International Journal of Advanced Multidisciplinary Application | IJAMA
Volume 2 Issue 11 November 2025
ISSN No: 3048-9350

A Comprehensive Analysis of Security Mechanisms in 5G Communication Systems

[1]Kamaldeep Kaur, [2]Sabhyata Uppal Soni, [3]Sarpreet Kaur
[1]Research Scholar, UIET, Panjab University, Chandigarh, India
[2,3]Assistant Professor, UIET, Panjab University, Chandigarh, India

Abstract
Wireless communication systems have been at risk of security attacks right from the very beginning. The first-generation wireless networks saw mobile phones and wireless channels as targets for illegal cloning and masquerading. The second generation of wireless networks was characterized by message spamming that became common not only for pervasive attacks but also injecting false information or broadcasting unwanted marketing information. Almost every security threat in 5G networks uses LTE weaknesses as a loophole. Some of them are illegal data consumption, target-type network device denial of service (DoS), information leaks, and audio eavesdropping. The various schemes to improve security of 5G network is proposed in the previous years. In this paper, various many techniques are analysed which in terms of certain parameters which can improve security of 5 G network.
Keywords:
Security Analysis, 5G, LTS, Software defined networks

1. Introduction

The idea of 5G mobile networks is to deploy node stations with advanced units, constant QoS, ultra-low latency, and super-fast data rates and coverage. Providing networking, service, storage, and processing are the technical innovations that are required for the service deployment of 5G technology to be realized. Operators can effectively manage data, services, and apps via cloud computing without having the necessary infrastructure. Consequently, mobile clouds that implement the same principles will bring together technologically heterogeneous systems into a single domain where various services can be executed to enhance flexibility and availability while reducing operating and capital expenses (CapEx and OpEx) respectively.Softwarizing the network functions will thus mean cloud computing will be easily portable and flexible to different kinds of networking systems and services.Software Defined Networking (SDN) is a technology that employs network function softwarization by directing the control and information data transmission separately. SDN gives a new dimension to networking by presenting an abstraction layer, but at the same time it makes the management of the network easier. Network Function Virtualization (NFV) is the enabler for placing various network functions in different network peripheries as per the demand and service-specific [1] hardware is not any more required. SDN and NFV, which are perfect complements to each other, are thus the most vital for the future networks as they are making the network elastic, simplifying the network control and management, breaking the vendor's proprietary solutions barrier, and so on.However, it should be noted that even with these innovative technologies and ideas, network security and user privacy are still major issues that need to be solved for the future of networks. Wireless communication systems have been at risk of security attacks right from the very beginning. The first generation (1G) wireless networks saw mobile phones and wireless channels as targets for illegal cloning and masquerading. The second generation (2G) of wireless networks was characterized by message spamming that became common not only for pervasive attacks but also injecting false information or broadcasting unwanted marketing information. The third generation (3G) wireless networks had IP-based communication that allowed the transfer of Internet security susceptibilities and issues to the wireless areas.Fourth Generation (4G) mobile networks were

the leap that made smart devices, multimedia traffic, and new services a part of the mobile domain that ever-increasing need of IP-based communication. The risk panorama turned out to be more dynamic and interactive due to this development. The dynamic nature of the 5G networking technology will provide a multiplied number of security threats and privacy concerns we have never faced before. Therefore, it becomes crucial to highlight the security risks concerning mobile networks which arise from their wireless nature as well as the different technologies which will play an essential part in 5G [2].

1.1 Key Security Challenges in 5G

Crucial infrastructure supported via 5G networks are at a risk to the security of both the electricity and society. As an example, the internet power supply systems could be hacked which would cause the disruption of electrical and electronic systems which are vital to society. In addition, we know that data is needed for the decisions, but what if that data gets corrupted during transmission over the 5G networks [3]. Therefore, it is important to consider, point out, and discuss the main security risks of 5G networks and also give a short overview of possible solutions that can lead to safe 5G systems.Almost every security threat in 5G networks uses LTE weaknesses as a loophole. Some of them are illegal data consumption, target-type network device denial of service (DoS), information leaks, and audio eavesdropping. One can distinguish wireless network security threats from core network security risks through an attack tree diagram, as shown in Figure 1.

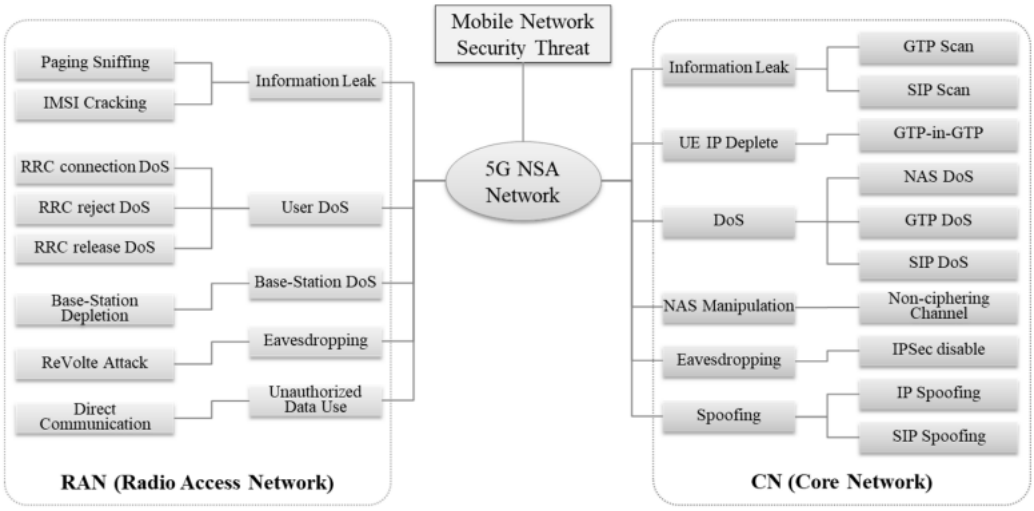

Figure 1: 5G attack tree

1.1.1 Types of RAN Security Threats

1. Type.R1. Information Leak: This attack exploits paging messages to obtain sensitive data such as S-TMSI and IMSI. By analyzing the paging cycle and inserting IMSI (international mobile subscriber identity) candidates, attackers can capture the victim's IMSI using software-defined radio (SDR) and paging sniffing techniques.

2. Type.R2. User DoS: RRC (Radio resource control) connection DoS attacks hurt the S-TMSI (SAE-temporary mobile subscriber identity) of victims, making them unable to use the airwaves because of sending RRC connection requests repeatedly. In this way, the victim's gadget is compelled to prolong disconnection almost indefinitely, leading to the non-accessibility of regular services.

3. Type.R3. Base-Station DoS: Attackers make it difficult for a base station to operate properly by bombarding it with RRC connection requests. These requests are sent using a randomly generated IMSI (international mobile

subscriber identity) of the victim, thus, depleting the resources of the base station and interfering with normal operations. Consequently, this results in the shortage of resources and the denial of services [4].

Type.R4. Eavesdropping: A repeatDRB ID (Data Radio Bearer ID) by an attacker is used to extract keystream from a voice call by the comparison of the ciphered and the plain texts of the subsequent calls. This enables to the discovery of already delivered calls, and thus the victim's voice communication is rendered unsecure.

5. Type.R5. Unauthorized Data Use: The two bearers, default bearer, and dedicated bearer, which are created in a terminal, can only be used for allowed purposes. However, the attacker may use them in a way that differs from the original intention and, therefore, use the data without permission. A dedicated bearer might be utilized to convey data communication among terminals, without incurring any communication fees. This, in turn, would result in charges for the service provider. Most importantly, caller spoofing can also be achieved via direct communication if utilized correctly [5].

1.1.2 Types of Core Network Security Threats

1. Type.C1. Information Leak: The GTP (GPRS tunneling protocol) and SIP (session initiation protocol) protocols are insecure and can be exploited by the attackers to obtain the sensitive information exchanged between the equipment of the EPC (Evolved packet core) and IMS. By injecting the packets and applying the tools like Packit, they can even find out the IP addresses of the core network equipment such as PGW (Packet Gateway) by using the GTP-C messages.

2. Type.C2. IP Depletion: Through the use of GTP-in-GTP packet injection, hackers can use a core network's IP pool by pushing GTP-C Create Session Requests with more than one IP. As a result, terminals unable to acquire IP addresses are affected and thus communication fails [6].

3. Type.C3. DoS: Attackers utilizing continuously sent attach-request messages via botnets, cause a huge traffic on 5G NSA. One attach request can trigger up to eight GTP-C messages, causing a significant traffic load on the core network.

4. Type.C4. NAS Manipulation: Attackers can deploy inebriate base stations to trick NAS attach-request messages. Through manipulating the UE network capability field, they will be able to reduce or even turn off encryption, thereby making the terminal more susceptible to attacks.

5. Type.C5. Eavesdropping: By using secret menus on 5G terminals, the attacker can turn off the IPSec settings, thus, resulting in the communication being unencrypted. If NAS (non-standalone) manipulation is used with the latter, then attackers can overhear and eavesdrop on the victim's voice traffic.

6. Type.C6. Spoofing: Attackers can conduct IP spoofing by altering data traffic IP addresses, causing invalid charges or DoS attacks. Attackers can use SIP (session initiation protocol) and MMS spoofing for voice phishing by making the outgoing number look different in the SIP packet header [7].

1.2 5G Security Overview

The 5G core network (5GCN), a combination of SDN, NFV (network function virtualization), distributed systems, and cloud computing, is a complicated system due to the convergence of the new technologies. The architecture of the 5GCN is a service-based and dynamic one, which is adjusting to the needs of both consumers and operators. However, by the incorporation of new technologies, the 5GCN is correspondingly becoming more vulnerable to cyberattacks as it inherits weaknesses of each of these technologies.

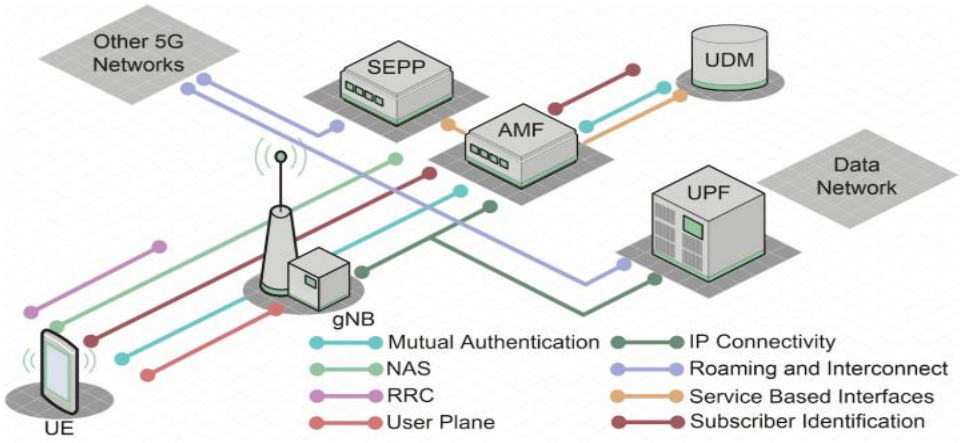

Figure 2: 5G Security Overview

Figure 2 shows the various functions of the network that make the 5G network more secure in general. In the image a number of components are depicted which are the ones involved in providing security for the 5G network. The first step in the authentication procedure is mutual authentication that is implemented in both 5G and older technologies. The user equipment (UE) and the Access and Mobility Management Function (AMF) are the parties involved. Unified Data Management (UDM), which keeps the information that is related to the identification of the UE, is also very important in the process [8]. The encryption and integrity protection features that 5G offers can protect many signaling types such as RRC, NAS (non-access stratum), and User Plane traffic. The security of signaling messages sent UE/gNB and AMF, are guaranteed by the identity verification of the sender and the receiver, as well as encryption, which also makes sure that the message is not tampered with during its transit. The potential for confidentiality protection via encryption is optional and not activated by default for any of the signaling use cases. However, integrity protection in NAS and RRC signaling is mandatory and cannot be disabled.

The UE, or user equipment, when roaming in the 5G networks, moreover, is the very thing that is guaranteeing the session stays active between the different 5G networks. New components and additional network functions make their way into the picture other than the interaction of the UE and AMFs; hence, the security edge protection proxy (SEPP) and user plane functions (UPFs) are the main components that provide protection for roaming and inter-connections. Moreover, there is IP connectivity that links the RAN to the core. In specific circumstances, this connection is actually owned by a third-party service provider and not the mobile service provider, in such a case the traffic can be protected through technologies like IPSEC [9].To sum up, OAuth 2.0 along with the required transport layer security can be applied to secure the service-based interfaces. This enables you to control which network functions have the authorization to access the services granted by other network functions. In the end, 5G usually applies a temporary ID known as the 5G Global Unique Temporary Identifier (GUTI) for the protection of subscriber identification. Nevertheless, if the UE has to transmit its IMSI through the radio network, that can be made secure by using asymmetric encryption, commonly referred to as SUCI (Subscriber Concealed ID) as well.

1.2.1 Fundamental Methods for Protecting 5G

Following is the description of the fundamental methods of protecting 5G environment.

1. Network Functions Virtualization NFVs and Network-Slicing: To support the 5G core, RAN, and MEC, the 5G Service-Based Architecture (SBA) is critically dependent on Network Functions Virtualization (NFV) technology. NFV turns the physical hardware into a shared resource that can perform functions like Open RAN (ORAN) and Cloud RAN (CRAN) as if it were a virtualized environment. The management and orchestration of these virtual

resources are the responsibilities [10] of NFV Management and Orchestration (MANO). Besides, network slicing allows the separation of multiple slices for various services, e.g., mobile broadband or latency-critical industry applications, by modifying control and user plane network operations according to individual users or companies' requirements.

2. Mutual Authentication: Mutual authentication was first introduced in 3G because it became obvious that the 2G algorithms had authentication flaws. This is by all means, an already existing near-5G technology. Nevertheless, in the case of 5G, a device first verifies that the network it is about to connect to is not fake and then responds to any security issues posed by the network. The device sends a response to the security challenge right after the network verification and allows the core network to check if the device is really legitimate.The AUSF (Authentication Server Function) is a vital component for achieving mutual authentication and key agreement processes, as it acts as an intermediary between AMF and UDM to acquire security information from UDM. In the first place, authentication confirmation is usually performed between the UE and AMF. The fact that the secret key of the device is stored at both the UDM and the UE enables the UDM to generate the 5G authentication vector using symmetric keys. Initially, the mutual authentication process along with the creation of the authentication vector is the first step before carrying out any other security measures in 5G. Figure 3 depicts this procedure of mutual authentication.

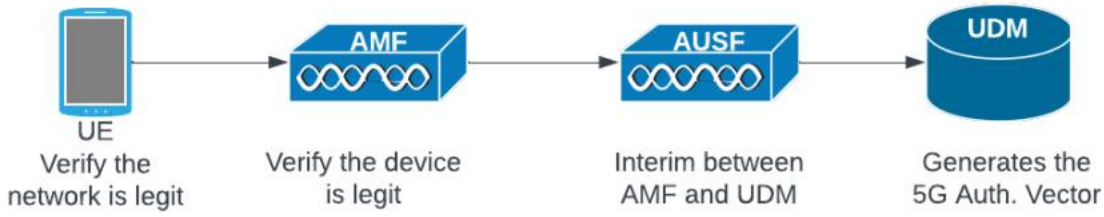

Figure 3: Mutual Authentication

3. Encryption and Integrity: As far back as the 2G, encryption and integrity check have been in place. 5G has included these functionalities for RRC, NAS, and user data plane signalling communications, in addition to other kinds of signalling messages. The UE and AMF now reveal the keys that are essential for the encryption and decryption of these signals during the 5G mutual authentication and key agreement process. Later on, these keys are disseminated all over the system wherever necessary. However, there are some disparities in the encryption standards of these message signalling systems [11].

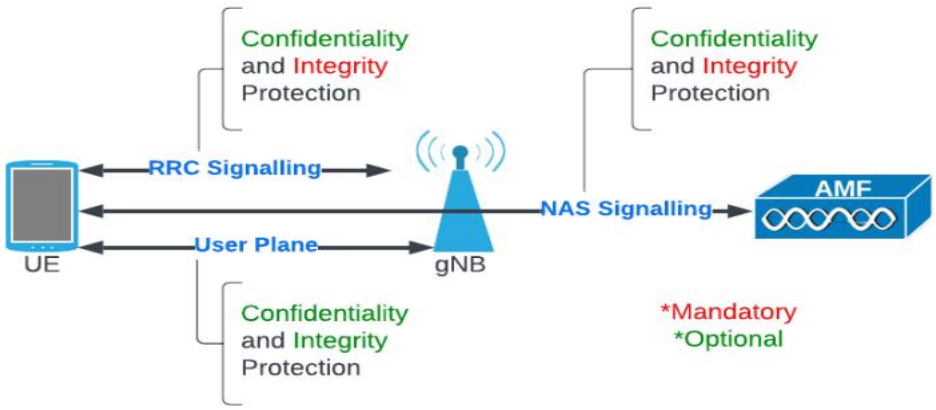

Figure 4: Encryption and Integrity

Figure 4 shows the fact that for RCC and NAS signaling messages, encryption is an optional means of protection, while integrity checking on the other hand is indispensable. For user-plane traffic, both encryption and integrity checking are optional, depending on the type of device that is connecting to the radio network and whether the encryption is necessary. In a way, the implementation of encrypting signaling messages between the user's device and network functions for confidentiality can act as a safeguard against man-in-the-middle (MITM) attacks and also against fake base station threats such as Stingray or IMSI catchers [12].

4. Service based interface protection: There are two main ways to secure 5G service-based interfaces. The first one is about protecting the protocol stack by using Transport Layer Security (TLS), which is a transport layer security protocol, between HTTP/2 and TCP. The TLS version must be 1.2 or higher. 3GPP has also clearly defined the cipher suites for TLS which are used to guarantee integrity as well as confidentiality of messages in transit. The second option is OAuth 2.0, which does not secure traffic in transit but rather protects service producers from malicious consumers who may try to invoke services with harmful requests.

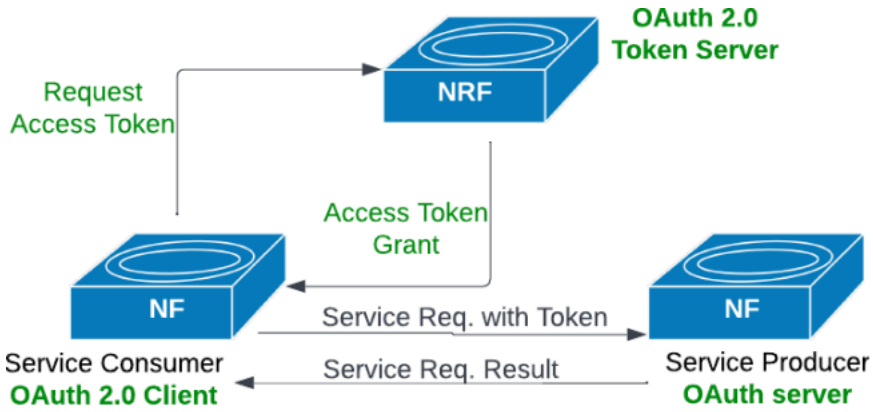

Figure 5: OAuth Token Based Authentication

OAuth 2.0 process is shown in Figure 5, which is between the service consumer and provider. OAuth 2.0 is a token-based authentication technique in which the network repository function [13] is the token server of the OAuth 2.0. A function on the network acting as a client invariably seeks an access token from the OAuth 2.0 server to access a particular service. These tokens can be limited to a certain category of network functions or very detailed so that only a specific service or operation can be executed. First, the server checks the authenticity of the token and then it gives the access. The two methods of security, TLS and token-based authentication, are used optionally.

5. Roaming and inter-connections security: Often, however, the connectivity between visited Public Land Mobile Networks (PLMN) and home PLMN is not direct. The exchange of traffic among these PLMs is mostly done via an IP Packet Exchange (IPX) provider, a third-party connection service, which the mobile operator does not own. Therefore, safeguarding traffic between these networks is a key factor. In a service-oriented architecture, this security is done by the Security Edge Protection Proxy (SEPP) service, which takes care of the control plane traffic. SEPP is the interface that provides functions such as topology hiding to obscure the sensitive addressing information, message filtering for the specific signaling messages, and traffic policing for the management of the traffic streams [14].

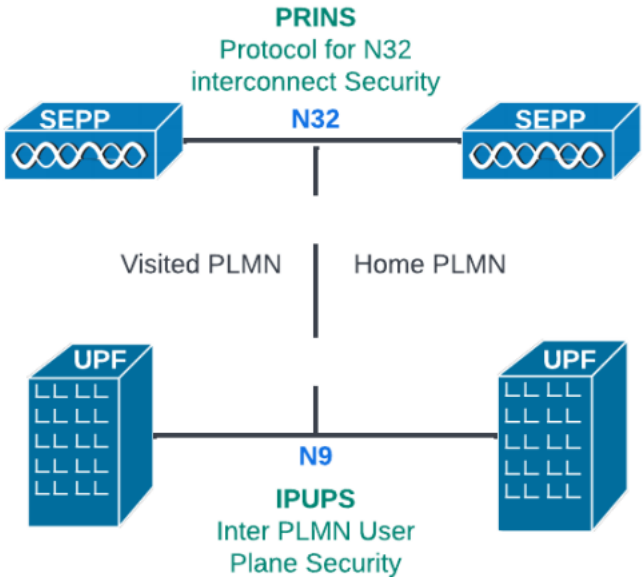

Figure 6: Roaming and inter-connections security

SEPPs, using the N32 protocol, an improvement over the 4G S6a protocol, are connected as illustrated in Figure 6. It uses TLS protection under HTTP/2 with some parts of the message optionally secured via PRINS (Protocol for N32 Interconnect Security), thus allowing protection of some parts and leaving the rest open for end-to-end routing in the interconnected network. For User Plane Function (UPF), Inter PLMN User Plane Security (IPUPS) is the used protocol which offers N9 protocol connectivity between UPFs. No traffic passes across N9 unless a pre-configured GTP v1-u tunnel is established, hence, preventing unauthorized or malicious traffic between UPFs when no tunnel is available. Moreover, both UPF should be informed about the exchanged traffic [15].

6. Subscriber Identity protection: 5G networks leverage a mechanism referred to as Subscription Concealed ID (SUCI) which ensures that user devices (UE) do not send clear text IMSI (Subscription Permanent ID (SIP) in 5G). The UE encrypts the Mobile Subscriber Identification Number (MSIN) using a public key provided by the 5G network. This SUCI is the result of IMSI being transformed into SUCI via encryption. The Mobile Country Code (MCC) and Mobile Network Code (MNC) are remaining to streamline routing while protecting the MSIN.

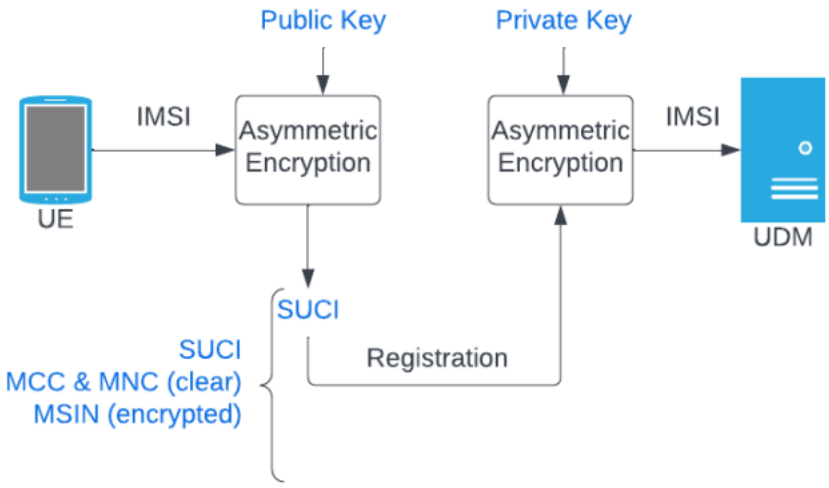

Figure 7: Subscriber Identity Protection

At the time of the registration process, the UE sends the SUCI to UDM, where it is decrypted by the corresponding private key to get IMSI. Nevertheless, including the encryption of the MSIN inside the SUCI is not an obligatory provision, and the encryption algorithm can be set to null, permitting the SUCI to be sent in clear text. Figure 7 shows the transfer process of SUCI from UE to UDM [16].

2. Literature Review

The deployment of 5G technology brings a lot of improvements in speed and connectivity but at the same time, new security challenges are also emerging. This literature review focuses on the current security solutions for 5G networks using blockchain-based frameworks, advanced cryptographic methods, and machine learning techniques. The purpose of the review is to show the way these solutions deal with the special risks that 5G networks have and their effects on the future deployments.

2.1 Blockchain-based Security Solutions for 5G Networks

M. S. P. Durgarao, et al. (2024) presented a novel blockchain -based security architecture designed to address the challenges of securing 5G WSN (Wireless Sensor Networks) [17]. The system leveraged cryptography, smart contracts, and decentralized consensus protocols to manage the uncertainty and resource constraints of wireless sensor networks. The analysis showed that this approach improved the overall security of 5G wireless sensor networks. The solution proved effective in reducing security risks and vulnerabilities, and advanced the understanding of secure communication in the 5G era. The findings paved the way for future research and practical applications of integrating blockchain technology with 5G-enhanced wireless sensor networks.

S. Wijethilaka, et al. (2024) developed a new method to solve the security issues related to authentication and authorization in 5G network slicing systems [18]. The framework included a blockchain-based multi-party decentralized credential management system with a secure communication protocol that utilized elliptic curve cryptography to facilitate multi-person single-round services. They also proposed a permissioned blockchain-based NF framework to solve the vulnerabilities related to the NF. They implemented this framework using the Hyperledger Fabric blockchain and Java chaincode, and extensive tests were conducted to demonstrate its effectiveness. It attempts to solve issues such as reduced points of failure compared to traditional and blockchain-based authorization units, verified the creation time of certificates, and investigated the ability to block against private authorizations. They also verified the security of the framework using informal and formal methods, including ROR (Real-Or-Random) logic and the Scyther verification tool.

S. M. Karim, et al. (2023) proposed and evaluated a novel BSDCE-IoV (Blockchain-Based Secure Data Collection and Exchange Scheme for IoV) using ECC (Elliptic Curve Cryptography) in a 5G environment [19]. This solution was designed to solve many challenges affecting the connected car. They verified its security and confidentiality through informal security checks as well as quality checks using real or random oracle samples and Scyther tools. Additionally, they measured the computational and communication overhead using the MIRACL (Multi-precision Integer and Rational Arithmetic Cryptographic Library). Compared to several current secure telematics methods, our BSDCE-IoV proposal performs best in terms of security, performance, and latency.

E. S. Babu, et al. (2023) proposed a blockchain system to tackle the limitations of integrating Edge Computing, IoT, and 5G networks by offering a trusted solution for edge-based 5G networks [20]. The proposed blockchain system efficiently identified and authenticates edge devices while provided address to them on demand. Additionally, it also ensured secure communication between these devices, protecting against DDoS and side-channel attacks.

Table 1 Comparative analysis of Blockchain-based Security Solutions for 5G Networks

Author & Year	Technique used	Performance parameters	Simulation Tool Used	Findings	Limitations
M. S. P. Durgarao, et al. (2024)	Blockchain-based security architecture, cryptographic techniques, smart contracts, decentralized consensus protocols	Enhanced security, reduced security risks and vulnerabilities	Not specified	Significantly improves overall security stance in 5G-enabled WSNs	No practical implementation or real-world testing performance.
S. Wijethilaka, et al. (2024)	Blockchain-based multi-party distributed certificate management using elliptic curve cryptography	Mitigation of single-point failure, time analysis for certificate generation	Hyperledger Fabric blockchain with Java chain codes	Secure framework for 5G network slicing, mitigation of NF sharing vulnerabilities, verified with formal/informal mechanisms	Experiments conducted were focused on authorization attacks, and limited practical deployments tested
S. M. Karim, et al. (2023)	Blockchain-based secure data collection and exchange scheme using Elliptic Curve Cryptography	Security, privacy, functionality, time delay	MIRACL, Real-or-Random oracle model, Scyther validation tool	Superior performance in terms of security and time delay in IoV security compared to existing approaches	High computational and communication overhead not fully optimized
E. S. Babu, et al. (2023)	Trusted blockchain system for edge-based 5G networks	Protection from DDoS and side-channel attacks, device authentication	Not specified	Secure communication among edge devices, eliminates limitations of integrating Edge Computing, IoT, and 5G networks	No mention of practical deployment or scalability concerns

2.2Artificial Intelligence and Machine Learning for 5G Security

A.Qasem, et al. (2024) introduced DTDD (distance-time directional delay) model to detect MITM attacks in various scenarios and situations [21] . This work examinedInH (Indoor hotspots) and UMi (urban micro-cellular) environments to evaluate its reliability using real 5G mmWavearrangements and formations. Simulations were performed using the millimeter wave 5G channel simulator tool NYUSIM along with ML (machine learning) algorithms including (XGBoost) extreme gradient boosting and (LGBM) light gradient boosting machine which formed the basis of the scheme. The results showed that the detection accuracy in InH condition was close to 100%, while the detection accuracy in UMi condition was close to 99%.

N. A. E. Kuadey, et al. (2022) presented DeepSecure, a framework that utilized LSTM (Long Short-Term Memory) deep learning techniques to distinguish between DDoS attacks from normal UE (user equipment) network traffic[22]. This framework also provided the correct connection path UE request. This comparative analysis with existing machine learning and deep learning methods in the literature showed that DeepSecure

outperforms these approaches. Specifically, the experiments showed that DeepSecure achieved a DDoS attack detection accuracy of 99.970% and an accuracy of 98.798% in predicting the appropriate network slice for legitimate UE requests.

T. Le, et al. (2022) highlighted the necessity to develop mechanisms to enhance the security of existing 5G networks and manage their privacy features to make them suitable use for IoT [23]. Their first reviewed was actual trust management and privacy preservation methods commonly used in IoT network communication. Then, they proposed an AI (artificial intelligence) based service that aim to solve the common challenges of privacy preservation and reliable communication in 5G IoT networks, an area neglected in current research. Finally, they discussed the future directions and related trust and privacy issues that need to be addressed in 5G IoT networks.

S. Rathore, et al. (2021) investigated the design and development of new services and services in 5G IoT. They proposed a 5G IoT security framework that combined DL (Deep Learning) with blockchain technology [24]. The framework used deep learning for intelligent data analysis and blockchain to ensure data security. They propose a set of frameworks in which deep learning and blockchain work at four layers: cloud, cloud, edge, and users. To verify its practical application, they simulate the framework using a wide range of search engines. Simulation results showed that the framework meets the design and development requirements in the 5G-enabled IoT environment, including scalability, reliability, performance, QoS, operational complexity, security and privacy, and QoE.

Table 2 Comparative analysis ofArtificial Intelligence and Machine Learning for 5G Security

Author & Year	Technique used	Performance parameters	Simulation Tool Used	Findings	Limitations
A. Qasem, et al. (2024)	Distance-Time Directional Delay (DTDD) model, machine learning (XGBoost, LGBM)	Detection accuracy in InH and UMi environments	NYUSIM 5G mmWave channel simulator	Detection accuracy approaching 100% for InH and 99% for UMi environment	Focused on MITM attacks; other 5G security threats not addressed
N. A. E. Kuadey, et al. (2022)	DeepSecure framework based on LSTM deep learning for DDoS detection and network slice assignment	Detection accuracy (99.970%), slice prediction accuracy (98.798%)	Not Specified	High accuracy in detecting DDoS attacks and assigning appropriate network slices	Simulation tool not mentioned; only tested for DDoS attacks
T. Le, et al. (2022)	AI-aided framework for privacy-preserving and trustworthy communication in 5G-enabled IoT	Trust management, privacy preservation, computational complexity	Not specified	Developed an AI framework for enhancing trust and privacy in 5G-enabled IoT networks	No simulation results provided; focuses only on trust and privacy challenges
S. Rathore, et al. (2021)	Deep Learning (DL) and blockchain-empowered security framework for 5G-enabled IoT	Scalability, reliability, QoS, computational complexity, security	MS COCOdataset containing 82,783 training instances and 40,504 validation instances of 80 different object classes	Demonstrated feasibility of DL-blockchain framework for secure 5G-enabled IoT, ensuring performance and privacy	Focuses only on security aspects; further real-world testing needed

2.3 Cryptography based Security solutions for 5G

Z. G. Al-Mekhlafi, et al. (2024) Introduces a 5G-supported vehicular fog network for anonymous authentication that utilized lattice-based cryptography to defend against quantum attacks. It operated on a 5G base station and integrates a TAs (trusted authorities) and a cloud server to manage vehicle authentication and facilitate anonymous reporting [25]. The TA was responsible for managing traffic and user-specific operations. This process, verified using ProVerif, protects data related to users, vehicles, and servers. The computational cost of signing was 0.3149 ms, the computational cost of data verification was 0.0724 ms, the computational cost of one verification was 0.0724 nm ms, and the communication cost of 18,448 bits. Although operating costs are low, transmission costs were high.

WojciechNiewolski, et al. (2023) proposed a new access control system that met the security requirements in transit and attrition for 5G MEC networks [26]. They first described its design and its main component, the MEC Enabler, which controlled access to security management and generated certificates (tokens). They described a way to protect packets during communication with services from MEC servers to prevent unauthorized. This protection measure prevented identification of packets connected to the protection service, as well as identifying information such as address and port number. Tests were performed in an experiment where the protection process was performed to prove that security solutions had a negative impact on the latency experienced by applications hosted by MEC.

O. Nait-Hamoud, et al. (2021) proposed to integrate the generic protocol that did not required multiple authentications for 5G multi-site/multi-tenant environments into a virtual cryptographic protocol, which should be a trusted location for the KGCs (Key Generator Center) [27]. The only assumption was that the KGC does not share shared keys. They used this new cryptocurrency algorithm in the integration, signature, and authentication key consensus scheme, and proved it based on new calculations on the Diffie-Hellman problem and bilinear stress assumptions in the random oracle model security against new models. they believe that this cryptographic technique could provide end-to-end security for multi-site/multi-tenant 5G management even with the integration of up to (n-1) KGCs.

B. Ying, et al. (2019) proposed a lightweight and untraceable authentication protocol for multiple server-based 5G networks by leveraging self-verifying public key cryptography based on elliptic curve cryptography to reduce complexity [28]. This solution improved efficiency by avoiding integration. They developed a good security model and proved that our method was secure against spoofing attacks based on the inequality logarithm problem and the Diffie-Hellman computation problem. Performance analysis showed that this scheme provided lower communication and computational overhead and also supported anonymous authentication sharing.

Table 3 Comparative analysis ofCryptography based Security solutions for 5G

Author & Year	Technique used	Performance parameters	Simulation Tool Used	Findings	Limitations
Z. G. Al-Mekhlafi, et al. (2024)	Lattice-based cryptography for anonymous authentication in vehicular fog systems	Computational cost: signing (0.3149 ms), batch verification (0.0724 ms), single verification (0.0724 ns), communication cost: 18448 bits	ProVerif	Low computational costs for authentication, but relatively higher transmission costs in the system	Higher transmission costs; focuses only on quantum attack resistance
WojciechNiewolski, et al. (2023)	New access control	Mathew Correlation	Testbed	Introduced a lightweight	Limited to MEC architecture; no

	architecture for 5G MEC using MEC Enabler for access control policies and token generation	Coefficient (MCC), Mean precision accuracy, F-measure, Detection Rate, Latency, and area under the Receiver Operating Characteristic (AUC		access control mechanism for 5G MEC with negligible impact on application delays	detailed analysis of large-scale deployment
O. Nait-Hamoud, et al. (2021)	Aggregation of Certificateless Public Key Systems in a 5G multi-domain/multi-tenant environment	Mean precision accuracy, F-measure, Detection Rate, Latency,	Not specified	Developed secure cryptosystem for multi-domain/multi-tenant 5G services, even in the case of collusion among KGCs	Assumes no more than (n-1) KGCs colluding; specific performance metrics not provided
B. Ying, et al. (2019)	Self-certified public key cryptography using elliptic curve cryptography (ECC) for mutual authentication	computational overhead and communication complexity	Not specified	Lightweight and untraceable authentication protocol for multi-server-based 5G networks; secure against forgery	No pairing operations; only theoretical validation and limited practical testing

Conclusion

In this paper it is concluded that, wireless communication systems have faced security risks since their inception. In the first generation of wireless networks, mobile phones and wireless channels were vulnerable to illegal cloning and identity masquerading. The second generation saw the rise of message spamming, which not only facilitated widespread attacks but also introduced issues like the injection of false information and the broadcasting of unwanted marketing messages. With the advent of 5G networks, many security threats exploit vulnerabilities from LTE, leading to risks such as illegal data consumption, denial of service (DoS) attacks on specific network devices, information leaks, and audio eavesdropping. Over the years, several schemes have been proposed to enhance 5G network security. This paper reviews and analyzes various techniques aimed at improving 5G network security, focusing on key parameters to assess their effectiveness.

References

[1] Y. Duan, Q. Wu, X. Zhao, and X. Li, “Mobile edge computing based cognitive network security analysis using multi agent machine learning techniques in B5G,” Computers & Electrical Engineering, vol. 117, pp. 109181–109181, Jul. 2024, doi: https://doi.org/10.1016/j.compeleceng.2024.109181.

[2] S. Gupta and Sonia, "An Analysis of Edge Computing with Multi Access in 5-G Technology," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 1641-1644, doi: 10.1109/ICACITE57410.2023.10183311.

[3] S. Wijethilaka, A. Kumar Yadav, A. Braeken and M. Liyanage, "Blockchain-Based Secure Authentication and Authorization Framework for Robust 5G Network Slicing," in IEEE Transactions on Network and Service Management, vol. 21, no. 4, pp. 3988-4005, Aug. 2024, doi: 10.1109/TNSM.2024.3416418

[4] T. Saha, N. Aaraj and N. K. Jha, "Machine Learning Assisted Security Analysis of 5G-Network-Connected Systems," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 2006-2024, 1 Oct.-Dec. 2022, doi: 10.1109/TETC.2022.3147192.

[5] A. K. Bhagat and J. Gandhi, "A Comprehensive Analysis of 5G Security Core Technologies and Services: Conceptual Frameworks, Challenges, and Solutions," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 1273-1281, doi: 10.1109/AISC56616.2023.10085449.

[6] M. A. Hasnat, S. T. A. Rumee, M. A. Razzaque and M. Mamun-Or-Rashid, "Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction," 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox'sBazar, Bangladesh, 2019, pp. 1-4, doi: 10.1109/ECACE.2019.8679326.

[7] S. Gupta, B. L. Parne and N. S. Chaudhari, "Security Vulnerabilities in Handover Authentication Mechanism of 5G Network," 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2018, pp. 369-374, doi: 10.1109/ICSCCC.2018.8703355.

[8] V. Adat Vasudevan, C. Tselios and I. Politis, "On Security Against Pollution Attacks in Network Coding Enabled 5G Networks," in IEEE Access, vol. 8, pp. 38416-38437, 2020, doi: 10.1109/ACCESS.2020.2975761.

[9] V. Adat, I. Politis, C. Tselios, P. Galiotos and S. Kotsopoulos, "On Blockchain Enhanced Secure Network Coding for 5G Deployments," 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, pp. 1-7, doi: 10.1109/GLOCOM.2018.8647581.

[10] A. Bozorgchenani et al., "Intrusion Response Systems for the 5G Networks and Beyond: A New Joint Security-vs-QoS Optimization Approach," in IEEE Transactions on Network Science and Engineering, vol. 11, no. 3, pp. 3039-3052, May-June 2024, doi: 10.1109/TNSE.2024.3358170.

[11] M. S. Siddiqui et al., "Policy based virtualised security architecture for SDN/NFV enabled 5G access networks," 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Palo Alto, CA, USA, 2016, pp. 44-49, doi: 10.1109/NFV-SDN.2016.7919474.

[12] R. Khan, P. Kumar, D. N. K. Jayakody and M. Liyanage, "A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196-248, Firstquarter 2020, doi: 10.1109/COMST.2019.2933899.

[13] WojciechNiewolski, T. W. Nowak, MariuszSepczuk, and Z. Kotulski, “Security architecture for authorized anonymous communication in 5G MEC,” Journal of Network and Computer Applications, vol. 218, pp. 103713–103713, Sep. 2023, doi: https://doi.org/10.1016/j.jnca.2023.103713.

[14] H. Sharma and N. Kumar, “Deep learning based physical layer security for terrestrial communications in 5G and beyond networks: A survey,” Physical Communication, vol. 57, p. 102002, Apr. 2023, doi: https://doi.org/10.1016/j.phycom.2023.102002.

[15] T. Madi, H. A. Alameddine, M. Pourzandi, and A. Boukhtouta, “NFV security survey in 5G networks: A three-dimensional threat taxonomy,” Computer Networks, vol. 197, p. 108288, Oct. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108288.

[16] G. Amponis et al., “Generating full-stack 5G security datasets: IP-layer and core network persistent PDU session attacks,” AEU - International Journal of Electronics and Communications, vol. 171, pp. 154913–154913, Nov. 2023, doi: https://doi.org/10.1016/j.aeue.2023.154913.

[17] M. S. P. Durgarao, D. Valluru, S. Saraswathi, P. Malathi, K. Thilagam and S. Loganathan, "A security framework for 5G-enabled wireless sensor networks based on blockchain technology," 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chikkaballapur, India, 2024, pp. 1-6, doi: 10.1109/ICKECS61492.2024.10617316.

[18] S. Wijethilaka, A. Kumar Yadav, A. Braeken and M. Liyanage, "Blockchain-Based Secure Authentication and Authorization Framework for Robust 5G Network Slicing," in IEEE Transactions on Network and Service Management, vol. 21, no. 4, pp. 3988-4005, Aug. 2024, doi: 10.1109/TNSM.2024.3416418.

[19] S. M. Karim, A. Habbal, S. A. Chaudhry and A. Irshad, "BSDCE-IoV: Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment," in IEEE Access, vol. 11, pp. 36158-36175, 2023, doi: 10.1109/ACCESS.2023.3265959

[20] E. S. Babu, A. Barthwal, and R. Kaluri, “Sec-edge: Trusted blockchain system for enabling the identification and authentication of edge based 5G networks,” Computer Communications, vol. 199, pp. 10–29, Feb. 2023, doi: https://doi.org/10.1016/j.comcom.2022.12.00

[21] A. Qasem and Ashraf Tahat, “Machine learning-based detection of the man-in-the-middle attack in the physical layer of 5G networks,” Simulation Modelling Practice and Theory, pp. 102998–102998, Jul. 2024, doi: https://doi.org/10.1016/j.simpat.2024.102998.

[22] N. A. E. Kuadey, G. T. Maale, T. Kwantwi, G. Sun and G. Liu, "DeepSecure: Detection of Distributed Denial of Service Attacks on 5G Network Slicing—Deep Learning Approach," in IEEE Wireless Communications Letters, vol. 11, no. 3, pp. 488-492, March 2022, doi: 10.1109/LWC.2021.3133479

[23] T. Le and S. Shetty, “Artificial intelligence-aided privacy preserving trustworthy computation and communication in 5G-based IoT networks,” Ad Hoc Networks, vol. 126, p. 102752, Mar. 2022, doi: https://doi.org/10.1016/j.adhoc.2021.102752.

[24] S. Rathore, J. H. Park and H. Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," in IEEE Access, vol. 9, pp. 90075-90083, 2021, doi: 10.1109/ACCESS.2021.3077069.

[25] Z. G. Al-Mekhlafi et al., "Lattice-Based Cryptography and Fog Computing Based Efficient Anonymous Authentication Scheme for 5G-Assisted Vehicular Communications," in IEEE Access, vol. 12, pp. 71232-71247, 2024, doi: 10.1109/ACCESS.2024.3402336.

[26] WojciechNiewolski, T. W. Nowak, MariuszSepczuk, and Z. Kotulski, “Security architecture for authorized anonymous communication in 5G MEC,” Journal of Network and Computer Applications, vol. 218, pp. 103713–103713, Sep. 2023, doi: https://doi.org/10.1016/j.jnca.2023.103713.

[27] O. Nait-Hamoud, T. Kenaza, and Y. Challal, “Certificateless Public Key Systems Aggregation: An enabling technique for 5G multi-domain security management and delegation,” Computer Networks, vol. 199, p. 108443, Nov. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108443

[28] B. Ying and A. Nayak, “Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography,” Journal of Network and Computer Applications, vol. 131, pp. 66–74, Apr. 2019, doi: https://doi.org/10.1016/j.jnca.2019.01.017.