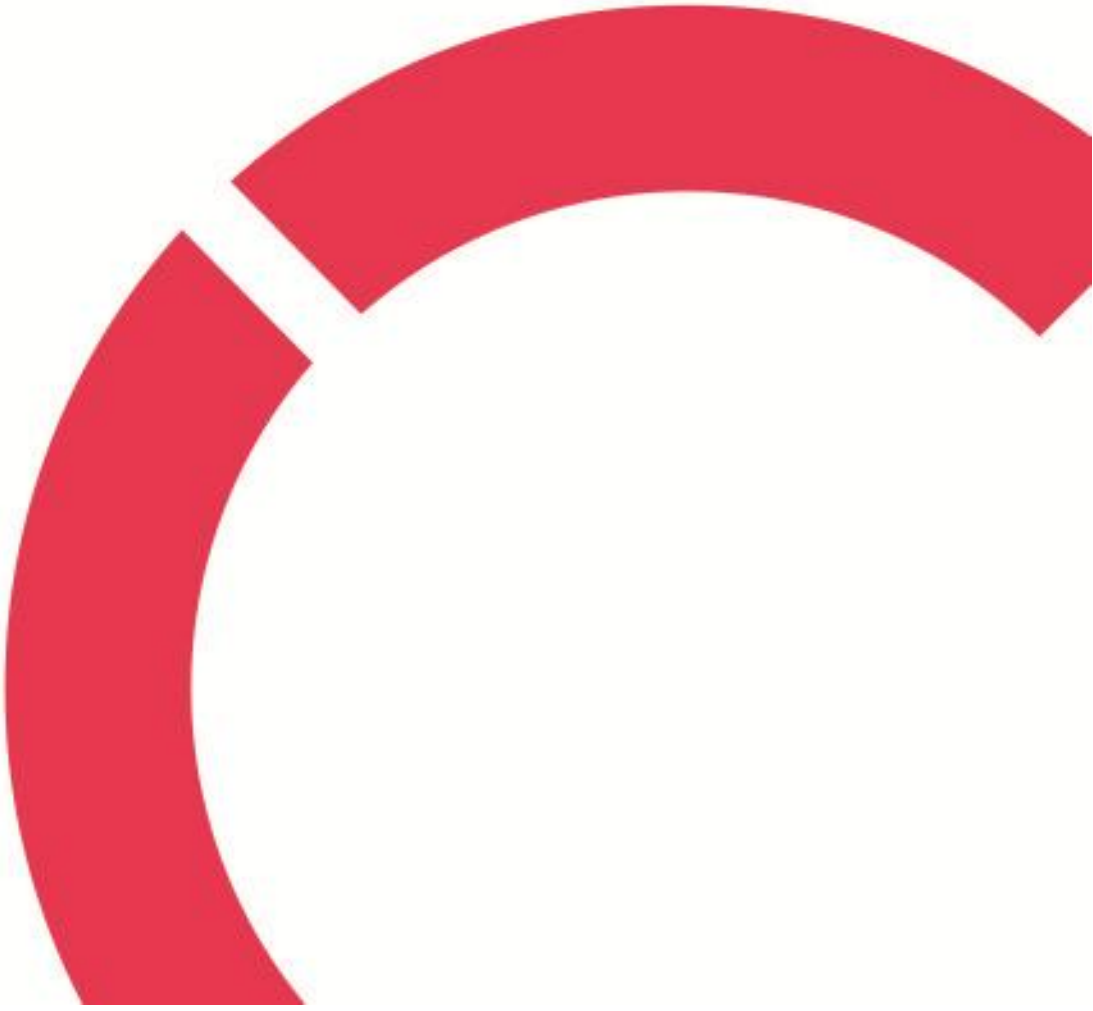
Sadikshya Satyal

ENHANCING IOT SECURITY IN THE 5G ERA: THREATS, VULNERABILITIES, AND SOLUTIONS

Thesis
CENTRIA UNIVERSITY OF APPLIED SCIENCES
Bachelor of Engineering, Information Technology
December 2023



ABSTRACT

Centria University of Applied Sciences	Date December 2023	Author Sadikshya Satyal
Degree programme Bachelor of Engineering, Information Technology		
Name of thesis ENHANCING IoT SECURITY IN THE 5G ERA: THREATS, VULNERABILITIES, AND SOLUTIONS		
Centria supervisor Henry Pannanen and Jari Isohanni		**Pages** 25 + 3
Instructor representing commissioning institution or company. -		

ABSTRACT

This in-depth research examines the changing convergence of IoT and 5G with a particular emphasis on security. This literature review travels through the already available information and prepares the way for an extensive examination of threats and vulnerabilities unique to the era of the 5G. Further, the finding of the research uncovers cybersecurity issues in the wider spectrum of Internet of Things (IoT) setting, while shedding light on novel challenges surfacing within the context of 5G (Fifth Generation) based IoT ecosystem. The research discusses the vulnerabilities of IoT devices as well as how the proliferation of 5G networks enhance them. This paper outlines practical security suggestions that stress the importance of cryptography, data authenticity tools, and hardy communication protocols that can strengthen nodes in the IoT 5G network confronted with such challenges. It develops more insightful case studies which illustrate what their proposals would work on i.e., how effective these solutions would be. The analysis concludes by advocating for a dynamic security model to maintain a healthy harmony among IoT and 5G amidst changing technologies.

Key words

5G networks, authentication mechanisms, case studies, challenges, cybersecurity threats, encryption, future directions, IoT security, secure communication protocols, vulnerabilities

CONTENTS

1 INTRODUCTION

IoT (Internet of Things) refers to the fast growing “things” that can communicate with each other by sharing data. IoT device is a smart device that is the combination of sensors and actuators. It is a type of device that requires network to function and to share data globally through IoT Protocols. These smart devices use their sensors and actuators to gather information and respond to the users based on the data. IoT devices range from sensors and lights to alarms and cameras. It plays an important role in monitoring the things like earthquakes, landslides and even floods. The field of IoT has been on research and development for more than twenty years. It has gained more momentum in the past decade which has resulted in a wealth of valuable studies. (S. Chahar and K. Kaur 2023) The expansion of IoT depends heavily on the development of 5G (Fifth generation).

The mobile communications have moved gradually from 1G to 5G. The first generation (1G) started from 1980 when the telecommunications revolution began. This early network had basic interpreter as the programming language of the microcomputers it had introduced. In 1991 there was a move from first generation to second generation (2G). This network had the advent of systems such as CDMA and GSM with the maximum speed of 1 Mbps. By stepping up, the third generation (3G) revolutionized communication with high-speed broadband technologies. After the 3G, in 2010 the fourth generation (4G) was introduced with improvements to 3G. 4G was improved in the information speed which ranged between 20 and 60 Mbps. After 4G, the present high pinnacle, the 5G, introduces its cornerstone of digital transformation known as MmTC (Massive Machine Type communication) which has important implications for IoT based application. It involves supporting inter-vehicle communication, enhancing Industry 4.0, developing advanced grids, intelligent infrastructure for transport, and even distant surgery with ultralow latency, ultrareliable communications (S. Chahar et al., 2023)

The Fifth Generation (5G) is being widely used in 21st century for its fast and efficient features. Since its establishment from 2019, it has been growing and expanding its horizon. With the integration of 5G with IoT devices are evolving its technology worldwide. As the network has been thinly lined by 5G, it has helped the IoT to upgrade and function effectively and efficiently. The IoT devices that are supported by the 5G networks are increasing in demand due to the fast data transfer rates, full and better coverage, and high efficiency. These features of the 5G will support and empower the IoT devices. For example, the drones, robots and even business solutions. The 5G is therefore being upgraded and increasingly in demand for the establishment of the unconnected and unmatched thing to be connected for everyone and

by everything. (Singh. G., Singh, J., Mitra, D., & Prabha, C. 2023) The wireless technology of 5G for IoT is expected to utilize the spectrum band. According to Singh J., Singh, G., Muskan, & Aggarwal, G 2022, for the efficient use of the spectrum band, it has to practically reach full utilization through the low-power wide-area networks (LPWANs) which is possible highly through 5G network.

IoT technology requires the massive and vital network along with effective communication infrastructure. For today's IoT era, the scientist and researchers are doing some profound research on platforms like 5G NR, MIMO (multiple-input/multiple output) and mm-wave (multimeter - wave) technology for broadening the IoT. But in comparison to the current technologies, 5G is the fastest and provides with the reliable connectivity. (Singh G. et al 2023) This thesis explores the relationship between 5G and the IoT with focus on how 5G will empower the IoT devices. The research seeks to uncover the threats, vulnerabilities, and solutions to the IoT devices/ environment in the era of 5G.

2 LITERATURE REVIEW

As IoT and 5G are the most trending technology in the current time, there has been continuous research on these topics individually as well as the combination of both technologies together. The combination of IoT and 5G presents a transformation in possibilities but along with the possibilities there exists security challenges as the researchers like N. Gupta, S. Sharma, P. K. Juneja and U. Garg 2020, have highlighted. With the high-speed 5G connectivity and numerous of IoT devices, there are potential attraction for cyber threats. There has been issue in this field in the concept of network slicing in 5G. The dynamic network slicing allows the network to be virtually divided into different parts based on specific needs and its flexibility on the everchanging environment. But the same dynamic nature has introduced complexities for consistent security measures for the evolving network configuration. Additionally, the total connected devices in the 5G enabled IoT environment consists of an alarming challenge for managing the security of a large number of diverse devices. For ensuring the safety of this expansive ecosystem requires a strong security protocols and continuous efforts.

To tackle and overcome these challenges posed by 5G- integrated IoT, researchers like D. Wu, M. Sun, P. Zhang, Y. Tu, Z. Yang and R. Wang 2023 have suggested to use strong security measures. They have highlighted about encryption and secure communication/ connection protocols as crucial tools. The studies explore advanced encryption methods to see how well they can protect the information. The main goal of this research is to prevent cyber attackers from eavesdropping unauthorized access to the data transmitted between IoT devices and through the 5G networks.

Until the date, the researchers have been emphasizing the importance of two key elements, which are authentication and access control. Authentication is like a digital ID checking, that makes sure that only authorized users or devices can access the information. Similarly, access control is the setting of rules for deciding who can do the manipulation of data with the given or shown data. R. M. Haris and S. Al-Maadeed (2020) has proposed using the technologies like Blockchain and Artificial Intelligence (AI) for real-time detection and response to the emerging cyber threats. The research conducted by R. M. Haris et al (2020) highlights the need for strong security plans that cover a range of issues from keeping the data safe with encryption. It can be kept safe and secret by using the smart technologies like blockchain and AI to protect against new and evolving threats in the world of 5G connected IoT devices. The experts are increasingly aware of the complex challenges that arises from the combination of IoT and 5G technology.

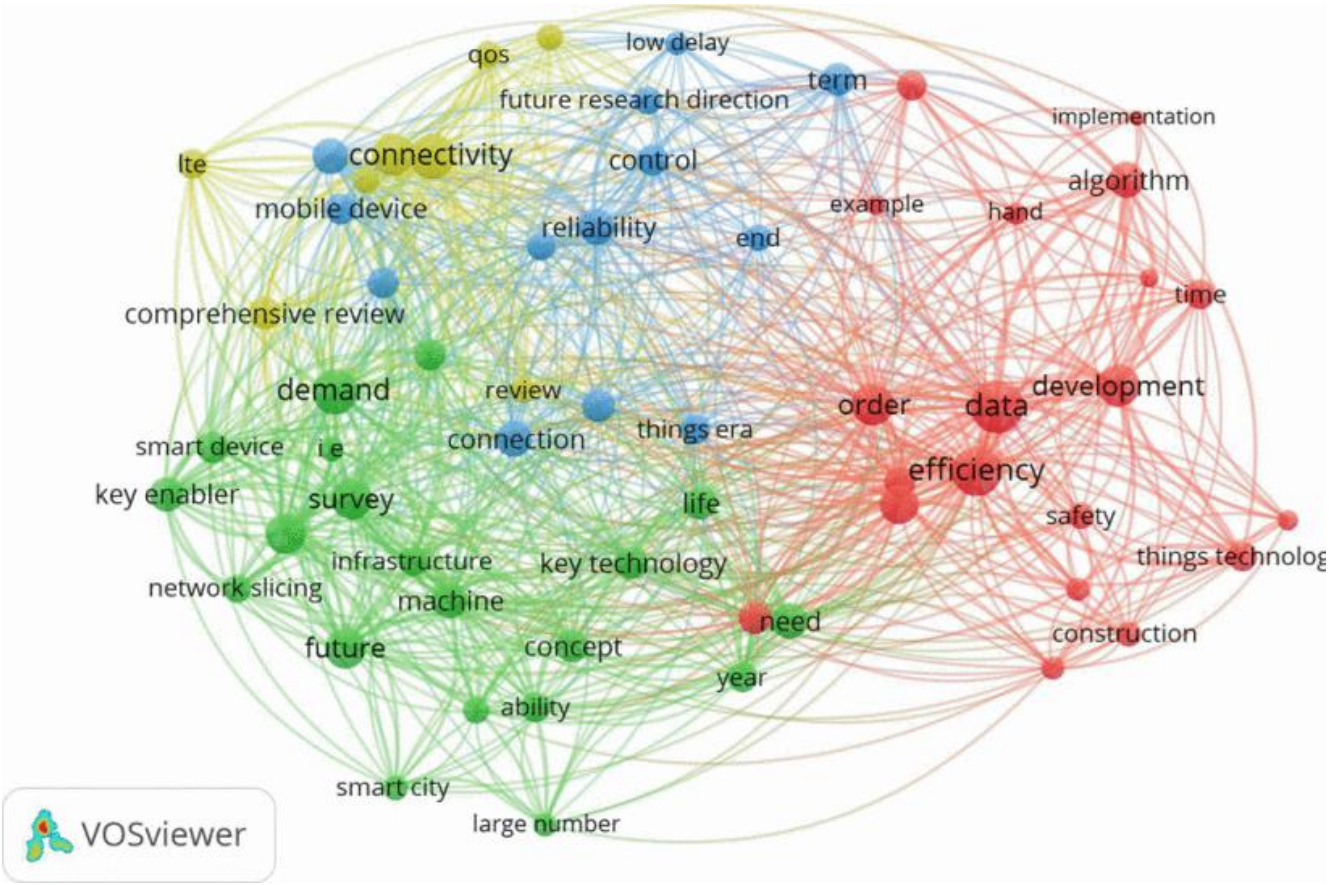


FIGURE 1. Strategic map of IoT landscape keywords (Singh. G et al., 2023)

According to the research done by Singh. G et al., 2023, the research key word “Internet of Things” has the highest frequency in web of science database. By the means of co-occurrences network, Singh. G et al (2023) had outlined significant components used on IoT. This technique was employed by conducting searches based on the number of times some of the key words were combined. It resembles a procedure of creating a strategic map for highlighting clusters of keywords throughout an IoT land space. FIGURE 1 shows the strategic map of the IoT landscape keywords. The result of this examination allows the researchers to know about the complicated combination between the specific terms. Hence, ultimately it will offer valuable insights into the complexities of the vast Internet of Things landscape.

3 THREATS TO IOT SECURITY IN THE 5G ERA

The Internet of Things (IoT) brings tremendous possibilities, but its security is a concern due to the vulnerability of numerous devices. To address this issue of security, a fusion of machine learning and cybersecurity has been applied. Most attacks in IoT occurs in intrusion patterns. (S. Dhinakaran, V. Bansal, K. Pant, S. K. Joshi, U. H. Maginmani and C. R. Prasad 2023). In other words, it means that attackers who attack the devices often modify the existing methods rather than establishing or creating an entirely new approach.

3.1 Cybersecurity Threats in IoT

The process through which the 5G global deployment is being practiced involves different actors including VMNOs, CSPs and network infrastructure providers. It marks a distinct difference from previous generations in which mobile operators enjoyed immediate access and control to system constituents. In 5G, operators lose the complete ruling on security and privacy making it harder for the operators to align the different policy concerns in this area from the other involved stakeholders who have varying interests on these areas. Within this multiplicity of challenges, however, one must look specifically at the privacy difficulties surrounding 5G networks and examine possible security measures. For adequate understanding of modern threats, it is important to take a brief look at the past threats mobile networks have encountered. The early 1980s saw some challenges on the part of 1G networks regarding security. With time as Global System for Mobile (GSM) evolved towards 2G, concerns arose regarding spamming messages with unsolicited information on broadcasts. With the introduction of 3G, it followed other communication systems that were already vulnerable and prone to attacks. In moving to 4G there was an explosion of smart devices and third-party applications which made the threats more sophisticated and complex. (NOKIA)

As 5G interweaves with IoT devices and environment, the cybersecurity field becomes increasingly complex. The expanded attack on the devices/environment of the IoT is a primary concern. People use IoT devices and networks that are safe for their information, this makes the IoT expansion, safeguarding against cybersecurity threats is crucial. The IoT devices can either be wired or be wirelessly connected. When the devices are wirelessly connected, they possess security threats like eavesdropping, falsification, and spoofing. These security threats can lower the integrity and confidentiality of the data being transmitted in the IoT networks as the IoT devices communicate and generate the data in large quantities.

The large data generated or received from IoT devices create a massive influx of data which poses security challenges. (D.K. Alferidah and N. Jhanjhi 2020)

The users of IoT devices demand high level security for their data in the network. When there are inadequate security measures, IoT networks become vulnerable to cyber threats. (D.K. Alferidah et al 2020). The Internet of Things (IoT) is turning and upgrading towards smart urban spaces, industrial applications, and intelligent healthcare which are driven by artificial intelligence responding to human gestures. The widespread adoption of 4G and 5G networks has notably amplified high-speed internet accessibility, particularly for mobile entities. Despite these features, the IoT grapples with persistent challenges, ranging from standard implementation and cryptographic protocols to problem-solving, privacy concerns, and data security. (H. Ghorbani, M. S. Mohammadzadeh and M. H. Ahmadzadegan 2020)

3.2 Specific Threats and Attacks in the 5G IoT Environment

During the coronavirus pandemic as well as the war with Ukraine, the cybersecurity challenges have greatly manifested in the dynamic digital arena. The European Parliament in response these to challenges have instituted a new EU directive that should align different cybersecurity measures in the European Union. The eight main threat elements have been identified in the Threat Landscape report 2022 of the European Union Agency for Cybersecurity (Enisa). Complexity of evolving ransomware attacks remain a top consideration. They have been made bigger than ever in this instance by crypto-jacking and IoT-focused malware. Additionally, according to European parliament, 2022, phishing has been the root cause behind of sixty percent (60%) of all breaches reported from Europe, Middle East and Africa.

These threats provide a great challenge in the context of 5G era and IoT environment. Such types of attacks include ransomware, malware and threaten the integrity of IoT devices and networks. Similarly, phishing belongs to such social engineering threats which interferes in the way people communicate by disrupting the human to IoT dialogues. These problems are compounded by the open nature of the network. In IoT environments, privacy concerns also involve numerous devices with varying hardware and software, which makes them susceptible to many types of malicious attacks like replay, man-in-the middle, spoofing or guessing passwords. Such devices send confidential sensitive data through them like name, addresses, contact numbers, date of birth, health data, and credit cards details that may expose victims to breach and alteration in sensitive data through unauthorized third parties. Considering such

possible attacks on IoT communication, it is critical to protect the integrity and security of user data. (Mohammad Wazid, A. K. Das, S. Shetty, P. Gope and J. J. P. C. Rodrigues 2020).

Ring, an Amazon-owned company, has experienced a notable IoT security breach surrounded by 5G networks. In this incident, cybercriminals exploited weak default credentials to access a live feed from a connected doorbell camera. The breach not only exposed user data but also allowed hackers to verbally harass using built-in microphones and speakers. (Consosco 2021) Similarly, IoT devices poses a significant threat, particularly in sectors like healthcare where data is transferred without encryption. An exploited IoT medical device could allow hackers to manipulate information, sending false signals that could have life-threatening consequences. The FDA has officially recognized vulnerabilities in St. Jude Medica's pacemakers and defibrillators in the year 2017. (CNN Business 2017) Abbott Laboratories, acquiring entity of St. Jude, promptly addressed the issue by developing a software path for the affected devices. Though no patients were harmed, the real-world example highlights the critical importance of strong security measures in IoT devices. Users are prompted to change default credentials, use unique login credentials, and adopt two-factor authentication to mitigate these security risks in the ever-evolving landscape of mobile devices where 5G is connected.

4 VULNERABILITIES IN IOT DEVICES AND NETWORKS

5G IoT networks are widely used in IoV (input/output virtualization), smart healthcare and smart home. Even after the wide use of IoT devices it still consists of unique challenges. The impact of 5G IoT is not just seen on technology but also on the economy and society. The combination of IoT with 5G demands wireless network structure and innovative user services. The traditional 4G (Fourth Generation) technology had the features like Long Term Evolution (LTE), high data rates, broader bandwidth, low-Latency Quality of Service (QoS) and minimal interference. In contrast to the features of 4G, the 5G's evolution include innovative technologies such as New Radio (NR), advanced Multiple Input-Multiple Output (MIMO) antennas, millimeter-wave communication, Heterogeneous Networks (HetNets), and the emergence of Low Power Wide Area Networks (LPWAN). (D. Lučić et al., 2021)

The last decade has witnessed a surge in internet-connected devices due to the rapid growth of wireless networks. These devices range from smart gadgets to health equipment, and it has become integral to daily human life. These devices have been established by the manufactures for affordable and easy-to-use IoT solutions for different economic classes thus becoming omnipresent. But unfortunately, economic considerations sometimes compromise security standards with numerous devices relying on budget-friendly hardware that are incapable of strong security protocols. Issues like neglected user updates and a lack of manufacturer-provided updates further worsens the security vulnerabilities. The diverse landscape of IoT devices becomes a fertile ground for intruders who are typically seeking unauthorized access to create botnet networks. The primary influencers of IoT vulnerability encompass encryption lapses, default passwords, custom platforms, insufficient support along with the lack of user awareness. (H. Ghorbani et al 2020) Understanding these challenges is crucial as deeper understanding of the integration of IoT and 5G, new set of vulnerabilities appears.

4.1 Vulnerabilities in IoT Devices

In today's technological era, human life is filled with smart devices that connect and interact with each other. Ensuring the security of this communication is one of the most important and challenging requirements to achieve. Unfortunately, some IoT devices face challenges in this area, often due to weak authentication methods or the use of default passwords. (D. K. Sharma et al 2020) The Internet of Things (IoT) comes with several security challenges, properly ranked in the top 10 IoT vulnerabilities by the Open Web Application Security Project (OWASP). (WIKI OWASP 2019) These vulnerabilities pose a

variety of risks which reflects the complexity of securing interconnected technologies. For example, easily guessable passwords provide a convenient entry point for attackers. By which it opens the door to common botnets and malware. Insecure network services on devices create opportunities for the intruder to compromise integrity of the information. Additionally, weaknesses in off-device interfaces, such as web, API, or cloud interfaces, can compromise the entire device.

These issues extend to the lack of a secure update mechanism. This increases the risks in unauthorized software and firmware updates, especially in critical sectors. Use of outdated components and insufficient privacy protection adds to the vulnerability landscape. Insecure transferring of data and storage of data with device management gaps are exposing the security vulnerabilities. Default settings and lack of physical hardware provide further negative opportunities for increased vulnerabilities. These vulnerabilities have real-world consequences for users and organizations. Exploitation of these weaknesses can allow movement within the network which increases the access privileges. The increased access privilege can ultimately lead to the formation of botnets used for malicious activities. Device security breaches can lead to unauthorized access to sensitive information. Similarly for home IoT devices can become access points to other connected devices. To meet these challenges, digital certificates managed by public key infrastructure (PKI) appear to be a powerful solution, facilitating identification, authentication, encryption and equipment chemistry. However, managing multiple digital certificates in an enterprise IoT ecosystem requires automation and scalability, necessitating a comprehensive machine identity management solution. Ultimately, understanding and addressing these vulnerabilities is essential for creating more secure IoT environments as the technology continues to evolve. (Venafi 2023)

In order for the IoT devices to function properly it requires an establishment of secure communications, controlled access to resources, and properly authenticating users. This authentication process involves confirming the identity of IoT devices before they access services, applications, or gateways. However, many IoT devices fail to authenticate using vulnerable methods such as weak passwords or default settings. Whether using one or multiple passwords, ensuring strong authentication mechanisms is critical to the security and reliability of IoT devices and servers. (Venafi 2023) Addressing these vulnerabilities is critical in promoting a more secure and productive environment for the connected devices.

4.2 The Role of 5G Networks in Exacerbating Vulnerabilities

Although the 5G has advanced features, it still has some vulnerabilities for the IoT devices as IoT is a vast technological domain which encompasses the critical network and communication infrastructure. In comparison to the existing technology, 5G operates at higher speed ensuring dependable connectivity. The IoT devices/ environment is categorized in five different layers of architecture in 5G networks. The five different layers includes: sensors, network, communication, architecture and application layers.

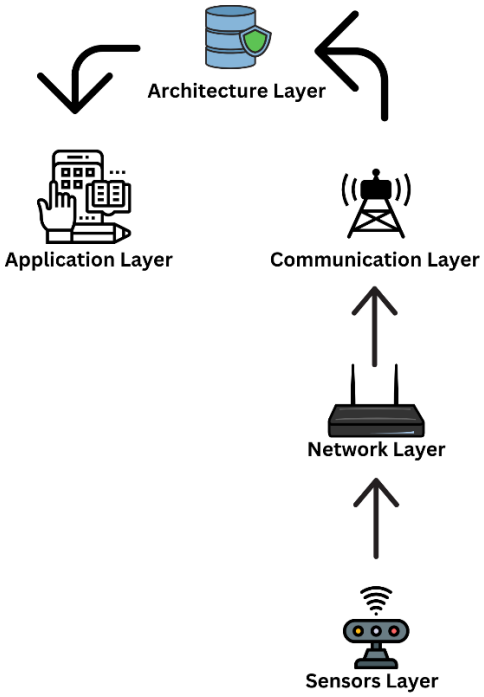


FIGURE 2. Architecture of 5G IoT

The sensor layer integrates smart sensors that participate in two-way communication in the IoT ecosystem. It facilitates effective interactions between the devices. The network layer strategically uses LPWANs such as Sigox and LoRa by establishing a long-range with low-power connectivity infrastructure. (L. Chettri and R. Bera 2020). From there, the communications layer seamlessly integrates 5G RAT technologies. It does this by using standards such as 5G NR to ensure seamless and standardized communications. At the application layer, 5G MTC supports a variety of applications by ensuring uninterrupted machine-to-machine connections with improved data rates, lower latency, faster speeds and connectivity of the flexible equipment. (Singh G et al 2023)

When 5G introduces innovative capabilities in combination with IoT, it also opens potential vulnerabilities across the system architecture. This can be more evident upon the exploration into the layers of the

5G IoT. At the foundational layer, i.e., sensor layer, where smart sensors engage in bidirectional communication, there arises the risk of unauthorized access and manipulation to the received data. Despite the strategic use of LPWANs like Sigfox and LoRa for long range and low-power connectivity in moving up to the network layer, the security challenges persist. Similarly, even though the communication layer seamlessly adopts the 5G RAT technologies are the threats like DoS attacks and sybil attacks. These attacks affect the integrity of the system. Data privacy, confidentiality and integrity becomes a focal point where the data is stored, and these will provoke the attacks in server and databases. Then in the application layer, it is responsible for facilitating and delivering the functionalities which poses the challenges like encompassing the code injections, buffer overflows and manipulations in the permission. Therefore, the complex security landscape situation highlights the importance of the strong protection to guard against the possible threats and vulnerabilities in the dynamic connection of the 5G and IoT. (Bahalul H. et al 2023)

Privacy issues for internet users become a critical issue in the transition from 4G to 5G networks. In contrast, 5G has a much narrower range that requires multiple antennas. However, this transition also gives rise to major concerns regarding the location tracing and anonymity. Such users become more prone to semantic attack due to regular connection with several antennas and exact position discovery in case of 5G network. Also, international mobile subscriber identity-catcher (IMSI catcher) is a vulnerability whereby an attacker captures mobile traffic in certain regions. The attacker, even though removed from the attack area, can login and predict history and future patterns of messages and calls. Moreover, data gathering concerns are heightened by the fact that information in the cloud has no definite borders and can be protected differently between different countries. Building a mutual understanding among all stakeholders with trust is crucial for successful 5G scale. (NOKIA)

5 SECURITY SOLUTIONS FOR IOT IN THE 5G ERA

There is numerous growth on the Internet of Things. In expanding landscape, the 5G mobile network generation has become a benchmark for hassle free communication. Some objects may participate in the network in long-term while others engage temporarily before departing. For instance, a node participates in group communications to give or receive services before exiting after fulfilling its objective. For example: video on demand, multi-cast media streaming. (G. Tsoukaneri, M. Condoluci, T. Mahmoodi, M. Dohler and M. K. Marina 2018) Simultaneously, the advent of 5G contributes a new layer of dynamics to networks, primarily facilitated by network software. Key technologies like Network Function Virtualization (NFV) and Software-Defined Networking (SDN) play very important roles in 5G. NFV involves running the network functions as software on standard virtual machines. NFV will organize through the virtualization platforms. SDN, on the other hand, separates the control and data planes which will enable collaboration among various Virtual Network Functions (VNFs) operating on different virtual machines. (J. G. Andrews et al., 2014) These technologies collectively empower the dynamic creation and organization of numerous services on demand. Network slicing is another crucial 5G concept, where virtual network slices are created up on a shared physical infrastructure. In this concept, each network slicling representing an independent virtualized network is tailored for optimized solutions. (H. Hellaoui et al 2020)

While these 5G functionalities originated in the transport network, they are increasingly becoming intertwined with IoT and IoT devices. The software solution and configurability of the network, championed by SDN and NFV has offered streamlined configuration and management of diverse objects and their associated services. This adaptability allows the network to evolve as new objects and services are introduced. Modern mobile networks are accommodating an array of heterogeneous devices with varying Quality of Service (QoS) requirements. The duration of services provided by these devices adds another layer of dynamics. Moreover, opportunistic network scenarios show dynamic service durations, such as data dissemination and delivery. The communication between involved IoT devices is opportunistic and dynamic which creates opportunities for secure adaptation. Recent attempts have explored the application of SDN to IoT operating systems like TinyOS and Contiki (T. Luo et al 2012). Slicing the IoT enables adaptation to distinct characteristics depending on end-user requirements and the abundance of vertical applications in which the IoT is involved. This translates into on-demand and dynamic

participation of nodes in communication. Therefore, beyond the deep-rooted dynamics of IoT, the dynamics introduced by 5G are essential considerations when deploying it as a communication infrastructure for the IoT. (T. Luo et al 2012) (H. Hellaoui et al 2020)

5.1 Encryption and Authentication Mechanisms for IoT Devices

Authentication in communication networks is similar to the accurate verification process seen in professional settings. Much like confirming identities in a formal gathering, the objective is to discover the authority of devices or users while preventing unauthorized access. This demands the presentation of a unique identifier. The unique identifier is comparable to a badge or credential which proves one's identity and establishes ownership. For instance, when making protocols on authentication there should be assumptions about existing identification procedures. The authentication should consist of the method of producing session keys that are needed for secure channel along with the list of allowed network members. Therefore, for authentication to be an effective policy, the mechanism needs to evaluate current protocols concerning all possible threats, preconditions and adequate session key generator operations including user engagement. (AK. Sahu, S. Sharma, S. S. Tripathi and K. N. Singh 2019)

In the context of IoT, the authentication serves as a dual purpose. Firstly, it validates the identity of users and secondly it ensures the authority of the connected devices. Communication in the IoT landscapes consist of the interactions between the users, devices, or the combination of both. This combination leads to scenarios like user-user, machine-machine, and machine-user interactions. The authentication in the IoT is trickier for the devices than users because the devices of IoT have limited resources. So, as they have limited resources, it makes the process more complex. (AK. Sahu et al 2019) In the world of IoT, making sure things are secure is very important at every step as all the five layers of the network should be secure.

5.2 Secure Communication Protocols for IoT Devices in 5G Networks

The 5G protocol is the type of protocol which sets the rules for how devices should communicate with the 5G network. It uses advanced technologies like artificial intelligence and the Internet of Things. It is designed to be more efficient, reliable, and secure than the previous wireless technology i.e., 4G LTE (Long Term Evolution). The notable features that are available in 5G includes the faster speeds up to 20

Gbps, the ability to support more devices simultaneously, lower delays in data transmission, also known as latency, improved reliability with seamless frequency switching and the enhanced security through encryption and authentication. The mentioned features bring many benefits like improved connectivity with faster speeds and greater capacity which leads to the possibility of connecting more devices. The faster speeds with lower latency of 5G also enhances the user experience. The user experience is better for the activities like streaming high-quality videos and playing online games. Additionally, 5G is more efficient for supporting more devices with less power which results in reduced energy consumption and lower costs. This is why, the advent of the 5G opens up new business opportunities in the ares of Internet of Things, smart cities, autonomous vehicles or even for fostering economic growth by establishing innovative markets. (LinkedIn 2023)

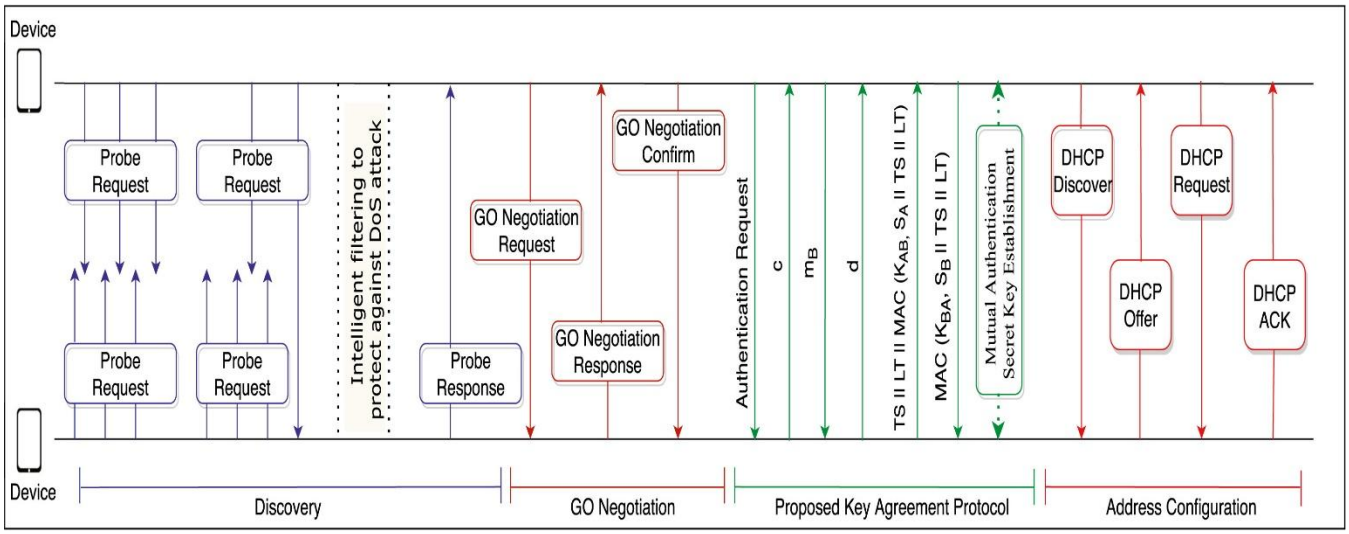


FIGURE 3. Proposed security protocol for WiFi Direct based smart city applications (Gurjot Singh Gaba et al 2021)

Device-to-device communication through WiFi Direct involves distinct phases, they are, discovery, negotiation, mutual authentication, and key agreement followed by address configuration. The vulnerable points for intruders are the discovery and key agreement stages. Operating devices in a WiFi Direct (WFD) environment stay partially active to respond to nearby devices' probe requests. However, intruders exploit this by sending false probe requests, depleting crucial resources like battery, and computing power, causing denial-of-service to legitimate devices. The key agreement phase is also susceptible to man-in-the-middle attacks, compromising future device correspondence. To counteract these threats, the proposed solution implements an intelligent filtering mechanism during the discovery phase and a robust, lightweight Mutual Authentication and Key Establishment (MAKE) system during key agreement.

The filtering mechanism weeds out malicious requests, and the Mutual Authentication and Key Establishment system prevents rogue devices from initiating sessions with legitimate ones. The FIGURE 3 illustrates this protocol, offering protection against DoS and man-in-the-middle attacks, presenting a potential solution for securing diverse smart city applications. This approach not only ensures the security of critical device-to-device communication but also highlights its applicability in enhancing the overall security infrastructure of smart city networks. (Gurjot Singh Gaba et al 2021)

Device security is one of the most important keys in today's technological era. For highly at-risk devices, multiple-level authentication is essential, while less vulnerable ones can be managed with a single level. Message Queuing Telemetry Transport (MQTT) is a communication protocol for devices which will ensure security by verifying users at the application level and the consumers at the transport layer through TLS. The framework involves three main players—Publisher, Broker, and Subscriber—similar to a TV broadcaster, mediator, and user. MQTT is popular in IoT because it is light and user-friendly. Security measures like SSL/TLS are common for IoT but the specifics depend on application designers. The approach utilizes different authentication methods like user ID and password, OTP, and certificates which can ensure security to each device's needs and capabilities. This framework, shown in FIGURE 4 below, shows the interactions between broker, publisher, and subscriber, offering flexibility for various techniques and functions. (D.K Sharma et al 2020)

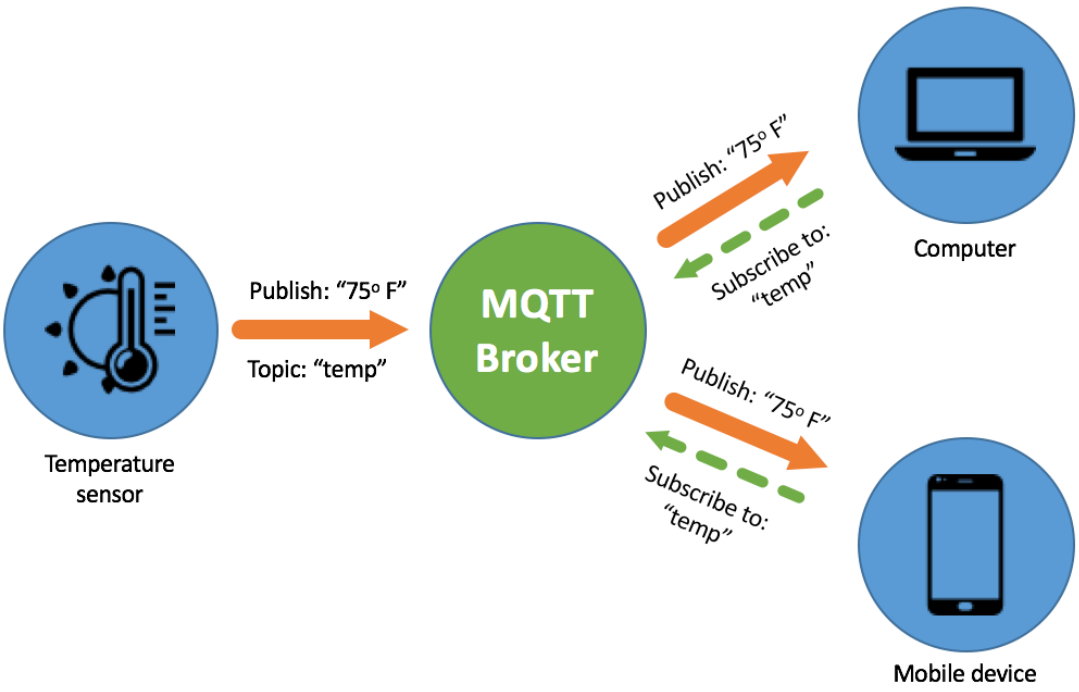


FIGURE 4. The framework of MQTT (Medium 2019)

6 CASE STUDIES AND ANALYSIS

In the contemporary landscape, the integration of IoT and 5G technology has become a transformative force. IoT is connecting and enabling communication among the devices with 5G's high-speed and low-latency capabilities. The combination of both moves towards advancements across various sectors. The partnership of these two technologies facilitates in the creation of smart environments where devices communicate seamlessly. Ultimately, it leads to enhanced efficiency and responsiveness in various sectors. Industries such as healthcare, manufacturing and transportation benefit from the real time data exchange which enables quick and informed decision making. The number of 5G smartphones subscription worldwide will rise to 600 million by the end of 2023, i.e., which is the almost triple amount of total subscription from the year 2020. (Ericsson 2023)

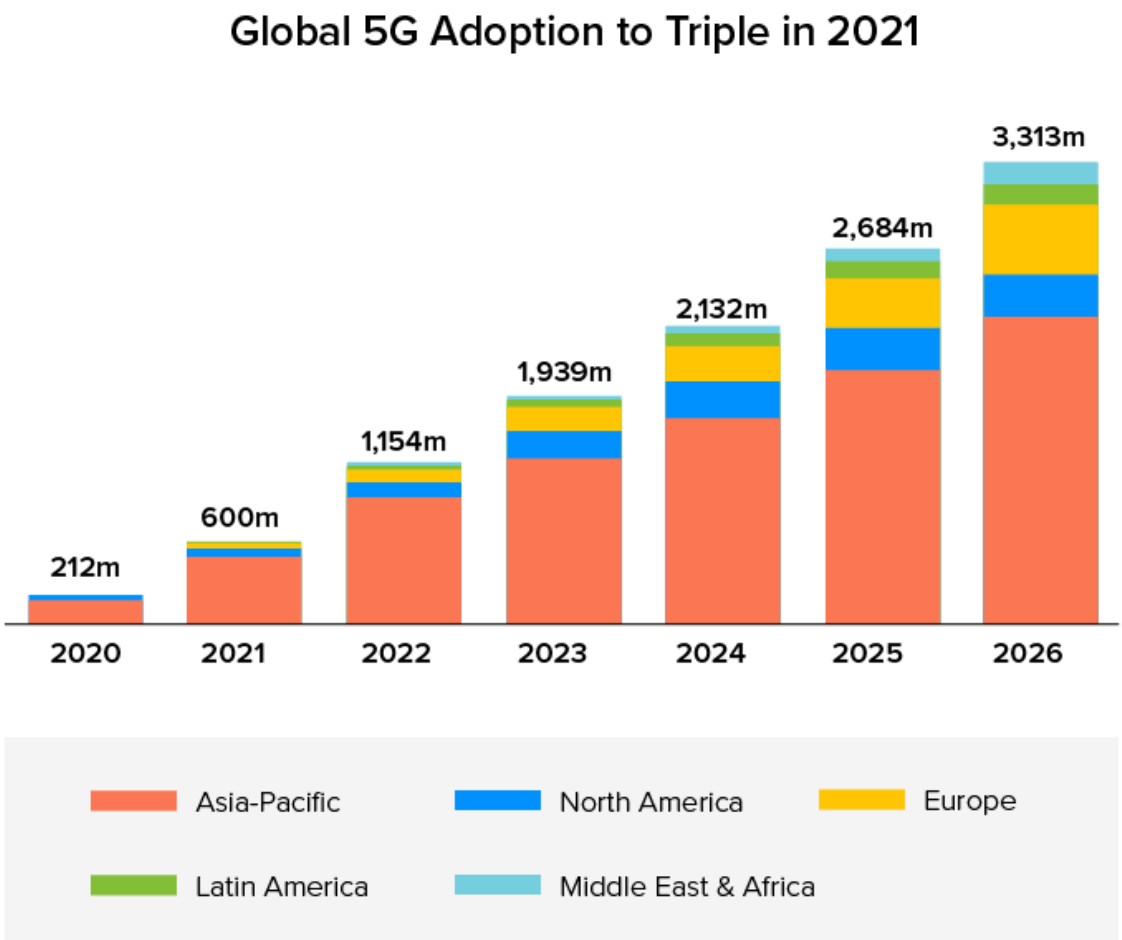


FIGURE 5. Global 5G Adoption (Appinventiv 2023)

The combination of 5G and IoT technologies, in today's landscape brings many possibilities across various sectors shaping the concept of smart cities. One of the notable applications of the 5G IoT is in traffic management, where real time data exchange between two or more vehicles. This roadside infrastructure improves road safety. Additionally, by utilizing transportation systems powered by 5G IoT drivers receive alerts about traffic conditions. It helps in leading to reduced accidents and balanced traffic flow. Another powerful use case is the evolution of automation in grids. With the increasing demand for, electricity 5G enables real time management and automation in grids. This innovation allows for detection and resolution of faults optimizing and grid maintenance. The lower cost of establishing the 5G compared to wired alternatives encourages utility operators to integrate sensors, control systems and renewable energy resources for responsive energy distribution. Furthermore, the application of 5G IoT brings a good change or progress to video surveillance. Governments are investing in video surveillance systems to enhance security on traditional wired setups. (Appinventiv 2023) This step taken by the government offers by implementation of cost savings, improved connectivity and performance while providing security solutions that protect critical assets. Forecasts indicate market growth from USD 2.6 billion in 2021 to an estimated USD 40.2 billion by 2026 highlighting the impact of 5G IoT, on security infrastructure. (Appinventiv 2023)

The topic of smart city is currently dominated by the powerful influence of the 5G and IoT technologies. The European Commission describes a smart city as an combination of traditional networks and services with digital and telecommunication technology to boost their productivity. This requires a combination of modern gadgets, sensors, connected automobiles, and data storages, where 5G and IoT operate in harmony to collect information and provide fast and economical solutions. Spreading over the remote work and education to environmental adaptability, this skilfully collaborative effort moves the urban progress towards the efficiency, sustainability, and resident welfare for every human being. (Appinventiv 2023)

The industries have been reshaped with the collaboration of 5G and IoT. With the fast speed of 5G and its quick response, the IoT devices and the environment is enhanced. The progress can be seen mostly in the fields like healthcare manufacturing and transportation. It has been predicted that by 2023, the subscriptions of 5G smartphones will triple its total. However, there are challenges that need to be considered such as ensuring the smooth radio transmission and updating the security to handle all the potential risks. The shift in hardware-based systems to software-based systems in 5G introduces cybersecurity issues. This issue emphasizes the need for strong protection. Ultimately, the main goal is to

streamline the connections on smaller, cost-effective devices which will also establish a sustainable future. Combining these connections with the 5G network will improve the overall quality of life, public safety, and utilities in the smart cities. (Future Networks IEEE)

7 FUTURE DIRECTIONS AND RECOMMENDATIONS

The Internet of Things has become important in daily lives. It is uplifting various sectors from healthcare to agriculture, automotive industry and business logistics. With the integration of automation, machine learning, machine intelligence and artificial intelligence with IoT is generating valuable insights that are empowering the decision-making. In healthcare, the IoT is contributing significantly to the advanced facilities, highly developed diagnostics and streamlined patient management. All these contributions of IoT are uplifting the healthcare systems. Similarly, in the agriculture sector, IoT is addressing the challenges arising from the climate change which has optimized the production. Additionally, the automotive sector is going through a transformative shift with IoT as it has contributed to the development of the self-driving cars. Furthermore, in business and logistics IoT has facilitated in efficient customer guidance, streamlined payment processes, allergen detection and has automated inventory management. The broad applications of IoT plays an advancing technological landscape across various sectors. (S. Chahar et al 2023) IoT heightens when it is collaborated with 5G.

For AI-driven IoT systems, a smooth flow of data is crucial. If there are any delays then it might disrupt the learning process. There are two kinds of IoT devices that are critical and massive. The critical devices are for things like telemedicine that needs quick and reliable connections. Similarly, the massive devices are for applications like smart agriculture. Moving to 5G brings new challenges specially in the field of cyber security because it transitions to a more software-oriented system. In the automotive world, there are connected vehicles. In this current era, the fully self-driving cars might not take any longer to be introduced. The power of 5G becomes clear in real time video and high-volume data processing as it is affecting everything from the graphics to the smart farming. (S. Chahar et al 2023) But the existing security protocols for the IoT often fall short as it is lacking the comprehensive protection against various attacks. The future research must focus on designing the protocols that are secure against multiple threats. The security protocols should be on low computation power, minimal communication cost and small storage requirements that will prioritize the security without compromising the efficiency.

In the growing landscape of 5G IoT networks, the primary goal is to build a robust system that handles lots of devices while dealing with different challenges. The challenges include making the devices energy efficient, ensuring security, and providing large coverage. The IoT devices, that has the limited energy and computing power make it challenging to find the right setup for different IoT uses. Many researchers are working hard to improve the systems architecture, the physical aspects, channel capacity

and how to efficiently use the available radio spectrum. However, there is a need for high-speed data for things like HD video an AR/VR applications. It is crucial for all the IoT devices to work together seamlessly. Integrating AI into 5G-IoT infrastructure is a strategic move to enhance the adaptability of 5G IoT. It is also important for the network to intelligently adjust configurations in response to changing the environmental parameters which will optimize overall performance. (Singh G et al 2023)

CONCLUSION

In conclusion, this thesis has dived into the transformative potentials of 5G technology and Internet of Things (IoT) with their impact on various sectors. The establishment of 5G has brought high level of speed and connectivity which is encouraging the communication of IoT devices. The combination of these two technologies has uplifted the sectors like healthcare, manufacturing, transportation and beyond. This thesis has demonstrated how 5G adjusts with IoT in the evolutionary process of mobile communication from 1G to 5G. There has been a journey of 5G IoT with great developments pushing for performance and creativity but also it has raised serious security issues. Examining the security issues surrounding this transition has shown that 5G implementation and IoT integrations is highly important. Effective anti-vulnerability mechanisms should be involved among the different users along with encryption, secure communication protocols, artificial intelligence as well as block chain technology. This thesis has enhanced the significance of dealing with the cybersecurity issues that are frequent in the current real-world space of 5G and IoT. There are numerous safety concerns ranging from ransomware risks to privacy dilemmas in IoT systems especially in health care setting. These include the introduction of strong authorization, secure communication protocols with modest incorporation of 5G features into IoT devices.

REFERENCES

AK. Sahu, S. Sharma, S. S. Tripathi and K. N. Singh, "A Study of Authentication Protocols in Internet of Things," 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2019, pp. 217-221, doi: 10.1109/ICIT48102.2019.00045.

Sudeep Srivastava, 2023. Appinventiv, 5G and IoT: Emerging Technologies with endless use cases, Available at: https://appinventiv.com/blog/5g-and-iot-technology-use-cases/ . Accessed 31 October 2023

Bahalul Haque, A.K.M., Nausheen, T., Al Mahfuj Shaan, A., Murad, S.A. (2023). Security Attacks and Countermeasures in 5G Enabled Internet of Things. In: Bhushan, B., Sharma, S.K., Kumar, R., Priyadarshini, I. (eds) 5G and Beyond. Springer Tracts in Electrical and Electronics Engineering. Springer, Singapore. https://doi.org/10.1007/978-981-99-3668-7_7, available at https://rdcu.be/doTkY , Accessed 18 October 2023

CNN Business, 2017. FDA confirms that St. Jude's cardiac devices can be hacked, Available at: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/ . Accessed 8 October 2023

Consosco, 2021. IoT Security Breaches: 4 Real-World Examples, Available at: https://conosco.com/industry-insights/blog/iot-security-breaches-4-real-world-examples Accessed 8 October 2023

D.K. Alferidah and N. Jhanjhi, "Cybersecurity Impact over Bigdata and IoT Growth," 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, 2020, pp. 103-108, doi: 10.1109/ICCI51257.2020.9247722.

D. K. Sharma, N. Baghel and S. Agarwal, "Multiple Degree Authentication in Sensible Homes basedon IoT Device Vulnerability," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2020, pp. 539-543, doi: 10.1109/PARC49193.2020.236671.

D. K. Sharma, N. Baghel and S. Agarwal, "Multiple Degree Authentication in Sensible Homes basedon IoT Device Vulnerability," 2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC), Mathura, India, 2020, pp. 539-543, doi: 10.1109/PARC49193.2020.236671.

D. Lučić and P. Mišević, "An Impact of Implementation of 5G Technology on Information Security," 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2021, pp. 412-416, doi: 10.23919/MIPRO52101.2021.9596777.

D. Wu, M. Sun, P. Zhang, Y. Tu, Z. Yang and R. Wang, "Personalized Secure Demand-Oriented Data Service Toward Edge-Cloud Collaborative IoT," in IEEE Internet of Things Journal, vol. 10, no. 1, pp. 378-390, 1 Jan.1, 2023, doi: 10.1109/JIOT.2022.3199937.

Ericsson, 2023. Ericsson Mobility Report, Available at https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/june-2023 Accessed 31 October 2023

European Parliament, 2022. Cybersecurity: main and emerging threats, Available at: https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats?&at_campaign=20234-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_audience=cyber%20security%20threats&at_topic=Cybersecurity&at_location=FI&gclid=CjwKCAjwg4SpBhAKEiwAdyLwvNMKc6rWVMSpHSz94tDiM0EgBPEGD98F3wd4zDfdHN4gy_nfEX8hfBoCbiwQAvD_BwE Accessed 7 October 2023

Future Networks IEEE, Charting an integrated future: IoT and 5G research papers, Available at https://futurenetworks.ieee.org/topics/charting-an-integrated-future-iot-and-5g-research-papers Accessed 31 October 2023

G. Tsoukaneri, M. Condoluci, T. Mahmoodi, M. Dohler and M. K. Marina, "Group Communications in Narrowband-IoT: Architecture, Procedures, and Evaluation," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1539-1549, June 2018, doi: 10.1109/JIOT.2018.2807619.

Gurjot Singh Gaba, Gulshan Kumar, Tai-Hoon Kim, Himanshu Monga, Pardeep Kumar, Secure Device-to-Device communications for 5G enabled Internet of Things applications, Computer Communications, Volume 169, 2021, Pages 114-128, ISSN 0140-3664, https://doi.org/10.1016/j.comcom.2021.01.010.

H. Ghorbani, M. S. Mohammadzadeh and M. H. Ahmadzadegan, "DDoS Attacks on the IoT network with the Emergence of 5G," 2020 International Conference on Technology and Entrepreneurship - Virtual (ICTE-V), San Jose, CA, USA, 2020, pp. 1-5, doi: 10.1109/ICTE-V50708.2020.9113779.

H. Hellaoui, M. Koudil and A. Bouabdallah, "Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6589-6602, July 2020, doi: 10.1109/JIOT.2020.2974618.

J. G. Andrews, Stefano Buzzi, Wan Choi, Stephen V. Hanly, Angel Lozano, Anthony C. K. Soong, Jianzhong Charlie Zhang, "What Will 5G Be?," in IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065-1082, June 2014, doi: 10.1109/JSAC.2014.2328098.

L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 16-32, Jan. 2020, doi: 10.1109/JIOT.2019.2948888.

LinkedIn, 2023. What is 5G Protocol: A Comprehensive Guide For Next Generation of Wireless Technology, Available at https://www.linkedin.com/pulse/what-5g-protocol-comprehensive-guide-next-generation/ Accessed 26 October 2023

Mohammad Wazid, A. K. Das, S. Shetty, P. Gope and J. J. P. C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," in IEEE Access, vol. 9, pp. 4466-4489, 2021, doi: 10.1109/ACCESS.2020.3047895.

Medium, 2019. Getting Started with MQTT- Part 1, Nitin Sharma, Available at: https://nitin-sharma.medium.com/getting-started-with-mqtt-part-1-a3c365e3a488 Accessed 26 October 2023

N. Gupta, S. Sharma, P. K. Juneja and U. Garg, "SDNFV 5G-IoT: A Framework for the Next Generation 5G enabled IoT," 2020 International Conference on Advances in Computing, Communication & Materials (ICACCM), Dehradun, India, 2020, pp. 289-294, doi: 10.1109/ICACCM50413.2020.9213047.

NOKIA, Privacy challenges and security solutions for 5G networks, Available at: https://www.nokia.com/thought-leadership/articles/privacy-challenges-security-solutions-5g-networks/ Accessed 3 November 2023

R. M. Haris and S. Al-Maadeed, "Integrating Blockchain Technology in 5G enabled IoT: A Review," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2020, pp. 367-371, doi: 10.1109/ICIoT48696.2020.9089600..

S. Chahar and K. Kaur, "Internet of Things with 5G Technology: A Critical Review," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 1402-1406, doi: 10.1109/ICACITE57410.2023.10183041.

S. Dhinakaran, V. Bansal, K. Pant, S. K. Joshi, U. H. Maginmani and C. R. Prasad, "A New Design for Protecting Cyber-Attacks and Harmful Threats in IoT Communication Network with Efficient Deep Learning-Based Detection System," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 959-962, doi: 10.1109/ICACITE57410.2023.10182981.

Singh. G., Singh, J., Mitra, D., & Prabha, C. (2023). A Roadmap Toward Prospects for IoT Enabled 5G Networks. In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 1405-1410). Erode, India.

Singh J., Singh, G., Muskan, & Aggarwal, G. (2022). Inclusion of Aerial Computing in Internet of Things: Prospects and Applications. In 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) (pp. 1664-1669). Kannur, India

T. Luo, H. -P. Tan and T. Q. S. Quek, "Sensor OpenFlow: Enabling Software-Defined Wireless Sensor Networks," in IEEE Communications Letters, vol. 16, no. 11, pp. 1896-1899, November 2012, doi: 10.1109/LCOMM.2012.092812.121712.

Venafi, 2023. Top 10 Vulnerabilities that Make IoT Devices Insecure, Available at: https://venafi.com/blog/top-10-vulnerabilities-make-iot-devices-insecure/ Accessed 21 October 2023

WIKI OWASP, 2019. Internet of Things Project, Available at https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 Accessed 21 October 2023