakes are high: meeting rising demand, enhancing power supply reliability and quality, increasing energy efficiency, and incorporating highly distributed and low-carbon emitting energy sources.

Observation and monitoring of smart energy grid are already in operation in the high and medium voltage divisions of the energy networks. The low voltage divisions are much less technologically advanced.

Homes and structures that can generate and consume energy are referred to as prosumers. Cyber monitoring and aerial surveillance of physical manning are the supervisory control applications of the smart grid. Fault localization, isolation, and energy re-routing are other examples of smart grid applications. Advanced metering applications that enable end-user infrastructure to be integrated into the grid in a large-scale, lock-in-free manner. In areas like smart EV charging, where dispatchable demand response can be used to maximize resource usage and reduce the risk of power becoming unavailable when needed, a combination of the above can be used. [29.]

5.5 Smart Agriculture

Farmers are looking for IoT-based automation technologies and solutions to help them increase operational performance, optimize yield, and reduce waste by collecting real-time field data, analysing it, and deploying control mechanisms. Smart agriculture solutions are aimed at improving productivity and food security [29]. Smart agriculture can be used in a number of ways:

- Acquiring real-time data on crop, soil, and air conditions is required for precise farming.
- Smart irrigation calculates the precise water requirements by measuring different parameters. It has been demonstrated that such a mechanism can help increase irrigation production.
- Farmers can grow crops with minimal human interference in a smart greenhouse. Within a greenhouse, climatic conditions are constantly controlled. Automated behavior would be triggered by changes in these conditions.
- These activities will then review the improvements and take corrective steps to ensure that the best growth conditions are maintained.
- Smart livestock farming utilizes real-time monitoring of livestock production, health and well-being to ensure optimum growth and production.

6 IoT Connectivity over Cellular Networks

The increasing demand for IoT connectivity has prompted various telecommunications industries to research evolutionary and innovative radio access technologies for IoT communications. The 3GPP LTE has launched several research projects to enable large-scale IoT communications over existing cellular infrastructure in order to comply with the in the IoT world. In release 12, the implementation of LTE standardization for massive IoT communications began, and in in release 13, it has continued. LTE category M (LTE-M) and narrow-band IoT (NB-IoT) systems were introduced in release 13 of LTE. [30.]

6.1 Serving IoT Traffic-over Shared Systems

In this section, the LTE-A air interface is introduced and its limitations are examined in terms of supporting large amounts of IoT traffic while conserving electricity. It is worth noting that this aspect of the air interface would stay the same with new launches, so this research is critical for 5G standardization. IoT devices cross the physical random-access channel (PRACH) and send their uplink scheduling requests to the BS over the physical uplink control channel using the LTE-A air interface (PUCCH). The scheduling is then carried out by BS, which then sends scheduling grants to users via the physical downlink control channel (PDCCH). [31.] The above-described connection procedure works well for legacy human-oriented communications traffic. This is because human-oriented communications, such as voice and web streaming, are made up of a small number of long-lived communications sessions [30]. However, the performance of this networking technique is called into question by the addition of IoT communications to cellular networks as shown in Figure 3 below [31].

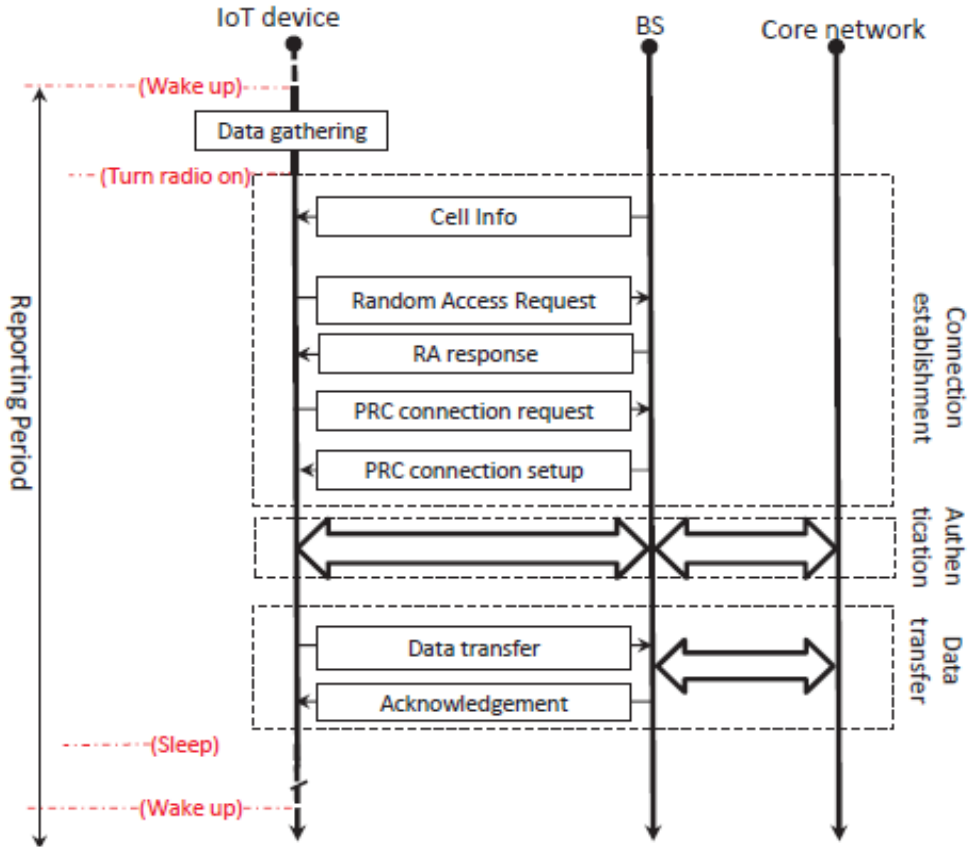

Figure 3. LTE access protocol exchange. Copied from [31].

6.2 Scalability and Energy Efficiency of the Connection Establishment Method

In response to RQ1.1, is necessary to look into the efficiency of LTE systems' random-access channels. In addition, scalability is investigated by determining the access rate of IoT devices, which is defined as the rate of link establishment success after K trials. First, battery life will be discussed. The energy usage of devices could be seen as a regenerative mechanism in most reporting IoT systems, with the regeneration point being at the end of each successful data set. The average reporting period (TRep) and the ratio between the remaining energy and the average energy consumption in each reporting period can then be used to calculate the estimated battery lifespan. E0, ESleep, NConEst, EConEst, ESched, EDataTx, and EOthSig are the stored energy, average energy consumption in the sleep mode in one reporting cycle, average number

of trials for a good connection establishment, average energy consumption in a connection establishment study, average energy consumption in receiving data transmission grant, and average energy consumption in receiving data transmission grant, respectively [32].

6.3 Enhancing the Contention Resolution Capability

Although collisions were viewed over each random-access resource as a loss for all devices involved in the collision in the previous section, one might consider improving the contention resolution capability of receivers. One possible solution is to determine the collision dimension, or the number of nodes involved in the collision, and then react to the contending nodes with a batch of resources. Then, to reduce the likelihood of collision in subsequent transmissions, each node will choose a subset of these resources at random. The accuracy of collision dimension calculation determines how well such a scheme performs. Furthermore, it was suggested that using the CFOs of involving devices to estimate collision dimension is needed. The received signal content is tested using a periodogram in this scheme to find any residual CFOs in the signal content. [33.]

6.4 IoT Traffic Scheduling

connection establishment procedure was looked at in the previous section. In turn, RQ1.2, which is the resource scheduling procedure, will be looked at in this section. Scheduling, on the one hand, is not part of the standardization process and it is handled differently by each vendor. Signalling for scheduling, on the other hand, is part of the standardization process, and each scheduling scheme adheres to the signalling requirements outlined in the standards. Prioritizing data transmission requests based on the KPI’s of interest, as well as allocating a collection of frequency radio resources to each system in order to ensure its efficient communications are all part of resource scheduling. In the literature, delay budget is the most commonly used KPI for prioritizing traffic, and IoT traffic is normally prioritized over non-IoT traffic for the remaining

capital. Given that every joule counts when it comes to the battery lifetime of IoT devices, and resource scheduling plays a critical role in system energy consumption, it is important to examine battery lifetime aware scheduling solutions and assess their effects on device energy consumption. [34.]

7 Challenges Relating to the Deployment of the IoT

In this section, six key IoT issue areas are examined to explore a number of the foremost pressing challenges and queries associated with the IoT technology.

7.1 Digital Security and Privacy Risks

The growth of the Internet of Things, as well as the realization of the economic and social benefits associated with its usage, will be driven in part by future users' confidence in the technology and the goods and services that rely on it. This means that users will have to accept the fact that connecting every physical device to the Internet exposes them to some level of cyber security risk, a risk that they will have to accept. The digital security issues faced by the Internet of Things are virtually the same as those posed by industrial automated control systems: digital accidents involving IoT can have serious physical effects in addition to impacting other aspects of an organization's finances and reputation. An effective framework, OECD's 2015 Recommendation on Digital Security for Economic and Social Prosperity offers digital security risk management. However, managing this digital security risk is exponentially growing as the Internet of Things links a much larger number of devices in both industrial and consumer contexts. [35.]

The IoT's privacy concerns are similar to those posed by other emerging technologies that produce and collect data, such as cloud computing and radio-frequency identification. The OECD Privacy Guidelines offer a structure for dealing with these issues, which is particularly important as IoT devices become more popular and users lose insight into how and what data is collected. Leaders and policy makers should regard digital security as an economic and

social risk rather than a technological problem, according to the OECD guideline on digital security risk management. [35.] They should understand the potential economic and social implications of a possible digital security incident while carrying out an operation that relies on digital technology, such as the IoT.

7.2 Inference and the Loss of Control

Users should be able to maintain hold of their data and opt out of the smart environment without facing negative consequences, according to privacy standards. Individuals can protect their privacy through a variety of methods. The most obvious way, intuitively, is to withhold or hide knowledge about them.

Geolocation data from mobile devices, for example, can be used to enhance the location-based services that many people rely on today, but it often leaves a trace of an individual's everyday routines and movements, which is increasingly being used for other services, such as process improvements. Tracking helps companies to change their processes by allowing them a clearer way to know their clients, and it can be used in a variety of ways to extend consumer behaviour analysis. The value comes from the data concerning about the person, their behaviours, their movements, and their preferences. [35.]

Data analytics removes information from data by exposing the context in which it is stored, such as patterns, associations between evidence, interactions between persons, and relationships between concepts [36]. As a result, data analytics allows for the discovery of new data. Data analytics is not a brand-new concept. However, as the number and variety of available data sets grows, as does the ability to connect them together, so is the ability to link them together, as well as the ability to extract additional information from them, such as for profiling purposes. Advances in analytics now enable sensitive information to be inferred from data that might seem innocuous at first, such as past purchases. The Internet of Things is expected to intensify this trend, resulting in a vast number of disparate but interconnected data sets that are related to economic and social activities directly or indirectly [35].

7.3 Transparency and Purpose of Data Collection

Since their initial introduction in 1980, the OECD Privacy Guidelines have promoted openness and rights to access and correction, having been adopted to varying degrees by many national laws globally. Both transparency and access have long been recognized as important resources for influencing data subjects to structuring informed decisions and establishing the basis for decisions made about them, minimizing the likelihood of discrimination. In certain cases, the Council of Europe advises that accountability standards involve the rationale that underpins the production [37]. However, IoT devices are often programmed to function contextually as part of environments deployed into, so users are unaware of their existence. As a result, it can be difficult for individuals to understand what information about them is being gathered, used, and released by such devices. Passive in-store monitoring and profiling, for example, raises concerns about how consumers enlighten on the aims of the collection of their personal data, how open all stakeholders' information management activities are, how process of informing individuals about such practices, and how through which these messages are communicated to them in order for them to understand. [35.]

7.4 Promotion Responsibility and Raising Awareness

These factors necessitate adopting a user-centric approach that allows users to have an active role around data and decisions. This necessitates education and knowledge, which are explicitly defined as complementary steps in the revised OECD Privacy Guidelines. Organizational initiatives to promote responsible consumption should be supplemented by efforts to increase accountability and customer empowerment. Policymakers and regulatory agencies will be expected to assist organizations in assessing acceptable substantive limits.

According to the White House big data study, placing more focus on a responsible usage system has several potential benefits. Instead of simply restricting who obligation to whether they have correctly received approval at

the time of collection, focusing on fair use keeps data collectors and consumers accountable for how they handle the data and any harm it creates.

7.5 Accountability and Privacy Risk Management

The privacy guidelines have a new key clause called accountability. To be kept accountable, an organization must be able to disclose what it is intended to do with personal data, as well as justify why.

Data sources and consistency, as well as the sensitivity of the intended uses, may all be included in a risk assessment. To be accurate, a privacy risk assessment's scope must be comprehensive enough to account for a wide variety of harms and benefits while still being clear enough to be used on a regular basis.

Due to the various stakeholders in the IoT climate, risk evaluation can be difficult. Some of these key stakeholders, such as device makers, social platforms can collect, use, or reveal data, and they may play a greater or lesser role in its security at different times. Determining where the line between them should be drawn can be difficult at the best of times. As a result, it is important to find out who is actually responsible for the data that the smart meter broadcasts, for example. Is it the homeowner profiting from using the unit, the device's suppliers, the power provider, a third-party company storing the data, a data processor crunching the numbers, or a mixture of all of the above?

Other important questions to ask are the following:

- Who can a privacy-conscious shopper complain to?
- Where does one party's liability end and another's begin if privacy is violated?

As a consequence, the degree to which a holistic risk management strategy will improve the implementation of the OECD Privacy Guidelines' principles is a focus for future study, which may include aspects that are relevant to the Internet of Things.

7.6 Interoperability of Technologies and Policy Frameworks

Several IoT projects and devices will exist as a result of the vast diversity of IoT application. The vast heterogeneity in their priorities and specifications, and interoperability will be critical. Although the current proliferation of goods and services may be perceived by some as a sign of a rising IoT market, a fragmented environment of non-interoperable technologies may jeopardize efficiencies. The IoT ecosystem can use hardware and software from a variety of vendors, and the ability to integrate features from a variety of devices and vendors is crucial to realizing the full potential of IoT techniques. Relying on international standards established by standards development organizations and industry conglomerates is an efficient way to solve this issue.

Radio technology, RFID, and mobility must all be considered in functional interoperability. The differences between various methods and procedures must be bridged. It is also important to consider and emphasize the positions and obligations of various actors. The customer experience in IoT connected utilities, for example, would almost certainly come under the control of the private sector. The position of governments may be more prominent to ensure consumer protection and safety. Governments could promote more dialogue through regulatory agencies and with sectors that are not typically interested in communications, such as transportation and energy services, to facilitate policy interoperability.

8 Conclusion

Both IoT and 5G are modern technologies, yet the concepts are not new. This thesis has explained the communication and security concepts linked to both technologies.

Looking at today's cutting-edge technology, it is possible to see how the Internet of Things can be applied on a global scale in the coming years. The key issues that need to be researched and developed further can also be seen in order to make large-scale IoT implementation a possibility.

It has been noted that substantial work in the field of IoT governance is urgently needed. Without a systematic solution, a plethora of architectures, authentication systems, protocols, and frequencies are likely to occur in parallel, each tailored to a specific application.

This would eventually result in the division of the IoT, which could stifle its adoption and become a significant roadblock to its introduction. Interoperability is a requirement, and inter-tag connectivity is a prerequisite for widespread acceptance of IoT.

The technology needed to achieve the universal network society is expected to mature in the coming years. When RFID implementations achieve popularity, a significant number of items would be addressable and connected to IP-based networks, becoming the first wave of the Internet of Things. In order to ensure smooth network connectivity, there will be two main challenges: the first is the fact that multiple networks coexist today, and the second is the sheer scale of the IoT.

The current IT industry has little experience building an infrastructure that connects hundreds of millions of artifacts to IP networks. Other existing problems, such as address limitation, automated address configuration, protection features such as authentication and encryption, and multicast

functions to effectively deliver voice and video signals, will most likely be resolved as technology advances.

IoT production would be reliant on technical advancements in large scaling and energy-efficient applications, as well as in obtaining data from heterogeneous sources, lowering prices, and increasing efficiencies.

The use of 5G in the IoT industry poses huge life transforming opportunities in the fields of health care, transport, and homes.

In conclusion, this thesis was done by studying the internet of things, the fifth-generation internet and the security aspects linked to the research and development of these two. The study will increase the understanding of upcoming thesis writers about IoT and 5G. In the future the IoT and a 5G-enablednetwork will have a crucial role. The research has been completed by reading a number of different sources, such as books, online material, journals, publications, and previous theses, have published about IoT and 5G. The thesis presents the IoT, 5G and the security aspects, their evolution history, future prospects and potential market shares. In conclusion, the thesis shows what IoT and 5G are, how they will change the near future, what should be invested in the future, and what challenges new frontiers are facing in the world of modern technology.

References

1 Heuveldop, N. June 2017. "Ericsson Mobility Report 2017". Stockholm: Ericsson.

2 Columbus, L. December 10th, 2017. "2017 Roundup of Internet of Things Forecasts". Forbes. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#753408e21480. [Accessed February 24th, 2021].

3 Innovations, Z. S. December 18th, 2015. "Generations in Telecommunication (1G, 2G, 3G, 4G)". [Online]. Available: http://www.zseries.in/telecom%20lab/telecom%20generations/. [Accessed February 24th, 2021].

4 Mashal, I. Alsaryrah, O. Chung, T.-Y. Yang, C.-Z. Kuo, W.-H. and Agrawal, D. January 28th, 2015. "Choices for interaction with things on Internet and underlying issues". Ad Hoc Networks, 68–90.

5 Desai, R. July 19th, 2016. "Internet of Things (IoT), an Educational Blog". https://drrajivdesaimd.com/2016/07/19/internet-of-things-iot/.

6 Saqlain, J. March 3th ,2018. "IoT and 5G History Evolution and its Architecture their Compatibility and Future". Semantic Scholar. https://www.semanticscholar.org/paper/IoT-and-5G-%3A-History-evolution-and-its-architecture-Saqlain/f2c5b604ceaca4d87810feeda5ebe950531c581e#references.

7 Tun, S.Y.Y. Madanian, S. and Mirza, F. April 10th, 2020. "Internet of things (IoT) applications for elderly care: a reflective review". Aging Clinical and Experimental Research (2020). SpringerLink. https://doi.org/10.1007/s40520-020-01545-9.

8 Peisi, C. Zishuo, N. March 5th, 2020. "The Seven Major Features of 5G". Alibaba. https://www.alibabacloud.com/blog/the-seven-major-features-of-5g_595947.

9 Nordrum, A. Clark, K. and IEEE Spectrum. January 27th ,2017. "Everything You Need to Know About 5G". [Online]. Available: https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g. [Accessed February 24th, 2021].

10 Alaba, F.A. Othman, M. Hashem, I.A.T. Alotaibi, F. June 2017. "Internet of Things Security: A Survey". Journal of Network and Computer Applications, 88, 10–28.

11 Maple, C. August 24th, 2017. “Security and Privacy in the Internet of Things”. Journal of Cyber Policy, 155-184. https://doi.org/10.1080/23738871.2017.1366536.

12 Khan, M.A. Salah, K. November 27th, 2017. “IoT Security: Review, Blockchain Solutions, and Open Challenges”. Future Generation Computer Systems 2018, 82, 395–411. [Online]. Available.

13 Zaldivar, D. Tawalbeh, L. Muheidat, F. June 15th, 2020. “Investigating the Security Threats on Networked Medical Devices”. Las Vegas, NV. Proceedings of the 2020 10th Annual Computing and CommunicationWorkshop and Conference (CCWC), 0488–0493.

14 Tawalbeh, L.A. Somani, T.F. November 29th ,2016. “More secure Internet of Things using robust encryption algorithms against side-channel attacks”. Agadir. Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA 2016), 1–6.

15 Koutroumpi, P. December 10th, 2018. “Study on Socio-Economic Benefits of 5G Services Provided in mmWave Bands”. GSMA. https://www.gsma.com/spectrum/wp-content/uploads/2019/10/mmWave-5G-benefits.pdf. [Accessed March 15th, 2021].

16 Koutroumpi, P. July 29th, 2020. “An introduction to 5g network slicing. GSMA. https://www.gsma.com/futurenetworks/5g/introduction-to-5g-network-slicing/. [Accessed March 10th, 2021].

17 L. HUAWEI TECHNOLOGIES CO. 2016. "5G Network Architecture A high level perspective". Shenzhen. HUAWEI TECHNOLOGIES CO., LTD.

18 Peisa, J. Persson, P. Parkvall, S. Dahlman, E. March 9th,2020. "The 5G Evolution: 3GPP Releases 16-17 overview", Ericsson. https://www.ericsson.com/49bdd9/assets/local/reports-papers/ericsson-technology-review/docs/2020/5g-nr-evolution.pdf.

19 Pantelis, K. February 12th, 2019. “NB-IoT Commercialisation Case Study” GSMA. https://www.gsma.com/iot/wp-content/uploads/2019/08/201902_GSMA_NB-IoT_Commercialisation_CaseStudy.pdf. [Accessed March 10th, 2021].

20 Evans, D. April 11th, 2011. “The Internet of Things: How the Next Evolution of the Internet is Changing Everything”. Cisco. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

21 Noy, K. Givoni, M. February 6th, 2018. “Is ‘Smart Mobility’ Sustainable? Examining the Views and Beliefs of Transport’s Technological Entrepreneurs”. Ramat Aviv. MDPI, 10, 422.

22 Barrachina-Munoz, S. Bellalta, B. Adame, T. and Bel, A. January 3th, 2018. “Multi-hop communication in the uplink for LP-WANs”. Computer Networks, 123,153- 168.

23 Mathews, E. Schmeitz, A. and Jansen, S. September 20th, 2019. "AUTOmated Driving Progressed by Internet of Things D.1.2". https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5c7a15c88&appId=PPGMS.

24 Karagiannis, G. Klein, T. June 7th, 2018. "IoT Relation and Impact on 5G", AIOTI. https://aioti.eu/wp-content/uploads/2018/06/AIOTI-IoT-relation-and-impact-on-5G_v1a-1.pdf.

25 Sanchez-Iborra, R. Sánchez-Gómez, J. Santa, J. Fernández, P. J. Skarmeta, A. F. October 2017. “Integrating LP-WAN Communications within the Vehicular Ecosystem”. Jeju Island. The 2017 International Symposium on Mobile Internet Security (Mobisec 2017).

26 Sanchez-Iborra, R. Sánchez-Gómez, J. Santa, J. Fernández, P. J. Skarmeta, A. F. February 2018. “IPv6 Communications over LoRa for Future IoV Services, 4th IEEE World Forum on Internet of Things (WF-IoT 2018)”. Singapore. MDPI. https://doi.org/10.3390/s19020264.

27 Carrillo, D. and Seki, J. October 23th, 2017. “Rural area deployment of internet of things connectivity: LTE and LoRaWAN case study”. Cusco. IEEE XXIV International Conference on Electronics, Electrical Engineering and Computing (INTERCON).

28 Kuenz, A. 2018. “City-ATM (Demonstration of a UAV Traffic Management in Urban Airspace)”. Braunschweig. DLR. http://www.dlr.de/fl/en/desktopdefault.aspx/tabid-1149/1737_read-50670/. [Accessed April 7th, 2021].

29 Bingham, R. Agelin-Chaab, M. Rosen, M. A. October 2nd, 2017. “2017 the 5th IEEE International Conference on Smart Energy Grid Engineering (SEGE)”. 187-205.

30 Nokia Networks, “LTE-M – optimizing LTE for the Internet of things,” Tech. Rep., 2015.

31 Hossain, M. I. Azari, A. Markendahl, J. and Zander, J. May 21st, 2017. “Enhanced Random Access: Initial access load balance in highly dense LTE-A networks for multi- service (H2H-MTC) traffic”. IEEE International Conference on Communications.

32 Cox, C. March 2012. “An introduction to LTE: LTE, LTE-advanced, SAE and 4G Mobile Communications”. John Wiley & Sons.

33 Uckelmann, D. Harrison, D. Michahelles, F. 2011. "Architecting the Internet of Things". Springer, 1-15. http://www.springer.com/gp/book/9783642191565.

34 EU. 2017. "5G PPP Architecture Working Group View on 5G Architecture (Version 2.0)". Europe. European Commission.

35 OECD. May 24th, 2016. “Working Party on Communication Infrastructures and Services Policy”. [online] Available: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En. [Accessed March 22th, 2021].

36 Merelli, E. Rasetti, M. June 1st, 2013. “Non-locality, Topology, Formal Languages: New Global Tools to Handle Large Data Sets”. Procedia Computer Science, 90–99.

37 Council of Europe. November 1st, 2011. “Recommendation on the Protection of Individuals with Regard to the Automatic Processing of Personal Data in the Context of Profiling”.