EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Overview of 5G & Beyond Security

Fawad Shokoor[1], Wasswa Shafik[2] and S. Mojtaba Matinkhah[2,*]

[1]Computer Engineering Department, Yazd University, P.O. Box 89175-741, Yazd, Iran
[2]Computer Engineering Department, Intelligent Connectivity Research Lab, P.O. Box 89175-741, Yazd University, Yazd, Iran

Abstract

Network security is a crucial concern when it comes to computation, concerns like threats can have high consequences, and critical information will be shared with unauthorized persons. This paper presents a detailed survey on Fifth Generation (5G) and security aspect. This is more predictable since the core technology; the synonymous approach is possible with Fifth Generation (5G) and Beyond Technologies though with limited access. Many incidents have shown that the possibility of a hacked wireless network, not just impacts privacy and security worries, but also hinders the diverse dynamics of the ecosystem. Security attacks have grown in frequency and severity throughout the near past, making detection mechanisms harder.

Keywords: 5G & Beyond, Network Security, Internet of Things, Software-Defined Networking, Network Function Virtualization

Received on 23 May 2022, accepted on 23 June 2022, published on 27 June 2022

doi: 10.4108/eetiot.v8i30.1624

*Corresponding author. Email: matinkhah@yazd.ac.ir

1. Introduction

Mobile network architecture has been offered to satisfy the changing needs of new network technology for increased capacity, accessibility, flexibility, and energy consumption [1]. Innovative networking technologies for instance Cloud Computing (CC), Software Defined Networking (SDN), Network Function Virtualization (NFV), Multi-Access Edge Computing (MEC), and Network Slicing (NS) technologies are being implemented into telecommunications networks by telecommunications standardization bodies [2] and [3].

These initiatives are aimed at developing a modern mobile software system. To satisfy the needs for the future evolution of mobile networks, this would help develop new and innovative network services. The concept of SDN offers decoupling of networking device regulation and user planes SDN based network-control and information are put in a controller logically centralized [4].

This could also give the control functions and the application layer for the company an overview of the underpinning system architecture. NFV provides a fresh method for the development, delivery, and management of networking services [5]. This idea is meant to separate network operations from branded hardware to be run as examples of software [6]. MEC and Cloud Computing can offer network scalability on-demand; see [7] and [8]. Network slicing increases support for various types of traffic in 5G networks. In this modern telecommunications network, privacy and security protection are now the key concerns, as threats can have high implications [9-12].

The network's software allows the 5G network to be perceived as a set of layers comparable to the SDN (software-defined network) networks. Where, 5G can accommodate a wide variety of items, from smartphones to different IoT devices [13] and [14]. IoT devices extend from basic kitchen appliances to sensors and other technologically sophisticated technology. Various RAT (Radio Access Technologies) for linking those computers would also be enabled by 5G [15].

In comparison to pre-4G technology, 5G will incorporate a variety of emerging wireless technologies, for example, Non-Orthogonal Multiple Access (NOMA), broad Multiple Input Multiple Output (MIMO), millimeter-wave (mm-Wave), and many more technologies for IoT networking [16-21]. Within Figure 1, an illustration of the high-level 5G system architecture is demonstrated.

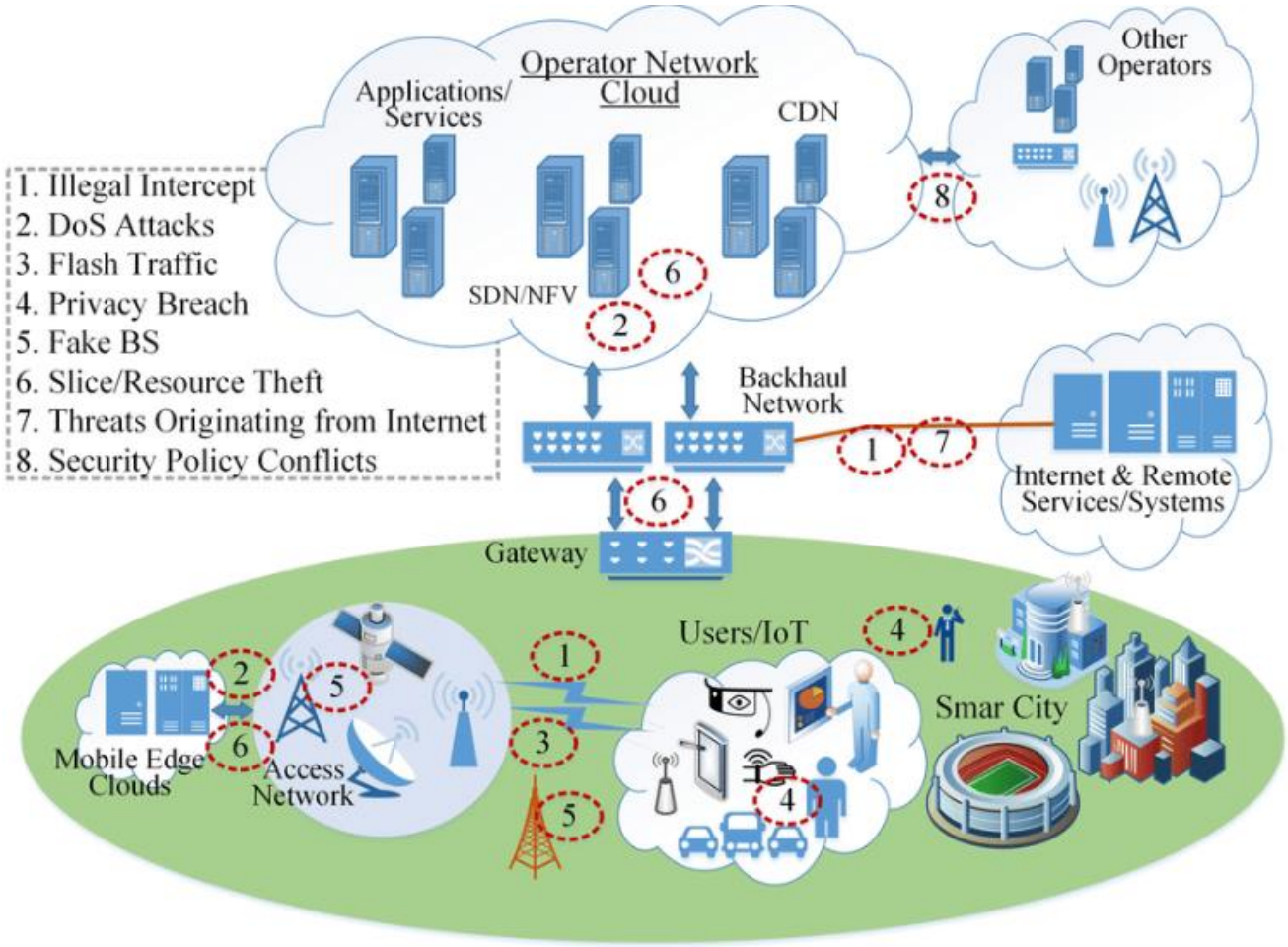

Figure 1. A 5g network and (8) eight security landscape threats.

In addition, most security architectures in pre-5G (that's to say, second-generation (2G), third generation (3G), and Fourth Generation (4G) networks will not be specifically used in 5G because of the current infrastructure and new technology [21] and [22]. But with some modification, some of the protection mechanisms can be used. The platform of Open-Air Interface (OAI) discussed compatibility backward in the large 5G sense with the prior generation and summary of the 5G Encryption Protocol enhancement [23, 24].

The main security goal of the telecommunications network ensuring the accurate operation of the payment system and the protection of the wireless medium by encrypting transmitting data. For 3G, double-way authentication is used to prevent links with fabricated BS from being established as illustrated in Figure 2. To authenticate users, modern cryptographic protocols are used by 4G. Also, it defends physical threats, like the actual destruction of base stations that can be installed in public and consumer properties.

Besides, any of the issues with privacy in the pre-5G network were addressed to some extent because consumer data was kept in mobile operators' records. 5G privacy and protection problems however overshadow these processes due to technological improvements and novel services. Three key components of 5G security and beyond 5G networks are made of, first, in 5G and beyond, practically most of the above vulnerabilities and pre-5G smartphone technology requirements are still applicable. Second, due to increasing customer numbers, a new set of security problems will be faced by 5G, connected device complexity, emerging network capabilities, elevated consumer privacy issues, emerging stakeholders, and IoT support requirements and mission-critical applications.

Third, the softwarization of the network and use of emerging technology like MEC, NS, SDN, and NFV will bring a whole new range of privacy and security issues. Fig. 3 describes the general perspective of the conditions for 5G Security that were developed based on these three elements. We intend to include a review of the cutting-edge technology (for example, NFV, MEC, SDN, etc.) that have been the key basic components of the 5G cellular network in this report. Another target is to consider the developments from MEC, NFV, SDN, and so on in security and privacy.

To this end, we concentrate mainly on the contributions that discuss the protection and privacy of 5G networks from both academia and industry.

As defined in Figure 4, also based on security risks and concerns relating to key 5G technology in this article. 5G is one of the widely popular areas of research for telecommunications professionals as the next wave of broadband networks. As a result, several reports on 5G networks have already been completed, [14-18].

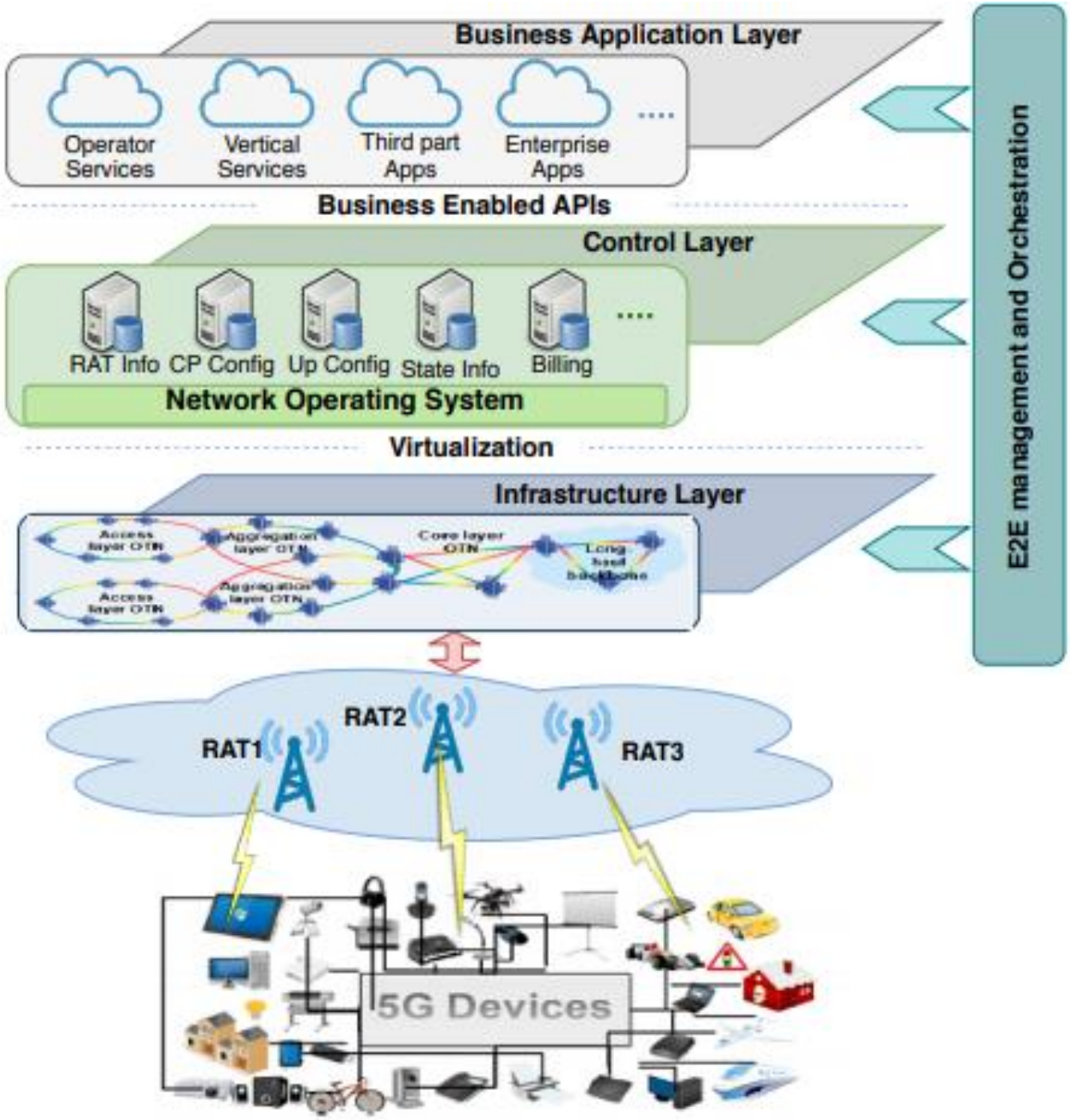

Figure 2. A 5g network top-level architecture with a different operating layer

These articles discussed many potential research opportunities, like infrastructure, flexibility organization, traffic organization, privacy, security, and technological economic features, which are extremely important to consider during the 5G implementation. The reliability of the 5G core network technologies is indefeasible consideration between these requirements. As one of the most critical criteria of the 5G testing area, therefore making security on spot.

A relatively small number of study articles have been released in the 5G security area [25-29]. Both facets of 5G technology have been considered in none of the above reports. But in the other hand, in various novel networks like MEC, NFV, SDN, NS, and cloud storage, 5G has produced software developments. Consideration of the protection of highlight 5G technology with security analysis in 5G networks is essential [30].

Many of these papers rely on certain technologies like protection NS, MEC, NFV, and SDN. Such reports are, however, very weak in resolving security concerns as they are incorporated into 5G networks. Such papers do not provide a thorough review of all the safety issues like hazard vectors, IoT protection, and network slicing, along with associated initiatives [31] and [32].

Therefore, this study includes a broad review of the cutting-edge security technologies and processes expected by the extension of previous 5G complementary security infrastructure works.

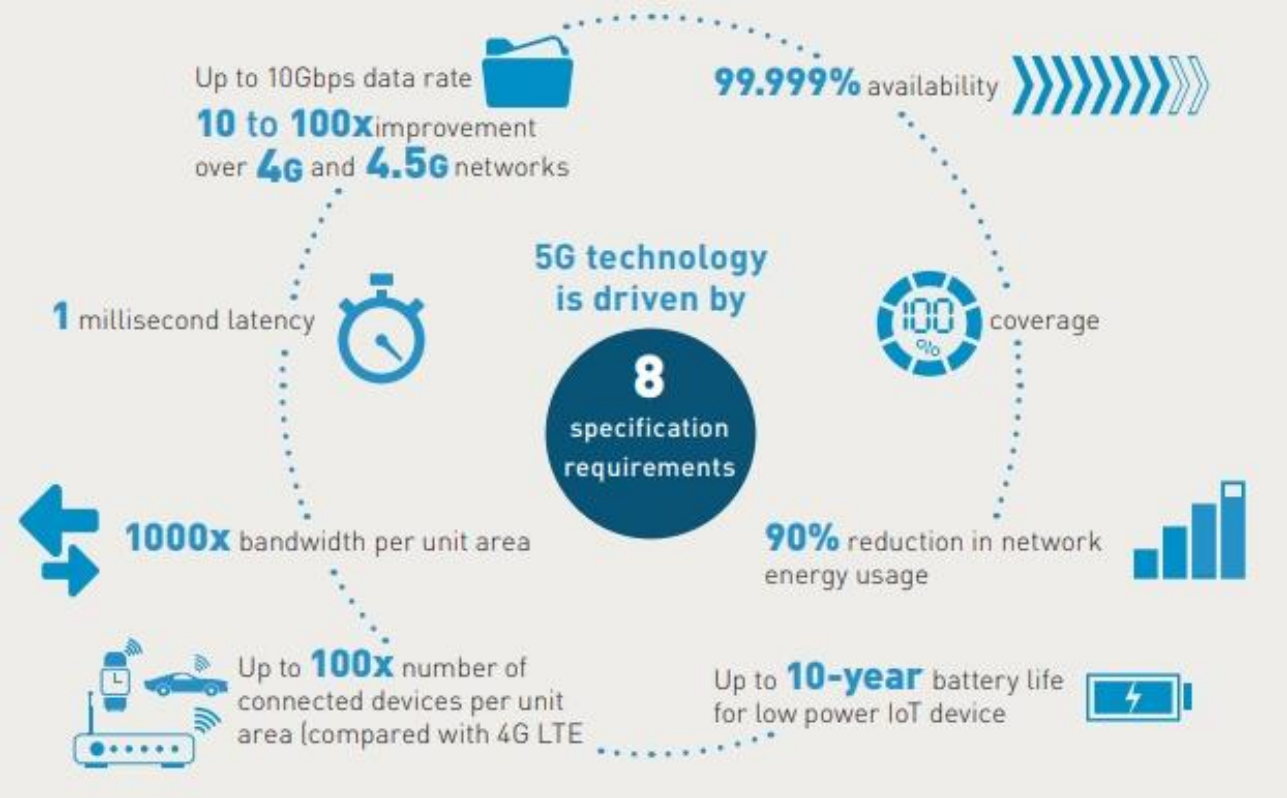

Figure 3. Eight specification requirements of 5G & beyond Technology.

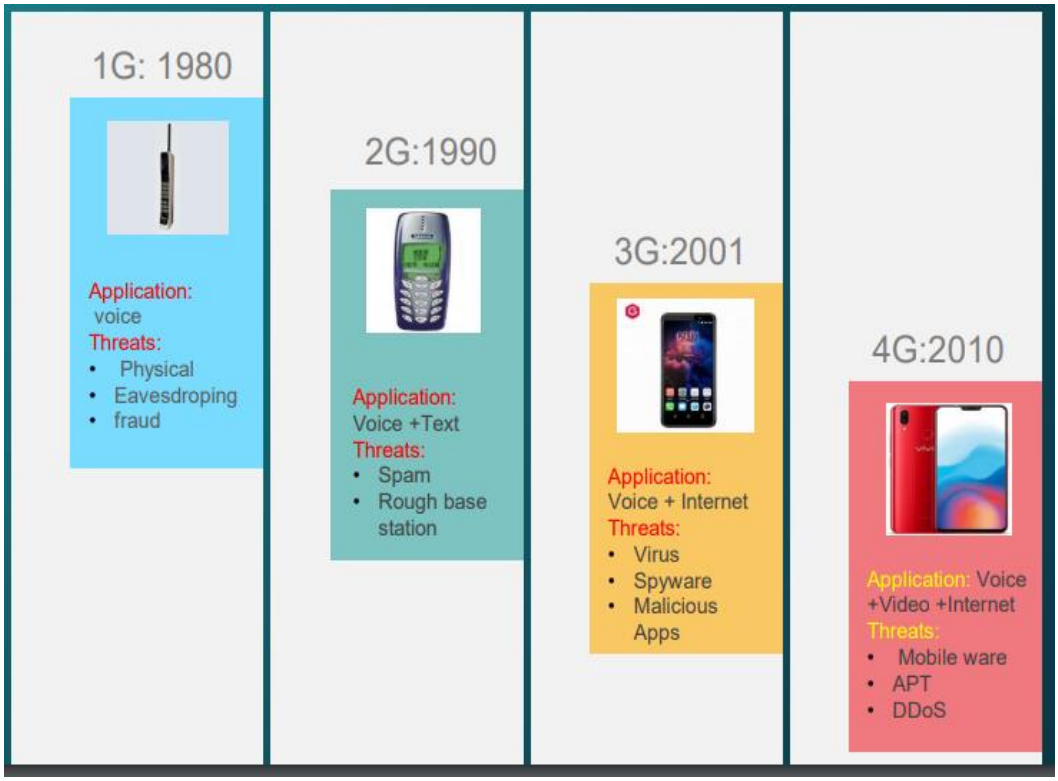

Figure 3. Mobile network security growth and threat environment

There is not a single report to the extent of our understanding that covers a wider spectrum of 5G security when including the whole of the main 5G innovations. Therefore, this is the first research on the main network softwarization techniques employed in 5G networks to address protection and privacy concerns. Because both network softwarization technologies are so important to 5G understanding, it is important to illustrate their protection and privacy interconnections, and security-associated interdependencies in future 5G networks in various network softwarization technologies.

The paper presents the following contributions to the security study in the 5G Networks a detailed review of 5G security architecture, a new generation 5G vulnerability environment, IoT vulnerability environments, and 5G network threat analyses. The paper also addresses the guidelines on security, that's to stay, NGMN and ITU-T define the core 5G security areas in state-of-the-art literature, and a variety of security concerns related to main 5G security zones in depth. Highlighting the main key security challenges belonging to key technologies: Identify and address the transparent protection and privacy problems relevant to main 5G high-tech; that say, CC, NS, SDN, NFV, and MEC. Focus on privacy at 5G, the study classifies consumer privacy and discusses data security issues for 5G networks.

The report outlined several policy priorities of the 5G networks in terms of data security and compliance mechanisms. And lastly a direction for future research: Based on our results, along with their early approaches and future guidance, we have outlined the potential and relevant study issues that need to be tackled. It helps prospective researchers find their paths for the prospective.

The rest of this paper is structured as the following: In section 2, the mobile network Securities are presented including Mobile network protection and vulnerability environment evolution, Generation Landscape of protection, and vulnerability. In section 3, 5G Developed Security Model are availed and presented including. In section 4, 5G security's main regions including communication security, encryption, data access, and authentication have been presented. Section 5 presents the conclusion of the article.

2. Mobile Network Security

The section presents the fundamental environment of the 5G communication system overall. The whole developed defined structure is addressed with a broad risk environment, Landscape of IoT Risks, review of 5G security vulnerabilities, and ITU-T protection guidelines, as well as NGMN in this unit.

2.1. Mobile network protection and vulnerability environment evolution

We have established telecommunications networks over four decades and are now at the beginning of the modern 5G broadband networks. With the growing generation of smartphones alongside, the environment of security for cellular networks also has improved [33]. The development of the mobile network security environment is demonstrated in Figure 4. By the beginning of the 1970s, only phreaking and hacking attacks left telephone networks vulnerable, and technological progress dramatically occurred at present [34] and [35]. Telecommunications have demonstrated that an informatics program has changed dramatically. Technological evolution occurred in tandem with growing safety concerns [36].

2.1.1. The 1G Landscape of protection and vulnerability

In the 1980s, the first mobile or 1G telecommunications network was formed. It was built on analogue technology. Only in a single country were 1G cell phones willing to afford voice call services [37]. 1G data networks were both named Advanced cell phone Service in the United States of America, and Nordic Mobile Telephony throughout the European Union. Roaming and services were not included in the list of coverage for the 1G Mobile Network. Nevertheless, with the implementation of 1G mobile access, network security risks remain.

Technology evolved rapidly mostly over time and created a complex environment to challenge. In 1G, hacking of the mobile network became easier because its radio channel had no cryptography protection owing to its analogue nature [38]. Hence it is easy to intercept the 1G calls. When the intruder tries to intercept a message, a radio scanner must be used and tuned to the appropriate frequency. The attacker intercepting such calls will access user identifications, for example, Mobile Identification Number and Electronic Serial Number [39]. To impersonate the user, those credentials can be used later to clone another machine. To deter attackers from listening to the channel, 1G networks later developed support for optional analogue scrambling. It was not as effective as cryptographic methods used in later generations of mobile devices, but they were able to avoid some scanning problems with these scrambling techniques [40].

2.1.2. 2G Security and Risk environment

The 2G telephone services were launched in 1991 after 1G mobile contact. 2G equipped smartphone users with a voice and messaging service. Introducing the data services was the first mobile generation, i.e., Quick Messaging Service (MS) [41]. In addition, it managed 2G networks in the digital domain. The 2G network provides a variety of security technologies, such as user

authentication using shared-secret cryptography, radio device traffic encryption, and anonymity of user identity protection. The SIM card used by 2G networks (Subscriber Identity Module) is a hardware identification system that holds a crypto function. It must be used on every smartphone, and it is tested for the identity of the phone subscriber [42] and [43].

The 2G suffered from a complex range of safety problems as well. In 2G networks, spamming was used by attackers as systemic attacks to send unwanted information to the users. This has contributed to a lot of malicious code in smartphone users. Attackers were using malicious code to malicious ends. One of the implemented hacking processes was interrupting mobile contact with fake authentication of rogue BSs [44]. In addition, all flux ciphers, that's to stay, using a text-only cipher attack, will crack in real-time using A5/1 and A5/2 used by the 2G in securing calls. Because of its store-and-forward nature, SMS still has security flaws. The contents of SMS roaming messages were leaked to foreign attackers residing on the Internet [45].

2.1.3. 3G Security and risk environment

These results encouraged smartphone researchers to introduce 3G mobile networking technologies to data applications and the Internet. Cell phones follow the simple ICT standards of human life. In 2001, the first commercial 3G network was introduced by NTT DoCoMo, using the Multiple Access WCDMA Wideband Code Division technology to allow access to mobile Internet. The 3G network bandwidth for mobile stations is originally 128 Kbps and 2 Mbps for wired systems. Quick data speeds and innovations like video calls, Multimedia Message Technologies (MMS), cell TV, and mobile Internet have been allowed in older 3G network models. The information gained from 2G protection concerns have worked to shape stronger 3G network safety mechanisms. Main vulnerability problems in 2G networks have been addressed in 3G, like shorter key lengths and a fake attack by BS [46]. In addition, the security of 3G technologies and frameworks have been developed in such a manner that it is possible to expand them and improved them to counter novel challenges and gratify emerging service protection necessities.

The security architecture in 3G was composed of five separate feature sets: (1) protection for the network; (2) protection for the client network; (3) the security of the user environment; (4) security for application; and (5) security visibility and security configuration. Several security risks to the operating system, user devices, and the computer were even revealed to 3G cellular phones [47]. The insecurity of cell phones has led to unauthorized access to malicious code that contains confidential user info.

Attacks like eavesdropping, subscriber impersonation, impersonation of compromised vector authentication, man-in-the-medium attacks, impersonation of the network, spoofing of location notifications, denial-of-service attacks like spoofing, and fake encampment for the base station were also subjected to 3G networks [48].

2.1.4. 4G Security and Risk Environment

In 2010, 4G was launched for 4G Long Term Evolution (LTE) and 4G networks, and earlier ones also made speeds of up to 100 Mbps possible. Using an upper layer protocol (IP) as a transmission channel provides awareness of service at each point within the network. 4G builds on the lessons learned by the 3G and 2G systems being applied. A new generation of encryption protocols and a key structure radically diverse from 3G and 2G is introduced by 4G. Advanced encryption algorithms are used for 4G, for instance, encryption algorithms and integrity Algorithms [49].

In comparison, in contrast to the 3G 128-bit keys, all 4G keys are 256-bit large. In addition, 4G supports diverse traffic control and user-plane algorithms and key sizes. The key 4G security method and authentication is known as AKA. (AKA) protocol and use include 3GPP TS 33.401. The non-access stratum besides the signalling protocol: radio resource control provides 4G air interface traffic with credibility and replay protection. The 4G traffic backhaul will then be encrypted via IPsec protocols [50].

The 4G-based open all-IP infrastructure is susceptible to many security attacks. 4G networks continue to suffer thousands of attacks and emerging challenges to Internet security, considering the consistent IP connection of the 4G core network to the Web. A wide variety of Internet-based threats, like TCP SYN DoS, IP address spoofing, User ID hacking, Network Hacking (ToS), intrusion attacks, and DoS (denial IP address), are vulnerable to 4G networks [51]. In addition, a certain amount of natural security was available for pre-4G networks due to the use of none of the key network IP protocols. This makes the attacker’s job hard. The attackers were finding it difficult to understand the complex mobile protocols. This barrier in 4G has been eased by the IP centre [52].

Furthermore, new 4G portable high-power systems are perfect outlets for worms, viruses, APT, DoS, and Botnet, to perform. In addition, several non-3GPP networks, like WiMAX and Wi-Fi, support 4G networks. The novel telecom providers with 4G technologies bring new deals, including fast coverage rates [53]. This also increased the importance of safety issues, however, APT and DDoS (Distributed Denial of Service) has a huge effect on network stability and have contributed to substantial financial losses. Attackers are trained and made smarter than wished. The existence of an IP-based 4G mobile network attack has been more difficult to detect in some of these threats.

2.1.5. 5G Risk Landscape

5G gives network infrastructure a mind-blowing upgrade. It will enable trillions of devices to work better than 4G devices with greater consistency, conveniences, speediness, structure efficiency, bandwidth usage, error tolerance, and dormancy. The 5G generation would provide a perfect platform for hackers because of IoT, the wired globe, and vital infrastructure networks. The high risk of attacks is against the politically and financially driven profits of perpetrators and practitioners with vast wealth and technological skills [54]. Thus, the provision of an acceptable standard of Défense is essential with the ever-evolving security hazard world of 5G connectivity. Incorporated transparency and uniform regulation into standard secrecy, integrity, and usability as two additional security standards to enhance consumer data security and privacy, as seen in Figure 5.

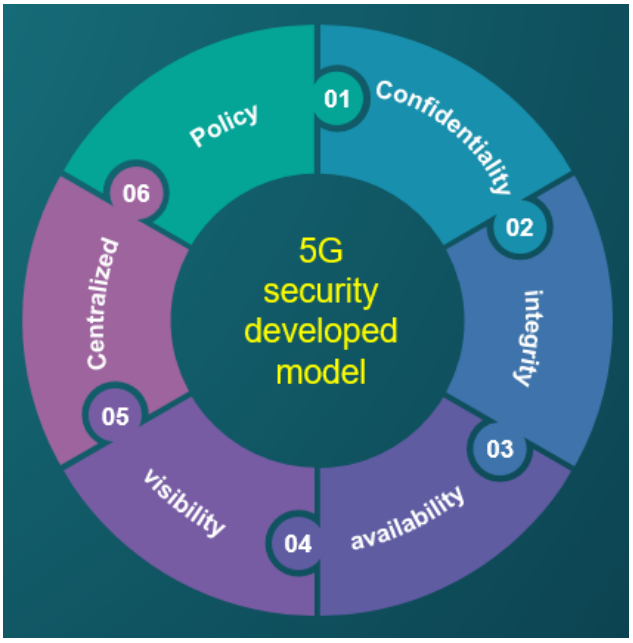

Figure 4. A 5g developed security model

3. 5G Developed Security Model

Not only are the standard audio and video calls restricted to wireless communication systems. We also endorse a host of apps that have unlocked up an extensive variety of testing problems for designers, including household applications, BYOD (Bring Your Device), cloud services, social media, games, and shopping. Phreaking is often not confined to the hacking of general records. Currently, it has developed into large cyber-attacks rings with powerful commercial, political, and private agendas [55]. The environment of IoT now has introduced additional great problems where the system link is initial a range of susceptibilities inside the 5G system [56].

3.1.1. Confidentiality

Information confidentiality is a key protection feature of the 5G security model; a property that can secure the transmission of data from unlawful disclosure and passive attachments (eavesdropping). All user plane info, considering the 4G-LTE and 5G architectures, must be confidential and protected against unauthorized applications. The implementations of the 5G network (like, the transport system and medical monitoring [57-61] the basic data encryption algorithms have been commonly used for user privacy. To encrypt or decrypt 5 G data with one private key, you can use the symmetrical key encryption algorithm. The correspondence actors (like a transmitter and a recipient) share this.

3.1.2. Integrity

This is to avoid the transition from one stage to another from tempering and loss of details. 5G Integrity traffic for NR (New Radio) is parallel to 4G security. Under 5G New Radio, layer security of the Packet Data Convergence Protocol (PDCP) is secured from wireless data traffic. For 4G LTE Integrity protection, the non-access stratum, and access stratum [61]. Nevertheless, 5G New Radio gives the security of the user plane's safety and a key advantage in 5G reputation protection. The reputation security of the customer plan was not promoted by 4G. This is significant. This novel function is particularly beneficial for minor IoT devices, for small data transmissions. In addition, integrity-protected signaling is used in the 5G-AKA authentication framework. It means that no unauthorized party can change or view airborne information [62].

3.1.3. Availability

Network accessibility within the 5G realm is structured to guarantee that system services could be reached anytime they are requested by legal consumers. as the availability impacts the service provider's reputation. In other words, the availability ensures that network infrastructure has a high probability of effectiveness. It also measures a network's sustainability against active assaults, such as a DDoS attack. On the system, DoS attacks would reduce performance. However, the network coverage could be attained by at minimum 95 percent and 99.99 percent correspondingly for 5G apps through the ultra-reliable machine-type-communication and extreme mobile broadband [63].

3.1.4. Unified Security Strategy

The developed structure of 3GPP 4G security in the 5G network cannot be extended explicitly to the latest 5G cases because they relate to the conventional operator-subscriber trust model. To support emerging technology (like SDN and NFV), a structured security policy management framework that gives consumers convenient

access to resources and applications is also required. A policy-based security management system (VISECO) was introduced by Thanh et al. to enable a unified security organization for 5G. The writers contended that mobile operators would protect their network infrastructure with the aid of VISECO [64].

3.1.5. Visibility

Visibility allows the E2E-control plane to be aware of mobile networks. It will handle the basic network problems effectively to guarantee a safe situation. The 5G technology can use robust end-to-end encryption strategies protecting all levels of the network, including application, signaling, and data planes. 5G operators will have full visibility, and inspection. To implement such a rigorous security system, 5 G providers would have complete visibility, monitoring, and control of total network layers [65].

5G technology can be paired with transparent APIs to manage security policies. SaaS (Security-as-a-Service) could also be approved by operators as a possible option for some customers, like IoT providers. In this way, the 5G network will provide clear device and hardware security policies within the network. Enhanced visibility through security and network policy will help incorporate dynamic protection frameworks that are suitable for emerging 5G services. In addition, enhancing visibility helps data-driven vulnerability monitoring to identify and separate the diseased devices previously attacks occur [66, 67].

3.1.6. Internet of Things Threat Landscape

Due to its attractive and unique features, a lot of interest has recently been drawn to IoT. The aim is to rely on millions of mobile computing devices to have a smart world. Considering Social-IoT based, Industrial-IoT based, fog-IoT, healthcare-IoT, and smart grids, smart power-IoT, several smart application networks have been offered. With the dramatic growth in technologies on the internet, the possibility of security risks and problems is also growing exponentially [68, 69]. Not simply is technology becoming better, but the threats are also becoming smarter. The issue requires to be urgently fixed. With its possible solutions Table 1; reveals a few of the threats found. Many scientists have obtained solutions to the risks found in various IoT domains.

The solutions to security problems for IoT systems are challenging because of low latency and high-density necessities. However, the authors studied statistically, systematically, and with hybrid detection, Commercial IoT network vulnerability risks, and identification schemes. To application designers, this review is especially helpful [76].

The authors evaluated risks to PLS and the industrial IoT environment, the plan for a wide variety of Physical Layer Security (PHY-Sec) technologies offers to fund better security for industrialized wireless systems. The potential vulnerabilities of man-in-the-middle attack attacks on the Open-Flow controller frequency in the fog-IoT, SDN schemes by implementing a feasible attack scenario into a fog-IoT architecture. The analysis of the S-IoT protection environment by offering a taxonomic overview from a ride, understanding, and stage of deployment viewpoint.

To define attacks on four levels, including networks, applications, communication, and device layers, the creation of the IoT smart water network to create the Model of risk, Abnormal Behavior Analyses-Intrusion Detection Systems (ABA-IDS). The authors addressed, while parts of the communication layer, the approach the proposed framework is used to protect the secure gateway. This model can detect a high detection rate of threats that are known and unknown [78].

3.1.7. Endorsements in Security by ITU-T

The security properties that ITU-T practically proposes are discussed in this subsection. As follows, these protection properties will address different facets of 5G domain ICT networks, applications, services, and records.

3.1.7.1. Access control

Systems prohibit a resource from being used maliciously, including preventing the use of a resource unlawfully. These systems (such as role-based management of access) usually guarantee that just designated customers, computers, or devices (for example write, read, among others) are enabled for network resources, files, flows of information, applications, and services.

3.1.7.2. Data confidentiality

Many apps capture and forward confidential data to a variety of stakeholders within a 5G network. In this way, privacy security protects data from unwanted exposure and assures that data information can be obtained by authorized users.

3.1.7.3. Data integrity

The attribute of Integrity assures that the transit information is not manipulated or that the information stays unaltered from source to destination.

3.1.7.4. Authentication

Person authentication is a tool used by a particular entity to assert its identity to a separate entity. A method of authentication will protect against impersonation attacks.

Table 1. Challenges and Strategies for IoT protection

Application	Attacks	Solutions	Protocols	References
Smart Water system- IoT	Cyber-attacks Security and Transferred Security.	ABA-IDS algorithm	Wi-Fi	[70]
IoT-based security components	Authorizations Authentications	OAuth 2.0-based oneM2M component	CoAP, MQTT	[71]
Generalized IoT	Eavesdropper collusions	PLS	Bluetooth, ZigBee, IEEE 802.15.4	[72]
IoT-based environment	Dolev-Yao threat	Signature-based AKA scheme	HLPSL	[73]
SDN-IoT-Fog	Man-in-the-middle Attack	Blood filter method	OpenFlow	[74]
Manufacturing Mobile-IoT based	Malware	Dynamic, static, and hybrid analysis		[75]

3.1.7.5. Network availability

This ensures that in regular operations, and even in disaster relief operations, the network is still available. Users and applications must be able to access network incidents that affect the system, like system crashes, security breaches, and natural disasters.

3.1.7.6. Non-repudiation

This feature would be used to show that a single peer is the owner of the message or obtained data. The validity of data or letters is not falsely questioned by this peer when the message is validated by the private key of the peer.

3.1.8. Risks and commendation by NGMN

Scientific advances introduce complex changes to the infrastructure design and the needs of the network. In 5G communications, attributable to a range of related devices, there seems to be a strong probability that security risks will develop. In line with network security demands and specifications, NGMN has given guidelines for its responses to some of the possible threats [79]. Table. 2, lists the possible safety risks and NGMN's recommendations. With many safety issues, for network management, network slicing, latency, MEC, and a basic user interface, NGMN has proposed both an explosion of the existing system and authentication.

4. 5G Security Main Regions

This section addresses the most challenging safety issues in 5G, for instance, connectivity, access management, authentication, and encryption, applicable to key areas of protection.

4.1. Authentication

Authentication plays a major safety function to verify the identity of users of any contact network. In each generation of mobile communication, various techniques had been used for authentication. This section however illuminates the authentication technique developed by 3GPP specifically for the 5G communication network. There is a simple authentication division preliminary, the primary and secondary authentication. In 3GPP Publication 15, the 3GPP fulfilled the 5G Step 1 regulatory requirement. Requires 5G phase 1 encryption authentication.

Primary authentication offers shared authentication to devices and networks in both 4G and 5G. However, primary authentication has also established slight variations due to the evolved 5G design. The built-in home search authentication system manages computer authentication information and call. Two mandatory solutions for 5 G phase 1 authentication are 5G-AKA and Extendable Authentication Protocol (EAP)-AKA.

Special instances, like private networks, optionally require authentication based on EAP. Because it is separate from the Radio Access (RA) scheme, in non-3GPP technologies, primary authentication will also work [80]. When the data network authentication is done outside the authority of a telecom provider is secondary authentication. In this process similar credentials and authentication mechanisms based on EAP are valid.

Table 2. Next Generation Mobile Networks Alliance (NGMN) risks and commendation

Area	Threats	Endorsements	Reference
Network Slicing	Contact is not safe between inter-network slices	Interaction between all slices, functions, and interfaces between them is managed and safe.	[76]
Access network	Chance of the main leakage between links of the operator	Powerful protection relation between operators or a new key sharing method	[77]
DoS Attack	Blocking services for a variety of users.	A sequence of defenses of overload, method of security overload, and design of new frameworks	[78]
MEC	Offering a third-party security firm	Expose protection resources only to trustworthy apps.	[79]
Latency	Mechanism of protection for latency goals	Adjustments in the 3GPP architecture, transferring the encryption mechanism to the lower layer.	[80]

Shared authentication and the supply of keyword content between the network and the UE can be done through key control and primary authentication procedures. The authentication protocols for the primary key and control require an essential key known as KSEAF. For network server SEAF, KSEAF provides the home network authentication service (AUSF) feature. The NF (Network Function) and AUSF provide UE authentication as per 3GPP and ETSI for NF petitioners in the core network of 5G. It permits the customer of the NF service to provide UE authenticated access and mobile management capabilities (AMF). For accomplishing the authentication, NF gives AUSF the identity of UEs and uses the name of the network. The info gained by AMF now AUSF is using the information for authentication based on the 5G-AKA or EAP [64].

Other researchers have studied 5G frameworks for security threats to different risks and scenarios. Conducted a systematic review of the 5G AKA protocol that included correct specifications from the 3GPP 5G guidelines and highlight the missed safety targets [73]. To authenticate BS, the necessity in the current 5G authentication protocol is met by an algorithm-supplied study above 5G-AKA. This has exposed 5G-reliance AKAs on the underlying infrastructure. The device vulnerability is abused by a restoration of the attack on 5G or protocol [74].

An analysis of 4G and 5G, and problems with AAA (Authentication Authorization and Accounting) implementation flaws. The consistency of the current Universal Subscriber Identity Modules with the 5G AKA full privacy protocol. In compliance with the heterogeneous 5G network criteria, an innovative community-based AKA threat model has been suggested by the authors [60]. Except for the IMSI-catcher attack, all recorded 5G-AKA attacks are still valid and have supported an updated preventive version of 5G-AKA [75].

4.2. Access control

To regulate selectively access to the network is the primary goal for access control. For providing reliable and harmless communication networks Access control systems have since been operated by network operators. For any network protection program, this is the key building block. The access management process just ensures access to the network by authorized users [77].

Network decentralization of some of the recent access management systems improves the network infrastructure's stable setting. An entry selection scheme alongside several eavesdroppers was suggested for D2D PLS [78]. In the current scheme, D2D networking systems are sharing bandwidth with cellular users in respect of distance thresholds. The authors caused interference that the authors used jamming to deceive eavesdroppers. The eavesdropper security norm was optimized by the optimum achievement of the access filtering scheme throughput. The security pair D2D is used to secure one single person.

An automated ConfigSynth system was developed to provide a precise network configuration that is affordable and synthesizing [79]. The proposed structure is further refined by creating a refinement mechanism to provide greater protection. Isolation is given by the suggested algorithm, improving traffic flow and safety system sharing. To prevent downgrade attacks with a fake LTE BS from IMSI (International Mobile Subscriber Identity), advocated using an existing approach based on pseudonyms and a method to change LTE pseudonyms. An attack called RPEDO is addressed to find security problems with the paging protocol [80].

A collection of proposed access control approaches has been presented by numerous scholars focused on key distribution, encryption, and authentication. To ensure user safety, Transparent and APAC (Privacy-Enhanced Access Control) were suggested. The protocol's validity by implementing minimal experimental tools. A special biometric-password authentication scheme for the information system. Without remote server participation, the proposed methodology provides secrecy, confidentiality, less computational expense, and effective authentication [81].

Table 1. Security concerns linked to 5G communication issues

Attacked part	Threat	Definition	Reference
User Equipment	Botnet	A botnet is a form of malware capable of exploiting a series of computers connected to the internet.	[65]
	Attacks through Mobile Malware	Mobile malware helps attackers to harvest private information stored on a computer.	
Access Network	Attacks focused upon evidence of incorrect buffer status	To gain data like load balancing, packet scheduling, and algorithms for admission control.	[66]
	Message Threat injection	The DoS attacks would be triggered by Message Injection Attacks on 5G networks.	[67]
	Microcell Attacks	BSs' overall footprint is greatly diminished and there are enclosed spaces like stadiums, public houses, malls, and hospitals.	[69]
Core Network	Denial-of-service Attack	DDoS attacks can be carried out using a botnet to monitor many infected UEs in the type of Signals Propagation and HSS overload.	[70]
	TLS/SSL Attacks	Attack assaults are vulnerable to SDN-based TLS or SSL contact.	[71]
	SDN Scanner	Through monitoring SDN traffic hackers	[72]

An access control scheme focused on updating the encrypted message and computation servicing for IoT in fog computing. User data is ABE-encrypted and then stored in the cloud [82]. A stable and productive safety scheme was provided. Centered on CP-ABPRE (Cipher Text-Policy Attribute-Based Proxy Re-Encryption) and top-secret distribution, the data distribution of a security system for several customers of OSNs (Online Social Networks) was implemented. A portion decryption design to decrease user overhead computing by assigning decryption processes to OSNs, checking the capacity of OSN to cross-check decrypted data, and attributing reversal methods for backward and forward secrecy [83].

Classification of 5G core network traffic, like customer data traffic and traffic management, into two forms. Several of these forms of traffic are prone to specific security attacks. The absence of protection at the IP level is the main security issue relating to traffic management. Upper layer authentication protocols like TLS (Transport Layer Security) or SSL (Protected Sockets Layer) connections are used to defend the control channel on the current SDN-based 5G core network. At the IP level, they have recognized weaknesses, like Spoofing, message manipulation attacks, eavesdroppers' attacks, IP spoofing, TCP SYN DoS, and TCP reboot attacks [84].

Consequently, it is important for using IP-level safety features alongside higher layer protection mechanisms. In wide SDN networks, several SDN controllers have been used for controlling small network sections like cell networks. To establish ICC (Inter-Controller Communication), the east or west-bound interface among these several SDN controllers is used. It aids execute various network functions in the sharing of control information, such as coordination of security policies, managing of mobility, traffic control, and surveillance of networks [85].

4.3. Encryption

Encryption is of particular importance for ensuring data confidentiality. E2Eencryption is important in the 5G environment, Because of the rich variety of novel internet services. This will be used to block overlooked segments of the network from unwanted conations to mobile data. Network data will be encrypted at the PDCP (Packet Data Convergence Protocol) layer in 5G. The user plan uses three separate 128-bit secret keys, the NAS (Non-Access Stratum) and the AS (Access Stratum), equivalent to the 4G LTE network. Moreover, to this, the 5G Modern Radio (NR) can use some of the 4G encryption algorithms [86].

The same EPS Encryption Algorithms (EEA) based null, SNOW 3G and AES (Advanced Encryption Standard) algorithms could also be used in 5G according to the 3GPP 5G standards. In 5G, however, the identifiers have been altered. 5G redefines 4G EPS Encryption Algorithm (EEA) as NR Encryption Algorithm (NEA).

One of the most important 5G traffic speeds is URLLC (Ultra-Reliable Low Latency Communication) [87].

4.4. Communication security

To endorse a wide variety of vertical elements in 5G Eco networks, 5G Connectivity aims to have high network speed, low latency connectivity, and wide signal coverage. Therefore, along with design updates and emerging infrastructure incorporation, 5G communication would be updated. Though, these enhancements can also cause major security problems for future 5G mobile networks [88].

Attacks will be carried out on 5 G networking in various parts, like UEs, access networks, and the core mobile operator network. The attacks associated with numerous 5G communication sections are also summarized in Tab. 3, to better explain the possible security vulnerabilities and risks concerning 5G communication. Attacks and threats on traditional mobile networks can also be discussed (such as 4G, 3G, and 2G). Any of these attacks are also taking place on 5G networks [89].

In addition, in protecting privacy, 5G cryptography plays an important role. In required to conform with the current regulations on privacy in Europe, such as GDPR (General Data Protection Regulation) and the continuing review of the Privacy Directive, it is also essential to mention that the need for private security in 5G networks is a major priority. Consequently, 5G systems are configured to provide user privacy rights. All these long-term and short-term user identities are secured by consuming a cover-up system focused on the ECIES (Elliptic Curve Integrated Encryption Scheme) and using the public key of the home operator [90] and [91].

In turn, the IMSI encryption is going to be included in 5G to prevent IMSI catcher threat. IMSI gathers and monitors customers. This is violating their privacy [92]. To accomplish this purpose, the authors suggest a new IMSI encryption algorithm. A new pair with its random number and asymmetric public or private key desires to be generated by a mobile application. In 5G it's possible because existing USIMs can now perform randomized asymmetric encryption [93-95].

5. Conclusion

The 5G network environment is changing rapidly, creating an increasing variety of security risks at multiple levels and implementations. Via spectacular views analyses and discussions focused on current literature, this paper addressed the 5G security challenge and sought to provide an accurate interpretation of security concerns. The comprehensive 5G security model analysis, next generation 5G threat setting, IoT threat scenarios, and 5G threat research of the network have been investigated. A detailed review of security problems in core 5G security areas was covered in our study, including access control, authentication, communication protection, and encryption.

Acknowledgements.

The authors in nutshell would like to distinguish the support and comments shared with us by the computer engineering department members to attain this paper's quality.

Data Availability Statement: All the data that was used to support the results of this study are encompassed within the paper.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding this study.

References

[1] M. Agarwal, A. Roy and N. Saxena, "Next generation 5g wireless networks: a comprehensive survey," IEEE Communication Surveys and Tutorial. vol. 18, no. 3, pp. 1617–1655, 2016.

[2] L. Zhao, D. Zhu, W. Shafik, S. M. Matinkhah, Z. Ahmad et al., “Artificial intelligence analysis in cyber domain: A review,” International Journal of Distributed Sensor Networks, vol. 18, no. 4, pp. 15501329221084882, 2022.

[3] W. Shafik, S. M. Matinkhah, F. Shokoor and L. Sharif, “A reawakening of machine learning application in unmanned aerial vehicle: future research motivation,” EAI Endorsed Trans. Internet Things, vol. 8, no. 29, pp. e3–e3, 2022.

[4] A. Irshad, S. A. Chaudhry, A. Ghani and M. Bilal, "A secure blockchain-oriented data delivery and collection scheme for 5G-enabled IoD environment" Computer Networks, vol. 195, pp. 108219, 2021.

[5] W. Shafik, S. M. Matinkhah and F. Shokoor, “Recommendation system comparative analysis: internet of things aided networks”, EAI Endorsed Trans IoT, vol. 8, no. 29, pp. 5, 2022.

[6] G. Maier and M. Reisslein, "Transport sdn at the dawn of the 5g era," Optical Switching and Networking, vol. 33, pp. 34-40, 2019.

[7] W. Shafik, S. M. Matinkhah, S. S. Afolabi and M. N. Sanda, “A 3-dimensional fast machine learning algorithm for mobile unmanned aerial vehicle base stations,” International Journal of Advances in Applied Sciences, vol. 2252, no. 8814, pp. 8814, 2020.

[8] H. Meng, W. Shafik, S. M. Matinkhah and Z. Ahmad, “A 5g beam selection machine learning algorithm for unmanned aerial vehicle applications,” Wirel. Commun. Mob. Comput., 2020.

[9] M. S. Bonfim, K. L. Dias and S. F. L. Fernandes, "Integrated nfv/sdn architectures: a systematic literature review," ACM Computing Surveys, vol. 51, no. 6, 2020.

[10] W. Shafik, S. M. Matinkhah, and M. Ghasemzadeh, “A fast machine learning for 5g beam selection for unmanned aerial vehicle applications,” Journal of Information

Systems and Telecommunication, vol. 7, no. 28, pp. 262–278, 2019.
[11] W. Shafik, S. M. Matinkhah and M. Ghasemzadeh, “A mobile fuzzy sink scheme for wireless sensor network period improvement,” 8th Iranian Joint Congress on Fuzzy and intelligent Systems, Mashhad, Iran, pp. 211–216, 2020.
[12] S. Kitanov, B. Popovski and T. Janevski, "Quality evaluation of cloud and fog computing services in 5g networks," Enabling Technologies and Architectures for Next-Generation Networking Capabilities, pp. 1-36, 2019.
[13] A. Irshad, S. A. Chaudhry, A. Ghani, G. A. Mallah, M. Bilal, B. A. Alzahrani, "A low-cost privacy preserving user access in mobile edge computing framework" Computers & Electrical Engineering, vol. 98, 107692, 2022.
[14] W. Shafik, M. Matinkhah, M. Asadi, Z. Ahmadi and Z. Hadiyan, “A study on internet of things performance evaluation,” Journal of Communications Technology, Electronics and Computer Science, pp. 1–19, 2020.
[15] S. A. Chaudhry, A. Irshad, M. M. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, and Y. B. Zikria "A Lightweight authentication scheme for 6G-IoT enabled maritime transport system." IEEE Transactions on Intelligent Transportation Systems, 2021.
[16] R. Ahmed, A.K. Malviya, M.J. Kaur and V.P. Mishra, "Comprehensive survey of key technologies enabling 5g-iot," 2nd International Conference on Advanced Computing and Software Engineering (ICACSE), Siltanpur, UP, India, pp.1-5, 2019.
[17] L. Shao-Yu, C.C. Tseng, I. Moerman and L. Badia, "Recent advances in 5g technologies," New Radio Access and Networking, pp. 1-9, 2019.
[18] W. Shafik and S. M. Matinkhah, “Admitting new requests in fog networks according to erlang b distribution,” 27th Iranian Conference on Electrical Engineering, Yazd, Iran, 2019.
[19] A. Irshad, S. A. Chaudhry, M. Alazab, A. Kanwal, M. S. Zia and Y. B. Zikria, "A secure demand response management authentication scheme for smart grid." Sustainable Energy Technologies and Assessments, 48, 101571, 2021.
[20] M. Azrour, J. Mabrouki, A. Guezzaz et al., "Internet of Things Security: Challenges and Key Issues" Security and Communication Networks, 2021.
[21] A. Gupta and R.K. Jhk, "a survey of 5g network: architecture and emerging technologies", IEEE Journals & Magazine, vol.3, pp. 1206-1232, 2020.
[22] [22]Y. Jun, A. Craig, W. Shafik and L. Sharif, “Artificial intelligence application in cybersecurity and cyberdefense,”Wireless Communications and Mobile Computing, vol. 2021.
[23] S. M. Matinkhah, W. Shafik and M. Ghasemzadeh, “Emerging artificial intelligence application: reinforcement learning issues on current internet of things,” in 2019 16th international Conference in information knowledge and Technology, Tehran, Iran, 2019.
[24] A. Gohil, H. Modi and S.K. Patel, "5G technology of mobile communication: A survey," International Conference on Intelligent Systems and Signal Processing (ISSP), Gujarat, pp. 288–292, 2013.
[25] N. Panwar, S. Sharma and A.K. Singh, "A survey on 5G: The next generation of mobile communication," Physical Communication, vol. 18, pp. 64–84, 2016.
[26] M. Jaber, M.A. Imran, R. Tafazolli and A. Tukmanov, "5G backhaul challenges and emerging research directions: a survey," IEEE Access, vol. 4, pp. 1743–1766, 2016.
[27] R.N. Mitra and D.P. Agrawal, "5G mobile technology: A survey," ICT Express, vol. 1, no. 3, pp. 132–137, 2015.
[28] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5g security challenges and solutions," IEEE Communication Standard Magazine, vol. 2, no. 1, pp. 36–43, 2018.
[29] M.A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," Journal of Network Computing Application, vol. 101, pp. 55–82, 2018.
[30] G. Choudhary and V. Sharma, "A survey on the security and the evolution of osmotic and catalytic computing for 5g networks," in 5G Enabled Secure Wireless Networks, Springer International Publishing, pp. 69–102, 2019.
[31] M. Chen, Y. Qian, S. Mao, W. Tang and X. Yang, "Software-defined mobile networks security," Mobile Network Application, vol. 21, no. 5, pp. 729–743, 2016.
[32] P. Gandotra and R.K. Jha, "A survey on green communication and security challenges in 5G wireless communication networks," Journal of Network Computing Application, vol. 96, pp. 39–61, 2017.
[33] W. Shafik, S. M. Matinkhah, and M. Ghasemazade, “Fog-mobile edge performance evaluation and analysis on internet of things,” Journal of Advance Research in Mobile Computing, vol. 1, no. 3, pp. 1–17, 2019.
[34] Z. Yang, L. Jianjun, H. Faqiri, W. Shafik, A. T. Abdulrahman, Yusuf M, Sharawy AM. et al., “Green internet of things and big data application in smart cities development,” Complexity, 2021.
[35] W. Shafik and S. M. Matinkhah, “How to use Erlang B to determine the blocking probability of packet loss in a wireless communication,” 13th Symposium on Advances in Science & Technology, Mashhad, Tehran 2018.
[36] Y. Lin, Z. Ahmad, W. Shafik, S. K. Khosa, Z. Almaspoor et al., “Impact of facebook and newspaper advertising on sales: a comparative study of online and print media,” Computational intelligence and neuroscience, 2021.
[37] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," IEEE Journals & Magazine, vol. 104, no. 9, pp. 1727-1765, 2020.
[38] Y.E.H.E. Idrissi, N. Zahid and M. Jedra, "Security analysis of 3gpp (lte) — wlan interworking and a new local authentication method based on eap-aka," in The First International Conference on Future Generation Communication Technologies, London, England, pp. 137–142, 2012.
[39] M. Liyanage and A. Gurtov, "Secured vpn models for lte backhaul networks," in IEEE Vehicular Technology Conference (VTC Fall), Quebec City, Canada, pp. 1–5, 2012.
[40] W. Shafik, S. M. Matinkhah, and M. Ghasemzadeh, “Internet of things-based energy management, challenges, and solutions in smart cities,” Journal of Communications Technology, Electronics and Computer Science., vol. 27, pp. 1–11, 2020.
[41] M. Liyanage, M. Ylianttila and A. Gurtov, "Ip-based virtual private network implementations in future cellular networks," Handbook of Research on Progressive Trends in Wireless Communications and Networking, pp. 44-66, 2020.
[42] S. Gold, "The rebirth of phreaking," Network Security, vol. 2011, no. 6, pp. 15-17, 2011.
[43] J. Granjal, E. Monteiro and J. Sá Silva, "Security for the internet of things: a survey of existing protocols and open

research issues," IEEE Communication Survey Tutorial, vol. 17, no. 3, pp. 1294–1312, 2015.
[44] W. Shafik and S. A. Mostafavi, “Knowledge engineering on internet of things through reinforcement learning,” International Journal of Computer Applications, vol. 975, pp. 8887, 2019.
[45] W. Shafik, M. Matinkhah, and M. N. Sanda, “Network resource management drives machine learning: a survey and future research direction,” Journal of Communications Technology, Electronics and Computer Science, pp. 1–15, 2020.
[46] W. Shafik and S. M. Matinkhah, “Privacy issues in social Web of things,” 5th International Conference on Web Research, Tehran, Islamic Republic of Iran, pp. 208–214.
[47] X. Zhang, A. Kunz and S. Schröder, "Overview of 5g security in 3gpp," in IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, pp. 181–186. 2017.
[48] M. H. Eiza, Q. Ni and Q. Shi, "Secure and privacy-aware cloud-assisted video reporting service in 5g-enabled vehicular networks," IEEE Transaction on Vehicular Technology, vol. 65, no. 10, pp. 7868–7881, 2016.
[49] Z. Chen, F. Zhang, P. Zhang, J.K. Liu and J. Huang, "Verifiable keyword search for secure big data-based mobile healthcare networks with fine-grained authorization control," Future Generation Computer System, vol. 87, pp. 717-724, 2018.
[50] W. Shafik, M. Matinkhah, P. Etemadinejad, and M. N. Sanda, “Reinforcement learning rebirth, techniques, challenges, and resolutions,” International Journal on Informatics Visualization, vol. 4, no. 3, pp. 127–135, 2020.
[51] S. M. Matinkhah and W. Shafik, “Smart grid empowered by 5G technology,” in 2019 Smart Grid Conference (SGC), Tehran, Iran, pp. 1–6, 2019.
[52] W. Shafik, S. M. Matinkhah, and M. Ghasemzadeh, “Theoretical understanding of deep learning in uav biomedical engineering technologies analysis,” SN Computer Science, vol. 1, no. 6, pp. 1–13, 2020.
[53] S. Choi, J. Song, J. Kim, S. Lim, S. Choi, etl., "5g k-simnet: end-to-end performance evaluation of 5g cellular systems," in 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, United States of America, pp. 1-6, 2019.
[54] S. Gupta, B.L. Parne and N.S. Chaudhari, "Security vulnerabilities in handover authentication mechanism of 5g network," in First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, pp. 369–374, 2018.
[55] M. S. Berger and H. L. Christiansen, "Fronthaul for cloud-ran enabling network slicing in 5g mobile networks," Wireless Communications and Mobile Computing, vol. 2018, 2020.
[56] W. Shafik and S. M. Matinkhah, “A Portable Fuzzy sink scheme for wireless sensor network life expectancy enhancement,” IEEE Iranian Joint Congress on Fuzzy and intelligent Systems, 2020.
[57] S. M. Matinkhah and W. Shafik, “A study on financial pricing and applications models on 5g,” 4th International Conference in Financial Mathematics, Yazd, Iran, pp. 54-60, 2019.
[58] S. M. Matinkhah and W. Shafik, “Broadcast communication analysis for 5g media radio access networks,” In 16th Conference on Broadcast and Exhibition, Tehran, Iran, 2019.
[59] T.Q. Thanh, S. Covaci and T. Magedanz, "Viseco: an annotated security management framework for 5g," In International Conference on Mobile, Secure, and Programmable Networking, Mohammedia, Morocco pp. 251-269, 2018.
[60] F. Al-Turjman, "5g-enabled devices and smart-spaces in social-iot: an overview," Future Generation Computing System, vol. 92, pp. 732–744, 2019.
[61] M. Agiwal, N. Saxena and A. Roy, "Towards connected living: 5g enabled internet of things (iot)," IETE Technical Review, vol. 36, no. 2, pp. 190-202, 2019.
[62] S. Sharmeen, S. Huda, J.H. Abawajy, W.N. Ismail and M.M. Hassan, "Malware threats and detection for industrial mobile-iot networks," IEEE Access, vol. 6, pp. 15941–15957, 2018.
[63] F. Jameel, M.A. Javed, D.N.K. Jayakody and S.A. Hassan, "On secrecy performance of industrial internet of things," Internet Technology Letters, vol. 1, no. 2 pp. 1-32, 2020.
[64] S. Mostafavi and W. Shafik, “Fog computing architectures, privacy and security solutions,” Journal of Communications Technology, Electronics and Computer Science, vol. 24, pp. 1–14, 2019.
[65] W. Shafik, S. M. Matinkhah, M. N. Sanda, and F. Shokoor, “Internet of things-based energy efficiency optimization model in fog smart cities,” International Journal on Informatics Visualization, vol. 5, no. 2, pp. 105–112, 2021.
[66] W. Shafik and S. M. Matinkhah, “Unmanned aerial vehicles analysis to social networks performance,” CSI Journal on Computer Science and Engineering, vol. 18, no. 2, pp. 24-31, 2021.
[67] F. Pan, Z. Pang, M. Luvisotto, M. Xiao and H. Wen, "Physical-layer security for industrial wireless control systems: basics and future directions," IEE Industrial. Electronic Magazine, vol. 12, no. 4, pp. 18–27, 2018.
[68] C. Li, Z. Qin, E. Novak and Q. Li, "Securing sdn infrastructure of iot–fog networks from mitm attacks," IEEE Internet Things Journal, vol. 4, no. 5, pp. 1156–1164, 2017.
[69] W. Shafik, S. M. Matinkhah and S. "Dimensional fast machine learning algorithm for mobile unmanned aerial vehicle base stations," International Journal of Advances in Applied Sciences, 2252, no. 8814, pp. 8814, 2020.
[70] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the iot world: present and future challenges," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2483–2495, 2018.
[71] J. Pacheco, D. Ibarra, A. Vijay and S. Hariri, "IoT security framework for smart water system," in IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia, pp. 1285–1292, 2017.
[72] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury and E. Bertino, "Insecure connection bootstrapping in cellular networks," Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, Miami, Florida, pp. 1-11, 2019.
[73] C. Cremers and M. Dehnel-Wild, "Component-based formal analysis of 5G-AKA channel assumptions and session confusion," Network and Distributed System Security Symposium (NDSS), pp. 21-27, 2019.
[74] R. Borgaonkar, L. Hirschi, S. Park and A. Shaik, "New privacy threat on 3g, 4g, and upcoming 5g aka protocols," Proceeding on Privacy Enhancing Technology, vol. 2019, no. 3, pp. 108–127, 2019.
[75] S. Behrad, E. Bertin and N. Crespi, "Securing authentication for mobile networks, a survey on 4G issues and 5G answers," in 21st Conference on Innovation in

Clouds, Internet and Networks and Workshops (ICIN), Paris, France, pp. 1–8, 2018.
[76] J. Arkko, K. Norrman, M. Näslund and B. Sahlin, "A usim compatible 5g aka protocol with perfect forward secrecy," in IEEE Trustcom/BigDataSE/ISPA, vol. 1, pp. 1205–1209, 2015.
[77] A. Koutsos, "The 5g-aka authentication protocol privacy," in IEEE European Symposium on Security and Privacy (EuroS P), Stockholm, Sweden, pp. 464–479, 2019.
[78] L. Wang, J. Liu, M. Chen, G. Gui and H. Sari, "Optimization-based access assignment scheme for physical-layer security in d2d communications underlying a cellular network," IEEE Transaction Vehicular Technology, vol. 67, no. 7, pp. 5766–5777, 2018.
[79] M.A. Rahman and E. Al-Shaer, "Automated synthesis of distributed network access controls: a formal framework with refinement," IEEE Transaction Parallel Distributed System, vol. 28, no. 2, pp. 416–430, 2017.
[80] M. Khan, P. Ginzboorg, K. Jarvinen and V. Niemi, "Defeating the downgrade attack on identity privacy in 5g," In International Conference on Research in Security Standardisation, Darmstadt, vol. 11322, pp. 95-119, 2018.
[81] D. He, S. Chan and M. Guizani, "Accountable and privacy-enhanced access control in wireless sensor networks," IEEE Transaction. Wireless Communication, vol. 14, no. 1, pp. 389–398, 2015.
[82] S. Chatterjee, "On the design of fine grained access control with user authentication scheme for telecare medicine information systems," IEEE Access, vol. 5, pp. 7012–7030, 2017.
[83] Q. Huang, Y. Yang and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for internet of things," IEEE Access, vol. 5, pp. 12941–12950, 2017.
[84] H. Qinlong, M. Zhaofeng, Y. Yixian, N. Xinxin and F. Jingyi, "Improving security and efciency for encrypted data sharing in online social networks," China Communication, vol. 11, no. 3, pp. 104–117, 2014.
[85] P.P. Sriram, H.C. Wang, H. G. Jami and K. Srinivasan, "5g security: concepts and challenges," in 5G Enabled Secure Wireless Networks, Springer International Publishing, pp. 1–43, 2019.
[86] J. Yao, Z. Han, M. Sohail and L. Wang, "A robust security architecture for sdn-based 5g networks," Future Internet, vol. 11, no. 4, 2019.
[87] M. Liyanage, A.B. Abro, M. Ylianttila and A. Gurtov, "Opportunities and challenges of software-defined mobile networks in network security," IEEE Security and Privacy, vol. 14, no. 4, pp. 34–44, 2016.
[88] M.C. Dacier, H. König, R. Cwalinski, F. Kargl and S. Dietrich, "Security challenges and opportunities of software-defined networking," IEEE Security and Privacy, vol. 15, no. 2, pp. 96–100, 2017.
[89] A. R. Prasad, "3gpp 5g security," Journal of ICT Standardization, vol. 6, no. 2, pp. 137-158, 2018.
[90] R. P. Jover and V. Marojevic, "Security and protocol exploit analysis of the 5g specifications," IEEE Access, vol. 7, pp. 24956–24963, 2019.
[91] V. Saraswat, R.A. Sahu, G. Sharma, V. Kuchta and O. Markowitch, "Public-key encryption with integrated keyword search," Journal of Hardware System and Security, vol. 3, no. 1, pp. 12–25, 2019.
[92] C. Li and B. Palanisamy, "Privacy in internet of things: from principles to technologies," IEEE Internet Things Journal, vol. 6, no. 1, pp. 488–505, 2019.
[93] K. Yan, W. Shen, Q. Jin and H. Lu, "Emerging privacy issues and solutions in cyber-enabled sharing services: from multiple perspectives," IEEE Access, vol. 7, pp. 26031–26059, 2019.
[94] P.F. Scott, "Secrecy and surveillance: lessons from the law of imsi catchers," International Review of Law, Computers and Technology, vol. 33, no. 3, pp. 349-371, 2019.
[95] A. Braeken, M. Liyanage, P. Kumar and J. Murphy, "Novel 5g authentication protocol to improve the resistance against active attacks and malicious serving networks," IEEE Journals & Magazine, vol. 7, pp. 64040 - 64052, 2019.