©IDOSR PUBLICATIONS
International Digital Organization for Scientific Research ISSN: 2550-7931
IDOSR JOURNAL OF APPLIED SCIENCES 6(1): 33-44, 2021

5G Network Technology and its Security Implications on Mobile Network Operations (MNOs) in Nigeria

Wesley O. Odumu

Computer Engineering Technology Dept.Plateau State Polytechnic, Barkin Ladi – Plateau State, Nigeria.
Email: writeodeh@yahoo.com

ABSTRACT

The hype on 5G network technologies has accorded mobile and telecommunication companies or standardization bodies the need for an improved Quality of Service (QoS) that would enable a fully mobile and connected society to empower socio-economic transformations which cuts across productivity, sustainability and well-being. In this light, the paper considered and concentrated on the Hardware Security Module (HSM) that separate out the cryptographic key storage and processing functions for a trusted device by the use of protection profile on the device side and dedicated, tamper-resistant, certifiable hardware such as 5G SIM cards which the mobile network operations in Nigeria can leverage on under the 5G network technology. It brought out the fact that there are limitations of the Software Defined Network (SDN) as experienced in the 4G technology.It also reviewed and summarized the evolutionary technologies that culminated to 5G networks from 1G to 4G; the security built into 5G and the frameworks like Flat IP architecture, Hierarchical architecture, IPv6 and Voice Over IP (VoIP). The paper is aimed at answering security challenges of confidentiality, integrity, availability and authenticationbrought to 5G networks by services, architectures and technologies using a mix between security at the edge (device)and security at the core (network).It recommended the need for security evaluation, validation and standards by the standardization bodies like International TelecommunicationUnion – RadiocommunicationSector(ITU-R),the3rdGenerationPartnershipProject (3GPP) and the Next Generation Mobile Networks (NGMN) Allianceand the Internet Engineering Task Force (IETF).

Keywords:5G Network, Security, Hardware Security Modules, Mobile Network Operators,Architecture, Standardization.

INTRODUCTION

The world globallyhas witnessed a heavily hyped 5G network technology in the technological progression ofboth mobile and telecommunication services [1, 2, 3, 4]. The technological pace is moving at a great pace which is not around one but two industry standards; 4G and 5G technologies [5, 6, 7, 8]. Fifth generation mobile network (5G) is a wireless networking architecture (cellular technology) built on the 802.11ac IEEE wireless networking standard, which aims to significantly increase data communication speeds compared to its predecessor 4G LTE (Long–term Evolution – IEEE 802.11n) [9, 10, 11]. It is defined by the name of International Mobile Telecommunications-2020 (IMT-2020), and it is expected totake the place ofbillions of smartphone users on today's 4G networks, utilizing gigabit connections spawning high-speed applications and driving a new generation of smartphones and consumer devices capable of utilizing the huge increase in bandwidth.User quality-of-experience (QoE) depends on

the mobile operator's ability to ensure the reliability of these connections and that network quality-of-service (QoS) meets the demands of each application [12, 13, 14]. Mobile Network Operators (MNOs) will also require insight into the different types of applications subscribers are using, including time of day, location and duration, in order to project future usage and provide sufficient network capacity.They are seeking innovative solutions to improve their network performance and efficiency, as well as to reduce the costs expended on network operation, maintenance, and new service deployment [14, 15, 16, 17].

5G will unleash a proliferation of embedded, smart devices that will utilize ultra-reliable, low latency communications channels for real-time, machine-to-machine (M2M) control of vehicles, homes, buildings, public infrastructure and industrial processes. The deployment of the 5G technology is a build-up on 4G infrastructure. The following will be discussed throughout the paper: an overview and basic concepts of 5G; security frameworks for 5G features, hardware security module (HSM) of a product and possible vulnerabilities identified with the software defined network (SDN) of 5G. The paper concludes with the need for security evaluation, validation and standards by the standardization bodies like International TelecommunicationUnionRadiocommunication Sector (ITUR), the 3rd Generation Partnership Project (3GPP) and the Next Generation Mobile Networks (NGMN) Allianceand the Internet Engineering Task Force (IETF). The 3GPP is an organization that brings together seven telecommunication standard development bodies into one group [18, 19, 20]. The IETF is an open international community of network professionals and researchers concerned with the future of internet architecture and operation [21].The ITU is an international specialized agency, that is a part of the United Nations, for information and telecommunication technologies [22]. The ITU is the organization leading the charge for 5G standardization and has defined a timeline and project for submission and approval of 5G requirements called IMT-2020.

Overview and Basic Concepts of 5G Technology

Mobile communication has become more popular in last few years due to fast revolution in mobile technology. This revolution is due to very high increase in telecoms customers. This revolution is from 1G- the first generation, 2G- the second generation, 3G- the third generation, and then the 4G- the fourth generation, 5G-the fifth generation [23].

A. First Generation(1G): 1G emerged in 1980s.It contains analog system and popularly known as cell phones. It introduces mobile technologies such as mobile telephone system (MTS),Advanced mobile telephone system(AMTS), Improved mobile telephone system(IMTS)and push to talk(PTT).It uses analog radio signal which have frequency 150 MHz, Voice call modulation is done using a technique called frequency division multiple access (FDMA). It has low capacity, unreliable handoff, poor voice links and no security at all since voice calls were played back in radio towers making these calls susceptible to unwanted eavesdropping by third parties [24].

B. Second Generation (2G): 2G emerged in late 1980s. It uses digital signals for voice transmission and has speed of 64 kbps. It provides facility of SMS (Short Message Service) and use the bandwidth of 30 to 200 KHz. Next to 2G, 2.5G system uses packet switched and circuit switched

domain and provide data rate up to 144 kbps. E.g. GPRS, CDMA and EDGE . C. Third Generation (3G): It uses Wide Brand Wireless Network with which clarity is increased. The data are sent through the technology called Packet Switching. Voice calls are interpreted through Circuit Switching. Along with verbal communication it includes data services, access to television/video, new services like Global Roaming. It operates at a range of 2100MHz and has a bandwidth of 15-20MHz used for High-speed internet service, video chatting.3G uses Wide Band Voice Channel that is by this the world has been contracted to a little village because a person can contact with other person located in any part of the world and can even send messages too [23]. D. Fourth Generation (4G): 4G offers a downloading speed of 100Mbps.4G provides same feature as 3G and additional services like MultiMedia Newspapers, to watch T.V programs with more clarity and send Data much faster than previous generations. LTE (Long Term Evolution) is considered as 4G technology. 4G is being developed to accommodate the QoS and rate requirements set by forthcoming applications like wireless broadband access, Multimedia Messaging Service (MMS), video chat, mobile TV, HDTV content, Digital Video Broadcasting (DVB), minimal services like voice and data, and other services that utilize bandwidth [24, 25, 26]. E. Fifth Generation (5G): 5G Technology stands for 5th Generation Mobile technology. 5G mobile technology has changed the means to use cell phones within very high bandwidth. User never experienced ever before such a high value technology. Nowadays mobile users have much awareness of the cell phone (mobile) technology. The 5G technologies include all type of advanced features which makes 5G mobile technology most powerful and in huge demand in near future. A user can also hook their 5G technology cell phone with their Laptop to get broadband internet access. 5G technology including camera, MP3 recording, video player, large phone memory, dialing speed, audio player and much more you never imagine. For children rocking fun Bluetooth technology and Piconets has become in market [27, 28]. A clearer view of the technology progression from 1G to 5G is stated in Table 1. [29, 30].

Technology	1G	2G	3G	4G	5G
Deployment	1970-1980	1990-2004	2004-2010	2000-2010	2020
Data Bandwidth	2 kbps	64kbps	2Mbps	1 Gbps	Higher than 1 Gbps
Key Differentiator	Mobility	Secure, mass adoption	Better internet experience, applications	Faster broadband internet, lower latency	Faster internet, wide range of applications, IoT
Technologies	AMPS, NMT, TACS	GSM/GPRS, D-AMPS, cdmaOne	WCDMA/HSPA+, CDMA2000/EV-DO, TD-SCDMA	LTE, LTE Advanced	Unified IP, seamless integration of broadband LAN/WAN/PAN/WLAN and advanced technologies based on OFDM modulation and IPv6
Services	Voice	SMS, Digital Voice, Higher capacity packetized data	Cohesive high class audio , video and data	Dynamic information access, wearable devices	Dynamic information access, wearable devices with AI capabilities
Core network	PSTN	PSTN	Packet N/W	All IP network	Flatter IP network, 5G network interfacing(5G-NI)
Weakness (addressed by subsequent generation)	Major security concerns, Poor spectral efficiency,	Narrow data rates, challenging to support request for internet/e-mail	Failure of WAP for internet access, Real performance failed to match hype, Tied to legacy	Mobile explicit architecture and protocols	May exist after implementation. (Current challenges include security, privacy, infrastructure etc)

Security Issues and Concerns

The different technologies have had their security systems evolving from one stage to a higher level. In 1G wireless, it was possible for intruders or a third party to gain fraudulent access to the network. 2G GSM had an improved security system over 1G but with a weak improved security authentication algorithm. The master security key could be disclosed by having a million interactions with a SIM card [31]. In 3G wireless network an enhanced process of a two-way authentication mechanism was adopted. Mutual authentication was achieved by the mobile device and network. For stronger security, 128-bit encryption and integrity keys were utilized (Spatz & Schmitz, 2000). Security was further enhanced by introducing some mechanisms to ensure freshness of the cipher keys. It was demonstrated by [32] that if a security key is compromised, the damage is limited for that period of validity of the key resulting to a short rather than long lasting effect.

The 4G system is an IP-base infrastructure and has an open nature. It has improved security mechanism compared to 3G. A detailed report in [33] showed that 4G uses temporary identifiers just like the 3G but further abstraction was used to narrow the opportunity for intruders to

steal identifiers compared to 3G.By design and mode of operation the 4G networks is meant to cover a wider geographical area in which there are different operating networks with their specific security schemes. It is expected that the 4G will offer seamless service to these heterogeneous networks. However, the heterogeneity of these wireless networks lead to complications in security and privacy [34]. Vulnerabilities at either the physical or MAC (multiple access control) layers of the network may be attributed to the challenges presented by these heterogeneous networks. [34] mentioned interference and scrambling attacks as the two key vulnerabilities at the physical layer. Interference can result to communication system failure as a result of a high SNR (signal-to-noise ratio) caused by interfering signals in the form of white Gaussian Noise (WGN) and multicarrier (narrow band signal), that are deliberately inserted into the system [35]. Scrambling is a more difficult form of attack to implement. This is because a particular or part of the frames is the target. To be successful, the attacker must be knowledgeable and sophisticated to be able to identify particular frames and time slots. The security requirements of 4G heterogeneous networks have been defined as having two levels. The first level is on mobile equipment and the second is on Operator networks. Mobile equipment requirements include protecting the device's integrity, privacy and confidentiality, controlling access to data, and preventing the mobile equipment being stolen or compromised and the data being abused or used as an attack tool [36]. Furthermore, the encryption and cryptography methods being used for 3G networks are not appropriate for 4G networks as new devices such as smart phones and other end-user equipment (UE) and services are introduced for the first time in 4G networks [1]. In this case the UE can also become a source of malicious attacks [2]. The application of the 3G's Authentication and Key Agreement (AKA) to a4G communication architecture was investigated by [7] using X.805 standard. Their analysis showed many threats to the network's security. This indicated that the current security threats in 3G and other new threats were inherent to 4G technology. The progression to 4G which is a heterogeneous network, results in openness to not just cellular attacks but internet based attacks. The security risks in 4G networks as discussed previously are due to the fact that it is a distributed and open architecture network and has a decentralized accountability for security. A distributed and open architecture network entails one that is not physically segregated as it is with 2G and 3G networks. These networks are owned and operated by single Mobile Network Operators (MNO) that can enforce security policies on their respective platforms. The 4G is an all IP with infrastructures and services of MNO interconnected to form a single aggregated service providing network. This makes it possible for one compromised device to create access for potential attackers. There is also decentralizedaccountability for security resulting to lack of overall control of security in 4G LTE [8]. This typical characteristic of 4G LTE allows seamless roaming across heterogeneous networks making it difficult for MNOs to present end-to-end security levels to their subscribers [8].

5G networks need to provide capabilities not only for voice and data communication but also for new services, new industries and for a multitude of devices and applications to connect society at large [9]. Therefore, as a result new services, applications and security

demands could vary significantly among services. For instance security demands for mobile Internet of Things (IoT) and high-speed mobile services will vary. This makes it technically necessary for the system to have a well-integrated security solution. [12], suggested that physical layer security and cryptography are two security measures that can efficiently safeguard devices and services. Physical layer security with proper planning and execution will protect the communication phase of the network while cryptography will protect the processed data after the communication phase. The network infrastructure has to be robust enough to allow security to be built for 5G services. The robustness should enable 5G to provide more options beyond node-to-node and end-to-end security available in today's mobile systems (Schneider, 2016). It entails how well the physical entities of the network elements (NEs) are isolated from each other. This may be done based on network visualization technology (VNT) by which a network could build different network slices (Huawei White Paper, 2015). These slices can be seen as 5G small nodes.

5G Network Technology and Architecture

Research that is ongoing considers the following technologies in the 5G domain [5]. Millimeter wave technologies: The use of much higher frequencies requires a wider frequency spectrum and also provides much wider channel bandwidth 1 – 2 GHz. However, this poses new aims for headphone development, where maximum frequencies are about 2 GHz and currently bandwidths 10 – 20 MHz. For 5G, frequencies above 50 GHz are considered, which presents a challenge to the design of circuits, technologies, and also how the system is used, since the signals of these frequencies do not travel as far and the obstacles almost completely absorb them.

Waveforms: There are many possibilities in this area, from the use of new modulation modes such as GFDM (Generalized Frequency Division Multiplexing), FBMC (Filter Bank Multi–Carrier), UFMC (Universal Filtered Multi–Carrier) and other multi–schema access. A higher signal processing level means that multicarrier systems do not have to be orthogonal such as OFDM (Orthogonal Frequency Division Multiplexing). This allows better maximization of spectrum utilization and flexibility. Massive MIMO (Multiple Input Multiple Output): Although MIMO is used in many applications (from LTE to Wi–Fi), the number of antennas is quite limited. Microwave frequencies create opportunity of using large number of antennas on the same equipment due to the size of the antennas and spacing in terms of wavelength. 4G base stations might typically have 12 antennas, while 5G base stations might support 100 antennas.Network density (using thousands of low power small base stations – femtocells): Reducing cell sizes enables more efficient use of the available bandwidth. Techniques are needed to ensure that small cells in large networks can function satisfactorily. Beam forming is employed to determine the optimum route to each connected user, which helps to reduce interference and increases the chances of easily blocked signals reaching their planned recipient [7]. Full duplex signal transmission: Signals travel on different frequencies in both directions – 1 GHz and 800 MHz with use of high speed switches.The architecture in 5G is based on a Public Key Infrastructure (PKI) system. A PKI system is one that uses cryptographic keys in order to establish identity. A public key and private key are created by a certification authority (CA) for each device. The private key should

only ever be known to the device that needs an identity and the public key can be distributed toany party that needs to encrypt messages to the device. The CA that creates these keys is trusted by all devices in the chain that need to check the validity of the certificates. When a device needs to connect, it will present a message signed by its private key to the authorization system. The authorization system will validate the message by decrypting it with the public key that corresponds to the private key of the device. The system will also verify that the public key it used was created by the trusted CA, so it knows the certificates are valid. If all these checks pass, the system will be able to confirm the identity of the device. The PKI system is the current authentication mechanism in 4G with the cryptographic keys placed permanently on the USIM chips. The devices present their digital certificates to the base station, which then determines whether or not to allow the device on the network. Having permanent keys causes an issue when the number of UE increases substantially with the suspected adoption of 5G for IoT. If keys are compromised, carriers cannot reissue keys instantly. Replacing the USIM card is the only remediation for changing keys. In the current 4G space with an approximate 4.7 billion devices, it would be near impossible to replace even 10% of keys if a catastrophic event were to occur such as a breach that exposes the private keys of all the subscribers. Extrapolating to the proposed 5G space, that number becomes extremely large and even more unfeasible to handle. A solution would be a global adoption of a single large-scale PKI system. [12], stated thatit would be the responsibility of each carrier to opt into the global PKI in order to create a usable and seamless system. The specifics of issuing, replacing, recovering, and revoking keys has already been drawn out by the Internet Engineering Task Force. According to [17], the PKI system could also be used for devices to authenticate with each other before carrying out device-to-device communication that would not traverse through the carrier security equipment. Implementation could be baked into the 5G requirements and would add a significant layer of defense to the architecture. 5G network uses Nanotechnology as defensive tool for security concern that arises due to flat IP. Flat IP network is the key concept to make 5G acceptable for all kind of technologies. To meet customer demand for real-time data applications delivered over mobile broadband networks, wireless operators are turning to flat IP network architectures. Flat IP architecture provides a way to identify devices using symbolic names, unlike the hierarchical architecture such as that is used in "normal" IP addresses. With the shift to flat IP architectures, mobile operators can:

a. Reduce the number of network elements in the data path to lower operations costs and capital expenditure.
b. Partially decouple the cost of delivering service from the volume of data transmitted to align infrastructure capabilities with emerging application requirements.
c. Minimize system latency and enable applications with a lower tolerance for delay; upcoming latencyenhancements on the radio link can also be fully realized.
d. Evolve radio access and packet core networks independently of each other to a greater extent than in the past, creating greater flexibility in network planning and deployment.
e. Develop a flexible core network that can serve as the basis for service

innovation across both mobile and generic IP access networks

f. Create a platform that will enable mobile broadband operators to be competitive, from a price /performance perspective, with wired networks.

Flat network architecture removes that voice-centric hierarchy from the network. Instead of overlaying a packet data core on the voice network, separate and much-simplified data architecture can be implemented that removes the multiple elements from the network chain.

Security Implications of 5G on Mobile Networks Operations

Security is very crucial and important in any technological feat and will arguably remain the biggest concern in the IT industry in the modern era.In 5G security will play a very important role because it not only supports basic packet transmission traffic but accommodates wide variety of applications. Linking industries and crucial applications to the internet; with 5G, it is anticipated that a new model of communication facilities will emerge for the users and industries [8]. In [6] it was considered that a technology may not be regarded as topclass until it amply and capably fulfills all the core requirements of modern cryptography, including confidentiality, authentication, integrity and non-repudiation. Security becomes particularly vital in 5G technology given the major use cases Massive Machine Type Communications (mMTC), Ultra-Reliable and Low Latency Communications (URLLC) and Enhanced Mobile Broadband (eMBB) the technology is envisioned to propagate.

i. Rigid authentication: In the environment of vertical industry, security requirements for different applications could differ considerably among services. In case of Internet of Things (IoT) devices, the requirement of lightweight security with high-speed mobile services demands high capable security method. The network based default of usual hop-by-hop security method might not be effective enough to form separated end-to-end (E2E) security for different types of services. As IoT is slowly being implemented and gaining popularity, a need of an enhanced and rigid authentication method is a necessity for IoT devices. In order to prevent unauthorized access for example, biometric based identification could be a very suitable authentication method for smart phones [13].

ii. Privacy Protection: Due to wide range of applications a need to offer differentiated QoS (Quality of service) is very important. There should be some method or ability within the networks which may need to sense the type of service being used by the user, so that it could offer better privacy. Due to recent major security and privacy issues over cellular network, which include mass surveillance and face network access points. The standardization bodies for telecommunication such as 3GPP and IETF (Internet Engineering Task Force), are being questioned [14]. Over here we must not forget that adding enhanced privacy methods makes implementation of 5G a greater challenge [13].

iii. Trust:The trustworthiness in general of the 5G system is dependent on five main security properties: communication security, identity management, resilience, privacy and security assurance. The specified properties provide a reliable platform that enables a large number of new services to be created. In 5G security area, several essential topics can be identified:

a. Security assurance – The Network Equipment Security Assurance Scheme (NESAS) is jointly formulated by GSMA

and 3GPP (3rd Generation Partnership Project) for evaluation of mobile network security. Developed according to security standards pertaining to vendors' product development, this scheme provides a baseline to evidence that network equipment satisfies a series of security requirements. Currently, 3GPP has initiated security evaluation of multiple 5G network equipment and major equipment vendors and operators are actively participating in the NESAS standard formulation [14].

b. Identity management – In this area, an identity is treated in two ways: as device identity and service identity. Each device (or physical) identity is globally unique and may be assigned to a device by the manufacturer. Service identities are assigned by service providers or networks. A physical identity may correspond to one or more service identities [15]. Network security – In modern network structure it is possible to identify four parts in general: access network (transmits data from user's phone to the mast), core network (processes the data and sends it back; the most sensitive part of the network as it handles all main customer data), transport network (sends this from the mast to the core network) and interconnect network. Each network part consists of three planes, each of which is related to specific type of traffic: the control plane carries the signaling traffic, the user plane carries the payload (actual traffic) and the management plane carries the administrative traffic. In the context of security, all planes can be exposed to special types of threats. There are also certain threats which can affect all three planes at the same time.

c. Flexible and scalable security architecture – The introduction of the concept of virtualization and dynamic configurations in 5G environment has imposed usage of more flexible and dynamic security architectures. New flexible solutions do not necessarily create a conflict between usability and security. For example, new versions of network APIs allow service chaining (or service function chaining (SFC) – capability that uses software-defined networking (SDN) to create a service chain of connected network services and connects them in a virtual chain) (David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler, 2018), while retaining end-to- end encryption of data.

d. Energy-efficient security – The implementation of energy efficient security schemes (used for key generation, processes of encryption and decryption) for data consolidation and aggregation on the way to the traffic destination represents one of the most needed factors in wireless networks.

e. Cloud security – Cloud security (or cloud computing security), consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data and infrastructure (Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, Elisa Bertino, 2019). Network functions virtualization (NFV), based on cloud approach, fundamentally changed the architecture, security and implementation of telecommunications networks.

CONCLUSION AND RECOMMENDATION

The paper discusses security implications of 5G on mobile network operations which it stated to be enhanced from previous generation. It started from the evolution from 1G through 4G and gradually approaching 5G to keep pace with the ever increasing bandwidth and security demands. Some of the very basic concerns regarding 5G security are being highlighted as well as some of the improved technologies are being pointed out.Security techniques are being put in place to safeguard today's mobile communication systems, although, a much tougher security mechanisms are still necessary for a heterogeneous network. It is expected as a new network 5G will experience some new use cases and thereby be exposed to new forms of security threats. Therefore, the paper recommends the need for Hardware Security Modules (HSMs) for the various devices of the network as this will separate out the cryptographic key storage and processing functions into a trusted device. Such a device should have a simple and strictlydefined interface, and if physical access is an issue, it should also resist tampering. Also,security evaluation should be developed and validated by the standard organizations like InternationalTelecommunicationUnionRadiocommunicationSector(ITUR),the3rdGenerationPartnershipProject (3GPP) and the Next Generation Mobile Networks (NGMN) Allianceand the Internet Engineering Task Force (IETF) to guarantee a certain level of security and to provide a method of comparing the security of one product with that of another. Common Criteria (CC) and the Federal Information Processing Standard (FIPS) are two main methods that exist to evaluate the security of a given product.

REFERENCES

1. 3GPP, (2019). url: https://www.3gpp.org/about-3gpp/about-3gpp.
2. 3GPP, (2018), "3GPP System Architecture Evolution (SAE) – Security Architecture" *technical specification* (TS) 33.401, v15.2.0.
3. 3GPP, (2018), "Security Architecture and Procedures for 5G System" (Release 15), *technical specification* (TS) 33.501, v15.5.0.
4. 5G Security: Forward Thinking, (2015) *Huawei White Paper.*Available (http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf)
5. Aiash, M., Mapp, G., Lasebae, A. & Phan, R. (2010). Providing security in 4G systems: Unveiling the challenges in telecommunications. *Sixth Advanced International Conference (AICT).* 439 – 444.
6. Barbeau, M. (2005). Wimax/802.16 Threat Analysis. *In Proceedings of the 1st ACM International Conference on Quality of Service & Security in Wireless and Mobile Networks.*
7. Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R and Stettler, V. (2018). A Formal Analysis of 5G Authentication, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (CCS '18).
8. Chavan, S. & Mane, V. (2013). 4G Wireless Networks Challenges and Benefits. *International Journal of Emerging Technology and Advanced Engineering,* 3(7).
9. Chokhani, S. et al. (2003). Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647. RFC Editor.
10. CISAR, P. and CISAR, S.M. (2019), SECURITY ASPECTS OF 5G MOBILE NETWORKS. ANNALS of Faculty Engineering Hunedoara –

International Journal of Engineering.
11. Dumbre, N., Patwa, M. and Patwa, K. (2013). 5G WIRELESS TECHNOLOGIES-Still 4G auction not over, but time to start talking 5G. *International Journal of Science, Engineering and Technology Research* (IJSETR) Volume 2, Issue 2.
12. Eluwole, O. T., Lohi, M. and Udoh, N. S. (2014). "Smart Card Technology: Contactless Payment System and Near Field Communication," SDPS *19th International Conference on Transformative Research in Science and Engineering, Business and Social Innovation*, Sarawak, Malaysia, pp. 19-26.
13. ERICSSON, (2015). Mobility Report, Available: (https://www.ericsson.com/res/docs/2015/ericssonmobility-report-june-2015.pdf).
14. Firdaus, H. (2016). 4G LTE Network Growth in India and Security Issue in Network, *International Journal of Computer Science and Network Security, 16 (11).*
15. Fonyi, S. (2019). Overview of 5G Security and Vulnerabilities: The Cyber Defense Review, Vol. 5, No. 1, *International Conference on Cyber Conflict* (CyCon U.S.) November 18-20, 2019: Defending Forward (Spring 2020), pp. 117134
16. Hong, B., Bae, S. and Kim, Y. (2018). GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier, *Proceedings of the Internet Society Symposium on Network and Distributed System Security* (NDSS).
17. Horncand, G. & Howard, P. (2000). An Introduction to the Security Features of 3GPP and Third Generation Mobile Communication Systems. IEEE VTS 51st *Vehicular Technology Cont.*
18. Housley, R. (2018). Internationalization Updates to RFC 5280. RFC 8399. RFC Editor.
19. Hussain, S.R., Echeverria, M., Chowdhury, O., Li, N., Bertino, E. (2019). Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information, *Network and Distributed System Security (NDSS) Symposium*, San Diego.
20. Intelligence,G. (2014). "Understanding 5G : Perspectives on future technological advancements in mobile," no. December, pp. 1–26.
21. ITEF, (2019). Who We Are. url: https://www.ietf.org/about/who/.
22. ITU, (2019). url: https://www.itu.int/en/about/Pages/ default.aspx.
23. Jover, R. P., and Marojevic, V. (2019). Security and Protocol Exploit Analysis of the 5G Specifications. *In IEEE Access 7*, 24956–24963. issn: 2169-3536. doi: 10.1109/ACCESS.2019.2899254.
24. Kachhavay, M.G and Thakare, A.P. (2014), 5G Technology-Evolution and Revolution. *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.3, pg. 1080-1087
25. Kakesh, K.R. (2016). A frame work for 4G wireless networks-overview and challenges. *Journal of Excellence in Computer Science and Engineering, 2(1), 1-10.*
26. Karthik K. and Sobharani kuracha, (2015). "SECURITY IN WIRELESS CELLULAR," vol. 4, no. 4, pp. 190–197, *IJAIEM.*
27. Pachauri, A.K., and Singh, O. (2012). 5G Technology – Redefining wireless Communication in upcoming Years. *International Journal of Computer Science and Management Research* Vol 1 Issue 1, ISSN 2278 – 733X.
28. Ravishankar, B. & Harishankar, M. (2008). Roaming issues in 3GPP security architecture and solution using UMM architecture. *2nd Conf. on Mobile Ubiquitous Computing Systems, Services and Technologies.*

29. Santesson, S. et al. (2013). X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 6960. http:// www.rfc-editor.org/rfc/rfc6960.txt. RFC Editor. url: http://www.rfc-editor.org/rfc/rfc6960.txt.
30. Sapakal, M. R. S. and Kadam,M. S. S. (2013). "5G Mobile Technology," vol. 2, no. 2, pp. 568–571.
31. Seddigh, N., Nandy, B., Makkar, R. & Beauoront, J.F. (2010). Security advances and challenges in 4G wireless network, *8th Annual International Conference on Privacy, Security Trust.*
32. Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V and Seifert, J. (2016). "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems", *Proceedings of the Internet Society Symposium on Network and Distributed System Security* (NDSS).
33. Shin, M., Ma, J., Mishra, A. & Arbangh, W.A. (2006). Wireless network security and interworking. *The Proceedings of IEEE in Cryptograph.*
34. Spatz, & Schmitz, R. (2000). Secure Interpretation Between 2G and 3G Mobile Radio Network. *First International Conference on 3G Mobile Communication Technologies.*
35. Tudzarov, A., and Janevski, T., (2011). Functional Architecture for 5G Mobile Networks. *International Journal of Advanced Science and Technology* Vol. 3.
36. Zheng, Y., He, D., Yu, W. & Tang, X. (2006). Trusted computing-based security architecture for 4G mobile networks. *In Parallel and distributed computing, applications and technologies, (PDCAT), Sixth International Conference,* Sichuan, 251 – 255