IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Major Security Challenges in 5G Network

Abid Hasan Khan[1], Abdullahi Hassan Yusuf [2], Tahorima Benzear Lira[3]
[1]ID: 012201050, Dept. of CSE, United International University, Dhaka, Bangladesh
[2]ID: 012203010, Dept. of CSE. United International University, Dhaka, Bangladesh
[3]ID: 012211064, Dept. of CSE, United International University, Dhaka, Bangladesh

ABSTRACT- With innovative technology concepts, 5G networks will meet broadband access requirements everywhere. Achieve high user and device mobility and connectivity for many devices (such as the Internet of Things) in a highly reliable and cost-effective manner. Software defined networking and network functions virtualization leveraging the developments in cloud computing such as mobile edge computing is the most spoken out technologies to meet these requirements. Security has ended up the essential concern in many telecommunications businesses nowadays as dangers can have high consequences. Particularly, as the center and empower advances will be related with 5G arrange, the secret data will move at all layers in future remote frameworks. However, firmly using these technologies and providing user privacy & more security in future wireless networks are the new major concerns. Hence, in this paper we tried to provide an overview of security challenges in clouds, software defined networking, and network function virtualization. In this paper further deliberates the new security features involving different technologies applied to 5G, like device-to-device communications, heterogeneous networks, massive multiple-input multiple-output, software defined networks, and Internet of Things. Henceforth, we'll try to demonstrate the presents solutions to these challenges and future directions for secure 5G systems strongly.

INDEX TERMS- Technology, Security, 5G Security, NFV, IoT, MIMO, Heterogeneous Networks, SDN etc.

I. INTRODUCTION

Cellular systems are without a doubt one of the foremost basic frameworks. The novel 5G cellular systems [1] will connect IoT gadgets and frameworks, and in this way guarantees to contribute to the change of cities, homes, healthcare imaging and diagnostics, fabricating, transportation, and mechanical autonomy. Encourage absent from past eras, 5G organize has presented major changes within the convention stack and framework structures. For occasion, 5G physical layer underpins versatile broadband, enormous machine sort communication, and ultra-reliable and idleness communication for a wide cluster of gadgets and applications. 5G networks will use software and virtualization to achieve service goals in terms of flexibility, configurability and scalability. In particular, the most important 5G network design concepts will be Network Slicing (i.e. dedicated logical networks for isolated applications), Mobile Edge Computing (MEC), Network Function Virtualization (NFV), and Software Defined Networking (SDN) [2]. 5G cellular systems are based on several different technologies, these are Millimeter waves, Small cells, Massive MIMO, Beamforming, Full duplex, Software defined networks (SDN). The combination of a few innovations can enormously increase communication capacity, diminish transmission latency, and spare vitality.

The 5G design can be divided into the taking after three main components: Client Gear (UE), the 5G radio get to network (5G-RAN) and the 5G center organize (5G-CN).

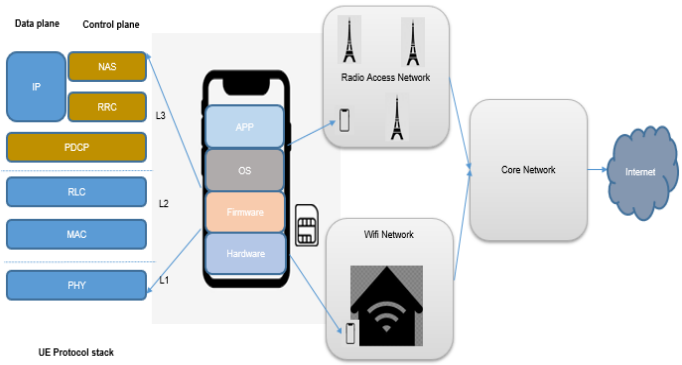

FIGURE 1. Simplified Architecture of 5G Network with layers.

In this overview, we point to get it the security and security progresses from the viewpoint of SDN, NFV, MEC, etc. To this point, we mainly focus on the commitments from both the scholarly world and industry that are tending to security and protection of 5G networks. As highlighted in Fig. 1, this overview has moreover centered on. On the other hand, 5G has created on different novel network softwarization innovations such as SDN, NFV, MEC, cloud computing and NS [2]. It is critical to consider the security of underline 5G innovations with investigations of the security in 5G systems. Here is a summary of recently published overviews of the security of 5G and higher technologies.. Most of these articles are centered on either individual advance such as SDN, NFV, MEC and NS security. Be that

as it may, these ponders are very shallow in addressing security issues whereas joining them in 5G systems.

In particular, security is required to authenticate massive devices, provide high availability, low latency, low power consumption, and other changes through IoT application scenarios [3]. 5G requires a considerable degree of security for new application scenarios, new network architectures, new air interface technologies, all of which are radically different from the existing 4G network. The introduction of SDN / NFV, virtualization, mobile edge computing, and other new technologies also bring with them certain changes and security risks [4]. 5G security architecture needs to support multiple application scenarios and include a unified authentication framework, service certification, network slice security, and user privacy protection.

The 3GPP Working Group, SA3, is responsible for 5G network security architecture design, and has determined that security architecture design should consider the areas shown in Figure 2 . Based on these design principles, 5GPP [5], ETSI, China's Future Mobile Communications Forum, the IMT-2020 (5G) Promotion Group, Ericsson (Ericsson) [6], Nokia, the Datang Telecom Technology Industry Group, Huawei Technologies Co., Ltd. , and other domestic and foreign enterprises have proposed their respective security architecture designs.

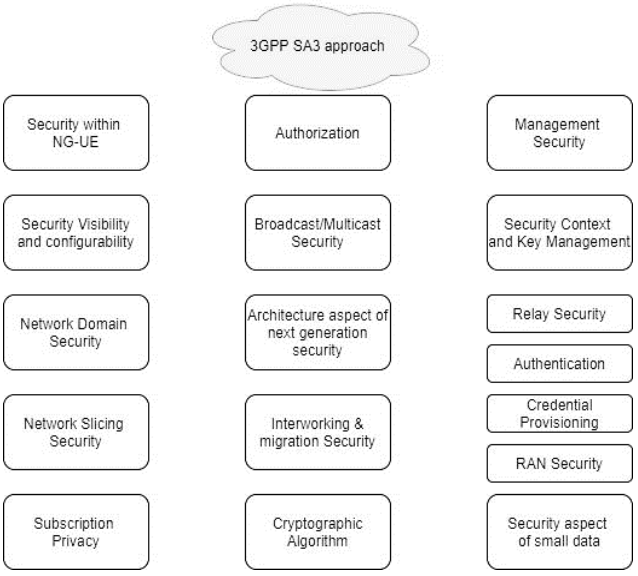

FIGURE 2. Security Area in 5G.

A. Motivation:

This paper examines the effect of unused advances such as SDN, NFV and cloud computing on the unused 5G mobile network. We display a list of conceivable security protection approaches that can be utilized to guarantee 5G protection. To the best of the authors' information, this can be a to begin with paper which provides a total diagram on 5G protection, security challenges and possible arrangements.

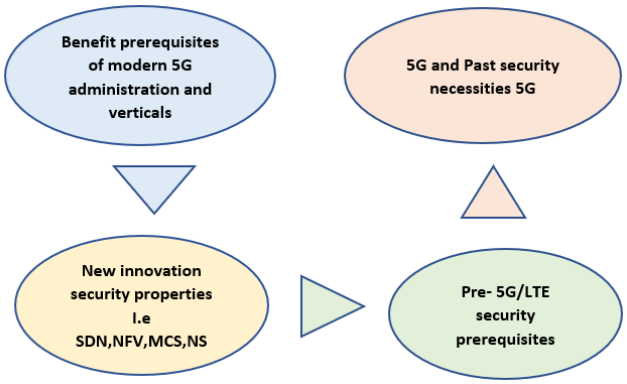

FIGURE 3. Development of 5G and Past security necessaires.

B. Problem Statement:

Security & privacy which is the protection of personal information of a specific user which may hint at any details of personal activities that might need to be secure. [8] If this information will not be secured that will cause harm from various means like used by any external group to notice their daily activity. Privacy doesn't mean that all user information should be private, some information must be shared with authorities under some criteria. Security also shows how much data should be protected & how much should be shared. Security and privacy in 5G is much more critical than 4G or 3G architecture because of the huge transformation of new daily life applications, devices and access mode of digital services. Furthermore, 5G will bring new enhancements in terms of architectural and service-oriented requirements compared with traditional network systems so it needs more privacy policies & regulations. To secure the user end of 5G mobile network can be categorized into three main categories, they are data, location and identity privacy. [8][9]

C. Paper Organization:

The paper organization is as follows. Section II gives a brief comparison with the related work. Section III describes the major security challenges what may occurs in 5G network. Section IV identifies future research directions, while Section V presents the conclusion. The paper structure can be visualized as Fig. 4.

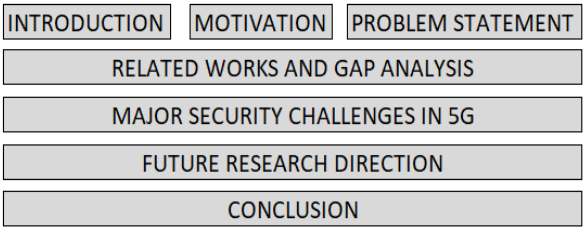

FIGURE 4. Paper Organization Topology.

II. RELATED WORKS AND GAP ANALYSIS

A. Security Architecture in 5G:

The aim of 5G is to become a reliable and trusted innovation platform for businesses and organizations to build and deliver new added value services, but it is also measured an enabler for digitizing and modernizing critical national infrastructures like energy, transport etc. The latter raises the bar for 5G systems to provide greater availability and better assurances of secure communication services. The horizontal, system-wide security approach spans crosswise the network from the user device to the orientation point where the operator terminates their services.

Horizontal security (fig. 5) is accomplished by combining and coordinating a multitude of security controls across diverse domains in telecommunication networks, including radio access (like antennas), transport networks, packet core (HSS), network support services (DNS, DHCP), cloud infrastructure, and various management systems (e.g., network management, customer experience management, security management). [10] Security across all these areas must be coordinated to deliver the targeted availability of services and confidentiality and integrity of data sent, stored, and handled within the 5G system. Horizontal security will protect the privacy of 5G users depending on that data sent over the system is always confidentiality and integrity protected.

Transport networks play an important role in the 5G system because they offer high-speed low-latency connectivity services between all 5G network functions. Thus, the availability of transport networks is directly related to the availability of the 5G system and the services it delivers [12]. To ensure availability of transport services during node failure, cable or fiber breaks, or overload events transport networks can employ various technical solutions as well as considerations during network design, including:

- Geo-redundant paths which allows traffic to be re-routed in case of a path failure.
- Link redundancy solutions for fast failover in case of port failure.
- Path redundancy mechanisms that re-routes traffic flows due to path failure or overload conditions.
- DDoS detection and moderation solutions.
- Port-based authentication to verify authorized network devices are attached to the network.

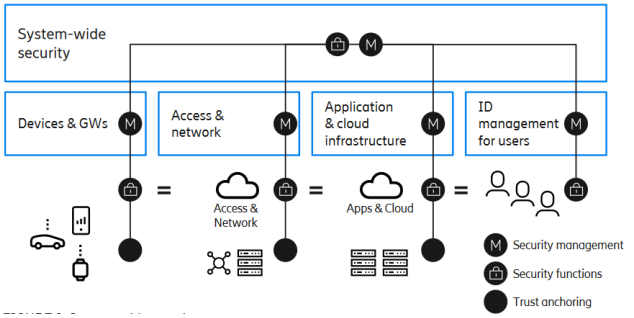

FIGURE 5. System-wide Security

The table below here shows the gap analysis of different reviewed paper by us:

No.	Paper title	Year	Important Features
1.	Prospects for Handling 5G Network Security: Challenges, Recommendations and Future Directions	2021	Highlighted some of the very basic security concerns of 5G networks presented recommendations and some future direction integration 5G They created a security framework for 5G networks and cost effectively deploy the 5G in an LTE Advanced network
2.	5G Security: Analysis of Threats and Solutions	2017	Authors presented 5G will use mobile clouds, SDN and NFV to meet the challenges of massive connectivity, flexibility, and costs. With all the benefits, these technologies also have inherent security challenges. They highlighted the main security challenges that can become more threatening in 5G. They highlighted key security challenges in 5G such as: High number of end-user devices and new IoT.

3.	The current state of affairs in 5G security and the main remaining security challenges	2018	This manuscript esents a summary d analysis of the rrent state of fairs in 5G otocol security.
4.	Security for 5G and Beyond	2020	The security threat landscape of 5G has grown enormously due to the unprecedented increase in types of services and in the number of devices. This article outlines the 5G network threat landscape, the security vulnerabilities in the new technological concepts that will be adopted by 5G.
5.	Security for 5G Mobile Wireless Networks	2017	This paper presents a comprehensive study on the security of 5G wireless network systems compared with the traditional cellular networks. They highlighted the current security solutions mainly based on the security services provided such as authentication, availability, data confidentiality, key management and privacy have been introduced.
6.	Security Challenges in 5G-Based IoT Middleware Systems	2020	They declared IoT middleware systems have security as one of their main challenges, and, with the arrival of the 5G, these systems will be target of new security threats. They present the main threats and security requirements envisaged to be introduced by 5G in IoT middleware systems.
			They also analyse the current security approaches of IoT middleware systems, and present some challenges related to security aiming the 5G-based IoT middleware technologies.
7.	Security and Privacy Challenges in 5G-Enabled Vehicular Networks	2020	5G-enabled vehicles can communicate with the core network via V2I service and other vehicles via V2V service. However, secure and efficient mobility management will face a great challenge due to frequent handover and largescale vehicular machine-to-machine (M2M) communications They have presented the architecture for 5G-enabled vehicular networks then security.
8.	Security for 5G Communications	2019	They presented representative examples of potential threats and attacks against the main components of the future 5G systems in order to shed light on the future security issues and challenges in the upcoming 5G era. They focused on examples of potential threats and attacks for the following 5G system components: the UE, the access networks, the mobile operator's core network and the external IP networks.

9.	A Security Architecture for 5G Networks	2018	5G networks will provide opportunities for the creation of new services, for new business models, and for new players to enter the mobile market. We note that a 5G (or any other) security architecture in itself does not provide answers to what the security threats to the network are and to which threats that have to be mitigated by specific countermeasures.
10.	Major Security Challenges in 5G Network	2021 (in this paper)	We will present different types of security threats We also will highlight challenges of 5G networks figure out possible solutions

Table 1. Summary table of literature review

III. MAJOR SECURITY CHALLENGES IN 5G

5G needs vigorous security architectures and solutions since it will connect every feature of life to communication networks. Therefore, we investigate and highpoint the important security challenges in 5G networks and overview the potential solutions that could lead to secure 5G systems. The fundamental challenges in 5G, which are highlighted by Next Generation Mobile Networks (NGMN) [12] and widely discussed in the literature, are as follows:

- **DoS attacks on end-user devices:** There is no security measures taken for operating systems, and configuration data and applications on user devices.
- **Flash network traffic:** High number of end-user devices and new things like IoT.
- **User plane integrity:** There is no cryptographic integrity protection for the user data plane.
- **Roaming security:** User security parameters are not updated with roaming from one operator network to another, principal to security compromises with roaming.
- **Denial of Service (DoS) attacks on the infrastructure:** Visible nature of network control fundamentals, and unencrypted control channels.
- **Security of radio interfaces:** Radio interface encryption keys can be sent through insecure channels.
- **Signaling storms:** Circulated control systems requiring coordination, such as Non-Access Stratum (NAS) layer of Third Generation Partnership Project (3GPP) protocols.

A. Most Well know attacks in 5G & Solution

As per the broadcast nature of the wireless medium, wireless information transmission is vulnerable to various malicious threats; like; Eavesdropping & Traffic Analysis. Its an attack that is used by an unintended receiver to intercept a message from others. Jamming can entirely interrupt the communications between authentic users. DoS is a security attack violation of the availability of the networks and DDoS can be formed when more than one distributed adversary exists.
On the other hand, MITM the attacker furtively takes control of the communication channel between two genuine parties.

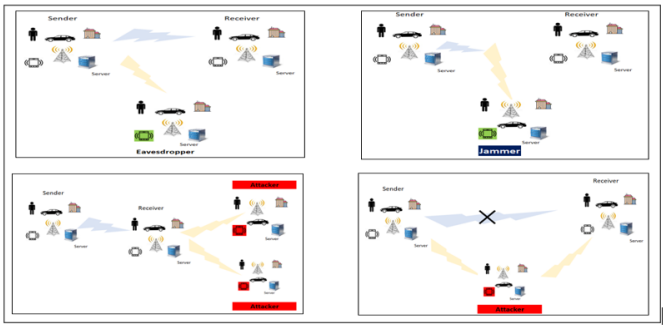

FIGURE 6, Attacks in 5G wireless networks

Denial-of-Service (DoS) – due to misconfiguration, congestion or overload situations leading to inaccessibility of network services. Denial-of-Detection (DoD) - avoiding ML from generating signals from events, attacks, or failures; enabling interruptions and other threats [13]. Leaking company secrets - challenger learns operational or business-critical information from network operators. Valuable private or confidential information can exist in collected or incidental data or in the ML model itself. Privacy leakage - customer specific, like sensitive parameters, data become available to outsiders.
Massive MIMO is an auspicious method for efficient transmission of massive information and is regarded as one of “big three” 5G technologies. In this section, we review the current security threats and measures of massive MIMO technology based on passive and active eavesdropper scenarios, respectively [14]. The impact of multicell interfering and pilot pollution on the achievable ergodic secrecy rate are examined and numerous matched filtering precoding and artificial noise (AN) generation designs are projected to degrade the eavesdropper’s channel and protect the desired user’s channel. For the same system model, normalized channel upturn and AN transmission system are designed in to further improve the secrecy rate performance. J. Wang et al. investigate AN-aided secure massive MIMO transmission over. [15][17]

Fake base stations: This lack of authentication allows adversaries to install rogue base Stations. Fake emergency

alerts: Along with incoming services (like, phone call), this unprotected message in both 4G LTE and 5G is also broadcast for sending emergency alerts to the device (e.g., Tsunami, Earthquake, and Amber).Identity exposure attacks: [16] exposures of permanent identifier(e.g., International Mobile Subscriber Identity or IMSI).Side-channel attacks: Side-channel attacks that exploit the fixed/static paging occasion in 4G and 5G networks

We've shown in Table 2, a summary of various types of security intimidations and attacks, the targeted elements or services in a network, and the technologies that are most disposed to the attacks or threats are tick-marked. [18] These security challenges are briefly described in the following sections.

Security Threat	Network Element	Effective Technology			Privacy	Links
		SDN	NFV	Cloud		
DoS Attack	Centralize control element	✓	✓	✓		
MITM	SDN controller	✓			✓	✓
Hijacking attacks	SDN controller	✓	✓			
Signaling Stroms	5G core network element			✓		✓
Timing attacks	Subscriber location			✓	✓	
IMSI catching attacks	Subscriber identity				✓	✓
Reset & IP spoofing	CC					✓

Table 2, Security Challenges in 5G Technologies

B. Security Challenges & Attack Related to SDN & NFV

This area contains a few of the foremost challenging security issues related to the key 5G advances, i.e., SDN/SDMN, NFV, MEC, cloud computing and arrange cutting. Furthermore, the effect of these advances on 5G security is also discussed in this segment.

Traditional mobile networks like GSM or LTE will ensure security & privacy mainly relies on the trust relationship between the communication equipment & communication channels. [19] But in such scenarios, traditional trust relationships are very difficult to maintain because of many wide-influencing factors & loopholes.

SDN/NFV technology has been introduced to overcome this barrier in new network architecture. It's mainly used for separating the data planes & control of the network equipment. It can create a favorable trust relationship based on the general hardware from different manufacturing groups. This concept is more compatible for cloud, virtualization & pooling architecture design and their security system/challenges. [20] Moreover, sharing computing resources, hardware, storage, network resources will introduce new problems for example, virtual machine security, cloud security or data security which is a very critical parameter for telecommunications. SO, it is very [23] important to make full utilization of 5G network architecture such as hardware & software decoupling, dynamization or virtualization to reduce the endangers security properties & build key security features for a highly reliable & secure 5G network based around the world with untrusted network components.

Within the past era versatile arrange, portable administrators had coordinate get to and control of the framework components but in 5G portable administrators are losing control over the system components and ought to depend on modern communication benefit suppliers. As 5G portable administrators are losing the complete control of security and security, client and information protection are genuinely challenged in shared situations where the same foundation is shared among different sellers, for occurrence VMNOs and other competitors. In addition, there are no boundaries (physical) of 5G systems as they utilize cloud-based capacity and NFV highlights. As diverse nations have diverse levels of information security instruments, security is challenged in case the client information is put away in a cloud in a diverse country.[21]

In [22] this paper the creators highlighted a few of the key security challenges in 5G engineering like Streak organize activity, Security of radio interfacing, Client plane judgment, signaling storms, Meandering Security along side their potential arrangement by utilizing modern advances like computer program characterized organizing (SDN), and organize capacities virtualization (NFV), Have Character Convention (HIP)-based plans too utilizing centralized frameworks that have worldwide perceivability. The challenges of streak organize activity can be unraveled by either including modern assets or expanding the utility of existing frameworks with novel innovations modern innovations such as SDN and NFV can fathom these challenges more fetched viably. The [21] security of the radio interface keys is still a challenge, because it needs secure trade of keys scrambled just like the proposed Have Character Convention (HIP)-based plans. The same end-to-end encryption convention can be utilized for client plane judgment. Roaming security and network-wide commanded security arrangements can be accomplished utilizing centralized frameworks that have worldwide perceivability of the users' exercises and organize activity behavior (e.g., SDN). IV. Signaling storms will be more challenging due to the intemperate network of UEs, little base stations, and tall client versatility. The cloud radio gets to arrange (C-RAN) and edge computing are the potential issue solvers for these challenges [15][22]

IV. FUTURE RESEARCH DIRECTION

Open air interfaces provide a path to effect aspects such as capacities of the physical radio layer properties. Argumentative attacks against signal classifications are more powerful than classical jamming attacks on the wireless channel. User plane integrity protection, which was familiarized in 5G is not mandatory feature and that's why it leaves the door open to fiddled application layer data from UEs.

A misbehaving UE may input spiteful data for ML functions which utilize information from the UE mechanisms. [24] Vulnerabilities in network security may also enable UEs to

advance access to ML functions, which do not exploit inputs directly from UEs. For example, part of 5G and 4G access network communication is unprotected. [25] A few security instruments must be executed to attain a secure arrange cutting system. However, these security instruments must be coordinated and safely communicate to guarantee the decrease the security overhead and impact of security instrument. To attain this goal, allotment of an free arrange cut for security is beneficial.[26] Depending on the utilize cases, portable systems have various potential assault surfaces. Where contaminated preparing and sidestepping operational information can come into play. Arrange components (BTS, SDN switches and cloud and edge servers facilitating ML capacities etc.) may be hindered upon. [27] A rival that has effectively entered the primary guards can carry out distinctive assaults too.

V. CONCLUSION

Wireless communication networks have been developing from linking simple mobile phones in 1G towards connecting almost all aspects of life in 5G. During this evolution, security landscape has equally progressed from simple phone tapping to various attacks on mobile devices, network equipment and services. For integrating new things (IoT) and services into the network, 5G will use new technologies such as advanced cloud computing concepts (MEC), SDN, NFV, and massive MIMO etc. These technologies have their own essential security challenges which can further obscure the network security scenery. Therefore, in this paper we'll have discussing the security challenges that exist in different parts of the network like access network, core network, and within the technologies that will be used in 5G networks. The accumulation of assorted devices, services, and new networking skills does increase the security threat scenario, and thus new security solutions must be required for efficient and secure connectivity.

To sum it up, it is highly possible that new types of security threats and challenges will arise along with the placement of novel communication technologies and services. However, considering these challenges right from the initial design phases to the placement phases will minimize the probability of potential security and privacy gaps.

ACKNOWLEDGMENT

We thank the authorities of the United International University, Dhaka, Bangladesh for providing an enabling environment and using their electronic resources. We are particularly grateful for the guidance of Prof. Dr. Md. Motaharul Islam for this research. It should be noted that this work is the result of teamwork by a group of Computer Science & Engineering students in 2021.

REFERENCES

[1] L. Paterson, and O. Sunay, "5G Mobile Networks: A Systems Approach", https://5g.systemsapproach.org/README.html

[2] Alcardo Alex Barakabitzea, Arslan Ahmadb, Rashid Mijumbic and Andrew Hinesd "5G Network Slicing using SDN and NFV: A Survey of Taxonomy"

[3] Ghadha Arfaoui, Pascal Bission, Rolf Blom, Ravishankar Borgaonkar, "A Security Architecture for 5G Networks" Received March 15, 2018, accepted March 24, 2018, date of publication April 17, 2018, date of current version May 9, 2018

[4] Niranjan Lal, Shobhit Mani Tiwari, Devbrat Khare and Megha Saxena, "Prospects for Handling 5G Network Security: Challenges, Recommendations and Future Directions https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/0120529/pdf.

[5] Extending the NetServ autonomic management capabilities using OpenFlow https://ieeexplore.ieee.org/document/6211961

[6] https://www.researchgate.net/publication/332960779_Blockchain-enabled_Authentication_Handover_with_Efficient_Privacy_Protection_in_SDN-based_5G_Networks

[7] 5G: rethink mobile communications for 2020+ https://pubmed.ncbi.nlm.nih.gov/26809577/

[8] Rabia Khan, Pradeep Kumer, Madhushanka Liyanage, " A Survey on Security and Privacy of 5G Technologies" https://www.researchgate.net/publication/334644935_A_Survey_on_Security_and_Privacy_of_5G_Technologies_Potential_Solutions_Recent_Advancements_and_Future_Directions

[9] Ji Xinsheng, Huang, Kaizhi, Jin, Liang Tang, Hongboi, "Overview of 5G security technology" https://ur.booksc.eu/book/71258618/b91d26

[10] Ericsson, "Ericsson Mobility Report," 2017, available online at https://www:ericsson:com/assets/local/mobilityreport/documents/2017/ericsson-mobilityreportjune-2017:pdf.

[11] Mobile Edge Computing https://sdn.ieee.org/newsletter/march-2016/mobile-edge-computing-an-important-ingredient-of-5g-networks

[12] Ijaz Ahmad, Shahriar Shahabuddin, Tanesh Kumar, Jude Okwuibe, Andrei Gurtov, Mika Ylianttila, "Security for 5G and Beyond" https://ieeexplore.ieee.org/document/87125532

[13] NGMN Alliance, "NGMN 5G white paper," Next Generation Mobile Networks, White paper, 2015

[14] Lightweight DDoS flooding attack detection using NOX/OpenFlow https://ieeexplore.ieee.org/document/5735752

[15] Chengzhe Lai, Rongxing Lu, Dong Zheng, and Xuemin (Sherman) Shen "Security and Privacy Challenges in 5G-Enabled Vehicular Networks"

[16] DONGFENG FANG, YI QIAN, AND ROSE QINGYANG HU, " Security for 5G Mobile Wireless Networks" Received October 25, 2017, accepted November 20, 2017, date of publication December 4, 2017, date of current version February 28, 2018

[17] Ankush Singla, Syed Rafiul Hussain, Omar Chowdhury, Elisa Bertino, and Ninghui Li, " Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks" https://www.researchgate.net/publication/338475577_Protecting_the_4G_and_5G_Cellular_Paging_Protocols_against_Security_and_Privacy_Attacks

[18] N. Panwar, S. Sharma and A. K. Singh, "A Suvery on 5G: The Next Generation of Mobile Communication", Physical Communication, vol. 18, no. 2, pp. 64-84, 2016.

[19] Jude Okwuibe, Mika Ylianttila, Andrei Gurtov, Tanesh Kumar, Madhusanka Liyanag, Ijaz Ahmad "Overview of 5G Security Challenges and Solutions" http://jultika.oulu.fi/files/nbnfi-fe201902124647.pdf

[20] https://www.researchgate.net/publication/305903647_Enhancing_Network_Security_through_Software_Defined_Networking_SDN

[21] ETSI, "GS NFV 002: Network functions virtualization (NFV); architectural framework," 2013, available online http://www:etsi:org/deliver/etsi_gs/nfv/001_099/002/01:01:01_60/gs_nfv002v010101p:pdf.

[22] Optimum Ultra-Reliable and Low Latency Communications in 5G New Radio https://www.researchgate.net/publication/320808215_Optimum_Ultra-Reliable_and_Low_Latency_Communications_in_5G_New_Radio

[23] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in IEEE Communications Standards Magazine (Volume: 2, Issue: 1, MARCH 2018), 2018.

[24] Enhancing Network Security through Software Defined Networking (SDN)

[25] Machine Learning Threatens 5G Security by JANI SUOMALAINEN, ARTO JUHOLA , SHAHRIAR SHAHABUDDIN, AARNE MÄMMELÄ AND IJAZ AHMAD, Date of publication- October 19, 2020 by IEEE Acess. https://ieeexplore.ieee.org/abstract/document/9229146

[26] M. E. Morocho-Cayamcela, H. Lee, and W. Lim, ‘‘Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions,’’ IEEE Access, vol. 7, pp. 137184–137206, 2019 https://ieeexplore.ieee.org/abstract/document/8844682

[27] Roger Piqueras Jover Bloomberg LP, "The current state of affairs in 5G security and the main remaining security challenges "REPORT BASED ON RESPONSE TO FCC NOI DA 16-1282 (HTTPS://BIT.LY/2KMYICZ) AND DEC. 2018 BLOG POST (HTTPS://BIT.LY/2XMKE4L).