Wireless Communication Networks For 5G And Beyond: Performance and Security Perspectives

PROF. DR. PARIN SOMANI
Director, Department of Skill Development, London Organisation of Skills Development Ltd, 27 Old Gloucester Street, London, United Kingdom

Abstract- ***The purpose of this study is to compile information regarding "5G & Beyond" wireless technology trends, innovations and development, network deployment, governance and geopolitics, global spectrum policy perspectives for policymakers, and societal benefits that will fuel a new generation of applications that will disrupt markets globally, thereby producing products, processes, and services that are superior over the course of the next decade and accelerating economic growth and security . Because the network is such an integral part of our daily lives, it is necessary to ensure the safety of all of its users as well as its components and services. In recent years, the security threat environment of 5G has greatly grown as a result of the exceptional development in both the diversity of services and the quantity of devices. This expansion has led to an increase in the overall size of the threat environment. Therefore, security solutions, even if they have not yet been implemented, need to be envisioned in advance in order to deal with the multiple dangers posed by a variety of services, new technologies, and more user information that is available via the network. This is necessary in order to deal with the numerous threats posed by a variety of services, new technologies, and more user information that is accessible via the network. This article proposes potential solutions to the problems with security that have been identified, as well as potential solutions to the problems that have already been identified. In addition to this, it offers an overview of the 5G network itself, explains the security flaws that are present in new technological concepts that will be embraced by 5G, and covers the threat environment that 5G networks operate in.***

Indexed Terms- ***Wireless, Communication, Networks5G, Beyond***

I. INTRODUCTION

The International Telecommunications Union (ITU) is a worldwide organization that was established in 1865 and has its headquarters in Geneva, Switzerland at the present day. Our mission is to create a global network that is accessible to all people, irrespective of the location in which they reside or the amount of money they own; this is our primary purpose. As part of an effort to establish global governance for the wireless industry, the International Telecommunications Union (ITU) was developed as a one-of-a-kind platform for global public-private cooperation.[1] This effort will compare the development of wireless markets around the world in order to offer insight into the process by which standards are formed in free markets in the absence of regulatory designations. The goal of this endeavor is to provide insight into the process. The World Telecommunication Policy Forum (WTPF) is a platform that enables policymakers from all over the world to meet and discuss policy concerns relating to wireless technologies, networks, and services in order to develop a common perspective regarding how these issues should be addressed in order to benefit society as a whole.[2] The goal of the World Telecommunication Policy Forum (WTPF) is to develop a consensus regarding how these issues should be addressed in order to benefit society as a whole. The World Telecommunication Policy Forum's (WTPF) overarching objective is to reach an international accord over the manner in which these concerns ought to be handled so that society can reap the benefits of doing so. The term "5G & Beyond" is used in the context of this research to refer to the fact that regardless of whether it's with 5G, 6G, 7G/7.5G, or another "G" wireless technology and/or network, the speeds will be incredibly fast with ultra-low latency as the key driver of empowering the Internet of Everything (IoE), as well as eXtended Reality (XR) services for

telemedicine, haptics, brain-computer interfaces, intelligent robotic Radio frequency communication, more commonly referred to as wireless communication, is becoming an increasingly prevalent method of communication.[3,4] This strategy is also getting more cost-effective while simultaneously becoming more socially meaningful. The consistent march of technical innovation and improvement over the course of a number of decades has made it feasible for new generations of wireless technology to be introduced at regular intervals throughout the course of several decades. As a result of the fact that these technologies are utilized by billions of people all over the world, possibilities have presented themselves to explore the legal system that governs the management and appropriation of the spectrum.[5] The rules that oversee the wireless sector are a convoluted jumble, and the authorities put in a lot of effort to make sure that spectrum is utilized properly. This is done so that society as a whole may benefit to the greatest degree possible from the good impacts that spectrum utilization has. Regulators have the ability to foster an atmosphere inside the mobile industry that is conducive to innovative thinking and healthy competition by following to international standards and regulatory best practices and adopting such practices themselves. There is a possibility that the mobile sector may benefit from this atmosphere. The interests of customers are prioritised within this atmosphere. The "5G & Beyond" networks are going to be significantly influenced by the key variables that originate from the business sector and society.[6,7] The transition to an economy that is based on the sale of data will give rise to challenges over data ownership, as well as the need to use ever-higher frequencies with fewer radio ranges, and the growing importance of networks, which will lead to an increase in network sharing and play a significant role in shaping the paradigm of telecom operators.[8] These challenges and needs will all arise as a result of the transition to an economy that is based on the sale of data. The shift toward a data-driven economy will bring about all of these difficulties and requirements, and it will do so as a direct outcome of the change. In contrast to the existing wireless ecosystem, the role of "5G & Beyond" stakeholders is going to be subject to continuous change, and as a result of this comparison, new roles are going to develop over the course of time.[9,10] It is up to one hundred times quicker than 4G, it is able to link one thousand times as many Internet of Things (IoT) and Internet of Medical Things (IoMT) devices as 4G can, and it is more responsive than 4G by a factor of five. "5G & Beyond" wireless networks are making it feasible to have self-driving cars, which may then be used for environmentally friendly logistics and transportation. Artificial intelligence (AI) that is dispersed over the network makes this feasible. Connectivity that is always on and everywhere will make it possible for innovation to occur in every facet of society. Because of this, it will be feasible for all facets of society to improve the public's safety, cut down on waste, and raise the bar for the quality of our environment.[11] The newly emerging problems that need special attention in the context of always-on ubiquitous connectivity provided by "5G & Beyond" are as follows: (i) consumer trust and protection; (ii) content regulation; (iii) data and privacy protection; (iv) freedom of expression; (v) digital identity and divide; (vi) human rights; and (vii) the socio-ethical impacts. 6G technology is only getting off the ground at this point. The majority of the efforts that researchers are devoting to finding a quantum world that is suitable for 6G at the moment are being directed toward this pursuit. Whoever is successful in putting into practice the 6G paradigm first will emerge triumphant in the struggle for preeminence in global technological development.[12,13] This will go down in history as the most earth-shattering battle that has ever taken place. The 6G archetype has the capability of offering backward and forward compatibility with 5G and 7G/7.5G respectively, integrating terrestrial wireless with satellite communication systems as well as space roaming for global ubiquitous mobile network coverage, and as a result, creating a strategic competitive advantage that offers virtually Internet of Everything (IoE) for everybody.[14,15] The technological capabilities of 5G and 6G would be surpassed by the capabilities of 7G/7.5GWireless, which would define satellite and space roaming characteristics in long-distance portable communication. These capabilities would be a step forward. In addition to this, it would have a variety of components that would rectify all of the problems that were inherent in the frameworks of the earlier generation. The results of this study shed light on wireless trends, innovations, governance, the global policy viewpoint, and the social advantages of establishing technology for next generation wireless networks (NGWN) for future spectrum

management. This study was carried out by the Wireless Broadband Alliance (WBA) and was funded by the National Science Foundation (NSF). More specifically, the advantages that these technologies may provide to society are the primary emphasis of the research.[16]

II. SECURITY IN WIRELESS NETWORKS: FROM 1G TO 4G

Because of the complexity of the underlying network, the use of proprietary and perimeter-based security solutions that are difficult to maintain, and the restrictions in identity management, ensuring the safety of communication networks has proven to be a challenging challenge. In addition to this, the architecture of the Internet has taken on the problems that have been developed as a result of the infrastructure; it is plagued with security concerns and is resistant to innovation.[17,18] Moreover, the Internet is a global communications network. In addition, the infrastructure has been the source of all of these problems. A method that is known as "progressive up-gradation" has been used to bring about a steady improvement in wireless network security ever since mobile networks were first introduced. This development can be traced back to the beginning of the mobile networking era. Since the beginning of their existence, mobile networks have always operated in this manner. The deployment of IP-based communication in wireless networks, on the other hand, created a rise in the number of Internet-based security concerns that were transferred to wireless networks.[19] Despite that, this was the most significant of the changes that took occurred. As a direct result of this, in the following section, we will offer an overview of the shifting security paradigm that is taking place in wireless networks as they transition from 1G to 4G or from non-IP wireless networks to IP-based wireless networks. These transitions are occurring as a result of the introduction of IP-based wireless networks. Due to the fact that both changes are taking place at the same time, this will be done.[20]

- Security in Networks Other Than IP

The first generation of cellular networks, often known as 1G, were primarily designed to provide speech-related services. These networks relied on analogue signal processing to transmit and analyze data. In 1983, AT&T and Bell Labs came out with the world's first iteration of a 1G system that was commercially feasible and would go on to become the most successful of all 1G systems. This system was called Advanced Mobile Phone Service. It was challenging to offer effective security services for 1G due to the nature of analogue communications, which prevented this from happening.[21] Because this cutting-edge telephone service did not employ encryption, neither information nor telephone calls could be kept private using it. As a direct consequence of this, almost the whole system and all of its users were exposed to a wide variety of security risks, such as cloning, unauthorized access, eavesdropping, and privacy breaches on the part of other users. Digital mobile systems were developed to boost the effectiveness of the restricted frequency bands.[22] As a direct consequence of this, the Global System for Mobile (GSM) communication became the most successful and extensively used standard in cellular communications, and it was eventually incorporated into 2G cellular networks. The GSM MoU association detailed the four distinct aspects of safety and protection that are to be given by a GSM system in their statement. The four components are anonymity, authentication, protection of signaling, and user data security . Anonymity is the most important. Users are able to maintain their anonymity while utilizing a system by employing ephemeral identifiers, which make it impossible to ascertain precisely who is logging into the system at any one time.[23,24] After the device has been powered on, a temporary identifier is broadcast, and the genuine IDs are not employed once again until and until the device has been powered off and then back on again. The authentication process will be utilized by the operator of the network in order to ascertain the user's identity. A method known as a challenge-response pair is utilized in order to carry it out successfully. Signaling as well as user data were both shielded by encryption, and the Subscriber Identity Module (SIM) was an integral component in the process of generating encryption keys. The safety of user data as well as signaling was carried out with the assistance of encryption.[25]

Despite this, the security provided by 2G had a number of flaws that made it susceptible to attack. The operators authenticated the user equipment (UEs) by employing a method that was unidirectional, but the user equipment (UEs) did not have the ability to authenticate the operators themselves.[26,27] As a consequence of this, it was

possible for a dishonest operator to carry out a man-in-the-middle attack by impersonating the legitimate operator and pretending to be the authentic one. In addition, the techniques used for encryption were also subjected to reverse engineering, and the ciphering algorithms were attacked in a number of different ways. As a result of the absence of encryption, GSM networks were not able to provide security for the data's integrity against channel hijacking and were also vulnerable to attacks that denied them service. In addition, the security capabilities of 2G systems were unable to be improved over time since the technology necessary to do so was not available for such systems.[28]

- Security in 3G

The fundamental objective behind the construction of the 3G cellular network was to make available data transfer speeds that were significantly quicker than those made available by 2G networks. With the introduction of 3G systems, previously impossible services have become practicable, including video telephony and the streaming of video via cellular networks. One of the remedies that was suggested by the 3G standard to solve the problems that were present in the 2G systems was the implementation of a more robust security architecture. The 3rd Generation Partnership Project (3GPP) has provided an overview of the three most significant areas of 3G security, which are as follows: (I) 3G security will inherit the main characteristics of 2G security, (II) 3G security will improve the limits of 2G security, and (III) 3G will include new security features that were not accessible in 2G.[29] The Third Generation Partnership Project, often known as 3GPP, is in charge of the investigation, development, and continuous upkeep of the Universal Mobile Telecommunications System, which is also sometimes referred to by its acronym, UMTS. The UMTS security architecture is comprised of five main sets of security features taken separately from one another. These components are described in greater depth in TS33.102, which is more often known to as Release 99. This set of UMTS security features safeguards the user equipment (UE) against nefarious attacks on the radio access connection and ensures that the user equipment (UE) may safely access 3G services". [30]

The Authentication and Key Agreement (AKA) protocol is one that is utilized by UMTS. Its development was carried out in such a way that it maximizes the degree to which it is compatible with the GSM standard. In spite of this, the UMTS AKA protocol is successful in accomplishing other protocol objectives such as mutual authentication of the network and, among other things, an agreement on the integrity key.[31,32] UMTS, as opposed to GSM's unilateral authentication, offers bidirectional authentication, which removes the possibility of employing a malicious base station. This is in contrast to GSM's authentication method, which is unilateral. Only one way of communication may be authenticated using GSM. [33] It is impossible to listen in on a conversation between a user and a radio access connection because to a characteristic of the access security system known as user identity confidentiality. The demand that user identities remain private must likewise be able to satisfy the requirement that user locations remain private and the need that user identities remain untraceable.[34] In order for the user to achieve these objectives, an encrypted identity will either be provided to them temporarily or permanently. Both of these identities will be encrypted. In a similar vein, the user should not be identified for a long length of time, and any data that may possibly betray the user's identity should be encrypted. This applies to both the desktop and mobile versions of the application.[35]

- Security in 4G

The version 10 from the 3GPP, which is more commonly known as LTE-Advanced (LTE-A), has satisfied the requirements of the 4G standard that were established by the International Telecommunications Union - Radio Communication Sector (ITU-R). An LTE-A network is made up of its basic components, which are the Evolved Packet Core (EPC) and the Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) . The EPC is a completely IP-based and packet switched backbone network that connects all other networks. The LTE-A system may communicate with access networks that do not conform to the 3GPP standard.[36]Machine-Type Communication, also known as MTC, home eNodeB or femtocells, and relay nodes are some of the new entities and applications that were made possible by LTE-A systems. For LTE-A, the 3GPP has compiled a set of safety measures that are quite similar to those already in place. The following are the components that make up it: (I) Access security, (Evolved Universal Terrestrial Radio Access Network), (II) Network domain security, (III) User

domain security, (IV) Application domain security, and (V) Visibility and the ability to adjust security settings.[37] However, in order to make the LTE-A systems more secure, each of the features has undergone substantial development. Additionally, all brand-spanking-new safety procedures have been developed for MTC, home eNB, and relay nodes respectively. The Evolved Packet System-AKA (EPS-AKA) had a considerable advantage over the UMTS-AKA in the form of something that was known as cryptographic network isolation. This was one of the most important advantages. This feature lowers the probability that a network's security will be penetrated, and it also lowers the probability that an attack will propagate across the network. [38,39] This is achieved by tying any cryptographic keys that are connected with EPS to the identity of the Serving Network (SN), which is the location to which the keys are delivered and is the site to which the keys are linked. In addition, with the help of this capability, the UE is able to validate the SN. It is essential to keep in mind that under UMTS, the user equipment (UE) is unable to perform SN validation. It is only able to check whether or not the UE's home network has given authorization to an SN to access the network. [40]

One of the enhancements that have been made to EPS in order to increase device secrecy is the fact that the identity of the device is not transmitted to the network until after the security measures for traffic protection have been put into place. [41,42] This is one of the changes that have been made. The user and signalling data confidentially both went through certain shifts as a result of the modifications made to the EPS. When it comes to third-generation (3G), the radio network controller acts as the terminal point for the encryption procedure on the network side. On the other hand, the base station is where the encryption process is completed.[43,44] In addition to this, a brand new mechanism of maintaining the signaling's confidentiality while it was sent between the UE and the core network was put into place. The 3GPP standardized the security components of mobility both inside the E-UTRAN and between the E-UTRAN and systems of previous generations or systems that did not use the 3GPP standard. This occurred both within the E-UTRAN and between the E-UTRAN and systems that did not use the 3GPP standard. When addressing non-3GPP access networks, there are two subcategories that need to be taken into consideration. The first type of non-3GPP access is known as trustworthy non-3GPP access, while the second type is known as untrusted non-3GPP access. [45]

In order to access a non-3GPP access network that is not trusted, the user equipment (UE) must first travel via a trusted evolving packet data gateway that is a component of the EPC. In addition, a brand-new key hierarchy as well as a handover key management mechanism have been created in LTE in order to ensure a risk-free mobility procedure. This was done in order to meet the requirements for LTE.[46] The early end point of the encryption presented a new challenge for the EPS structure, which resulted in the deployment of the new solution. As a result of a security issue in the early termination point, the early network node B, also known as the eNB, became more vulnerable to assaults than the 3G security architecture. Additionally, the architecture of EPS makes it feasible to put the eNB in locations that are not physically safe, which indicates that it may be placed outside of the security zone of network operators. This is because the design of EPS makes it possible to position the eNB in these locations. As a result, the eNB is susceptible to active assaults (such as denial of service attacks) as well as passive attacks (such as eavesdropping on long term keys). In order to protect users from the flaws that were found, the 3GPP mandated that the eNB comply with a number of stringent standards. The safe installation and configuration of the base station software (3GPP standards), the secure administration of keys inside the BTS, and a secure environment for managing user and control plane data are only some of the needs .

III. SECURITY IN 5G: AN OVERVIEW

5G will make broadband services widely available, make it possible to link a large number of objects to the internet via the Internet of Things (IoT), and

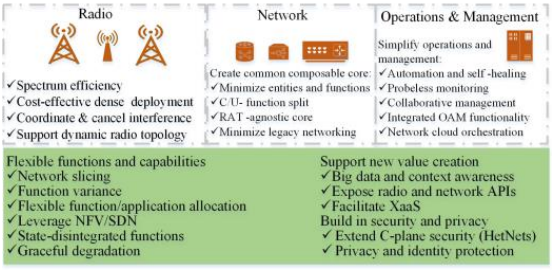

Fig. 2. 5G Design Principles.[47]

As a result of the complexity of the underlying network, the use of proprietary and perimeter-based security solutions that are difficult to maintain, and the weaknesses in identity management, maintaining the security of communication networks has proven to be an activity that is fraught with difficulty. In addition to this, the architecture of the Internet has taken on the problems that have been developed as a result of the infrastructure; it is plagued with anxieties surrounding security, and it is resistive to innovation. Mobile network security has been undergoing a rigorous and regular process of development ever since the creation of mobile networks. This process is known as "progressive up-gradation," and it has been facilitated by a technique called "progressive up-gradation." On the other hand, the implementation of communication protocols based on Internet Protocol (IP) in wireless networks brought about the most significant shift. Because of this, the number of Internet-based security issues that were transferred to wireless networks increased, which ultimately resulted in a general decrease in the quality of security that was present in wireless networks. As a result of this, in the following section, we will offer an overview of the changing security paradigm that is occurring in wireless networks as they migrate from 1G to 4G or from non-IP wireless networks to IP-based wireless networks.[48] This will be done as a consequence of the fact that in the preceding section, we will provide an overview of the evolving security paradigm that is occurring in wireless networks. As a direct consequence of the transformations that are currently taking place, this activity will be carried out .

- An Outline of the Core Design Principles for 5G

Because there will be new kinds of services and devices, as well as new user expectations for things like decreased latency, greater throughput, and ubiquitous coverage, a new set of design principles is required for 5G. In addition, 5G must be able to satisfy these newly developed user requirements. The importance of a highly elastic and robust system architecture is demonstrated in Figure 2, which shows how the 5G design principles developed by NGMN were formed. A high spectrum utilization efficiency, dense deployment that is also cost-effective, efficient coordination, robust interference cancellation, and dynamic radio topologies are all required for the radio component. The standards that will be applied to the network that will go beyond radio will be unique, and they will place a higher focus on the incorporation of technology that is completely cutting edge. Software-defined networking (SDN) and network function virtualization (NFV) will be utilized by the common composable core in order to, among other things, enable dynamic network function placement and segregation of the user plane and control plane. In order to do this, we need to simultaneously reduce the quantity of outdated networking that is utilized while simultaneously increasing the number of new interfaces that are built between the core and Radio Access Technologies (RATs). The design of the 5G network has to be capable of enabling the deployment of security mechanisms and services (including virtual security firewalls), whenever and wherever those components are required in the perimeter of any network. In light of the information that is shown in Figure 2, it is necessary to simplify the facility's administration and the activities that take place on a daily basis. In recent years, software-defined networking, often known as SDN, has become the primary technology that is used to simplify the administration of network systems. The software-defined networking (SDN) architecture divides the network into two distinct planes: the data-transfer plane and the control plane. Application Programming Interfaces (APIs), which may be programmed, are utilized in order to exercise control over network resources. These APIs are positioned on the control plane, which is conceptually centralised to manage the whole network that lies below it. Both the centralization of network administration and the integration of programmable application programming interfaces (APIs) into network hardware introduce vulnerabilities in network security that might be exploited. Centralized network management is especially problematic since it makes it easier for hackers to get unauthorized access. Control that is centralized via networks is especially susceptible to attack. Due to the fact that this is the case, it is very necessary for us to do study on the various security concerns that are raised by SDN. Inter-federated disputes and resource hijacking are two of the potential security vulnerabilities that might surface as a consequence of network function virtualization (NFV) and network slicing. Both of these developments are aimed at improving efficiency. Both of these problems provide difficulties that are analogous to one another. As a consequence of this, there is a demand for sufficient research into the

security issues related with all of the technologies that are utilized by 5G in order to satisfy regulatory requirements. In continuation with the last section, we will now present a brief summary of the 5G security architecture, with the primary focus being focused on the security domains that are specified by 3GPPP.

- Contextualization of the 5G Security Architecture

According to ITU-T, a security architecture logically splits the architectural components that make up security features into their own individual architectural components. These individual architectural components then make up the security features. The term "individual architectural components" is used to refer to these architectural components once they have been included into a security architecture. As a result of this, it is possible to adopt a methodical approach to assuring the security of new services from beginning to finish. This, in turn, makes it simpler to plan for new security solutions and evaluate the security of current networks. The security architecture that has been built for 5G networks is included in the most recent version of the 3GPP technical standard, which is release 15. This architecture is made up of multiple distinct domains all working together. Figure 3 is a representation of the security architecture, omitting the virtual infrastructure (VI), and it is composed of the primary domains that are stated below:

- Network access security (I): Consists of the collection of various different security characteristics that, when combined, make it feasible for user equipment (UE) to authenticate itself and receive secure access to network services. This is done through the use of a gathering. The conveyance of security context from the serving node (SN) to the user equipment is also considered to be an element of access security. The protection of non-3GPP access technologies is another component of access security.
- Network domain security (II): Consists of a collection of security functions that enable network nodes to safely share user plane and signaling data with one another. These functions are known as the safety features. These elements come together to provide the safety qualities.
- User domain security (III): comprises of security components that, when combined, provide users with a secure means of accessing the user environment.

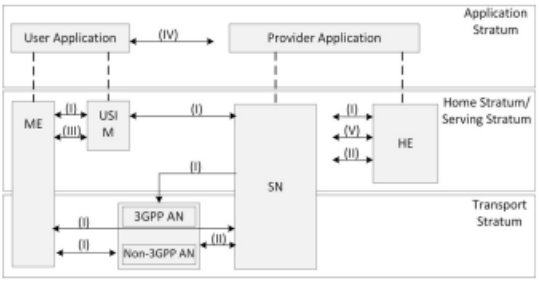

Fig. 3. An overview of the architecture that safeguards the data.[49]

- Application domain security (IV): Contains security features that make it possible for apps (in both the user domain and the provider domain) to communicate with one another in a safe and secure way. Contains characteristics that make it possible for applications to communicate with one another .
- Service Based Architecture (SBA) domain security (V): It provides security components for the registration, detection, and authorisation of network parts in addition to providing security for service-based interfaces".
- Visibility and configurability of security (VI): Includes safety features that provide users with information on the status of the security measures, such as whether or not they are currently operational .

In and of itself, the 5G security architecture does not identify particular security concerns or the solutions to address those dangers. On the contrary, all it does is identify who they are. However, there are some security solutions that have been made, and they either derive from the generations that came before 5G with alterations for improvements, or they have been produced from scratch in line with the domain of 5G. Regardless, there are certain security solutions that have been built. Even though the security ideas that are utilized in LTE are only the beginning of the process, they are already being looked at as prospective standards for the security of future wireless networks.[50] This is the case despite the fact that LTE is just the beginning of the process. In any event, according to Nokia's explanation, the high-level vision of 5G security is based on i) Supreme built-in security, ii) Flexible security techniques, and iii) Automation. These are the three pillars that make up the 5G security architecture. These three elements make up the

fundamental framework of the 5G security architecture. After providing a concise overview of how authentication is handled in 5G in the next area, we will then go on to the following part. The 3rd Generation Partnership Project (3GPP) has placed a significant focus on a variety of factors of safety, including authentication, which serves as the foundation of security.

- A High-Level Overview of the Security Measures in 5G

The Next Generation Mobile Networks (NGMN) has prepared suggestions for 5G based on current network designs and the gap in security measures that have either not been constructed at all or have been established but have not yet been put to use. These recommendations were made because there is a lack of security measures that have either been built at all or have been created but have not yet been put to use. These recommendations are derived from the designs of already-existing networks and the deficiencies in existing security mechanisms. The shortfall in security measures that either have not been developed at all or have been produced but have not yet been put into practice is the foundation for these suggestions. These measures have not yet been put into practice. The guidance emphasises the cautionary observations, which include elements such as the immaturity of 5G with many unknowns, the absence of stated design concepts, and the unknown end-to-end and subsystems architectures. A number of other characteristics are present, such as the lack of explicit design concepts, as well as the lack of specified end-to-end and subsystem designs. There is a scarcity of design concepts that are clearly articulated, which is one of the many factors that must be taken into consideration. The proposal draws attention to the vulnerabilities in network access security that are now existing, as well as the cyberattacks that are currently being carried out against users and the infrastructure of the network (as depicted in Fig. 4). You may look at the specific suggestions and limitations imposed on the level of security right here, and down below you'll find a summary of the most important aspects of those recommendations and limitations. Transactions carried out on the flash network: It is anticipated that the number of devices used by end users will rapidly increase in 5G, which will result in significant shifts in the traffic patterns of the network. These shifts might occur by mistake or with the intention of causing harm to the system. These alterations may have been brought about by someone purposefully inflicting harm to the network, or they may have been the consequence of an accident. As a result of this, the 5G systems will need to be able to properly manage massive swings in traffic and give resilience if surges of this type occur, all while maintaining an acceptable degree of performance. This will be required of them. These requirements will be placed on the 5G systems. Security measures for the radio interface's keys are as follows: In older network topologies, such as 4G, the encryption keys for the radio interface were generated in the user's home network and then sent to the visited network across unsecured lines. This provided an apparent point of exposure for the keys. In 5G, the encryption keys for the radio interface are produced in the visited network rather than being sent over the air. These keys will be generated locally within the 5G network that is being accessed. This will be possible thanks to 5G. As a consequence of this, it is advised that either the keys should be encrypted before they are supplied or that they should not be transmitted at all across insecure channels such as SS7 or DIAMETER.

Alternatively, it is also possible that the keys should not be provided at all. User plane integrity: despite the fact that the 3G and 4G systems offer some degree of security for certain signaling messages, they do not offer any level of cryptographic integrity protection for the user data plane. This is because user plane integrity is not a concern for either of these generations of mobile networks. As a consequence of this fact, it is strongly recommended that protection be implemented at the application or transport layer, which culminates outside of mobile network environments. On the other hand, application-level end-to-end security may involve an excessive amount of overhead for the data transfer in the form of packet headers and handshakes. The flow of data may be slowed down as a result of this overhead. As a consequence of this, the legislation may include an exception for network-level security for 5G applications that are sensitive to latency or for devices that are linked to the Internet of Things but have limited resources. Detailed requirements for the appropriate degree of network security, including: Certain service-driven restrictions, such as latency, may, in some security designs, lead to the deployment of security measures only if they are genuinely essential. One example of this would be an increase in the amount of time it

takes for a request to be processed. One instance that exemplifies this would be one in which a service is needed to wait for a response from the customer. and

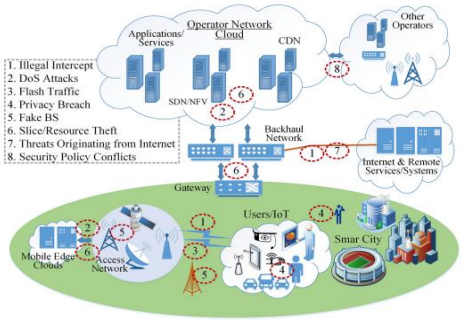

Fig. 4. The nature of the security vulnerabilities faced by 5G networks.[51]

could not be taken out of the equation in its totality for elimination to work. The difficulty of an issue is enhanced if there are several operators participating in a circumstance. This is due to the fact that it is possible for one operator to suffer as a result of the inadequate security measures conducted by another operator. This might have a negative impact on both operators. In light of this, there is a strong call for some level of security to be controlled in 5G once a thorough assessment has been conducted to identify the most pressing security concerns. To put it another way, the 5G industry has to get its act together. ensuring that the numerous security rules that are implemented on subscribers are consistent with one another: The security settings of a user are required to remain unchanged under any and all situations when the user transfers from the network of one operator to that of another operator. When a user goes from one area to another, or when the user roams from one operator network to another as is the case when they use their mobile device, there is a significant possibility that the security services that the user makes use of will not receive frequent updates on a per-user basis. This is a situation in which frequent updates are not received. As a consequence of this, it is very necessary for the operators of the various networks to work together and share information concerning the subscriber services and the laws governing the security of the networks. This proposal draws attention to the idea of utilizing virtualization methods in order to enable per-service slice setup in order to maintain the user's or service's security even while they are traveling. denial of service attacks, often known as DoS attacks, are ones that are launched against the infrastructure. An assault that is either a distributed denial of service (DDoS) or a denial of service (DoS) has the potential to interfere with the normal functioning of essential infrastructure, such as the networks that provide electricity, medical services, and transportation. This might have catastrophic consequences. In most cases, the design of a denial of service attack will be such that it will use up all of the logical and physical resources of the devices that are the focus of the attack. The vast majority of situations fit within this category. This threat will be substantially more dangerous as a result of the increasing possibility that assaults may originate from Internet of Things devices that have been hacked. These devices may be located in a wide variety of locations and in large numbers. As a direct consequence of this, the network has to increase its resistance to disruption by putting in place strict security mechanisms.[52] The variety of different devices and services that could be enabled by 5G networks only serves to make an already tough situation much more challenging to manage securely. In the next section, we will provide a high-level overview of the multiple potential solutions to security concerns, as well as the perspectives and suggestions of several regulatory and standardization authorities operating within the sector. In the following parts, we will offer a complete analysis of the security weaknesses that are presently present in the network in addition to the primary supporting technologies that are a part of the 5G infrastructure. This analysis will be presented alongside the sections in which we will discuss the 5G infrastructure.

CONCLUSION

The evolution of wireless communication networks has been going on for quite some time now, and it began with the linking of simple mobile phones in the 1G standard and will eventually involve the linking of nearly everything in life in the 5G standard. During this time period, there has been a simultaneous growth in the threat environment, with simple phone tapping giving way to a spectrum of assaults on mobile devices, network infrastructure, and services. During this time period, there has also been a parallel increase in the number of threats that are being faced. During this same period, there has also been an increase in the danger environment, which has been simultaneous to this expansion. 5G will make use of new technologies such as improved cloud computing concepts (for example, massive

MIMO), software-defined networks (SDN), network functions virtualization (NFV), and other technologies of a similar nature in order to incorporate new things (Internet of things) and services into the network. This will be accomplished through the use of software-defined networks (SDN). It is possible that the overall picture of network security will grow even more convoluted as a direct result of the fact that each of these technologies comes with its own distinctive set of inherent security threats. As a result of this, for the aim of this study, we have studied the security risks that are present in many different sections of the network, such as the access network, the core network, and within the technologies that will be utilized in 5G networks. These risks are present in all of these various parts because of the nature of the network itself, which is a distributed system with many interconnected elements. The security threat environment has in reality risen as a result of the proliferation of a wide variety of devices, services, and new networking technologies. This expansion has led to an increase in the likelihood of security breaches. As a result, new security solutions need to be sought out in order to guarantee that the connection is both effective and secure.

REFERENCES

[1] K. Tanaka, “GSM security: A description of the reasons for security and the techniques,” in Proc. IEEE Conf. History Telecommun., 2001, pp. 1–4.

[2] A. Ghosh, J. Zhang, J. G. Andrews, and R. Muhamed, Fundamentals of LTE. Englewood Cliffs, NJ, USA: Prentice-Hall, 2010. [32] P. Chandra et al., Wireless Security: Know It All. Burlington, MA, USA: Newnes, 2011.

[3] J. G. Sempere, “An overview of the GSM system,” in Proc. IEEE Veh. Technol. Soc., 2002, pp. 1–33.

[4] M. Paetsch, The Evolution of Mobile Communications in the U.S. and Europe: Regulation, Technology, and Markets. Boston, MA, USA: Artech House, 1993.

[5] C. Brookson, “GSM security: A description of the reasons for security and the techniques,” in Proc. IEE Colloquium Security Cryptography Appl. Radio Syst., 1994, pp. 1–4.

[6] P. S. Pagliusi, “A contemporary foreword on GSM security,” in Proc. Int. Conf. Infrastruct. Security (InfraSec), 2002, pp. 129–144. [Online]. Available: http://dl.acm.org/citation.cfm?id=647333.722873

[7] P. Bouška and M. Drahanský, “Communication security in GSM networks,” in Proc. Int. Conf. Security Technol., Dec. 2008, pp. 248–251.

[8] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.

[9] M. Toorani and A. Beheshti, “Solutions to the GSM security weaknesses,” in Proc. Int. Conf. Next Gener. Mobile Apps Services Technol., Cardiff, U.K., 2008, pp. 576–581.

[10] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[11] Bose–Chadhuri–Hocquenghem (BCH) codes, 244, 245f BPSK modulation, and error probability, 173–5

[12] D. Kutscher, “It’s the network: Towards better security and transport performance in 5G,” in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2016, pp. 656–661.

[13] J. G. Andrews et al., “What will 5G be?” IEEE J. Sel. Areas Commun., vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[14] Navaneetha Krishnan Rajagopal, Mankeshva Saini, Rosario Huerta-Soto, Rosa Vílchez-Vásquez, J. N. V. R. Swarup Kumar, Shashi Kant Gupta, Sasikumar Perumal, "Human Resource Demand Prediction and Configuration Model Based on Grey Wolf Optimization and Recurrent Neural Network", Computational Intelligence and Neuroscience, vol. 2022, Article ID 5613407, 11 pages, 2022. https://doi.org/10.1155/2022/5613407

[15] Navaneetha Krishnan Rajagopal, Naila Iqbal Qureshi, S. Durga, Edwin Hernan Ramirez Asis, Rosario Mercedes Huerta Soto, Shashi Kant Gupta, S. Deepak, "Future of Business Culture: An Artificial Intelligence-Driven Digital Framework for Organization Decision-Making Process", Complexity, vol. 2022,

Article ID 7796507, 14 pages, 2022. https://doi.org/10.1155/2022/7796507

[16] Eshrag Refaee, Shabana Parveen, Khan Mohamed Jarina Begum, Fatima Parveen, M. Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[17] Rajesh Kumar Kaushal, Rajat Bhardwaj, Naveen Kumar, Abeer A. Aljohani, Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit, "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, Article ID 8741357, 13 pages, 2022. https://doi.org/10.1155/2022/8741357

[18] Bramah Hazela et al 2022 ECS Trans. 107 2651 https://doi.org/10.1149/10701.2651ecst

[19] Ashish Kumar Pandey et al 2022 ECS Trans. 107 2681 https://doi.org/10.1149/10701.2681ecst

[20] G. S. Jayesh et al 2022 ECS Trans. 107 2715 https://doi.org/10.1149/10701.2715ecst

[21] Shashi Kant Gupta et al 2022 ECS Trans. 107 2927 https://doi.org/10.1149/10701.2927ecst

[22] S. Saxena, D. Yagyasen, C. N. Saranya, R. S. K. Boddu, A. K. Sharma and S. K. Gupta, "Hybrid Cloud Computing for Data Security System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 2021, pp. 1-8, doi: 10.1109/ICAECA52838.2021.9675493.

[23] S. K. Gupta, B. Pattnaik, V. Agrawal, R. S. K. Boddu, A. Srivastava and B. Hazela, "Malware Detection Using Genetic Cascaded Support Vector Machine Classifier in Internet of Things," 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), 2022, pp. 1-6, doi: 10.1109/ICCSEA54677.2022.9936404.

[24] Natarajan, R.; Lokesh, G.H.; Flammini, F.; Premkumar, A.; Venkatesan, V.K.; Gupta, S.K. A Novel Framework on Security and Energy Enhancement Based on Internet of Medical Things for Healthcare 5.0. *Infrastructures*2023, *8*, 22. https://doi.org/10.3390/infrastructures8020022

[25] V. S. Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Natural Language Processing using Graph Neural Network for Text Classification," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060655.

[26] M. Sakthivel, S. Kant Gupta, D. A. Karras, A. Khang, C. Kumar Dixit and B. Haralayya, "Solving Vehicle Routing Problem for Intelligent Systems using Delaunay Triangulation," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060807.

[27] S. Tahilyani, S. Saxena, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "Deployment of Autonomous Vehicles in Agricultural and using Voronoi Partitioning," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060773.

[28] V. S. Kumar, A. Alemran, S. K. Gupta, B. Hazela, C. K. Dixit and B. Haralayya, "Extraction of SIFT Features for Identifying Disaster Hit areas using Machine Learning Techniques," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060037.

[29] V. S. Kumar, M. Sakthivel, D. A. Karras, S. Kant Gupta, S. M. Parambil Gangadharan and B. Haralayya, "Drone Surveillance in Flood Affected Areas using Firefly Algorithm," 2022 International Conference on Knowledge Engineering and Communication Systems (ICKES), Chickballapur, India, 2022, pp. 1-5, doi: 10.1109/ICKECS56523.2022.10060857.

[30] Parin Somani, Sunil Kumar Vohra, Subrata Chowdhury, Shashi Kant Gupta. "Implementation of a Blockchain-based Smart Shopping System for Automated Bill

Generation Using Smart Carts with Cryptographic Algorithms." CRC Press, 2022. https://doi.org/10.1201/9781003269281-11.

[31] Shivlal Mewada, Dhruva Sreenivasa Chakravarthi, S. J. Sultanuddin, Shashi Kant Gupta. "Design and Implementation of a Smart Healthcare System Using Blockchain Technology with A Dragonfly Optimization-based Blowfish Encryption Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003269281-10.

[32] Ahmed Muayad Younus, Mohanad S.S. Abumandil, Veer P. Gangwar, Shashi Kant Gupta. " AI-Based Smart Education System for a Smart City Using an Improved Self-Adaptive Leap-Frogging Algorithm." CRC Press, 2022. https://doi.org/10.1201/9781003252542-14.

[33] Rosak-Szyrocka, J., Żywiołek, J., & Shahbaz, M. (Eds.). (2023). Quality Management, Value Creation and the Digital Economy (1st ed.). Routledge. https://doi.org/10.4324/9781003404682

[34] Dr. Shashi Kant Gupta, Hayath T M., Lack of it Infrastructure for ICT Based Education as an Emerging Issue in Online Education, TTAICTE. 2022 July; 1(3): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.03.A004

[35] Hayath T M., Dr. Shashi Kant Gupta, Pedagogical Principles in Learning and Its Impact on Enhancing Motivation of Students, TTAICTE. 2022 October; 1(2): 19-24. Published online 2022 July, doi.org/10.36647/TTAICTE/01.04.A004

[36] Shaily Malik, Dr. Shashi Kant Gupta, "The Importance of Text Mining for Services Management", TTIDMKD. 2022 November; 2(4): 28-33. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04.A006

[37] Dr. Shashi Kant Gupta, Shaily Malik, "Application of Predictive Analytics in Agriculture", TTIDMKD. 2022 November; 2(4): 1-5. Published online 2022 November doi.org/10.36647/TTIDMKD/02.04.A001

[38] Dr. Shashi Kant Gupta, Budi Artono, "Bioengineering in the Development of Artificial Hips, Knees, and other joints. Ultrasound, MRI, and other Medical Imaging Techniques", TTIRAS. 2022 June; 2(2): 10–15. Published online 2022 June doi.org/10.36647/TTIRAS/02.02.A002

[39] Dr. Shashi Kant Gupta, Dr. A. S. A. Ferdous Alam, "Concept of E Business Standardization and its Overall Process" TJAEE 2022 August; 1(3): 1–8. Published online 2022 August

[40] A. Kishore Kumar, A. Alemran, D. A. Karras, S. Kant Gupta, C. Kumar Dixit and B. Haralayya, "An Enhanced Genetic Algorithm for Solving Trajectory Planning of Autonomous Robots," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099994

[41] S. K. Gupta, V. S. Kumar, A. Khang, B. Hazela, N. T and B. Haralayya, "Detection of Lung Tumor using an efficient Quadratic Discriminant Analysis Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111903.

[42] S. K. Gupta, A. Alemran, P. Singh, A. Khang, C. K. Dixit and B. Haralayya, "Image Segmentation on Gabor Filtered images using Projective Transformation," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111885.

[43] S. K. Gupta, S. Saxena, A. Khang, B. Hazela, C. K. Dixit and B. Haralayya, "Detection of Number Plate in Vehicles using Deep Learning based Image Labeler Model," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-6, doi: 10.1109/ICRTEC56977.2023.10111862.

[44] S. K. Gupta, W. Ahmad, D. A. Karras, A. Khang, C. K. Dixit and B. Haralayya, "Solving Roulette Wheel Selection Method using Swarm Intelligence for Trajectory Planning of Intelligent Systems," 2023 International Conference on Recent Trends in Electronics and Communication (ICRTEC), Mysore, India, 2023, pp. 1-5, doi: 10.1109/ICRTEC56977.2023.10111861.

[45] Shashi Kant Gupta, Olena Hrybiuk, NL Sowjanya Cherukupalli, Arvind Kumar Shukla (2023). Big Data Analytics Tools, Challenges and Its Applications (1st Ed.), CRC Press. ISBN 9781032451114

[46] Shobhna Jeet, Shashi Kant Gupta, Olena Hrybiuk, Nupur Soni (2023). Detection of Cyber Attacks in IoT-based Smart Cities using Integrated Chain Based Multi-Class Support Vector Machine (1st Ed.), CRC Press. ISBN 9781032451114

[47] Parin Somani, Shashi Kant Gupta, Chandra Kumar Dixit, Anchal Pathak (2023). AI-based Competency Model and Design in the Workforce Development System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[48] Shashi Kant Gupta, Alex Khang, Parin Somani, Chandra Kumar Dixit, Anchal Pathak (2023). Data Mining Processes and Decision-Making Models in Personnel Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[49] Alex Khang, Shashi Kant Gupta, Chandra Kumar Dixit, Parin Somani (2023). Data-driven Application of Human Capital Management Databases, Big Data, and Data Mining (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[50] Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta, Anchal Pathak (2023). Data-centric Predictive Modelling of Turnover Rate and New Hire in Workforce Management System (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[51] Anchal Pathak, Chandra Kumar Dixit, Parin Somani, Shashi Kant Gupta (2023). Prediction of Employee's Performance Using Machine Learning (ML) Techniques (1st Ed.), CRC Press. https://doi.org/10.1201/9781003357070

[52] Worakamol Wisetsri, Varinder Kumar, Shashi Kant Gupta, "Managerial Autonomy and Relationship Influence on Service Quality and Human Resource Performance", Turkish Journal of Physiotherapy and Rehabilitation, Vol. 32, pp2, 2021.