IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 4, April 2024

Securing the Next Wave: A Comprehensive Review of 5G System Security

More Meghana Laxman and Prof. Sapike N. S.
Department of Computer Engineering,
Viswabharti College of Engineering, Ahmednagar, India
meghanamore415@gmail.com

Abstract: *This review paper delves into 5G system security, examining various research papers encompassing various technologies. Through an extensive analysis, explore the multifaceted landscape of 5G security, including but not limited to authentication protocols, encryption mechanisms, threat detection, and mitigation strategies. By synthesizing insights from diverse sources, this paper provides a comprehensive understanding of the current state of 5G security, highlighting both challenges and advancements. The findings presented herein aim to contribute to the ongoing discourse on fortifying the security posture of 5G networks, which is crucial for fostering trust and reliability in the burgeoning era of ultra-fast connectivity.*

Keywords: 5G, Security, Authentication, Encryption, Threat Detection

I. INTRODUCTION

The 5G architecture differs significantly from its 4G predecessor in several key respects. To begin with, the basic 5G system broadens coverage to include more frequency bands, which is ideal for micro-cells and massive MIMO (Multiple-Input Multiple-Output), enabling much higher data speeds. Transmitters operating in the millimeter-wave spectrum (including the Ka-band and beyond) provide spatial multiplexing capabilities more easily than those operating at lower frequencies due to their high directivity. Atmospheric absorption rates are often high, and there is still room for improvement in power output in these frequency ranges. So, macro-cells, presumably using the same frequency bands as 3G and LTE networks, cannot utilize them. Nearby frequencies of 3GHz also provide an additional untapped spectrum for 5G applications. This frequency range will likely be used for bandwidth expansions since it is in a previously unallocated band (in terms of cellular communications).

Support for use cases like vehicle-to-vehicle (V2V) collision avoidance is promised by the 5G architecture in standalone systems, along with much-reduced latencies to establish a communications channel. The added delays are too great for some use cases to be feasible with greater latencies, especially for missions where safety is paramount. Additionally, a service-based architecture lies at the heart of 5G networks. This is shown by the fact that the network functions' service-based interfaces are built on HTTP/2 over TLS over TCP/IP. EPC networks continue to form the backbone of those that are not self-contained. An eNB connection manages the control plane for the mobile devices, while the gNB is only responsible for user plane traffic. This indicates the presence of two radio interfaces on the end user's side. This means the NSA 5G network will not have access to the newly implemented 5G standards' core network features. As stated in the 5G-NR section of the requirements, the use of a new radio spectrum is the primary distinction between this 5G system type and 4G systems. Because connection latency is proportional to subframe time, even an NSA system may reduce latency. 5G core systems are the only ones that provide network slices. Therefore, in an NSA deployment, all devices, ranging from low-power machines to those managing the "massive Machine Type Communications" (mMTC) service and even a URLLC device, share the radio resources equally.

New use cases, which are not possible with earlier mobile communications standards, will reportedly be able to be deployed with the launch of fifth-generation mobile networks. Everything from device-to-device (D2D) communications to device-to-cloud (D2C) communications and beyond falls under the umbrella of large machine-to-machine (M2M) communications. For instance, in the vehicle-to-everything (V2X) domain, there are specific needs for mobile devices and fixed devices in the Internet of Things (IoT). Different types of devices have vastly different needs regarding power, latency, and data throughput.

DOI: 10.48175/IJARSCT-17427

It is believed that these variations in functional needs will be addressed by introducing network slices. Currently, the transition from 4G to 5G systems is happening by launching 5G solutions in an NSA fashion, which means that the first rollout of 5G will only include the new radio features of 5G (5G-NR). Also, the core network is still the old 4G EPC network, and user equipment control is still based on 4G protocols. New models of trust are necessary due to the absence of human contact. The 5G standard resolves privacy issues that 4G could not handle. Researchers were actively concerned with the 5G system's security, as described in TS 33.501 [4], before the standard's widespread implementation (cf. [5]), in contrast to earlier generations of standards. Before deploying 5G standalone (SA) systems, a rigorous examination of the security processes (Basin et al., 2016) has identified vulnerabilities that might be addressed.

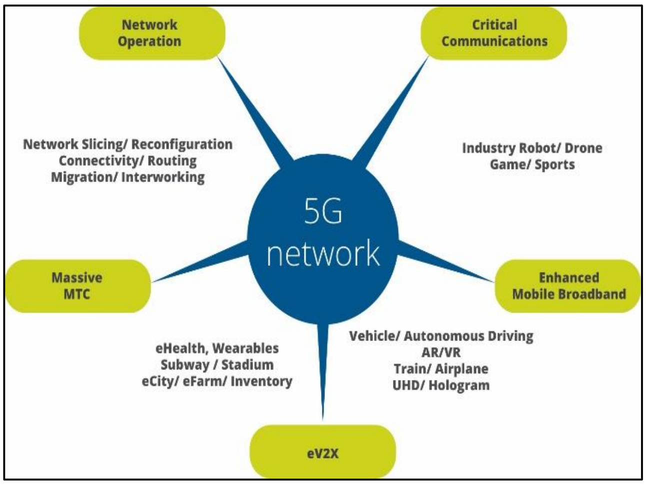

Fig.1 5G Technologies

II. LITERATURE REVIEWS

The article presents assessments within the domain of mobile communication technologies. Using next-gen mobile networks, able to overcome the many obstacles encountered along each development. Unlike any previous mobile network, 5G offers a high-speed internet service to everyone, anytime, wherever. Because of its unique characteristics, 5G is significantly different. These qualities allow it to link people, control devices, objects, and machines. New user experiences and business connections will be possible with the 5G mobile system's varied performance and capabilities. So, it is crucial to understand how the business can use 5G. Focusing on the 5G mobile system and its future research goals, this article primarily aims to showcase some of the latest advancements in the field.[1]

The widespread availability of low-latency, high-speed connections is widely anticipated to be a byproduct of developing next-generation wireless networks. So, making sure the network is safe is paramount. The increasing variety of services and devices that 5G will enable has made the network's security environment more complex. This is why it is critical to start working on security solutions immediately. Our review's results have shown the several paths that will be taken to create next-gen wireless networks. The implementation of SDNs and AI are two examples of such technologies. This comprehensive literature review will equip future researchers to understand the 5G network threat environment, the security vulnerabilities in the new technological paradigms that 5G will adopt, and the remedies offered in the most important 5G cyber security studies. Beyond 5G, potential avenues for further study in wireless network security will also be discussed. [2]

Research into and experimentation with enormous Multiple-Input Multiple-Output (MIMO) wireless access technologies have been prompted by the worldwide bandwidth scarcity in the wireless communication industry. Together, the transmitter and reception antennas in massive MIMO achieve great spectrum and energy efficiency with simple processing, making it a crucial enabling technology for next-generation networks. To successfully deploy 5G networks and beyond and to realize the intelligent sensing system's many applications, a greater understanding of the massive MIMO system is essential for overcoming the technology's core difficulties. This article thoroughly reviews the essential enabling technologies for 5G and 6G networks. It also reviews the most current developments in large MIMO systems, including terahertz communication, visible light communication (VLC), machine learning, and deep learning.

DOI: 10.48175/IJARSCT-17427

Furthermore, reviews important unanswered questions that will guide future studies of huge MIMO systems for networks beyond 5G. [3]

The latest and greatest 5G network slicing options are available using SDN and NFV. Begin with an overview of the 5G service quality and business needs, then discuss the ideas, history, and many use cases of 5G network slicing and softwarization. Then, go on to a lesson on the technologies allowing 5G network slicing. To further accelerate 5G network slicing, provide a detailed overview of several industry projects and activities driving SDN and NFV adoption. Here, compare and contrast several 5G architectural concepts based on how well they work in practice, the technologies they use, and how they plan to deploy their networks. In addition, provides several industry-representative proof of concept projects and open-source orchestrators. It also highlights the current state of 5G network slicing and network softwarization standardization initiatives in academia and business. [4]

5G networks will use innovative technical ideas to reliably and affordably link many devices (such as the Internet of Things), provide high levels of user and device mobility, and satisfy the need for ubiquitous Internet access. Technologies that use software-defined networking and virtualized network services, taking advantage of cloud computing advancements like mobile edge computing, are highly sought after for meeting these needs. However, now the focus shifts to future wireless networks and how to safely employ these technologies while protecting user privacy. In light of the importance of user privacy, this article summarizes the difficulties associated with cloud security, SDN, and the virtualization of network operations. This essay then discusses how these problems may be solved and where to go regarding secure 5G networks. [5]

This research covered a range of technical elements and services related to 5G security, including availability, authentication, integrity, nonrepudiation, and secrecy. This is in light of the plans and developments for 5G wireless networks. Laid up a taxonomy of 5G communication security concerns at a high level and gave detailed tabular solutions. Possible overarching goals for integrating several 5G-related emerging technologies. In addition, covered new uses such as smart grid, smart drones, large data, smart healthcare, smart cars, and Internet of Things services for 5G safety. Lastly, it outlined the current research gaps on 5G network security. Smart city applications like smart manufacturing, transportation, and healthcare will benefit from future proposals for an enhanced architecture and framework for 5G security, using fundamental technologies like Blockchain, CPS, MEC, AI, D2D, Tactile Internet, and Industry 4.0. [6]

Data traffic levels have grown tremendously due to the mobile generation's fast evolution and emerging data networking capabilities and use. This load drains many important problems with 5G mobile backhaul networks. Despite the critical nature of mobile backhaul security, very few papers have addressed this need. Secure 5G mobile backhaul architecture is the subject of this article, which also explores possible design concerns and important challenges. There has been an examination of the current state-of-the-art systems for secure mobile backhaul, comparing them and highlighting their key contributions. Using tools like Software Defined Networking and millimeter Wave technology, the article also covered other important topics like Quality of Service (QoS), scheduling and routing, managing resources, increasing capacity, latency, security, and handovers. Additionally, avenues for future study and difficulties encountered along the way are detailed. [7]

With 5G networks, new applications, industries, and business models may be easily integrated. These networks can greatly enhance people's quality of life by facilitating many use cases, including eHealth, autonomous cars, smart cities, smart grid, and the Internet of Things (IoT). Secure servicing and resource policing are necessary for these apps to function properly in network structures. While several studies have focused on the flexibility of 5G networks, others have highlighted the security elements of these networks. More research is needed to address the need to incorporate new computing paradigms to bolster security. To address this, this paper presents a comprehensive overview of 5G network security and discusses the development of security modules based on osmotic and catalytic computing. In addition to comparing the current state-of-the-art solutions, the presentation contains a taxonomy based on security criteria. The study provides a security model called "CATMOSIS," which envisions 5G networks with security features built on top of osmotic and catalytic computing. Lastly, future research in this area should be highlighted, and many security difficulties and outstanding issues should be addressed. [8]

The next generation of cellular systems has a dual challenge: meeting the demands of data-intensive applications while simultaneously reducing energy consumption and maintaining excellent service quality in the face of an onslaught of massive data sets. Massive MIMO and tiny cells are the most prominent technologies to tackle these difficulties. The massively multiple-input multiple-output (MIMO) approach improves wireless networks' spectrum and energy efficiency by installing many antennas at the base station. Small cells can cut transmit power by bringing the user closer to the base station while maintaining a high data rate and excellent coverage. This study uses a tiny cell network to examine the current status of massive MIMO techniques. To begin, over the basics of massive MIMO. The next step is to research system analysis modeling tools and performance measures. In the next section, the article outlines the technologies that make the massive MIMO small-cell network possible. The report concludes by outlining potential difficulties and areas for further study. [9]

Current 4G networks are adapting to meet the demands of upcoming Internet of Things (IoT) applications and have seen extensive deployment in the IoT. With the advent of 5G networks, the Internet of Things (IoT) stands to grow exponentially, addressing concerns about cellular operations, security, and network congestion while propelling the Internet of Things (IoT) into the periphery. Problems with security, new standards, and a high number of connected nodes are just a few of the obstacles that current Internet of Things solutions must overcome. Current research on 5G IoT, including its state-of-the-art, important supporting technologies, and major research trends and obstacles are reviewed in this study. [10]

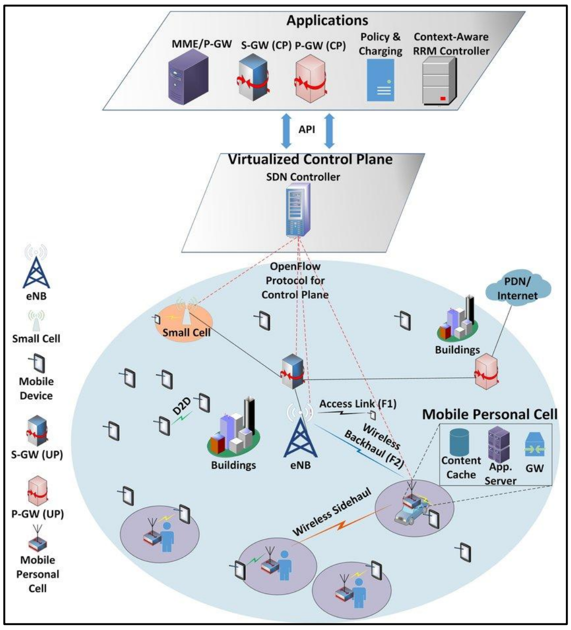

Fig.2 5G System Design

By 2020, all networks will have adopted the same standard for 5G wireless networks, which aims to increase connection density, decrease latency, and boost capacity, dependability, and energy efficiency. An essential part of 5G is the ability to send real-time communication similar to touch perception, made possible by appropriate haptic devices and robots at the network's edge. The core and RAN must substantially change the network architecture to get end-to-end latency of 1 ms or less. This article covers the present state of the art in low latency communications in three separate areas of solution development. 2) core network, 3) caching, and RAN are the first two. Furthermore, provides a high-level summary of key components of 5G cellular networks, including SDN, NFN, caching, and mobile edge computing, all of which can fulfill latency and other 5G expectations.[11]

At its basic level, a wireless sensor network enables scalability, dependability, mobility, and other desirable network properties. In a WSN, different nodes are linked via radio or other non-wired media. These nodes are sensors that collect data and send it to the user. Energy is needed for this transfer. The number of users has grown, necessitating continuous connection, thanks to the upgrade from 4G to 4GLTE in mobile communication. The effect is that the power of the mobile batteries is depleted. Need a plan to reduce energy usage, which will increase the life of mobile batteries if you want them to last longer. This study examines and compares several existing techniques to provide a secure, energy-efficient, and effective communication method in wireless sensor networks and mobile ad hoc networks. [12]

According to the research, the most recent cellular network generations will be the primary means of transmitting data worldwide. This might be problematic for service providers attempting to enhance the QoS promised in an SLA, which must then be validated in practice. Adopted quality of service measurements, including bandwidth and Round-Trip Time (RTT), need methodologies and instruments for measurement. This study made use of InfoVista's BlixtTM proprietary tool. The study delves into the importance of probing packet properties in deciding measurement accuracy, intrusiveness in shared-resources networks, and the application's sustainability. Compared the results to other state-of-the-art bandwidth measuring tools in a multi-carrier scenario and ran the tests on a real-world commercial network. [13]

5G System Security Analysis

According to current security research, the standard still includes vulnerabilities that attackers might exploit. Furthermore, the transition from 4G to 5G systems is being accomplished by initially implementing 5G solutions in an NSA fashion. This means that the initial phase of 5G deployment is focused on the new radio components of 5G, while the user equipment control is still grounded in 4G protocols. In other words, the core network remains the legacy 4G evolved packet core (EPC) network. The upshot is that contemporary 5G deployments still have many of the same security flaws as 4G networks. This article systematically analyzes both standalone and non-standalone 5G networks regarding their risks. The rundown on 5G's new security features and how they differ from 4G in the 5G system standard. Next, the STRIDE threat categorization methodology will identify potential dangers. Then, a risk matrix will be created by calculating the chances and consequences of 12 threat scenarios that might compromise the network's core and radio access. Lastly, go over several potential safeguards and mitigation strategies. Considered any 5G network vendor or operator details in general research. Further research is needed to understand the security risks and vulnerabilities of individual 5G deployments and implementations. [14]

5G will make high-speed Internet available everywhere, allow more mobile users, and link many devices. Despite the increasing worries about user privacy, critical security issues remain with these systems. This document presents a synopsis of the privacy concerns surrounding 5G and the security problems surrounding these technologies. Also included are plans for safe 5G systems and security solutions to these problems. [15]

Five security concerns stemming from 5G's technological benefits are outlined in this paper: 1) addressing security concerns related to the response to distributed denial of service attacks (DDoS) that are caused by vulnerabilities in Internet of Things (IoT) devices; 2) managing RAN failure and small cells in an environment with expanding coverage and heterogeneous wireless networks; 3) gaining visibility into security monitoring and expanding protection targets in a decentralized mobile network structure; 4) fixing security problems with third-party apps, API dependability, and connection routes to internal mobile communication networks brought on by MEC; and 5) establishing dynamic security management and access control as a result of sharing physical HW equipment with virtualization platforms and network slicing technologies. Furthermore, categorized 5G control and user plane pathways that were attacked using network protocols. Problems with non-encryption, unauthenticated message origin, and error handling are common in network protocol-based assaults on the core network since these attacks are often conducted in a closed internal network. To tackle these security challenges, 5G standards have improved several security functions, including the SEPP function across domains and the prohibition of IMSI capture.

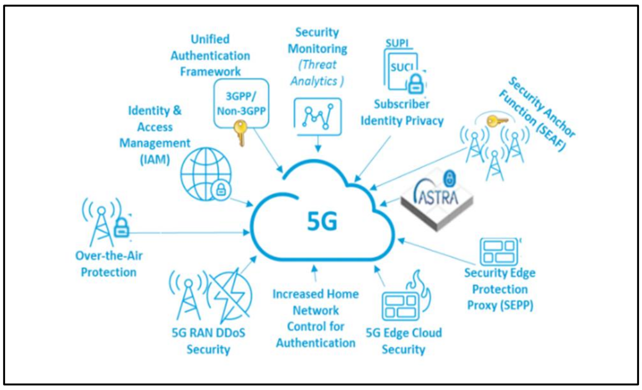
Unified Authentication Framework
3GPP/ Non-3GPP
Security Monitoring (Threat Analytics)
SUPI
SUCI
Subscriber Identity Privacy
Security Anchor Function (SEAF)
Identity & Access Management (IAM)
ASTRA
5G
Over-the-Air Protection
Security Edge Protection Proxy (SEPP)
5G RAN DDoS Security
Increased Home Network Control for Authentication
5G Edge Cloud Security

Fig. 3 5G Security Overview

Nevertheless, 5G network security standards primarily address the control plane's signaling, whereas the user plane's security functionalities, about protocol availability and integrity, could be improved. Also, because it relied on the HTTP and REST API of the IP network, the SBI interface structure that 5G is aiming for has become a security risk by including traditional HTTP security flaws. [16]

Cellular networks are essential today, and the telecom industry is always inventing new infrastructures and technologies to serve its customers better. There are many advantages to newer generations, such as 5G, over older ones (1G to 4G). Every 5G stakeholder benefits from the system's adaptability, decreased latency, interoperability, and tenfold speed increase over 4G. Many new problems will emerge due to technological advancements, especially as the 5G network expands. Before creating and implementing 5G, this article provides context for the technology, discusses the security concerns with 5G networks, and offers suggestions for the future. Conclude by outlining a course of action to address these concerns. [17]

Contemporary backhaul practices depend on wireless technology deployed in point-to-point (PTP) or point-to-multipoint (P2MP) arrangements. The wireless backhaul is more susceptible to a variety of security risks and assaults than the wired one, unfortunately, because of the transmission medium's nature. Various researchers developed key exchange schemes to safeguard the backhaul. However, these security standards need to meet all of the security needs of the next 5G networks, such as updating security policies and keys and finding the right balance between security and efficiency. Research and propose a novel security protocol for the backhaul connection of wireless access networks based on the P2MP paradigm, primarily for this reason. The suggested protocol is 5G-aware and offers features such as secure key exchange, mutual authentication, confidentiality, integrity, and perfect forward secrecy. It also prevents resource depletion attacks and updates security policies and keys securely. Scyther and BAN-logic, two popular formal security analysis tools, formally verify the protocol's validity. The security criteria are also shown to be met by the derived lemmas. At last, compared to other conventional protocols, the suggested protocol proves superior. [18]

This study presents an edge computing-aware NOMA approach that may reduce the uplink energy usage of MEC users while still enjoying the advantages of uplink NOMA. This will help capture NOMA's potential gains in the context of MEC. Specifically, to reduce MEC users' energy usage by developing an optimization framework based on NOMA. This system optimizes user clustering, computer and communication resource allocation, and transmit powers. The cloudlet's available processing capacity is divided into computing resource blocks (RBs) comparable to frequency RBs. As a result, investigate how NOMA clusters' distinct order indices affect the distribution of computing RBs and frequency. In addition, develop a heuristic method that efficiently clusters users and allocates RBs. A convex optimization problem that each NOMA cluster must solve individually for power control. The suggested NOMA system is tested using simulations to see how well it works. [19]

Internet, mobile-cellular, and service commerce in South Korea are the subjects of this empirical research. From this vantage point, the primary goal of this research is to use the modified gravity model to isolate important factors influencing service trade from 1990 to 2018. This investigation uses a log-linear regression model using ordinary least squares techniques to estimate the unknown parameter. The report acknowledges that using the Internet and mobile-cellular communication tools increases the likelihood of South Korea engaging in service commerce. According to the data, service exports and imports are both positively impacted by mobile-cellular technology and the Internet. Furthermore, the research provides substantial evidence linking service trade to GDP and trade openness. Since the research relies on aggregated data for service trade, the impact of the Internet and mobile-cellular factors is minimal in quantitative evaluation. Hence, future studies should use service-specific disaggregated trade data to maximize the Internet's and mobile-cellular's beneficial effects on service trade. Conversely, growing Internet availability and use are anticipated to play an increasingly vital role in future service trade expansion, given the impact of the COVID-19 pandemic on people's lives and the disruption of international commerce.[20]

5G System using IoT

One of the most fundamental tracking control methods is inversion-based feedforward control. Considering both on-sample and intersample behavior, this study aims to build a MIMO multirate feedforward controller that optimizes the continuous-time tracking performance of MIMO LTI systems. The 2-norm of the control inputs is used to construct and evaluate different forms of MIMO multirate feedforward controllers. In simulations, the method is contrasted with a

DOI: 10.48175/IJARSCT-17427

traditional MIMO feedforward controller that only handles one rate. This method optimizes the selection of input multiplicities with MIMO multirate system inversion, which enhances the intersample behavior. [21]

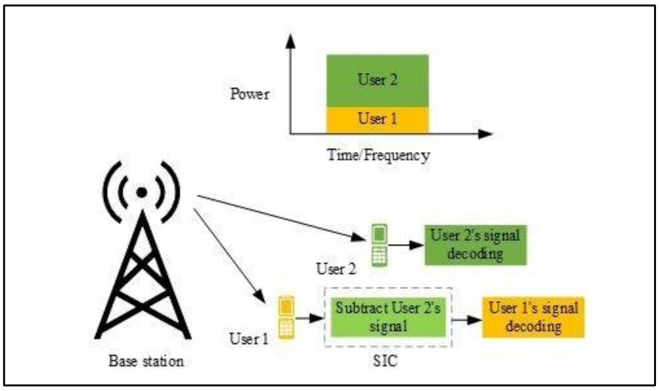

Fig.4 NOMA in 5G Network

Since HNOMA achieves better spectrum efficiency, it is investigated in this study as a potential solution to the problem of huge multiple access in uplink settings. Because real-world channel conditions vary, HNOMA incorporates both the power and code domain NOMA methods. Research shows that HNOMA-based wireless networks may benefit from polar coded data transmission regarding reliability and latency. In addition, because of non-orthogonal connections, the base station (BS) does not have perfect or particularly complicated channel state information (CSI) for each link. Hence, the efficiency of uplink-based systems that use HNOMA transmission in imperfect CSI should be studied and assessed. Additionally, lays out the major technological obstacles and how future Internet of Things (IoT) applications may use HNOMA transmission to overcome them. Lastly, provide some recommendations for the architecture of HNOMA-based systems that use deep learning to build efficient and adaptable wireless networks. [22]

The mMTC service ensures high-quality communication among many machines and devices. The eMBB service enables fast data throughput, even at the cell boundary. Communications with very low latency requirements are handled by the uRLLC service, which is known for its ultra-reliability. In every particular cell, these services are delivered independently. Nevertheless, bit rates and energy consumption are rising, and the number of linked items is also beginning to climb. The 5G network has to be able to accommodate a large number of users across all of its service types. Methods for call admission control (CAC) place more emphasis on coverage and bit rate availability. Here, propose an approach, mostly focused on energy efficiency, for CAC modeling in a 5G access network's three service categories. With this method, low-power network connectivity may be achieved by linked items, paving the way for the expansion of the Internet of Things. [23]

5G System Analysis using Machine Learning

In today's world, wireless communication networks are indispensable for many reasons, including but not limited to entertainment, commerce, health, and safety. These technologies are constantly improving with each new generation, and the latest example of this is the widespread implementation of 5G wireless networks. Beyond 5G wireless networks, the next generation (6G) is already being discussed in academia and business. Regarding 6G systems, one of the most important things is that these wireless networks employ AI and ML. The physical, network, and application layers—all already acquainted with our understanding of wireless technologies up to 5G—will somehow use AI/ML approaches. This review article aims to provide a current and comprehensive understanding of the ideas and use of ML approaches in future wireless systems, including 6G. highlight the use and function of ML approaches in each layer of a hypothetical 6G model that offers. Within the framework of wireless communication systems, examine many traditional and modern ML methods. At the end of the study, several potential future uses and obstacles to further research in the 6G network ML and AI field will be discussed.[24]

Many problems with 5G mobile networks are anticipated to be solved by machine learning (ML). On the other hand, ML will expose the network to several major security holes. Data collected from the environment is the primary source for learning in ML. Machines that take in data without filtering it will have difficulty using it to make network intelligence. Conversely, privacy concerns arise from data scrutiny. Most ML systems, however, are rip-offs from other fields that

DOI: 10.48175/IJARSCT-17427

succeed in controlled settings. Consequently, due to such ML algorithms, the 5G network might unwittingly be exposed to major security risks like resource abuse, denial of service, and the disclosure of sensitive data. Therefore, this paper delves into the shortcomings of the leading ML systems that are now being extensively studied for 5G implementation. To further prevent these problems using ML in 5G networks, categorize them and examine potential remedies. [25]

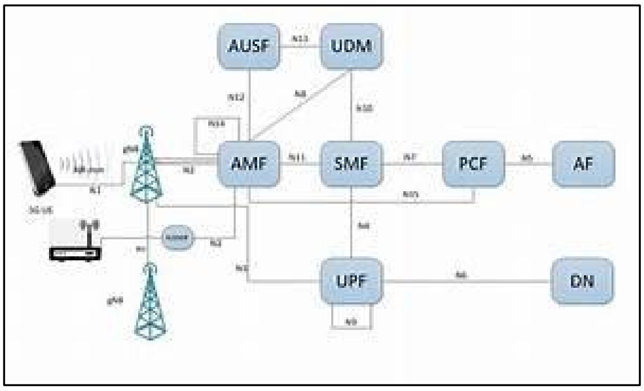

Fig.5 5G Network Architecture

Networks have evolved significantly in recent years to cater to customer needs. Take 5G as an example; it unifies the vast majority of the spectrum that is now accessible. This study aims to find a solution to the issue of resource distribution in 5G networks, namely in C-RANs or cloud radio access networks. When deploying a 5G network, the mechanisms of the radio access network should be improved with a plethora of access technologies, and the network topologies should be separated according to the frequency bands. The C-RAN is a great method to make the most of all the available spectrum bands. On the other hand, current C-RAN systems do not consider intelligence while selecting spectral bands. As a result, to distribute network resources for heavy traffic, the C-RAN mechanism necessitates a sophisticated tool for determining the network topology. So, it is important to suggest a system that manages spectral resources according to user needs and the network's operation. With certain modifications, it presented a novel C-RAN design for 5G environments as multitier heterogeneous cloud radio access networks. This design efficiently manages the spectrum of resources. From a network management standpoint, the simulation results show that the proposed multitier H-CRAN architecture with an upgraded control unit may increase granularity, optimize from end to end, and ensure the quality of service by 15% compared to the current system. [26]

Based on two-tier virtualization for vehicle networks, employing SDNs provides a flow-based policy framework in this research. This research aims to develop and test an architecture that can handle the complex needs of today's vehicle Internet networks using machine learning. Effectively managing network slicing has become challenging because the 5G-enabled networks tended towards robust communications. Through the experimental assessment of a special-purpose testbed set up in a bespoke mininet arrangement, this study also provides a proof of concept for using machine learning-enabled resource categorization and management. In addition, LSTM, CNN, and DNN have all been used to assess the effectiveness of the outcomes. At the end of the article, it is shown that LSTM has done better than the other classification methods, which is encouraging. [27]

mmWave communications' directional nature and vulnerability to obstruction cast serious doubt on the practicality of mmWave vehicle communications. With 5G vehicle circumstances often changing and directional mmWave communication being complicated, there is a need for more context awareness and adaptation. To achieve this goal, provide an online learning method that tackles the issue of beam selection in mmWave vehicular systems about environmental awareness. Our specific paradigm for this issue is that of a contextual multi-armed bandit. Then, present fast machine learning (FML), a small, context-aware, online learning algorithm that has a demonstrated performance constraint and will converge reliably. Using aggregated data and coarse user location information, FML learns and adapts to its surroundings. In addition, suggesting a standard-compliant protocol that considers the current and future cellular network design proves that FML can be used in the real world. Using real-world traffic patterns sourced from Google Maps, conduct a thorough examination. Testing confirms that mmWave base stations may learn from their surroundings and reach near-optimal performance (on average) in 33 minutes after deployment, thanks to FML. By quickly adjusting to changes in the system, such as blockages or traffic, FML can maintain performance within around 5% of its ideal level. [28]

. At the outset, this article lays out the 3GPP standard papers that specify the structure and protocols of NWDAF. The next step is to create a 5G network synthetic data set based on cells using the fields specified by the 3GPP standards. In addition, some outliers (such as a sharp spike in traffic to a certain cell) should be added to this dataset, and then these outliers should be classified according to the cell, subscriber type, and user equipment. Next, three machine learning models investigate NWDAF's capacity to estimate behavior information (such as network traffic abnormalities) and anticipate network load. The mean absolute error, determined by subtracting the model forecast value from the actual produced data, is minimized using three separate models for network load prediction. Results from the simulation show that when it comes to predicting network loads, neural network techniques are superior to linear regression, and when it comes to detecting anomalies, the tree-based gradient boosting approach is superior to logistic regression. According to these predictions, the 5G network's performance will be enhanced with NWDAF. [29]

Network slicing is designed to provide a wide variety of novel applications necessitating enhanced performance and adaptability by partitioning the physical network into many logical networks. As a result, these apps have caused a large influx of data from many mobile phones. The network slicing performance has been significantly affected by these extraordinary obstacles. This study aims to find an effective network-slicing method using a mixed-learning approach. After that, the OWFE, which produces a lot of scale variation by multiplying the attribute values with a weight function.. Using a hybrid classifier that combines deep belief and neural networks, classifies the specific network slices for each device based on the provided characteristics. In both networks, the GS-DHOA optimizes the weight function. The experimental findings showed the model's ability to impact the supply of precise 5G network slicing. [30]

The interconnection of numerous devices and machines, made possible by 5G and subsequent wireless networks, is essential for a wide range of vertical applications; yet, this diversity makes the networks more susceptible to spoofing assaults. Complex, dynamic wireless environments present unique problems for traditional cryptographic and physical layer authentication methods, such as high-security overhead, poor reliability, difficulty pre-designing an accurate authentication model, inability to provide continuous protection, and learning of attributes that vary over time. Using opportunistic exploitation of physical layer properties, propose novel machine learning-based authentication methodologies in this research, including supervised/unsupervised and reinforcement learning methods and parametric/non-parametric approaches. Machine Learning validates devices in unpredictable dynamics and unknown network conditions. These approaches are more cost-effective, reliable, continuous, and situation-aware. [31]

The DNS protocol is notoriously vulnerable as it uses unencrypted data. Sniffing, tangling, or just blocking it is possible. On the other hand, the attacker must be situated between two endpoints, and the attack model requires a malicious device. Despite increased DNS exchange latencies, this article demonstrates how Customer Edge Switching may be made more secure using the dedicated DNSCrypt and DNSSEC modules.

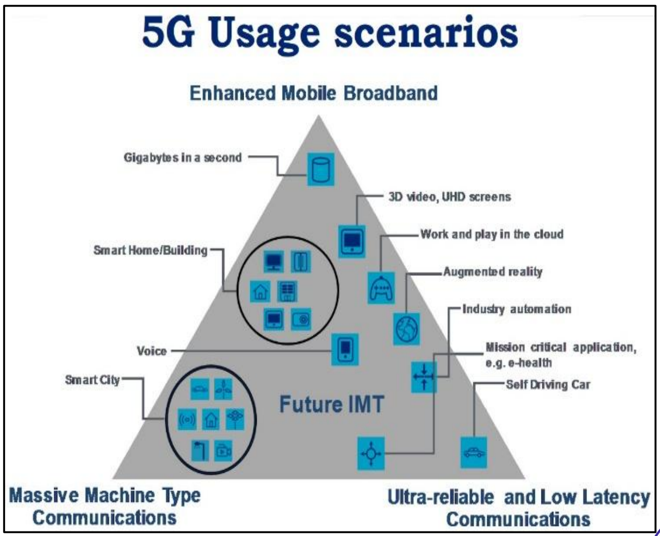
5G Usage scenarios
Enhanced Mobile Broadband
Gigabytes in a second
3D video, UHD screens
Work and play in the cloud
Smart Home/Building
Augmented reality
Industry automation
Voice
Mission critical application, e.g. e-health
Smart City
Self Driving Car
Future IMT
Massive Machine Type Communications
Ultra-reliable and Low Latency Communications

Fig.6 5G Usage Scenarios

It has been shown that both the CES and RGW scenarios are susceptible to assault. The outcomes of using DNSCrypt and DNSSEC to secure DNS and CETP packets are as anticipated. Based on the experimental findings, our key contribution is to assess the communication and demonstrate the extra latencies produced by these solutions. Further analysis reveals that the Google Public DNS server had an average latency of 63.575 ms and a median of 24 ms. DNSCrypt's median latency is 11.5 ms, and the average latency is 59.38 ms, making it somewhat quicker. Lastly, with an average value of 325.984 ms and a median of 286.5 ms, DNSSEC is noticeably slower than the previous options. It is recommended that DNSCrypt and DNSSEC be employed to protect CES, considering all of the experimental findings that have been achieved. Using DNSCrypt may be quicker than a regular method, and an authentication mechanism with DNSSEC adds a significant delay to DNS packet exchange latencies, according to experimental data. [32]

In this comprehensive 5G system security review, we conducted an exhaustive analysis of diverse research papers spanning various technologies. Through meticulous examination, the literature was categorized based on key security aspects such as authentication, encryption, threat detection, and mitigation strategies. Our findings underscore the critical importance of addressing security challenges in 5G networks, given the transformative potential of this technology. From exploring novel authentication protocols to investigating encryption mechanisms and advanced threat detection methodologies, the literature reveals a dynamic landscape fraught with challenges and opportunities. Despite facing interoperability issues and evolving cyber threats, promising advancements in AI-driven security analytics, zero-trust architectures, and collaborative threat intelligence platforms offer pathways to enhance 5G system security. By synthesizing insights from diverse sources, this review contributes to a deeper understanding of the current state of 5G security. It underscores the imperative of prioritizing security-by-design principles to safeguard the integrity and reliability of 5G networks in an increasingly interconnected world.

III. RESEARCH GOALS AND CONTRIBUTIONS

This study aims to examine 5G cybersecurity and its applications literature. The research catalogs cybersecurity, 5G networks, and security to identify key advancements, issues, and trends in this dynamic field. This report tries to illuminate 5G cybersecurity developments and operations.

There are many 5G security and cybersecurity breakthroughs from this study:

- Find First-Held Research: After a comprehensive search, the study team uncovered 41 significant articles on cybersecurity and 5G security in the business. Based on this unique study, an analysis follows.
- Data Analysis and Presentation: The data from the chosen studies is examined in depth. Combining inquiry findings, the study improves our knowledge of 5G security and cybersecurity. This assessment covers new advancements, common challenges, and industry trends.
- Concentrated View of Future Events: The summary of this study's findings may help researchers, stakeholders, and practitioners comprehend 5G security and cybersecurity. The paper identifies key areas for further research and development to improve 5G security.

This research fills a literature vacuum by analyzing 5G cybersecurity and its applications. The report provides insights into the current status and future directions to enable 5G networks to secure and resist cyber-attacks.

IV. CONCLUSION AND FUTURE SCOPE

After analyzing much information, this review paper sheds light on 5G system security. Have identified critical 5G security issues and trends via extensive research. The environment is changing, from authentication flaws to AI-powered attacks. Blockchain-based security frameworks and AI-based anomaly detection show promise despite these issues. The complex 5G network security issue requires policymakers, academia, and industry collaboration. By exploiting shared knowledge and promoting innovation, 5G security ensures that next-gen communication infrastructures are resilient to shifting threats.

Our extensive literature evaluation on 5G cybersecurity and its usage suggests many promising research pathways. The threat information feed integration must be examined to improve 5G security frameworks' threat identification and response. Due to the advent of quantum computing, 5G-specific cryptography approaches that are safe for quantum computers must be studied. Edge computing is crucial to 5G networks; hence, research on protecting distributed architectures and edge environments is needed. Consider the security risks of 5G network slicing and blockchain

DOI: 10.48175/IJARSCT-17427

integration for decentralized trust management. Future research should examine regulatory frameworks and privacy problems. By pursuing these approaches, researchers may improve 5G networks' security, resilience, and regulatory compliance, making them more trustworthy digitally.

REFERENCES

[1]. Ramraj Dangi, Praveen Lalwani, Gaurav Choudhary, Ilsun You, and Giovanni Pau, "Study and Investigation on 5G Technology: A Systematic Review", MDPI Sensors (Basel). 2022

[2]. Ishika Sahni, "A Systematic Literature Review on 5G Security", arXiv:2212.03299v1, 2022

[3]. Chataut R., Akl R. Massive MIMO systems for 5G and beyond networks—Overview, recent trends, challenges, and future research direction. *Sensors.* 2020

[4]. Alcardo Alex Barakabitze [a], Arslan Ahmad [b], Rashid Mijumbi [c], Andrew Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures, and future challenges", Computer Networks, 2020

[5]. Ahmad I., Kumar T., Liyanage M., Okwuibe J., Ylianttila M., Gurtov A. Overview of 5G security challenges and solutions. *IEEE Commun. Stand. Mag.* 2018

[6]. Park J.H., Rathore S., Singh S.K., Salim M.M., Azzaoui A.E., Kim T.W., Pan Y., Park J.H. A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions. *Hum.-Centric Comput. Inf. Sci.* 2021

[7]. Choudhary G., Kim J., Sharma V. Security of 5G-mobile backhaul networks: A survey. *arXiv.* 2019

[8]. Choudhary G., Sharma V. *A Survey on the Security and the Evolution of Osmotic and Catalytic Computing for 5G Network.* Springer; Berlin/Heidelberg, Germany: 2019

[9]. Rajoria S., Trivedi A., Godfrey W.W. A comprehensive survey: Small cell meets massive MIMO. *Phys. Commun.* 2018

[10]. Li S., Da Xu L., Zhao S. 5G Internet of Things: A survey. *J. Ind. Inf. Integr.* 2018

[11]. Parvez I., Rahmati A., Guvenc I., Sarwat A.I., Dai H. A survey on low latency towards 5G: RAN, core network, and caching solutions. *IEEE Commun. Surv. Tutor.* 2018

[12]. Dash L., Khuntia M. Energy efficient techniques for 5G mobile networks in WSN: A Survey; Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 2020

[13]. Jasim A.H.H., Ögren N., Minovski D., Andersson K. Packet probing study to assess sustainability in available bandwidth measurements: Case of high-speed cellular networks. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* 2020

[14]. Gerrit Holtrup; William Lacube; Dimitri Percia David; Alain Mermoud; Gerome Bovet; Vincent Lenders, "5G System Security Analysis", arXiv:2108.08700v2, 2021

[15]. Ijaz Ahmad; Tanesh Kumar; Madhusanka Liyanage; Jude Okwuibe; Mika Ylianttila; Andrei Gurtov, "5G security: Analysis of threats and solutions", IEEE Conference on Standards for Communications and Networking (CSCN), 2017

[16]. Kim H. 5G core network security issues and attack classification from network protocol perspective. *J. Internet Serv. Inf. Secure.* 2020

[17]. Lal N., Tiwari S.M., Khare D., Saxena M. Prospects for Handling 5G Network Security: Challenges, Recommendations and Future Directions. *J. Phys. Conf. Ser.* 2021

[18]. Kim J., Choudhary G., Heo J., Duguma D. G., You I. 5G wireless P2MP backhaul security protocol: An adaptive approach. *EURASIP J. Wirel. Commun. Netw.* 2019

[19]. Kiani A., Ansari N. Edge computing aware NOMA for 5G networks. *IEEE Internet Things J.* 2018

[20]. Kang M. The Study on the Effect of the Internet and Mobile-Cellular on Trade in Services: Using the Modified Gravity Model. *J. Internet Serv. Inf. Secur.* 2020

[21]. Mae M., Ohnishi W., Fujimoto H. MIMO multirate feedforward controller design with selection of input multiplicities and intersample behavior analysis. *Mechatronics.* 2020

[22]. Deka K., Sharma S. Hybrid NOMA for Future Radio Access: Design, Potentials and Limitations. *arXiv.* 2020

[23]. Slalmi A., Chaibi H., Saadane R., Chehri A., Jeon G. 5G NB-IoT: Efficient network call admission control in cellular networks. *Concurr. Comput. Pract. Exp.* 2021

DOI: 10.48175/IJARSCT-17427

[24]. Kaur J., Khan M.A., Iftikhar M., Imran M., Haq Q.E.U. Machine learning techniques for 5g and beyond. *IEEE Access.* 2021

[25]. Suomalainen J., Juhola A., Shahabuddin S., Mämmelä A., Ahmad I. Machine learning threatens 5G security. *IEEE Access.* 2020

[26]. Bashir A.K., Arul R., Basheer S., Raja G., Jayaraman R., Qureshi N.M.F. An optimal multitier resource allocation of cloud RAN in 5G using machine learning. *Trans. Emerg. Telecommun. Technol.* 2020

[27]. Tayyaba S.K., Khattak H.A., Almogren A., Shah M.A., Din I.U., Alkhalifa I., Guizani M. 5G vehicular network resource management for improving radio access through machine learning. *IEEE Access.* 2020

[28]. Sim G.H., Klos S., Asadi A., Klein A., Hollick M. An online context-aware machine learning algorithm for 5G mmWave vehicular communications. *IEEE/ACM Trans. Netw.* 2018

[29]. Sevgican S., Turan M., Gökarslan K., Yilmaz H.B., Tugcu T. Intelligent network data analytics function in 5g cellular networks using machine learning. *J. Commun. Netw.* 2020

[30]. Abidi M.H., Alkhalefah H., Moiduddin K., Alazab M., Mohammed M.K., Ameen W., Gadekallu T.R. Optimal 5G network slicing using machine learning and deep learning concepts. *Comput. Stand. Interfaces.* 2021

[31]. Fang H., Wang X., Tomasin S. Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks. *IEEE Wirel. Commun.* 2019

[32]. Nowaczewski S., Mazurczyk W. Securing Future Internet and 5G using Customer Edge Switching using DNSCrypt and DNSSEC. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* 2020

DOI: 10.48175/IJARSCT-17427