5G Security Challenges & Solutions: A Comprehensive Survey

Sachin Mishra[1], Pragya Rathore[2]

[1,2] M.Tech CSE Scholars (specialization in Cyber Security)
[1,2] Department of Computer Engineering & Technology
Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra, India

Abstract: 5G technology offers faster connections than ever before, but it also poses a variety of new security vulnerabilities. 5G is expected to enhance user mobility, and facilitate ultra-reliable and cost-effective networking of a vast array of devices, including the Internet of Things (IoT). The primary technology accelerators, including Network Function Virtualization (NFV), Software Defined Networking (SDN), and cloud computing, are developing in preparation for their application in 5G. This paper describes the primary 5G security issues and provides workarounds for these problems. The challenges include network slicing vulnerabilities, a growing attack surface due to the growth of connected devices, insufficient mechanisms for authentication and authorization, and growing privacy concerns. Moreover, supply chain security, interference and jamming, and vulnerability to distributed denial of service (DDoS) attacks pose significant risks. Treatments include using blockchain technology, implementing a zero-trust architecture, and using AI-driven security measures. In this paper, we give a summary of the privacy concerns in 5G as well as the security challenges in these technologies. We also outline future directions for secure 5G systems as well as security solutions to these problems.

Keywords: Wireless Communication, Software Defined Networking (SDN), Network Function Virtualization (NFV), Cloud, Network Slicing, Distributed Denial of Service (DDoS)

I. INTRODUCTION

By implementing dense base stations with greater capacity, noticeably better Quality of Service (QoS), and incredibly low latency, 5G wireless networks are expected to provide exceptionally high data rates and wider coverage. Adoption of cutting-edge networking, service deployment, storage, and processing technologies is required to meet the anticipated services of 5G. Operators can effectively manage data, services, and applications with cloud computing without having to worry about maintaining the infrastructure. As a result, mobile clouds use analogous principles to combine many systems into a single domain, allowing for the deployment of several services for increased availability and flexibility, all at the same time saving on both capital expenditures (CapEx) and operating expenses (OpEx).

Improved flexibility and smooth transferability of networking systems and services are made possible by the softwarization of network functions. Network function softwarization is accomplished via Software Defined Networking (SDN), which introduces innovation and simplification to network administration by dividing the network control and data forwarding planes. The foundation for placing different network functions in different perimeters according to requirement is Network Function Virtualization (NFV), which removes the need for hardware tailored to individual services or functions. Jointly, SDN and NFV improve network elasticity, simplify network control and management, get around vendor-specific proprietary solutions, and are considered essential for networks of the future. Network security and user privacy still present major obstacles for networks in the future, notwithstanding recent developments.

Since the systems' beginnings, security flaws in wireless communication have existed. One of the main targets of unauthorized cloning and masquerade in 1G wireless networks was mobile phones and networks. In addition to being used for extensive attacks, message spamming also became popular during the 2G era for disseminating unsolicited marketing content and injecting fake information. Concerns and weaknesses related to Internet security have moved into the wireless domain with the introduction of IP-based communication in 3G wireless networks. The threat landscape became increasingly complex with the introduction of new services, multimedia traffic, and smart device proliferation in 4G networks. Concerns about privacy are likely to increase as 5G wireless networks become more prevalent and present new security threats.

II. LITERATURE REVIEW

- The study paper "5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey" by Mamoona Humayun, Bushra Hamid, NZ Jhanjhi, G.Suseendran, M N Talib, offers a thorough analysis of the security-related aspects of 5G networks. The issues faced by researchers and practitioners in this domain are highlighted in the study, which highlights the necessity for robust solutions and architecture to maintain the security and privacy of 5G networks. The article lists a number of difficulties, such as denial-of-service attacks on infrastructure and end-user devices, roaming security, flash network traffic, user plane integrity, security of radio interfaces, and signaling storms. The authors emphasize that in order to give 5G researchers and practitioners a thorough understanding, it is crucial to summarize the most important security issues, difficulties, and opportunities. The report also highlights the need for additional understanding of 5G prospects, problems, and major security risks, as well as mitigation strategies backed by actual case studies.
- The study "5G Security: Analysis of Threats and Solutions" by Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Ylianttila, Andrei Gurtovk offers a thorough examination of the security issues and possible fixes in 5G networks. Cloud computing, Software Defined Networking (SDN), and Network Function Virtualization (NFV) are among the key technology advancements that are making 5G possible. The concerns mentioned in the report include the requirement for security solutions to handle flash network traffic, potential privacy issues, and security threats and assaults in mobile clouds. The authors suggest using cutting-edge technologies like SDN and NFV to manage flash network traffic and improve network security more affordably as answers to these problems. In addition, it highlights the need of looking into and exposing the security issues in 5G networks and offers a summary of some possible fixes to create secure 5G systems.
- A thorough summary of the security issues and possible fixes related to 5G networks can be found in the research paper "5G Security Challenges and Solutions: A Review by OSI Layers". The review's writers, S. Sullivani, Alessandro Brighente, S. A. P. Kumar, have arranged it according to the OSI layers, giving readers an understanding of the particular protocols and architectures associated with each layer. Each OSI layer—application, presentation, session, transport, network, data link, and physical layers—is examined in detail with regard to security issues. In addition to discussing potential fixes, obstacles, and gaps, the paper discusses specific security risks and vulnerabilities for each layer. In order to defend against risks like data fabrication and eavesdropping, they emphasize the necessity for security measures that go beyond conventional cryptography techniques, especially at the physical layer. In order to achieve the design goals of 5G networks—which include higher connection, reduced latency, and high reliability—it highlights the necessity of comprehensive and effective security mechanisms.
- The research paper “5G Security Issues- A Compilation With Industry Insight” by Albert Severo & Téllez Martínez, focuses on identifying and prioritizing security issues in 5G technology. The author conducted a Delphi study and literature review to identify eight key issues, including virtualization, IoT and MTC, and network slicing. The paper also discusses the three pillars of 5G technology: Enhanced Mobile Broadband (eMBB), Massive Machine-Type Communication (mMTC), and Ultra Reliable Low Latency Communication (URLLC). The paper provides insights into the challenges and solutions for 5G security, including the need for secure network architecture, encryption, and authentication. The author also suggests that future research should focus on evaluating risk analysis methods and identifying new security issues as 5G technology continues to evolve.
- The study paper "A Review of Security Challenges and Solutions in 5G Network" by Sunil Kumar Shah, Snehal Jani, Rinkoo Bhatia, Neeta Nathani, offers a thorough synopsis of the issues surrounding 5G technology security. It highlights how important it is for 5G networks to have strong security measures in place because of the extraordinary rise in the quantity of devices and services as well as the expanding interest in the Internet of Things (IoT). Non-cryptographic security, unknown misbehaviors caused by attacks, smart Denial of Service (DoS) threats, frequency of handover, Distributed IP Mobility Management (DMM), defense against jamming attacks, and eavesdropping in Device to Device (D2D) communication are some of the challenges that are covered in the paper. The paper suggests several solutions to mitigate DoS attacks, including the use of Reinforcement Learning (RL) algorithms for intrusion detection systems, Security Operation Centers (SOC) to fend off DoS attacks, Distributed IP Mobility Management to provide effective and fault-tolerant solutions, and the deployment of RL algorithms to defend mobile devices and the 5G network against jamming attacks. The report also emphasizes how crucial new technologies are to addressing security issues in the 5G wireless network, including Software Defined Networking (SDN), Network Function Virtualization (NFV), and multiple input multiple output (MIMO).
- The goal of the research project "A survey on Cybersecurity in 5G" by Seyed Mohammad Mousavi, is to examine the security features of 5G technology and pinpoint any possible weak points or dangers. Papers from peer-reviewed journals, books, white papers, reports, and internet articles are among the many sources of pertinent literature that are studied and analyzed in this work. In order to safeguard our digital communications environment, the paper highlights the necessity for infrastructure equipment providers to focus more on the cybersecurity of 5G mobile

networks. The research problems pertaining to 5G security are addressed in the study, including potential attacks on 5G networks, existing methods for detecting cyberattacks, the minimal degree of cybersecurity that may be tolerated, and the most recent strategies for enhancing 5G network security. The status of 5G and its security in Italy are also covered in the report, along with some information regarding the impending 6G mobile communications generation and its associated security issues.

- The study "Mitigating 5G security challenges for next-gen industry using quantum computing" by Cherry Mangla, Shalli Rani, Nawab Muhammad Faseeh Qureshi, Aman Singh, explores the security issues that 5G networks have and suggests that quantum computing could be a viable way to address these issues and safeguard 6G networks in the future. The study underscores the necessity for quantum solutions to guarantee the security of next-generation industry networks and exposes the shortcomings of classical cryptography in addressing the security flaws of 5G networks. A number of significant issues have been noted about 5G networks, such as attacks on the infrastructure, user plane integrity, security of radio interface keys, required network security, and uniformity in subscriber level security rules. To solve the security problems in 5G networks and guarantee a safe transition to 6G networks, the suggested solution makes use of quantum concepts, such as quantum computing and quantum cryptography. In order to improve the security of 5G networks and establish the groundwork for future secure 6G networks, the study investigates the potential uses of quantum solutions, such as Quantum Key Distribution (QKD) and quantum walks.
- In addition to discussing the application of network slicing in 5G technology, the research paper "Network Slicing in 5G: Admission, Scheduling, and Security" by Raneem Jassim Alghawi addresses related issues and possible solutions. It explores the nuances of network slicing and how 5G networks' efficiency, security, and performance are affected by it. The study outlines the key specifications for 5G technology, which include scalability, low latency, and high data rates. For services like enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine type communication (mMTC), it highlights the necessity of high throughput, low latency, and energy efficiency. Furthermore included in the study are the 5G enabling technologies, like massive MIMO, beamforming, and full duplex, which are crucial for handling the growing network traffic and enhancing spectral efficiency. In addition, the paper discusses the difficulties in implementing network slicing in 5G, such as the requirement for a flexible architecture to facilitate low-latency communication, high scalability to support IoT services and autonomous vehicles, and effective resource allocation to prevent traffic from becoming unimportant.

III. WHAT IS 5G TECHNOLOGY?

5G refers to the fifth generation of mobile networks. Following the 1G, 2G, 3G, and 4G networks is a new worldwide wireless standard. In order to connect almost everyone and everything, including machines, objects, and gadgets, 5G enables a new type of network.

Massive network capacity, extremely low latency, faster multi-Gbps peak data rates, increased availability, and a more consistent user experience are all intended benefits of 5G wireless technology. Enhanced effectiveness and efficiency stimulate new user experiences and establish links with new industries.

4G technology can only reach a peak speed of 1 Gbps, whereas 5G technology can reach a theoretical peak speed of 20 Gbps. Lower latency is another benefit of 5G, which might enhance the efficiency of business apps and other digital activities (such online gaming, video conferences, and self-driving cars).

5G takes connectivity to the next level by giving customers connected experiences via the cloud, whereas previous generations of cellular technology (such 4G LTE) concentrated on assuring connectivity. Utilizing cloud technology, 5G networks are software-driven and virtualized.

With smooth open roaming between cellular and Wi-Fi connections, the 5G network will also make mobility easier. Without user involvement or reauthentication, mobile users can seamlessly transition between indoor wireless networks and outside wireless connections.

Improved performance is one of the characteristics that the new Wi-Fi 6 wireless standard, sometimes called 802.11ax, has in common with 5G. Better geographic coverage and reduced costs can be achieved by positioning Wi-Fi 6 radios where consumers require them. A sophisticated automated software-based network powers these Wi-Fi 6 radios.

In cities where demand may exceed current 4G technology's capability, as well as underserved rural areas, 5G technology should enhance connection. Along with having a dense, distributed-access design, new 5G networks will also relocate data processing closer to the edge and the users to allow for speedier data processing.

A. Network Architecture

The definition of a new generation of cellular technology is provided by the International Telecommunication Union about every decade. Fourth generation (4G) cellular technology is the one that is currently in use. In architecture, every

generation is distinct from the previous one. Hence, 5G, or fifth generation cellular technology, will differ from 4G in terms of architecture.
The kind of machinery and how it interacts with other machinery determine the differences in architecture. A huge cell-dense network makes up the architecture of 5G technology. It functions better and makes improvements over earlier generations.
It offers:

- Data transfer speeds of several gigabits per second
- allows for the support of a big number of network devices
- very low latency

B. 5G Core Features

A consortium of organizations known as the Third Generation Partnership Project, or 3GPP, establishes telecom standards. It states that the fundamental characteristics of 5G are:

- Modular
- Service-Oriented
- Reusable
- Self Contained

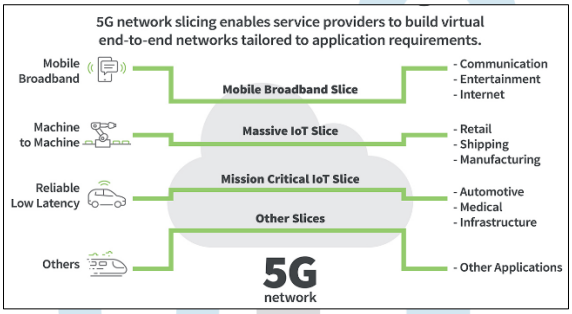

Fig 1: Features of 5G

The following characteristics that distinguish 5G wireless technology from earlier generations will also be present in its architecture.

- Its frequency range is broad, spanning from roughly 300 MHz to 300 GHz. Low frequencies work well for long-distance communication, whereas high frequencies are appropriate for heavily populated locations.
- Data from centralized data centers is brought closer to the end user with Multi-Access Edge Computing (MEC).
- A more open design is produced by virtualized network components, which separate hardware from software and include RAN.
- An improved Common Public Radio Interface, or eCPRI, will be used by 5G to lower network latency.
- Several logical networks on a single physical grid is known as "network slicing."
- Beamforming is the process of sending data via the most direct route to every user.

C. 5G Core Network Architecture

The 5G core architecture was created from the ground up by developers, with network functions divided based on the nature of the service. For this reason, it is also known as 5G core Service-Based architecture (SBA). The 5G core network architecture has the following features.

- User Equipment, or UE, connects to 5G New Radio (NR) via 5G smartphones or cellular devices. Next up are data networks, or DN (like the internet).
- For UEs, the Access and Mobility Management Function (AMF) is the sole point of entry.
- For a certain service, UE asks the AMF for it. For managing the user session, it chooses a Session Management Function (SMF) based on the service.
- Transporting IP traffic to and from the UE and the external network is the responsibility of the User Plane Function (UPF).
- In order for the UE to access 5G core services, AMF authenticates it using the Authentication Server Function (AUSF).
- The foundation for policy control that oversees network behavior is provided by all other services.

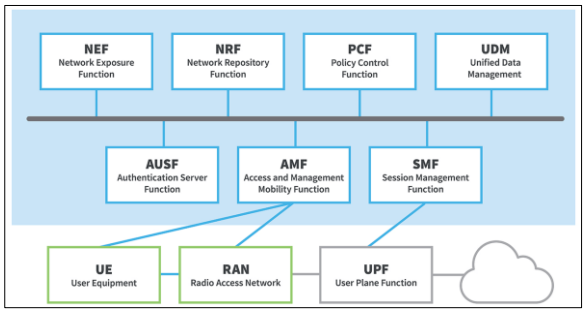

Fig 2: 5G Network Core Architecture

D. MIMO Technology

The fifth generation of mobile networks, or 5G, uses cutting edge technologies to provide wireless communication that is quicker and more dependable than that of its forerunners. MIMO, or multiple input/multiple output, is one of the core technologies of 5G.

MIMO stands for multiple input, multiple output, and it refers to the use of multiple antennas in a communication system at both the transmitter and the receiver ends. The main concept is to use numerous spatial streams to increase data transmission efficiency. This boosts the system's total data throughput by allowing it to send and receive numerous data streams at once.

MIMO technology is essential to 5G in order to achieve high data rates and enhance network performance. In the context of 5G, the following are some important MIMO points:

i. Spatial Multiplexing: Multiple data streams can be delivered concurrently using various antennas thanks to MIMO technology. This facilitates a faster pace of data transport.

ii. Beamforming: 5G networks employ beamforming, a MIMO-enabled technology, to target the signal toward the user rather than dispersing it throughout the space. Better coverage, stronger signals, and improved mobile device communication are all made possible by this.

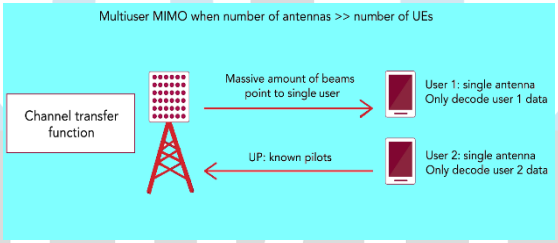

Fig 3: Wireless communication: MIMO Technology

iii. Massive MIMO: 5G frequently uses Massive MIMO, which calls for the base station to employ a huge number of antennas. This improves spectral efficiency and enables serving numerous customers at once.

iv. Enhanced spectrum Efficiency: The spectrum efficiency of the wireless communication system is enhanced by MIMO technology, which separates data streams spatially. This implies that faster data rates can be achieved by transmitting more data over the same amount of bandwidth.

v. Enhanced Capacity and Throughput: The overall throughput and capacity of the 5G network is greatly increased by the usage of MIMO. Supporting the expanding number of connected devices and the rising need for high-bandwidth applications requires this.

A key element of 5G networks, MIMO technology helps them to deliver higher capacity, better coverage, and quicker data rates. The issues brought about by the growing demand for mobile data and the variety of applications and devices in the 5G era are partially addressed by the employment of numerous antennas for simultaneous data transmission and reception.

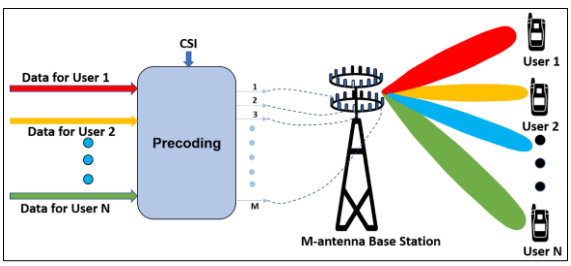

Fig 4: Massive MIMO System for 5G Network

IV. SECURITY THREATS EVOLUTION

In the 1980s, the first generation of mobile networks (1G) marked the introduction of telecommunication networks. Over the next forty years, these networks have grown to become the 5G. Originally designed as an analog network for voice-only communications and lacking in security measures, it now offers improved security and privacy guarantees along with ubiquitous connectivity for a variety of users. While providing new threat vectors as a result of newly deployed technologies, successive generations also served to mitigate the vulnerabilities of the preceding generations.

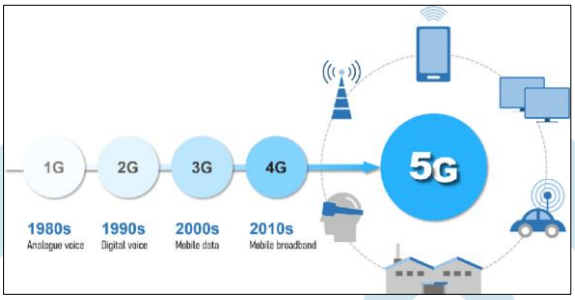

Fig 5: Evolution of Mobile Networks

A. 1G Security

With voice call services as its primary and only goal, the 1G network was primarily built on analog technologies. Only a few countries might be included in the scope. Other names for the 1G networks included Nordic Mobile Telephony (NMT) in Europe and Advanced Mobile Phone Systems (AMPS) in the USA. The maximum speed on the 1G network was 2:4 Kbps, and roaming and data network services were not included. It demonstrated a great deal of flaws, including inadequate capacity, careless handoffs, poor spectrum utilization, and poor voice call quality. It also didn't offer any security features that would have prevented unauthorized listeners from listening in on calls.

Because 1G networks were analog in nature, encryption was not possible, which made the security threat even more problematic. Because these connections were in clear text, an attacker may readily access other data, including the electronic serial number or mobile identification number, in addition to the phone conversation. An attacker could conduct impersonation attacks by cloning the phone and pretending to be the subscriber by taking note of these settings. The first security feature added in 1G was scrambling, which made it possible to prevent eavesdropping.

B. 2G Security

A decade after the introduction of 1G, 2G mobile networks added SMS messaging capabilities in addition to voice calls. Numerous technologies were introduced globally by 2G, including Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), North America Time Division Multiple Access (NA-TDMA), and Personal Digital Cellular (PDC). Additionally, mobile communications was the first to support email. The implementation of numerous security measures was made possible by 2G, which enabled the transition of mobile communications from the analog to the digital realm. Cryptography, in which secret keys were employed to encrypt traffic and ensure communication confidentiality, is credited for introducing authentication to mobile communications first. The Subscriber Identity Module (SIM) devices—physical devices that store a cryptovariable used in the authentication process—were introduced to verify the identities of the subscribers. Nonetheless, 2G was open to several assaults. One of the primary ways that attackers spread malicious content to victims was by spamming, for example.

Moreover, certain security solutions' design and implementation were improperly addressed. Cryptographic algorithms A5 and COMP128 are pertinent examples. Moreover, communications lines were considered secure and so not shielded from eavesdroppers, while GSM encryption was restricted to the radio interface. Due to the fact that SMS roaming left messages open to assault over the Internet, they were also susceptible to attacks.

C. 3G Security

A decade after the 2G was released, the 3G mobile network offered the benefit of Internet Protocol (IP)-based services. The quality of service provided by 3G advanced significantly, enabling features like enhanced voice quality and international roaming. High Speed Uplink/Downlink Packet Access (HSUPA/HSDPA), Universal Telecommunication Systems (UMTS), and Wideband CDM (WCDMA) were the primary technologies launched with 3G. The technologies that underpin mobile data services, including as Long-Term Evolution (LTE) and Fixed Worldwide Interoperability for Microwave Access (WIMAX), were launched with the transition from 3G to 4G, or 3.75G. Each and every vulnerability

found in 2G was taken into account and fixed by 3G security. The network access security, network domain security, user domain security, application security, visibility and configurability security, and application security were the five sets that made up the security architecture used in 3G communications.
Higher flexibility and the potential for extension to mitigate new risks that may be discovered after their implementation were also offered by the architecture of the 3G security features. The attack surface expanded in tandem with the number of devices connected to the network. As a matter of fact, there have been several reports of security threats aimed at the computer system, the phone of the user, and the operating system. These flaws included impersonation attacks, eavesdropping, and gaining authorization to access users' private information.
In addition to being restricted to the subscriber, impersonation could also be used to pretend to be a user or the network. Additional assaults including denial-of-service, man-in-the-middle, location update spoofing, and camping on an illusory base station.

D. 4G Security

The inclusion of a comprehensive and dependable IP-based solution in 4G enhanced the current network. Data and multimedia may be shared throughout the network because of the increased data rate over what the earlier generations had managed to achieve. Mobile TV, High Definition TV content, video chat, Digital Video Broadcasting (DVB), and Multimedia Messaging Service (MMS) were the primary technologies introduced with 4G. In addition to new cryptographic algorithms with enhanced key structures, 4G included the security measures required to counteract every attack discovered in earlier generations. Double the length of the keys used in 3G, the 256-bit keys employed in the primary algorithms presented were the EPS Encryption Algorithms (EEA) and EPS Integrity Algorithms (EIA).
An additional notable distinction from the preceding iterations is the utilization of distinct algorithms and key sizes for control and user plane traffic. The integrity and security against replay attacks were ensured by the NAS (Non-Access Stratum) and RRC (Radio Resource Control)-signaling protocols, while authentication was supplied by the Authentication and Key Agreement (AKA) protocol in this sense. There was backhaul traffic encryption using IPSec.
However, 4G is susceptible to numerous attacks from the internet because of the end-to-end IP infrastructure that connects the cellular network to the internet. There are now several effective ways to attack the cellular network, all of which focus on the fundamental operations of the IP protocol.
Various attacks that fall under this category are address spoofing, intrusion attacks, Denial of Service, TCP SYN flood attack, TCP RST attack, and hijack. Mobile devices' greater computing capacity also opens up new attack vectors since cellular network devices themselves are capable of producing strong attacks. Additionally, Wi-Fi and WIMAX, which are 4G enabled technologies, inherit all of their security flaws.

E. 5G Security

A network with even more connectivity will be made possible by 5G, requiring interoperability across devices with varying capacities and QoS requirements. As a result, users' need for connections and constant network access is growing, and 5G must also meet this demand. Higher capacity, higher data rate, lower end-to-end latency, larger device connectivity, lower cost, and consistent Quality of Service are the six problems that 5G is intended to address in comparison to prior generations. In comparison to earlier generations, attackers' capabilities also improved at the same period. The ability to conduct complex attacks from within a mobile network is really made possible by the computational capacity of modern mobile devices. Malware and attacks of this generation are also more potent and efficient than those of prior generations.
As a result, attacks today are motivated by more powerful goals than in the past. Examples of these include large-scale cybercrime networks with evident monetary, political, and personal gain. This is also driven by the fact that mobile networks allow a wide range of other services and devices in addition to voice and video conversations, which opens up a large attack surface and might seriously impair the operation of one of the networks that are interconnected.
Although security measures have been implemented, 5G may still be susceptible to many forms of assaults because of the increased quantity of services and linked devices. As we organize the technologies and related threat vectors based on the OSI model, we will talk about the vulnerabilities that have been identified in the upcoming parts.

V. SECURITY CHALLENGES

A. Security Challenges in SDN and NFV

Through SDN, programmability in communication networks is made possible and network control platforms are centralized. Nonetheless, there are chances for network hacking and cracking thanks to these two disruptive characteristics. If the vital Application Programming Interfaces (APIs) are made accessible to unauthorized applications, for instance, the entire network may crash due to the centralized control's favoritism for denial-of-service attacks.

It is easy to identify controller traffic because the SDN controller alters the flow rules in the data stream. DoS attacks prefer to target the controller since it becomes a visible entity in the network as a result. If malicious applications are allowed access, they can cause havoc on a network because the majority of network functions can be implemented as SDN applications.
NFV poses fundamental security issues such confidentiality, integrity, authenticity, and nonrepudiation, despite its importance for future communication networks. The dynamic nature of Virtual Network Functions (VNFs), which can result in configuration problems and security failures, is one of the primary obstacles to the continued usage of NFV in mobile networks.
The primary issue that requires quick attention is that if the hypervisor is penetrated, the entire network could be compromised. Additional issues are indicated in Table 1.

B. Security Challenges in Communication Channels

In addition to connected cars, cloud-driven virtual reality, drones and air traffic control, smart factories, cloud-driven robots, transit, and eHealth, 5G will have a complex ecosystem.
Because of this, the apps require secure communication protocols that enable more frequent authentication and the sharing of more private information. These services will also see the involvement of numerous new businesses, including cloud operators, MNOs, and public service providers. Several levels of encapsulated authentication are necessary in such an eco-system for network access and service, and regular authentication between actors is also necessary.

C. Privacy Challenges in 5G

Data, location, and identity could be the main sources of privacy problems from the user's point of view. Before being installed, the majority of smartphone applications ask for personal information from the user. What uses will it be put to, according to the program developers? Threats include timing assaults, boundary attacks, and semantic information attacks primarily target subscribers' location privacy.
In 5G mobile networks, access point selection algorithms have the potential to expose location privacy at the physical layer. By obtaining the IMSI of the user's User Equipment (UE), it is possible to identify a subscriber through International Mobile user Identity (IMSI) capturing attacks. Such attacks may also be initiated by creating a fictitious base station that the UE recognizes as its preferred base station, prompting subscribers to react with their IMSI.
Additionally, there are a variety of parties in 5G networks, including network infrastructure providers, communication service providers, and virtual mobile network operators (VMNOs). Each of these players has distinct security and privacy priorities. In a 5G network, coordinating various entities' incoherent privacy standards will be difficult. All system components were directly accessible and under the control of mobile operators in prior generations. But because 5G mobile carriers will be dependent on new players like CSPs, they would lose total control over the systems. 5G operators will thus no longer have complete control over security and privacy.
In shared environments, where different actors like VMNOs and other competitors share the same infrastructure, there is a severe risk to user and data privacy. Furthermore, because 5G networks leverage cloud-based data storage and NFV characteristics, they have no physical borders. As a result, 5G operators have no direct influence over where data is stored in cloud settings. If user data is hosted in a cloud in another country, privacy may be compromised because different nations have varying levels of data privacy laws based on their preferred contexts.

D. Network Slicing Security

One important aspect of 5G technology is network slicing, which allows several virtual networks to be created on a single physical infrastructure. To accommodate the various demands of various applications and services, each network slice is customized to satisfy precise specifications including bandwidth, latency, and dependability. Although network slicing offers a great deal of flexibility and customization, there are security issues that must be resolved as well. The following security issues with 5G network slicing include:

- Separation and Disturbance: The challenge is in ensuring that network slices are properly isolated from one another in order to avoid interference and unwanted access. If the isolation is not properly put into place, malevolent actors or attackers could breach one slice's security and perhaps affect others.
- Network slicing presents a challenge in terms of intricate orchestration and management procedures needed to set up network operations and allocate resources in a dynamic manner. Attackers may use any holes or incorrect setups in the orchestration and management components to obtain unauthorized access or interfere with normal operations.

- Physical resource sharing is a challenge faced by network slices, and effective resource usage is a fundamental component of network slicing. Poor resource management could cause resource congestion, jeopardizing the network slices' security and performance.
- Security of Data: Several slices might contain various kinds of private information with distinct security needs. Inadequate data security within network slices might result in sensitive data leaks, unauthorized access, or data breaches.
- Network slices are dynamic and subject to on-demand creation, modification, and decommissioning. If security policies and controls are not modified appropriately, quick changes in network settings could result in vulnerabilities.
- User and Device Authentication: Difficulty: The services that various slices support may necessitate varying authentication standards. Vulnerabilities in authentication protocols could lead to unapproved access and identity-related attacks.
- Threats Particular to Services: Different services or applications may be supported by different network slices, each with its own set of security considerations. The security risk associated with IoT devices and mission-critical apps is that they pose a specific danger that must be addressed within the context of each network slice.

E. Vulnerabilities in IoT Devices

Several security risks are revealed by the integration of Internet of Things (IoT) devices into 5G networks. A primary area of concern pertains to inadequate authentication and authorization protocols, which may provide unauthorized access to Internet of Things devices. This could lead to compromise or manipulation, giving unauthorized parties access to or control over private information. Furthermore, insufficient encryption during data transfer from Internet of Things devices could leave data vulnerable to possible collection and eavesdropping, jeopardizing the privacy of communications. Another weakness that could allow unwanted individuals to obtain access or cause disruptions is the insufficient management of device IDs. This could result in spoofing or impersonation attacks.

Many IoT devices have limited resources, which makes it harder to maintain updated security measures and leaves them open to known flaws being exploited. IoT devices' accessibility raises physical security concerns since it makes it more likely that they may be tampered with, stolen, or gained physical access without authorization. Implementing crucial security features like encryption and safe communication protocols may be hampered by IoT devices' constrained processor and memory capacities. Moreover, supply chain risks are introduced by the intricate supply chains for IoT devices, with the possibility for malevolent actors to compromise devices during production, assembly, or distribution. To mitigate these weaknesses, a complete strategy incorporating strong authentication and encryption systems, frequent security updates, and ongoing monitoring to identify and address new threats is required.

F. Security in MIMO

The use of Multiple Input Multiple Output (MIMO) in 5G technology presents a number of security risks. An important worry is the possibility of interception and eavesdropping, in which adversaries could have unauthorized access to data that is being transferred. Security measures for communication channels, such as encryption and authentication, are necessary to lessen this. Manipulation of Channel State Information (CSI) is another problem, as CSI is essential to efficient signal processing in MIMO systems. It becomes imperative to use strong authentication and secure techniques to acquire and update CSI in order to thwart malicious interference. Beamforming is a crucial MIMO method, and its flaws make it possible for users or regions to be the target of focused attacks. To combat such threats, secure beamforming algorithms and authentication procedures are required.

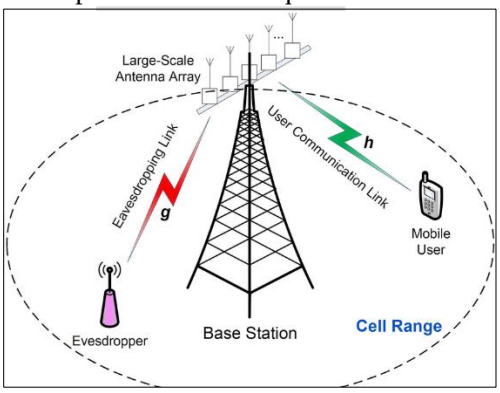

Fig 6: Security Challenges in MIMO

Additional factors that exacerbate the security issues include resource allocation assaults, dynamic channel conditions, physical layer attacks, and possible manipulation of MIMO antenna arrays. For the secure implementation of MIMO

technology in 5G networks, it is essential to have an all-encompassing security architecture that includes authentication, encryption, adaptive algorithms, and intrusion detection systems.

G. Distributed Denial of Services (DDoS)

Based on the new network architecture's expanded capabilities and complexities, distributed denial of service (DDoS) attacks become a major security risk in the field of 5G technology. 5G networks offer bad actors a chance to overwhelm network resources, disrupting services and preventing legal users from connecting. This is due to the increased bandwidth and connection density of these networks. By enabling DDoS attacks to target particular slices, network slicing has further complicated the situation and affected the vital services connected to such virtual networks. 5G's inherent edge computing capabilities highlight areas where DDoS assaults could threaten network performance by interfering with critical processing tasks. It is possible for DDoS attacks to exploit 5G networks' dynamic resource allocation techniques, resulting in traffic jams and poor service.

The infrastructure for Multi-access Edge Computing (MEC) becomes vulnerable, putting network edge services and applications at risk. Due to the wide variety of devices and services available in 5G, the attack surface is quite extensive, making it more vulnerable to massive DDoS attacks. A complete strategy including traffic filtering, secure network slicing, persistent device and service upgrades, intrusion detection and prevention system deployment, and adaptive resource allocation is needed to mitigate these issues. Combined, these safeguards ensure the robustness and resilience of the network by fortifying the 5G ecosystem against the disruptive effects of DDoS attacks.

H. Supplied Chain Security

In the context of 5G technology, supply chain security presents a number of difficulties due to its intricate and international character. The vast supply chain makes it challenging to manage and secure each component because it involves several vendors, manufacturers, and distributors around the globe. Dependence on several vendors creates a risk whereby flaws in software or hardware from one vendor could endanger the security of the entire 5G network. Strong vendor security assurance programs that include careful screening, audits, and adherence to security standards are crucial to addressing issues. Preventing the introduction of compromised pieces during manufacture or distribution necessitates maintaining the integrity of both hardware and software components across the supply chain.

A significant risk that is exacerbated by insider threats within supply chain organizations is the requirement for monitoring systems, background checks, and access controls. Preventing malicious use of insecure update mechanisms is essential when it comes to firmware and software updates. The risks and vulnerabilities associated with geopolitics are brought about by reliance on global production, which makes supplier and manufacturing site diversity imperative. To maintain the entire security posture and prevent legal repercussions, regulatory compliance with national and international standards is crucial. In order to overcome these obstacles, the 5G supply chain as a whole needs to work together with manufacturers, suppliers, regulators, and operators to prioritize openness, ongoing oversight, and strict adherence to security regulations.

VI. SECURITY SOLUTIONS

VII.

A. End-to-End Encryption

In 5G technology, End-to-End Encryption (E2EE) plays a key role in security by guaranteeing the privacy, confidentiality, and integrity of communication across a wide range of devices and applications. E2EE is essential to the security of data transmission in 5G since it encrypts data at the source and permits decryption only at the intended destination. This guards against possible attackers or network operators gaining illegal access. Because E2EE keeps middlemen from viewing or accessing communication content, it is very important for protecting user privacy. E2EE protects the secrecy of sensitive data Security Challenges in 5G Technology transferred between devices and applications in the complex world of 5G, enabling applications like IoT, driverless cars, and healthcare while maintaining the integrity of vital services. Additionally, by reducing the likelihood of illegal communication interception and manipulation, E2EE lessens the risk of man-in-the-middle attacks. E2EE provides autonomous security inside each slice in the context of network slicing, which creates virtual networks for certain services and avoids cross-slice interference. Only authorized devices may decrypt and access sent data thanks to the strong authentication procedures and secure key management that are essential to E2EE. Beyond its technological features, E2EE ensures that sensitive user data is secured during transfer, assisting enterprises in adhering to data protection

laws. Additionally, it strengthens defenses against a range of network-level attacks, including packet sniffing and eavesdropping, giving a secure base even in the event of network breaches.

Table-1:

Security Threat	Target Point/Network Element	Affected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information databases				✓	✓
TCP level attacks	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

B. Zero Trust Security Model

No matter if a user is inside or outside the conventional network perimeter, the Zero Trust security model is a thorough approach to cybersecurity that operates under the assumption that there is no trust. The setting of 5G technology, which brings additional complications and challenges, makes this paradigm more and more valuable. As a security measure for 5G, the Zero Trust security paradigm works as follows:

- Constant Authentication: Constant authentication is essential in a world where users and devices are dynamically linked and disconnected. By implementing Zero Trust, the chance of unwanted access is decreased by ensuring that people and devices are validated at all times.
- Micro-Segmentation: In order to provide targeted services, virtual networks known as network slicing are frequently implemented in 5G networks. By limiting the lateral movement of threats and restricting possible breaches within particular segments, Zero Trust uses micro-segmentation to legally isolate these slices.
- Verification of Devices and Users: Zero Trust analyzes the security posture and identification of every device and user trying to access resources, given the large number of devices connected to 5G networks. Thus, there is less chance that hacked devices will be used without authorization.
- Access with the Fewest Privilege: Zero Trust uses the idea of least privilege to make sure that devices and users have access to only the resources required for the job at hand. This lessens the possible impact of security breaches and lowers the attack surface.
- Enforcement of Dynamic Policies: Function in 5G Allocating resources dynamically and adjusting network circumstances are features of 5G networks. Using contextual data that is updated in real-time, Zero Trust dynamically enforces security regulations that change to accommodate 5G environments' ever-changing needs.
- Encryption Everywhere: Throughout Zero Trust advocates encryption at all stages, including during transmission, at rest, and even within network slices, in light of 5G's enhanced data transmission capacity. Integrity and confidentiality of data are protected, particularly when transferred between different devices and services.
- Constant Monitoring and Analytics: In order to find anomalies and possible security risks, Zero Trust uses ongoing analytics and monitoring. With so many different types of mobile devices in a 5G setting, ongoing monitoring is essential to spot odd patterns that could point to security breaches.
- Transparency throughout the Ecosystem: 5G ecosystems encompass a wide variety of devices, services, and applications. In order to detect and address possible security threats, Zero Trust places a strong emphasis on visibility, offering a thorough picture of all network activity.
- Multi-factor authentication (or MFA), is a security measure that Zero Trust frequently uses to bolster security. Because different devices with different security postures are connected to the network in 5G, this is very crucial.

C. Authentication

Entity authentication and message authentication are the two primary forms of authentication in a 4G cellular network. The former verifies that the communicating entity is, in fact, the same entity that it purports to be. Message authentication also makes sure that the message being sent is authentic and hasn't been altered in route. In a 4G cellular network, symmetric-key authentication is used between UEs (user equipment) and MMEs (mobility management entities); however, this approach is impractical for 5G. UE and MME mutual authentication as well as service provider mutual authentication are required for 5G.

Flexible and hybrid mutual authentication of UE is necessary since 5G networks have different trust models, new service delivery models, and more privacy concerns than previous cellular networks. There are three methods that this mutual authentication is implemented in the EU: first, by the network alone; second, by the network and service providers alone. Additionally, the multi tier architecture of 5G necessitates reciprocal authentication and fast handover, which can be met by service-based architecture and SDN-enabled fast authentication. Three authentication methods are defined by 5G networks to enable authentication: EAP-TLS (extensible authentication protocol-transport layer security), 5G-AKA (authentication and key agreement), and EAP-AKA.

D. Security Solutions for SDN and NFV

Through a cycle of gathering intelligence from the network resources, states, and flows, SDN enables rapid threat identification. This is made possible by the logically centralized control plane with global network visibility and programmability. As a result, the SDN architecture enables security service insertion, traffic analysis, and response systems to provide both preemptive and highly reactive security monitoring, network forensics, and policy modification. Global network visibility allows uniform network security policies to be implemented throughout the network, while Intrusion Detection Systems (IDS) and firewalls can be tailored to specific traffic by adjusting the flow tables of SDN switches.

In accordance with the ETSI NFV design, the security of VNFs is provided by a security orchestrator in.

Security for both the physical and virtual components of a telecommunication network is offered by the suggested design in a multi-tenant environment. Remote verification and integrity checking of virtual systems and hypervisors using trusted computing is suggested as a way to detect defective software in virtualized settings and offer hardware-based security for sensitive data.

E. Security Solutions for Privacy in 5G

5G has to implement privacy-by-design strategies, meaning that many essential elements must come pre-installed and privacy must be taken into account from the system's inception. In order to store and process highly sensitive data locally and handle less sensitive data on public clouds, mobile operators must adopt a hybrid cloud-based strategy. Operators will be able to choose where to exchange data and will have increased access to it. Similar to this, 5G's service-oriented privacy will result in more workable solutions for maintaining privacy.

Improved systems for access control, accountability, transparency, openness, and data minimization will be necessary for 5G. Strong privacy laws and regulations should therefore be considered during the 5G standardization process. There are three categories for the regulatory approach.

First, regulations are made at the government level. Through multilateral organizations like the European Union (EU) and the United Nations (UN), states primarily create privacy laws that are specific to each nation. The best practices and guidelines for protecting privacy are drafted cooperatively by a variety of sectors and organizations, including 3GPP, ETSI, and ONF, at the industry level. Thirdly, there are regulations at the consumer level that guarantee privacy by taking into account the needs and preferences of the consumer.

Where the subscriber's true name could be concealed and replaced with pseudonyms, anonymity-based approaches must be used to ensure location privacy. In this situation, encryption-based techniques are also helpful; for example, a message can be encrypted before being sent to a location-based services (LBS) provider.

When location privacy is being protected, techniques like obfuscation—which lower the quality of location data—are also helpful. Additionally, several of the most common location privacy threats, like timing and boundary assaults, can be effectively handled using location cloaking-based algorithms.

F. AI and Machine Learning for Anomaly Detection

Notably, anomaly detection is one of the primary ways that artificial intelligence (AI) and machine learning (ML) contribute to strengthening 5G security measures. In order to examine the typical behavior patterns displayed by devices, users, and apps in the ever-changing 5G network environment, this security solution makes use of AI and ML algorithms. These tools facilitate the identification of abnormalities or departures from normal patterns by creating baselines of anticipated behavior. Artificial intelligence (AI) and machine learning (ML) are highly adaptive technologies that are useful in adapting to the constantly changing conditions of 5G networks. Through anomaly detection, which is fueled by AI and ML, possible security risks may be identified in real time, and problems can be quickly resolved by automated reactions or notifications.

In 5G, network slicing creates virtual networks for particular services; AI and ML can monitor and analyze activity in each network slice to offer customized security measures. Utilizing historical data and discovering patterns that are invisible in rule-based systems, these technologies are especially good at identifying unknown or unique risks. User and Entity Behavior Analytics (UEBA), powered by artificial intelligence, examines how users and entities behave in 5G networks in order to identify unusual activity that may be a sign of a security risk. By improving their comprehension of typical network behavior over time, AI and ML play a significant role in lowering false positives. In the ever-changing world of 5G, their capacity for ongoing learning and adaptation helps enterprises to remain ahead of new risks and preserve efficient security.

Furthermore, through feed integration, these technologies improve threat intelligence by deepening their comprehension of recognized danger indicators and facilitating anticipatory reactions to possible security incidents. Fundamentally, enterprises implementing 5G technology may safeguard themselves against new attacks in the intricate and ever-changing network environment by utilizing AI and machine learning for anomaly detection, which offers a proactive and adaptable security approach.

G. Regulatory Compliance and Standards

Ensuring the strong security of 5G technology requires both regulatory compliance and adherence to security standards. Standards and rules have been set by governments, industry associations, and international organizations to direct the installation and functioning of 5G networks. The following are some ways that standards and regulatory compliance help to secure 5G:

- Privacy and Data Protection Rules: The treatment of sensitive and personal data is governed by international data protection laws and regulatory frameworks like the General Data Protection Regulation (GDPR) in the European Union. User data security and privacy in 5G networks are guaranteed by following these rules.
- Standards groups for network security, such as the Third Generation Partnership Project (3GPP) and the International Telecommunication Union (ITU), create guidelines and standards. A 5G network's construction and operation will adhere to security best practices if these requirements are followed.

- Standards related to authentication and access control include the Subscriber Identity Module (SIM) authentication protocols and the Evolved Packet System Authentication and Key Agreement (EPS-AKA), which specify how users and devices in 5G networks must authenticate themselves. Respecting these guidelines improves security against unwanted access and strengthens access control.
- Standards for Cryptography: The introduction of encryption algorithms and key management in 5G is guided by cryptographic standards, such as those established by the National Institute of Standards and Technology (NIST). The integrity and confidentiality of transferred data are guaranteed when these requirements are followed.
- Security protocols for 5G infrastructure components, such as base stations and core network parts, are outlined by standards groups. 5G infrastructure implementation and operation are guaranteed to be secure when these criteria are followed.
- Security Guidelines for the Supply Chain: The supply chain of 5G devices and equipment is secured by rules set forth by governments and industry associations. The overall security of the 5G ecosystem is ensured by following these standards, which assist prevent the introduction of compromised components.
- The obligations for reporting incidents and responding to them are frequently outlined in regulatory frameworks. By adhering to these responsibilities, organizations implementing 5G technology can promote a more robust security posture by quickly addressing and mitigating security events.
- Regulatory organizations are responsible for allocating and managing spectrum in order to facilitate the implementation of 5G. Complying with spectrum management laws reduces the likelihood of interference and improper use, enhancing the general dependability and security of 5G networks.
- Protection of National Security and vital Infrastructure: To preserve interests in national security and to safeguard vital infrastructure, governments may set rules and guidelines. Adherence to these standards is essential in order to guarantee that 5G networks do not present threats to national security.
- Guidelines for Interoperability and Compatibility: Guidelines that support the interoperability and compatibility of various 5G devices and providers make the ecosystem more stable and secure. Adherence to these standards enables the integration of heterogeneous components while maintaining security.

H. Security Solutions for Communication Channels

To safeguard against known security risks and preserve SDN's extra benefits, like programmability, centralized policy administration, and global network state visibility, 5G requires adequate communication channel security.

Today's 4G-LTE networks and other modern telecommunication networks employ IPsec as their primary security protocol to lock down communication channels. IPsec tunneling can be used, with minor adjustments, to secure 5G communication connections.

Moreover, a variety of security methods, including encryption, integrity, and authentication, are integrated to ensure security for LTE communications. But the biggest problems with these kinds of current security plans are their excessive resource usage, their high cost, and their lack of coordination. For 5G's crucial infrastructure communication, these methods are therefore impractical.

Therefore, by employing novel security techniques like physical layer security that uses Radio-Frequency (RF) fingerprinting, asymmetric security schemes, and dynamically adjusting security parameters based on the circumstance, a greater level of security for crucial communication is conceivable. The usage of cryptographic protocols like HIP, which are described in, can also secure end-to-end user communication.

I. Security for Network Slicing

One of the key and novel aspects of 5G technology is network slicing, which enables the development of unique virtual networks, or "slices," within the same physical infrastructure, each suited to particular services or apps. Enforcing strong safeguards is essential to guarantee the security of network slicing in 5G. To prevent interference between slices, robust isolation methods should be in place between them. Additionally, each slice should have a unique security policy that is designed according to its requirements. Controlling user and device interactions inside each slice and preventing unwanted access requires the enforcement of authentication protocols and access constraints. Data integrity and confidentiality are protected by encryption inside slices, especially when it comes to sensitive data. Automated anomaly detection systems and routine monitoring are necessary to quickly spot odd activity or security risks. To ensure compliance with industry standards like 3GPP, frequent security assessments for every network slice are helpful in locating and resolving any vulnerabilities. The autonomy, security, and best-in-class performance of individual network slices are further preserved by flexible resource allocation strategies and cooperation with slice operators. In summary, network operators can make the most of network slicing in 5G while still upholding a strong and secure network environment by following certain security protocols.

VII. CONCLUSION

In summary, the examination of challenges and solutions related to 5G security unveils the complex terrain of the latest wireless technology. A solid grasp of the foundational aspects of 5G, encompassing its core network architecture, essential features, and the groundbreaking MIMO technology, lays a strong groundwork for understanding the dynamic security environment. As we charted the progression of security threats from 1G to the current 5G era, it becomes clear that the growing intricacy and interconnectivity of networks have given rise to unprecedented challenges.

The scrutiny of security challenges in the 5G context has emphasized the urgent necessity for robust measures to tackle vulnerabilities arising from elements such as network slicing, virtualization, and the sheer abundance of connected devices. Threats, including the potential compromise of user privacy, data integrity, and disruptions to critical services, underline the imperative for a proactive and all-encompassing security strategy.

The range of defenses against evolving threats in 5G is broadening, encompassing encryption techniques, authentication protocols, intrusion detection systems, and security mechanisms driven by artificial intelligence. Ensuring the successful implementation of these solutions requires critical collaboration among industry stakeholders, regulatory bodies, and researchers.

It is clear that a comprehensive strategy is imperative for navigating the complex landscape of 5G security. The key to securing the transformative potential of 5G lies in the integration of advanced technologies, the promotion of collaboration, and an unwavering commitment to ongoing research and development.

VIII. REFERENCES

[1.] Mamoona Humayun, Bushra Hamid, NZ Jhanjhi, G.Suseendran, M N Talib, "5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey", International Conference on Recent Trends in Computing (ICRTCE-2021).

[2.] Ijaz Ahmad, Tanesh Kumary, Madhusanka Liyanagez, Jude Okwuibex, Mika Ylianttila, Andrei Gurtov, "5G Security: Analysis of Threats and Solutions"

[3.] S. Sullivan, Alessandro Brighente, Satish Kumar, and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers"

[4.] Albert Severo Téllez Martínez, "5G Security Issues- A Compilation With Industry Insight"

[5.] Sunil Kumar Shah, Snehal Jani, Rinkoo Bhatia, Neeta Nathani, "A Review of Security Challenges and Solutions in 5G Network", Engineering and Technology Journal for Research and Innovation (ETJRI)

[6.] Politecnico Di Torino, "A survey on Cybersecurity in 5G."

[7.] Cherry Mangla, Shalli Rani, Nawab Muhammad Faseeh Qureshi, Aman Singh, "Mitigating 5G security challenges for next-gen industry using quantum computing", Journal of King Saud University – Computer and Information Sciences 35 (2023) 101334

[8.] Raneem Jassim Alghawi, "2022

[9.] Network Slicing in 5G: Admission, Scheduling, and Security"

[10.] Fatima Salahdine, Tao Han, Ning Zhang, "Security in 5G and beyond recent advances and future challenges", John Wiley & Sons Ltd.

[11.] Mohammad Wazid, Ashok Kumar Das, Sachin Shetty, Prosanta Gope, and Joel J.P.C. Rodrigues, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges,and Future Research Roadmap"

[12.] https://www.qualcomm.com/5g/what-is-5g

[13.] https://www.cisco.com/c/en/us/solutions/what-is-5g.html

[14.] https://stl.tech/blog/5g-network-architecture