DOI: http://dx.doi.org/10.26483/ijarcs.v14i6.7033

Volume 14, No. 6, November - December 2023

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

COMPARATIVE SURVEY OF 5G NETWORK ON DIFFERENT TECHNOLOGIES IN NETWORK SECURITY

Aderonke A. Adegbenjo, Amanze Ruth, Afolarin I. Amusa, Fatade Oluwayemisi
Babcock University, Ilishan-Remo,
Ogun State, Nigeria

Abstract: The prominence of security has been a central concern in several telecommunications industries in recent years, mostly owing to the potential for substantial consequences linked to dangers. In forthcoming wireless systems, it is expected that confidential information will be sent across several layers, with a special focus on network security and fundamental and supporting technologies. The exposure of several instances has shed light on the potential dangers linked to a hacked wireless network. These risks not only jeopardize security and privacy but also disrupt the complex dynamics of the communication ecosystem. Consequently, there has been a significant increase in the complexity and effectiveness of security breaches in recent years, presenting a global challenge in terms of detecting and preventing acts of sabotage. This article presents a comprehensive analysis of several technologies used in the realm of network security, with particular emphasis on their ramifications for both security and privacy. This article further evaluates the relevant security measures and technologies, using insights from several standardization organizations, and provides a succinct overview of the security entities engaged in standardization. In summary, a segment has been included to promote more academic investigation, focusing on future paths and unresolved issues. This paper provides a succinct overview of the security forces engaged in the process of standardization. In summary, a segment emphasizing prospective avenues and unresolved issues has been included to foster more academic investigation.

Keywords: Security, Technologies, Network, Telecommunication, 5G

1. INTRODUCTION

The fifth generation (5G) is the most recent advancement in cellular mobile communications. The 5G network is of utmost importance in contemporary commercial telecommunications networks because of its notable advantages in high data rate, decreased latency, and extensive device connection. Nevertheless, the implementation of the 5G network is not without its practical problems. This is due to the presence of a multitude of distinct components, referred to as heterogeneity. The presence of heterogeneity inside the 5G network yields two notable outcomes. Firstly, it hinders the uniform use of this technology, hence impeding its widespread adoption. Secondly, it introduces complexities into the structure of the 5G network, making the monitoring of network activities a challenging endeavor. In recent years, there has been rapid growth in 5G networks, which are a novel wireless communication technology. As seen in Figure 1, this methodology has been extensively used in several facets of our everyday existence. In contrast to the antiquated commercial 4G (LTE/WiMax) system, this technology offers significant benefits in terms of enhanced data rate, decreased latency, and extensive device connection. Consequently, it is poised to become an essential component of wireless communication infrastructure in the foreseeable future. Driven by the notable benefits it offers, several researchers have developed their methods (Fan et al., 2016; Ravindran et al., 2017; Zhang et al., 2015) to align with the demands of practical applications. Software-defined networking (SDN) emerges as a crucial design paradigm in this study. Software-defined networking (SDN) is a methodology aimed at enhancing network performance and monitoring via the facilitation of network administration and the enablement of programmatically efficient network setup (Benzekki et al., 2016). The separation of data and control planes in software-defined networking (SDN) facilitates the development of several novel applications, such as traffic engineering, data center virtualization, and fine-grained access control (Casado et al., 2014). The use of this approach has been shown to provide significant benefits in many commercial networks (Felix et al., 2014; Kukliński & Chemouil, 2014), thus making it a viable option for implementation in the realm of 5G networks. Notwithstanding these benefits, the establishment of an SDN-based 5G network incurs costs and presents several security concerns. The vulnerability of SDN's intelligence centralization is attributed to its susceptibility to a range of threats. Numerous scholarly studies have previously explored security applications developed on the software-defined networking (SDN) controller, each with distinct objectives. The applications of distributed denial of service (DDoS) detection and mitigation (Braga et al., 2010; Giotis et al., 2014), as well as botnet (Feamster, 2010) and worm propagation (Jin & Wang, 2013), are specific instances where these technologies are used. The concept primarily involves the regular collection of network information from the forwarding plane of the network in a standardized way, such as via the use of OpenFlow. Subsequently, classification algorithms are employed to analyze these statistics and identify any potential network abnormalities. If an anomaly is identified, the application provides instructions to the controller on how to reprogram the data plane to mitigate the abnormality. An alternative security application utilizes the SDN controller to include moving target defense (MTD) algorithms. MTD (Moving Target Defense) algorithms are often used to enhance the resilience of a targeted system or network against attacks by regularly altering or concealing critical attributes. The implementation of Moving Target Defense (MTD) algorithms

in conventional networks is a significant challenge due to the complexity involved in establishing a central authority with the capability to identify and conceal or modify critical attributes for each component of the system that requires protection. In a software-defined networking (SDN) network, the execution of tasks is simplified due to the centralization of control inside the controller. One potential use is the periodic allocation of virtual IP addresses to hosts inside a network, with the subsequent mapping of virtual IP addresses to real IP addresses being carried out by the controller (Jafarian et al., 2012). According to Kampanakis et al. (2014), an additional software program can replicate fictitious open, closed, or filtered ports on various hosts inside a network. The purpose of this application is to provide substantial interference during the first reconnaissance stage, such as scanning, conducted by a malicious actor. Further enhancement in terms of security in software-defined networking (SDN) enabled networks may be achieved by the use of FlowVisor and FlowChecker, as suggested by Al-Shaer and Al-Haj (2010). The previous approach aims to use a single hardware forwarding plane that is capable of accommodating numerous distinct logical networks. By adopting this methodology, it becomes possible to use the same hardware resources for both production and development objectives, while also segregating monitoring, configuration, and internet traffic. Each distinct scenario might own its logical topology, referred to as a "slice." In tandem with this methodology, the validation of newly installed OpenFlow rules by users using their slice is accomplished by FlowChecker (Canini et al., 2012). SDN controller applications are mostly implemented in extensive-scale situations, necessitating thorough examinations of potential programming flaws. The authors of a study published in 2012 (Canini et al., 2012) described a system known as NICE for this purpose. The implementation of a complete and extended approach to Software-Defined Networking (SDN) is necessary when introducing a comprehensive security architecture. Since its introduction, designers have been exploring potential methods to ensure the security of Software-Defined Networking (SDN) without compromising its scalability. The architecture known as SN-SECA (SDN+NFV) Security Architecture was proposed by Bernardo and Chua in 2015.

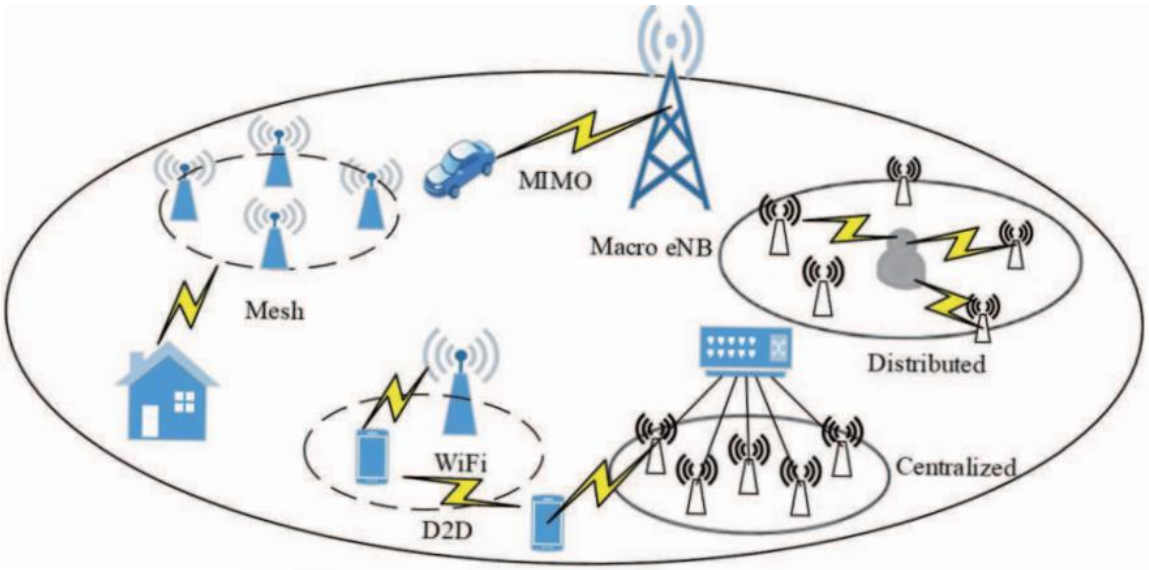

Figure 1. 5G networks.

2. LITERATURE REVIEW

The advent of the Internet, computers, artificial intelligence (AI), and hardware technologies has resulted in the creation of a virtual world that has significantly impacted the lives of individuals, as noted by Fu et al. (2023). This digital transformation has occurred to varying extents. The proliferation of virtual reality has led to a surge in the popularity of the metaverse, an emerging social ecosystem that facilitates the integration of physical and virtual realms. Nevertheless, the metaverse's ongoing development encounters several needs and obstacles like as privacy, security, high synchronization, and low latency because of the exponential increase in data volume and its corresponding value. Fortunately, the dynamic advancements in blockchain and intelligent networking technologies may be effectively used to meet the requirements of trustworthy construction, continuous data exchange, and processing needs inside the metaverse. Hence, it is essential to undertake a comprehensive examination of the function and benefits of blockchain technology, intelligent networking, and their amalgamation in facilitating the immersive experiences of the metaverse. This review starts by examining the developmental trajectory, distinguishing features, and structural framework of the metaverse. Next, a comprehensive examination is conducted on the current body of research on blockchain, networking, and the integration of these two technologies. This evaluation encompasses an analysis of the fundamental concepts, practical implementations, and obstacles encountered in these domains.

The subject of computer networking has been included in university curricula for a considerable period. A network comprises an intricate combination of applications, communications protocols, connecting technologies, traffic flows, and routing algorithms. When instructing on the networking idea, the process of network design is a formidable challenge, as designers must effectively manage the trade-off between user performance expectations and the associated costs and capabilities. One of the evident strategies

used to address the intricacy of the subject is using modeling and simulation methodologies. This study investigates three optimal instructional methods suitable for integration into the Computer Networking curriculum at Cardiff Metropolitan University or any other university, to enhance educational outcomes. This study illustrates that an effective pedagogical program necessitates the integration of several instructional strategies to accomplish its objectives. The assessment of the overall effectiveness of the tools may be achieved by analyzing several components of the course. Numerous network design and simulation technologies have been subject to extensive research and analysis. The instructional materials that were chosen for the aim of teaching computer communications networks were picked based on our study and experimentation. According to Rahman and Pakstas (2023), the integration of the wide area network modeling tool Delite, the network simulator ns-3, and the topology creation tool Brite may be used as an educational approach to impart networking principles to students. These technologies have the potential to enhance students' comprehension of computer network fundamentals and enhance their practical network abilities.

The use of Software Defined Networking (SDN) has seen a notable surge in recent years, mostly driven by diverse network management needs. The use of Software-Defined Networking (SDN) in computer network applications has yielded several advantages for users. These benefits include reduced operating expenses, enhanced hardware administration, more flexibility, and the ability to construct networks in a centralized manner. In contrast, the Internet of Things (IoT) represents a rapidly expanding technological domain. The two fundamental characteristics of the Internet of Things (IoT) are distributed infrastructures and dynamic systems. According to Ahmadvand et al. (2023), The aforementioned attributes give rise to some difficulties when using Software-Defined Networking (SDN) in the context of the Internet of Things (IoT) concerning security and privacy concerns. This study aims to examine the security and privacy concerns associated with Software-Defined Networking (SDN)--based Internet of Things (IoT) systems, while also proposing potential solutions to mitigate these difficulties. In this study, we examine the methodologies used in prior research to provide a satisfactory degree of security and privacy preservation in Internet of Things (IoT) systems based on Software-Defined Networking (SDN). Within the realm of the data plane, scholarly works of software-defined networking (SDN)-based Internet of Things (IoT) have extensively examined the utilization of hashing and encryption methods. In the control plane, thorough analyses have been conducted on certificate authority and access control mechanisms. Furthermore, in the application plane, the scholarly discourse has revolved around the topics of attack detection and authentication. Additionally, a comprehensive statistical analysis of the current body of research is offered. This analysis demonstrates that there has been a disparity in the attention given by scholars to different fields of study in recent years. The last examination furthermore brings attention to concerns that prior researchers have overlooked.

Artificial Intelligence is a medium for machine intelligence that presents significant prospects for the intelligent industrial revolution. The fast advancement of networking technology has shown to be advantageous for several domains such as smart transit, computer networks, and networked intelligent cities. The advancement has introduced novel opportunities in the domains of traffic safety, comfort, and high-quality solutions. Artificial intelligence, a prevalent methodology used across diverse scientific domains, is utilized to enhance and optimize data-driven methodologies. The advent of the new 5G network architecture presents a paradigm shift in the realm of networking, as it aims to rectify the limitations and deficiencies seen in the preceding 4G technology. These nascent technologies provide intelligent urban environments and self-governing networks with a new avenue for achieving comprehensive connectivity, even in places characterized by high mobility or dense populations. This is made possible by the facilitation of extensive simultaneous connections and the pervasive presence of the internet. This article utilizes an artificial intelligence-based Vehicle to Everything (AI-V2X) technology. According to the study conducted by Liu et al. (2023), The suggested methodology can acquire information from many sources, enhance driver consciousness, and predict potential crashes, hence augmenting driving convenience, safety, and efficiency. By integrating high-speed, resilient, low-latency networking and artificial intelligence (AI) technology, the interaction between physical reality and digital data in Industry 4.0 is revolutionized, resulting in the development of an intelligent vehicle. The objective of AI-V2X is to investigate the potential impact of novel AI methodologies on the development of autonomous vehicle detection and navigation systems.

The progression of computer network technology has consistently seen significant advancement. Software Networking (SDN) and Blockchain (BC) have emerged as synergistic technologies that offer enhanced security and improved network performance across various domains of application, such as the Internet of Things (IoT) ecosystem. This convergence holds the potential to positively impact our overall quality of life. The widespread adoption of Internet of Things (IoT) devices may be attributed to a diverse range of practical applications and their pervasive accessibility. According to the research conducted by Turner et al. (2023), The convergence of SDN and BC, in conjunction with the current climate, offers significant prospects for several upcoming research endeavors. This serves as a driving force behind the motivation for this work. In this paper, we provide an extensive overview of the research conducted on the integration of Blockchain (BC) and Software-Defined Networking (SDN) inside the Internet of Things (IoT) ecosystem. This integration is often referred to as BC-enabled Software-Defined IoT (BC-SDIoT) in the literature. The study first examines the underlying motives and determinants for the integration of blockchain-enabled software-defined networking (BC-SDN) and blockchain-enabled software-defined Internet of Things (BC-SDIoT), along with an analysis of their respective advantages and disadvantages. Furthermore, the pertinent studies are classified based on six primary implementation objectives and concepts that integrate BC, SDN, and IoT technologies to establish intelligent, protected, and efficient frameworks. These objectives include security, computing paradigms (specifically edge and fog computing), trust management, access control and authentication, privacy, and networking. In the following sections, we will outline the categories, or issue domains, of the aforementioned innovative taxonomy and

provide a comprehensive analysis of relevant research, or solutions. In conclusion, we identify significant obstacles, unresolved matters, and future opportunities that need more research focus and dedicated efforts to develop comprehensive and innovative frameworks that expand the scope of study in the field of Blockchain-enabled Smart and Sustainable Internet of Things (BC-SDIoT). This survey study may be considered a valuable introductory resource for anyone interested in exploring the use of blockchain technology in software-defined networking (SDN) and Internet of Things (IoT) ecosystems.

According to the study conducted by Mazhar et al. (2023), Through the use of machine learning, complex activities may be autonomously accomplished without human intervention. The use of computers and mobile devices inside a smart grid (SG) facilitates enhanced control over interior temperature regulation, security monitoring, and regular maintenance operations. The Internet of Things (IoT) is used to establish connectivity among the many elements inside intelligent buildings. With the increasing proliferation of the Internet of Things (IoT) paradigm, there is a growing trend of incorporating Smart Grids (SGs) into broader network infrastructures. The Internet of Things (IoT) plays a significant role in Smart Grids (SGs) since it offers a range of services that contribute to the enhancement of individuals' quality of life. The safety and efficacy of the existing life support systems have been well-established in supporting human life. The primary objective of this study is to ascertain the underlying factors driving the installation of Internet of Things (IoT) devices in smart buildings and the grid. The significance of the infrastructure and components that underpin IoT devices is paramount from this particular perspective. The use of remote configuration for smart grid monitoring systems has the potential to enhance both the security and comfort of those occupying buildings. Sensors play a crucial role in the operation and monitoring of a wide range of devices, spanning from consumer electronics to smart grids (SGs). Network-connected devices must exhibit reduced energy consumption and possess the capability of remote monitoring. The objective of the writers is to facilitate the development of solutions grounded on artificial intelligence (AI), the Internet of Things (IoT), and smart grids (SGs). In addition, the writers conducted a study on the subjects of networking, machine intelligence, and SG. Lastly, we will analyze the existing body of research on Serious Games (SG) and the Internet of Things (IoT). There is ongoing controversy about several components of IoT platforms.

In recent years, there has been a significant advancement in networking systems. The emergence of network setups such as the Internet of Things (IoT) may be attributed to the advancements in network and communication technologies. The Internet of Things (IoT) framework facilitates the interconnection of various devices, including computers, mobile phones, and other similar devices. Therefore, it is essential to ensure the security of networks. One potential solution for enhancing the security of these networks is the use of Intrusion Detection Systems (IDS). The operational functionality of these systems is contingent upon the use of techniques and ideas related to anomaly detection. This study primarily focuses on the installation of a Software-Defined Network (SDN) in Internet of Things (IoT) networks. The use of this solution results in significant cost savings by reducing the need for several hardware components inside the networks. This study focuses on the use of Intrusion Detection Systems (IDS) inside Software-Defined Networking (SDN)-based Internet of Things (IoT) networks. Various research are presented, examined, and contrasted. According to the study conducted by Hassan et al. (2023),

In this study, we aim to reproduce Low-rate Denial of Service (LDoS) assaults against the Software-Defined Networking (SDN) data plane. Additionally, we provide a novel framework named GASF-IPP, which focuses on the detection and mitigation of such attacks. Our proposed framework leverages the analysis of network abnormalities by considering different traffic and IP-port data. The monitoring of switch traffic is facilitated by the use of the OpenFlow protocol. The Gramian angular summation field (GASF) transformation is used in conjunction with timing analysis to examine network data and integrate additional characteristics to detect potential attacks. By identifying the assailant and the target, it is possible to develop flow regulations to mitigate the situation. The experimental results demonstrate the accuracy and efficacy of our proposed framework. The detection and mitigation module exhibits real-time functionality with a minimal false positive rate (FPR) and an average response time of 6.77 seconds (Tang et al., 2023).

The platform-centric security system, which operates on the Internet of Things (IoT), can establish real-time communication with the associated equipment. The system is comprised of many components, including the voice sensor/microphone, motion/activity sensor, LTE/Wi-Fi module, and camera. The central processing unit (CPU) serves as the crucial component of the system, facilitating the interaction between each of these sensors. The financial system as a whole will include the Internet of Things (IoT) in real-time, enabling mobile devices and computers to remotely monitor actions occurring at the physical location of IoT devices. This will enable the system to achieve greater efficiency. Furthermore, it will document all of these actions and save them in the cloud storage account linked to the user. The Internet of Things (IoT)-based security system provides an added layer of protection to the property of the user or client. Security systems are purposefully designed to execute certain functions upon the occurrence of a breach inside a safeguarded vicinity. This document will send a notice to the relevant party as a cautionary measure. During that specific period, individuals will possess the capability to undertake appropriate measures as a result of being properly informed in advance (Marie, 2023).

The process of packet categorization has significant importance in determining the most suitable course of action within various networking paradigms. The classification of packets has always been seen as a challenging offline undertaking. The advancement of networking paradigms such as software-defined networking (SDN), exemplified by Open Flow, and network function virtualization (NFV), has posed challenges in terms of characterizing and modifying packet insertion or deletion suggestions in online environments. While there exist software solutions capable of packet classification, their effectiveness is limited when it comes to performing high-speed link operations. Software tools often prioritize protocol layers, IP addresses, or port numbers while doing categorization. (Adiseshaiah and Sailaja, 2023; Marie, 2023) In the context of wire speed processing, the inclusion

of several field inspections by software solutions is considered undesirable. Hardware solutions are often used for ensuring secure communication and achieving high-speed computing. The process of classifying packets may be accomplished by examining the whole of the packet header data. Within a hardware-based packet classification system, the arriving packets undergo a process where several fields are examined and compared against the rules specified in a given rule set. A ruleset often consists of a range of rules, typically ranging from one hundred to one thousand. One of the primary challenges associated with the implementation of a hardware solution is the substantial memory requirements necessitated for storing the rules. The limited capacity of on-chip memory in Field Programmable Gate Arrays (FPGAs) presents constraints, making the use of external memory a tough endeavor.

3. DISCUSSION

Figure 2 depicts the overarching architectural framework of 5G networks. The process of network softwarization has facilitated the capacity to depict the 5G network as a layered model, akin to SDN networks. According to previous studies (Ahmed et al., 2019; Li et al., 2018), the implementation of 5G technology is expected to provide extensive support for various devices, such as mobile phones and Internet of Things (IoT) devices. The Internet of Things (IoT) encompasses a range of devices that have evolved from basic home appliances to sophisticated sensors and other advanced technology. Additionally, the implementation of 5G will facilitate the use of various Radio Access Technologies (RATs) to establish connections between these devices. Security has emerged as a crucial issue throughout several telecommunications businesses in contemporary times due to the potential for significant repercussions associated with various hazards. In particular, the core and enabling technologies will be closely linked to networking. The backhaul of the 5G network may be categorized into three distinct layers: the infrastructure layer, the control layer, and the business application layer. The infrastructure layer encompasses fundamental connection equipment, including Base Stations (BS), routers, and switches. In contrast to the pre-5G network, devices at the infrastructure layer cannot possess intelligence. The control layer is responsible for housing all network control features and decision-making entities. The control layer engages in interactions with the business layer. Additionally, the system can convert network service requests originating from the business layer into control instructions, which are then sent to the devices in the infrastructure layer. Therefore, the implementation of both network services and business applications occurs inside the business layer. Furthermore, the E2E (End-to-end) management and orchestration layer is used concurrently to ensure the coordinated functioning of all three levels.

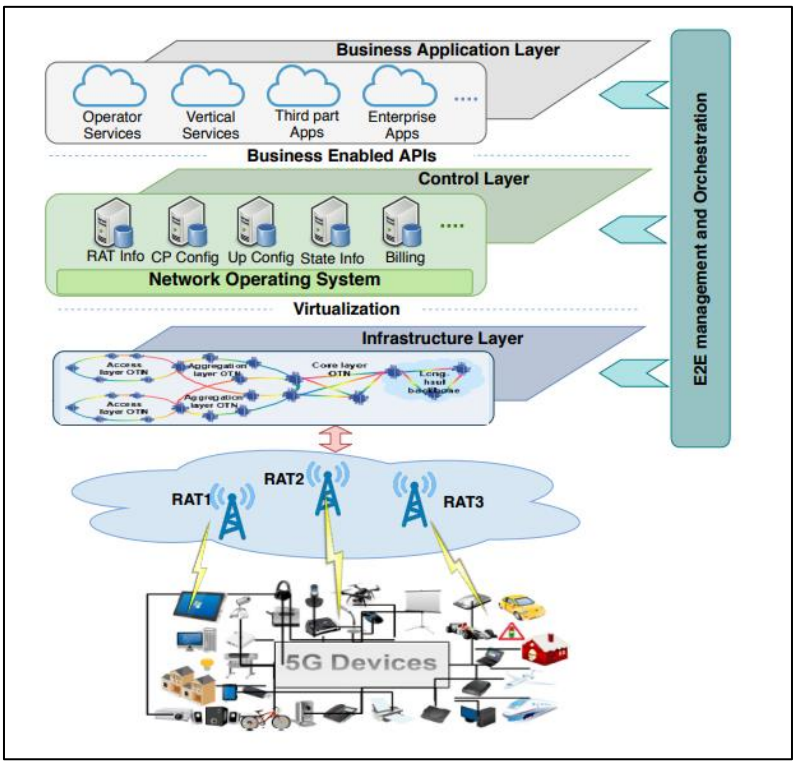

Fig. 2. The High-level Architecture of the 5G Network with different operational layers.

The importance of security to 5G technologies has been recognized as a crucial need for both current 5G systems and future systems. Furthermore, the majority of security models used in pre-5G networks, such as 2G, 3G, and 4G, cannot be immediately applied to 5G networks owing to the introduction of new architectural elements and services (Jayakody et al., 2019). Nevertheless, some security techniques may be used with appropriate adjustments. The Open Air Interface (OAI) platform, as detailed by Nikaein et al. (2018), is designed to provide backward compatibility with the previous generation. This platform is situated within the broader framework of 5G and is accompanied by an overview of the security protocol enhancements in 5G, as presented by Lien et al. (2019). Historically, the primary objective in securing the telecommunication network was to guarantee the effective operation of the billing system and safeguard the radio interface by using encryption techniques to protect communication data. In the context of 3G

technology, the implementation of two-way authentication serves the purpose of mitigating the potential risks associated with establishing connections with fraudulent base stations. In conclusion, 4G networks use sophisticated cryptographic techniques to facilitate user authentication. Additionally, it provides safeguards against physical assaults, such as the manipulation of base stations, which have the potential to be deployed in both public and user locations. Furthermore, some privacy concerns were partially addressed in the pre-5G network since user data was retained inside the databases owned by cell operators. Nevertheless, the security and privacy concerns around 5G technology are of paramount importance.

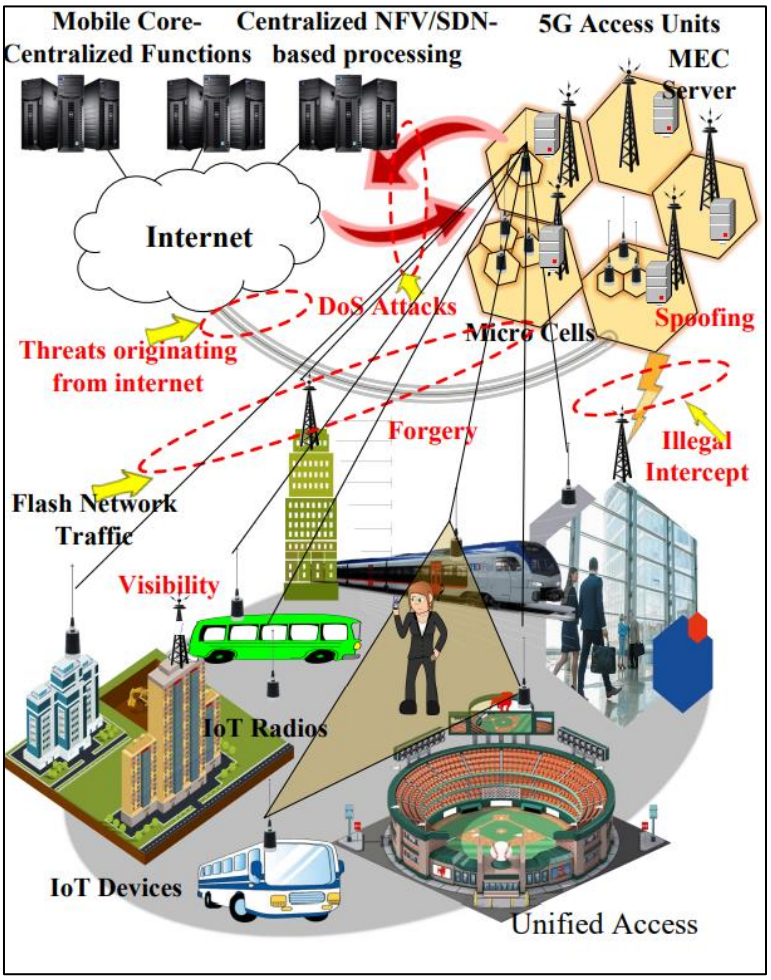

Fig. 3. The Overall View of 5G Security Impact for Heterogeneity of Connected Devices and More Users.

The mechanisms are being overwhelmed by challenges as a result of architectural changes and the introduction of new services. The security of 5G and subsequent generations of networks include three primary components. The majority of the aforementioned security concerns and security needs of pre-5G mobile generations remain relevant in the context of 5G and subsequent generations. Furthermore, the implementation of 5G technology will provide a fresh array of security difficulties. These challenges arise from the amplified user base, the diverse range of connected devices, the emergence of novel network services, the heightened concerns about user privacy, the involvement of new stakeholders, and the need to accommodate the Internet of Things (IoT) and mission-critical applications (as shown in Figure 3). Furthermore, the implementation of network softwarization and the adoption of emerging technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), Multi-Access Edge Computing (MEC), and Network Slicing (NS) may give rise to a novel array of security and privacy concerns. Figure 4 presents a comprehensive depiction of the 5G Security requirements, which have been developed by including three key components.

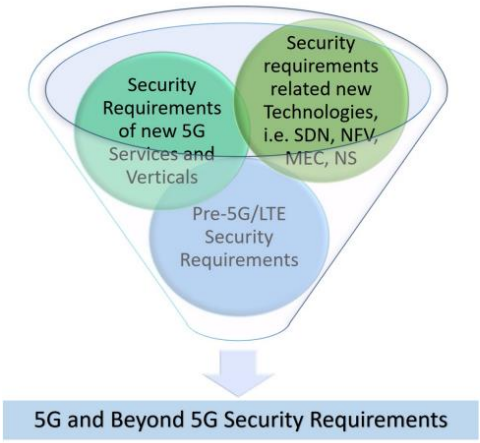

Fig. 4. Formation of 5G and Beyond Security Requirements

4. CONCLUSION

The environment of the 5G network is always developing, producing a growing number of security vulnerabilities at various levels and applications. This article has conducted a comprehensive examination of the security threats associated with 5G technology by conducting an extensive assessment and analysis of existing literature. This study aims to provide a comprehensive knowledge of the many security challenges that arise in the context of 5G networks. We have conducted an extensive examination of the security model for 5G, the evolving threat landscape for the next generation of 5G technology, the danger landscapes associated with the Internet of Things (IoT), and the study of threats inside 5G networks. The study conducted included a comprehensive examination of security concerns within the primary domains of 5G security. These areas include authentication, access control, communication security, and encryption. The poll also brought attention to the security concerns that are linked to the major technologies of 5G.

REFERENCES

1. Adiseshaiah, M., & Sailaja, M. (2023). A parallel decision-making design for highly speedy packet classification. Microprocessors and Microsystems, 99. https://doi.org/10.1016/j.micpro.2023.104826
2. Ahmadvand, H., Lal, C., Hemmati, H., Sookhak, M., & Conti, M. (2023). Privacy-Preserving and Security in SDN-Based IoT: A Survey. IEEE Access, 11. https://doi.org/10.1109/ACCESS.2023.3267764
3. Ahmed, R., Malviya, A. K., Kaur, M. J., & Mishra, V. P. (2019). Comprehensive Survey of Key Technologies Enabling 5G-IoT. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3351007
4. Al-Shaer, E., & Al-Haj, S. (2010). FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures. Proceedings of the ACM Conference on Computer and Communications Security. https://doi.org/10.1145/1866898.1866905
5. Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. Security and Communication Networks, 9(18). https://doi.org/10.1002/sec.1737
6. Bernardo, D. V., & Chua, B. B. (2015). Introduction and analysis of SDN and NFV security architecture (SN-SECA). Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 2015-April. https://doi.org/10.1109/AINA.2015.270
7. Braga, R., Mota, E., & Passito, A. (2010). Lightweight DDoS flooding attack detection using NOX/OpenFlow. Proceedings - Conference on Local Computer Networks, LCN. https://doi.org/10.1109/LCN.2010.5735752
8. Canini, M., Venzano, D., Perešíni, P., Kostić, D., & Rexford, J. (2012). A nice way to test OpenFlow applications. Proceedings of NSDI 2012: 9th USENIX Symposium on Networked Systems Design and Implementation.
9. Casado, M., Foster, N., & Guha, A. (2014). Abstractions for software-defined networks. In Communications of the ACM (Vol. 57, Issue 10). https://doi.org/10.1145/2661061.2661063
10. Fan, K., Gong, Y., Liang, C., Li, H., & Yang, Y. (2016). Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Security and Communication Networks, 9(16). https://doi.org/10.1002/sec.1314
11. Feamster, N. (2010). Outsourcing home network security. Proceedings of the 2010 ACM SIGCOMM Workshop on Home Networks, HomeNets '10, Co-Located with SIGCOMM 2010. https://doi.org/10.1145/1851307.1851317
12. Felix, A., Borges, N., Wu, H., Hanlon, M., Birk, M., & Tschersich, A. (2014). Multi-layer SDN on a commercial network control platform for packet optical networks. Optics InfoBase Conference Papers. https://doi.org/10.1364/ofc.2014.th5a.1
13. Fu, Y., Li, C., Yu, F. R., Luan, T. H., Zhao, P., & Liu, S. (2023). A Survey of Blockchain and Intelligent Networking for the Metaverse. IEEE Internet of Things Journal, 10(4). https://doi.org/10.1109/JIOT.2022.3222521
14. Giotis, K., Argyropoulos, C., Androulidakis, G., Kalogeras, D., & Maglaris, V. (2014). Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments. Computer Networks, 62. https://doi.org/10.1016/j.bjp.2013.10.014
15. Hassan, H. A., Hemdan, E. E., El-Shafai, W., Shokair, M., & El-Samie, F. E. A. (2023). Intrusion Detection Systems for the Internet of Things: A Survey Study. Wireless Personal Communications, 128(4). https://doi.org/10.1007/s11277-022-10069-6
16. Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012). OpenFlow random host mutation: Transparent moving target defense using software-defined networking. HotSDN'12 - Proceedings of the 1st ACM International Workshop on Hot Topics in Software Defined Networks. https://doi.org/10.1145/2342441.2342467
17. Jayakody, D. N. K., Srinivasan, K., & Sharma, V. (2019). 5G-enabled secure wireless networks. In 5G Enabled Secure Wireless Networks. https://doi.org/10.1007/978-3-030-03508-2
18. Jin, R., & Wang, B. (2013). Malware detection for mobile devices using software-defined networking. Proceedings - 2013 2nd GENI Research and Educational Experiment Workshop, GREE 2013. https://doi.org/10.1109/GREE.2013.24
19. Kampanakis, P., Perros, H., & Beyene, T. (2014). SDN-based solutions for Moving Target Defense network protection. Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, WoWMoM 2014. https://doi.org/10.1109/WoWMoM.2014.6918979
20. Kukliński, S., & Chemouil, P. (2014). Network management challenges in software-defined networks. IEICE Transactions on Communications, E97-B(1). https://doi.org/10.1587/transcom.E97.B.2

21. Li, S., Xu, L. Da, & Zhao, S. (2018). 5G Internet of Things: A survey. In Journal of Industrial Information Integration (Vol. 10). https://doi.org/10.1016/j.jii.2018.01.005
22. Lien, S. Y., Tseng, C. C., Moerman, I., & Badia, L. (2019). Recent Advances in 5G Technologies: New Radio Access and Networking. In Wireless Communications and Mobile Computing (Vol. 2019). https://doi.org/10.1155/2019/8202048
23. Liu, B., Han, C., Liu, X., & Li, W. (2023). Vehicle Artificial Intelligence System Based on Intelligent Image Analysis and 5G Network. International Journal of Wireless Information Networks, 30(1). https://doi.org/10.1007/s10776-021-00535-6
24. Marie, O. A. (2023). An Intelligent Security System for Commercial Establishments Based on the Internet of Things (IoT). International Journal of Intelligent Systems and Applications in Engineering, 11(11s).
25. Mazhar, T., Irfan, H. M., Haq, I., Ullah, I., Ashraf, M., Shloul, T. Al, Ghadi, Y. Y., Imran, & Elkamchouchi, D. H. (2023). Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques: A Review. Electronics (Switzerland), 12(1). https://doi.org/10.3390/electronics12010242
26. Nikaein, N., Chang, C. Y., & Alexandris, K. (2018). Mosaic5G: Agile and flexible service platforms for 5G research. Computer Communication Review, 48(3). https://doi.org/10.1145/3276799.3276803
27. Rahman, M. A., & Pakstas, A. (2023). Tools and Techniques for Teaching and Research in Network Design and Simulation. SN Computer Science, 4(3). https://doi.org/10.1007/s42979-023-01684-6
28. Ravindran, R., Chakraborti, A., Amin, S. O., Azgin, A., & Wang, G. (2017). 5G-ICN: Delivering ICN Services over 5G Using Network Slicing. IEEE Communications Magazine, 55(5). https://doi.org/10.1109/MCOM.2017.1600938
29. Tang, D., Wang, S., Liu, B., Jin, W., & Zhang, J. (2023). GASF-IPP: Detection and Mitigation of LDoS Attack in SDN. IEEE Transactions on Services Computing. https://doi.org/10.1109/TSC.2023.3266757
30. Turner, S. W., Karakus, M., Guler, E., & Uludag, S. (2023). A Promising Integration of SDN and Blockchain for IoT Networks: A Survey. IEEE Access, 11. https://doi.org/10.1109/ACCESS.2023.3260777
31. Zhang, Z., Chai, X., Long, K., Vasilakos, A. V., & Hanzo, L. (2015). Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection. IEEE Communications Magazine, 53(5). https://doi.org/10.1109/MCOM.2015.7105651