5G SECURITY THREATS AFFECTING DIGITAL ECONOMY AND THEIR COUNTERMEASURES

Conference Paper · January 2021

DOI: 10.1049/icp.2021.2419

Azhar Ghafoor
COMSATS University Islamabad

Maham Iftikhar
COMSATS University Islamabad

5G SECURITY THREATS AFFECTING DIGITAL ECONOMY AND THEIR COUNTERMEASURES

Azhar Ghafoor, Munam Ali Shah, Mudassar Mushtaq, Maham Iftikhar

Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan
azharghafoor39@gmail.com, mshah@comsats.edu.pk, mudassarmushtaqganai@gmail.com, maham.iftikhar97@gmail.com

Keywords: 5G THREATS, NFV, USERS PRIVACY, SECURE COMMUNICATION, SDN

Abstract

The 5G (fifth generation) network will provide a wide range of connectivity to share information and data with a low latency rate, higher bandwidth and more frequency spectrum to increase speed. Massive Internet of Things (IoT) devices' security is critical to secure communication between different devices. 5G wireless communication offers new services and frameworks, but it is also amplifying security impacts. However, there are a lot of challenges to users' privacy as well. This report provides an overall view of threats and challenges in 5G networks and presents solutions to these challenges. In addition, 5G is being used to increase communication security while providing essential building blocks for physical layer security.

1. Introduction

The 5G network provides portability, higher bandwidth, low latency rate and enhanced network performance. The 5G network adopts a new framework and technologies to improve these features[1]. 5G is also working to integrate networking ideas such as network function virtualisation (NFV), software defined network, and cloud computing to wireless communication networks [2], [3], [4], [5].

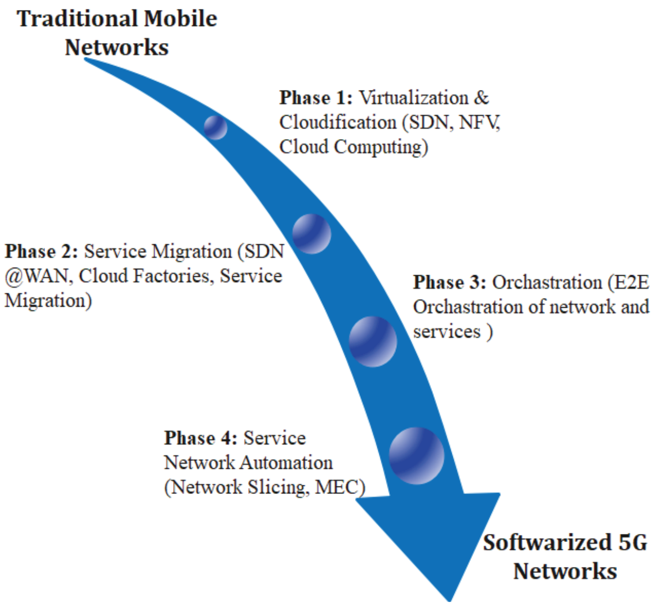

Traditional Mobile Networks
Phase 1: Virtualization & Cloudification (SDN, NFV, Cloud Computing)
Phase 2: Service Migration (SDN @WAN, Cloud Factories, Service Migration)
Phase 3: Orchastration (E2E Orchastration of network and services)
Phase 4: Service Network Automation (Network Slicing, MEC)
Softwarized 5G Networks

Fig. 1 Phases of network transformation to softwarised 5G networks [6]

The target of implementing these features is to define a fast software wireless network. The software defined network (SDN) proposes a solution to control network devices through a central point controller using software [7], [8]. The network function virtualisation (NFV) offers to deploy and create network services and decouple network services to run as software instead of hardware. Cloud computing enhances the scalability of the network and provides a platform to store data [6], [9]. Network slices in 5G increase the support to improve traffic classes in the fifth-generation network.

Table 1 5G key performance indicators [10]

5G parameters	KPI requirements	Category
Data rate	D: 20 Gbps U: 10 Gbps	eMBB
Spectral performance	D: 30 bits/sec/Hz U: 15 bits/sec/Hz	eMBB
Latency	04 ms (eMBB) 01 ms (URLLC)	eMBB, URLLC
Density of connection	01 Million/Km2	Massive IoT
Interruption time for mobility	0 ms	eMBB, URLLC
Mobility	Urban: up to 30 Km/h Rural: up to 500 Km/h	eMBB
Bandwidth	100 MHz to 01 GHz	eMBB, IMT-2020

Privacy and security in the 5G communication network is a significant concern. Risks, threats, and challenges have high consequences.

Fig 1. depicts how technologies enabled a softwarised 5G network and describes the phases and path to a 5G wireless network. The 5G network increases the bandwidth and performance of the network. 5G provides us with a low latency rate and fast-speed internet.

Table 1. points out the differentiation that defines the five key performance dimensions of 5G. 5G use cases and KPI performance vary according to conditions in dense areas, and there are fewer performance indicators.

Fig 2. summarise the 5G networks. 5G will support a massive number of devices [11]. 5G will support radio access technologies (RAT) to provide service on the 5G network [12].

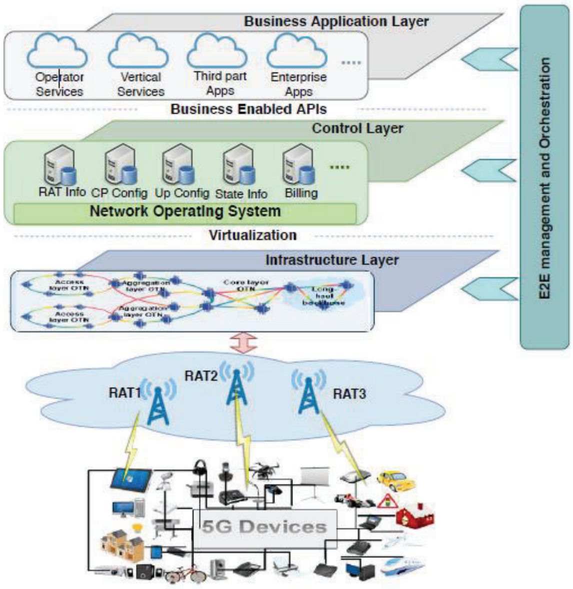


Fig. 2 The high-level architecture of 5G network with different operational layers [6]

The 5G network architecture comprises three layers: infrastructure, business application layer, and control layer. The infrastructure layer consists of base stations, routers and switches, and it communicates with the application layer via the control layer. The control layer has network functionalities, decision making and can translate the command received from the application layer and deliver it to the infrastructure layer. The control layer controls the end-to-end communication and management.

1.1 5G security threats and challenges

5G will connect many devices and critical infrastructure, so it is imperative to secure user data and this infrastructure. We know data is essential if data is corrupted or compromised during 5G transmission, so it is critical. However, for secure 5G communication, evaluation of threats and their solutions are very important. Users' privacy and data are the most important [13].

1.1.1 Traffic (flash): larger number of devices, applications, and IoT.

1.1.2 Interfaces threats: key sent over an insecure channel.

1.1.3 Integrity of user plane: data is not in encrypted form.

1.1.4 DDoS attack on infrastructure: unencrypted control channels and visibility of network channels.

1.1.5 Signalling storms: distributed control channel.

1.1.6 End-users DoS Attacks: No mechanism of security on end devices to access safely.

I will further discuss the security solutions for the threats in this paper. The rest of the paper is organised as follows. Section II reviews the related studies. The comparison on different papers is shown in Section III and our conclusions and future direction in Section IV, and details of existing threats in Section V.

2. Related work

In this section, I have presented the most challenging threats to the 5G network and technologies such as software defined network (SDN), network virtualisation (NFV), and Internet of Things (IoT). Furthermore, the possible solutions and impact of these technologies.

2.1 Security issues in SDN/SDNM

SDN is used to provide a central network control platform and enables functionality in communication networks. SDN is an essential technology in the 5G network to provide high speed and reliability. The authors of [6] use two threat models to provide a comparative analysis of the SDN network. It means that the most critical contributions on the network are required for SDN network production.

The control layer is the essential layer in the 5G network. Authors of [14] have proposed an architecture related to security using machine learning and AI mechanisms for control planes. They also provide authentication techniques to optimise the control plane. Using the multi-tier base security mechanism, authors [15], [16] have proposed security vulnerabilities of 5G SDN/SDNM. They also provide some cryptographic and authentication techniques to secure SDN.

2.2 (NFV) Security issues in 5G

The authors of [17] proposed a mechanism for NFV application to prevent manipulating and stealing physical resources by using Intel SGX. NFV has security challenges such as network monitoring, E2E security, and service provisioning. They also proposed an architecture to provide NFSV security for the application layer.

2.3 Physical layer security and privacy challenges

The 5G communication network's major privacy concerns could be data, privacy and users' locations. Details of subscribers are the most crucial part of phone application installation. They correctly mention how to store user data and use our data to secure users' information. Authors of [18], [19], [10] have proposed the threats and challenges of user location privacy and physical layer attacks. Timing attacks and semantic information attacks are the main reasons to leak user location privacy. They also proposed that access point selection mechanisms are used at the physical level to spread user privacy.

Table 2 Security challenges in 5G technology [5]

Threats	Technology			Privacy
	SDN	NFV	Cloud	
MitM attack	✓	X	✓	✓
Hijacking attack	✓	✓	X	X
DoS attack	✓	✓	✓	X
TCP attack	✓	X	X	X
Timing attack	X	X	✓	✓

By employing phoney base stations and IDs to identify the Identity of International Mobile Subscribers (IMSI) [19], data privacy becomes more concerning in the 5G network. There is no direct space to store data in the cloud. However, every country has a mechanism to store data in the cloud. So, data privacy is a challenge if there is not direct space to store data.

Table 2. summarises the security issues of 5G core technologies such as IoT and cloud. There are many attacks on different layers of 5G that can affect the privacy and security of users. The SDN layer is the central control point for network devices. Therefore, TCP, hijacking and DoS attacks are most common on the control infrastructure layer. 5G is more concerned with location and data privacy [20]. Using timing attack techniques on the physical layer, attackers can identify a subscriber's identity and trace their location. IoT is the most vulnerable device in the 5G network. The massive number of devices also increases the security threats landscape in 5G network communication [1].

3. Technical details and results

The 5G network has a more significant number of threat challenges. This section will discuss the threats and appropriate solutions for 5G core technologies such as massive IoT devices. I will also discuss the physical security threats and answers for 5G and see simulation results for threat solutions. I will go over the best practices and mechanisms for securing a 5G network [13]. I am explaining the best security solutions for 5G security of core technologies according to my research.

3.1 5G IoT threats and solutions

The IoT is an attractive and significant feature of technology. Several applications are providing IoT applications such as Fog-IoT, Environmental-IoT. Millions of devices are more intelligent devices and are part of the IoT. 5G-based IoT is essential to connect millions of devices through 5G. However, the security challenges are also more intelligent than technology. Security of IoT devices in 5G is one of the most critical challenges [21], [22].

Table 3 5G enabled IoT threats and solutions.

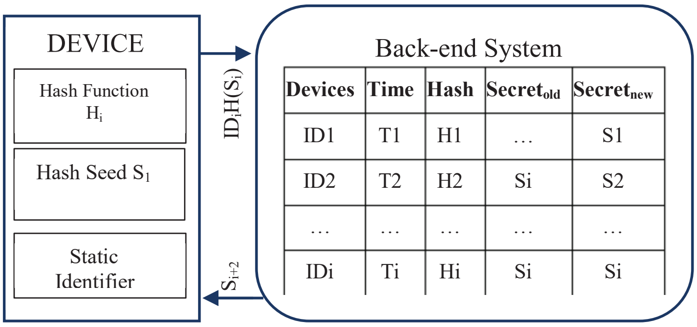
Application	Attacks	Countermeasures
IoT security component	i) Code injection ii) Authentication iii) Authorisation	Secure Authorisation
5G based IoT	i) Eavesdropping	i) PLE ii) PLS
IoT using SDN	i) Authentication ii) MitM adversary	i) Secret keys ii) Encryption
Fog based IoT	i) Interception of info. ii) MitM	i) AES ii) RSA iii) ECC

Table 3. summarises the IoT threats and provides some appropriate solutions against these threats. IoT is the most vulnerable device in 5G. To avoid attacks such as MITM, IP spoofing, authentication, we need security mechanisms to secure 5G-based IoT devices.

3.2 Security solutions for SDN-based 5G network

3.2.1 Basic idea: in this section, I propose an authentication mechanism to secure SDN devices on the 5G network. SDN is a central controller used to control network devices using software through the main point. The authentication mechanism is one of the best solutions to secure SDN devices. There is a secret key stored in all SDN devices and stored in backend systems in this feature. A private key is generated by using encryption techniques that are used by backend systems.

3.2.2 Security mechanism: in this subsection, I will adequately explain the security mechanism I propose to secure SDN devices on the 5G network. The secret key is generated by the backend system and stored in both SDN devices and backend systems. Si denotes the private key, and the hash value is represented by Hi, computed by the backend system using the device's secret key. Each time, the secret key will be changed so the attacker cannot pass the authentication process. Each machine has its ID, secret key, hash value. Time interval is essential in this authentication mechanism because the secret key will be changed whenever SDN devices want to communicate with backend systems [23].



Devices	Time	Hash	$Secret_{old}$	$Secret_{new}$
ID1	T1	H1	…	S1
ID2	T2	H2	Si	S2
…	…	…	…	…
IDi	Ti	Hi	Si	Si

Fig. 3 SDN security authentication architecture

Fig 3. Summarises the correct detail of authentication at both levels. There are two levels. One is data, and the other is control level. The data level contains the SDN switch devices, and the control level is a control infrastructure.

4. Future directions

There are different 5G standards such as IEEE, NFV and 5G PPP that are working to evaluate the threat landscape of the 5G network and provide an appropriate solution. Core security features such as confidentiality, availability, and integrity will be essential features of 5G in the future. 5G standards are operational and provide security mechanisms, M2M security and 5G layer security.

4.1 Physical layer security

5G standards are working on physical layer security. Physical layer security is one of the most critical features to secure end devices. IoT's massive number of devices also increases the threat landscape of the 5G network at a physical level. Physical level security (PLS) includes encryption techniques and mechanisms to secure communication using a 5G network. Moreover, the best cryptographic techniques and jammers are needed to secure D2D communications [24]. A physical layer, AI techniques and machine learning approaches are most important to provide security.

4.2 Key processing and communication

Key management is an essential feature to secure communication between several devices. Using cryptographic techniques, we can ensure the security of IoT device's communication on a 5G network. Man-in-the-middle attacks and spoofing are the most common attacks on wireless communication networks. 5G will support a large amount of traffic. Therefore, communication security and private key management is a significant task to secure the data of users. Cryptography is the best technique to connect keys and share data through wireless communication channels. Quantum and other cryptographic methods ensure the security of devices.

4.3 5G network slicing security

The leading technology in the 5G network is the software network. Network slicing issues are significant to secure communication. Various researchers are working on mechanisms and solutions to ensure the notarisation network concept. Message authentication, firewall implementation, is related to the network slicing of the core layer and the security of network slicing and implementing a new mechanism to secure the network layer [25], [6].

4.4 5G Privacy

IoT devices, industrial devices, vehicles, and smart devices will connect to 5G to communicate and share critical data. Many researchers are working on how to secure users' data on the 5G network. There are a lot of challenges and threats at the physical level. Data will be processed, stored, and analysed by devices, so data security is critical to secure communication. 5G is a new technology, and several papers focus on the privacy of 5G. Operators that are used to process data are crucial [26].

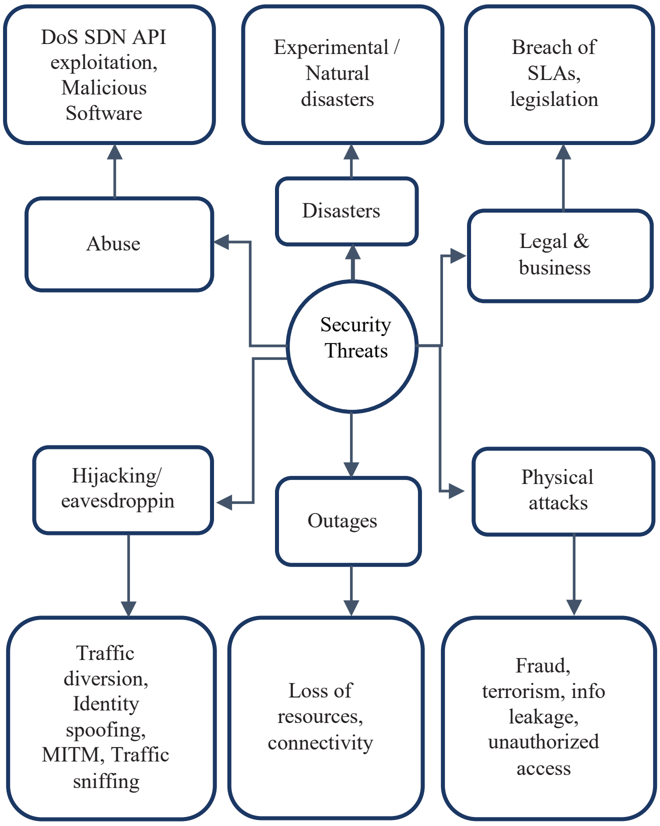

DoS SDN API exploitation, Malicious Software
Experimental / Natural disasters
Breach of SLAs, legislation
Abuse
Disasters
Legal & business
Security Threats
Hijacking/ eavesdroppin
Outages
Physical attacks
Traffic diversion, Identity spoofing, MITM, Traffic sniffing
Loss of resources, connectivity
Fraud, terrorism, info leakage, unauthorized access

Fig. 4 5G security threats taxonomy

5. Existing threats to 5G

5.1 DoS (denial-of-services)

DoS attacks can occur at any layer of the SDN network. The purpose of these attacks is to consume the network's bandwidth and pass multiple requests at a time. DoS can affect the data plane and destroy the space of data that is processed. Different anti-DoS techniques are used in the 5G network to secure the data plane.

5.2 Channel attacks

This attack is related to elements of the data plane network. The attacker focuses on connection establishment and performs these attacks on the data plane channel network. Try to exploit the pattern of the network.

5.3 Flooding

Flooding attacks can occur on both the data plane channel and the control plane channel. This attack aims to flood the system resources with malicious messages and use the control channel plane. Defense against this attack is related to network function virtualisation.

5.4 Sniffing

A sniffing attack can occur between the data plane and the control plane to access configuration data and application data such as credentials. This is an MITM attack in which attackers sniff the traffic between data and control planes and get important information. By using cryptographic and encryption techniques, we can stop these attacks. After applying encryption techniques, data is not in plain text, and it's impossible to understand [27].

5.5 Authentication attack

Authentication attacks can occur at the SDN infrastructure level. Attacks spoof the identity of the SDN controller and try to authenticate by using their individuality and sniffing the network traffic. Using authentication and authorisation techniques, we can avoid this type of attack. Their ID uniquely identifies users, and they have their value to communicate and authentication. However, the attacker cannot access your private key, instantly changing after each time interval [7], [28].

Table 4 5G threats and solutions

Attacks	Effects	Layers	Solutions
i) Configuration errors ii) Data manipulation	i) Integrity ii) Availability error iii) Destruction	Application Control Data	Encryption Techniques PLS
i) Controller attack ii) XSS iii) Overflow	i) Integrity ii) Availability error iii) Destruction	Control Data	Authentication Authorisation
i) DoS attack ii) Flooding	i) Availability error	Application Control Data	Authentication PLS IP blocking

6. Open issues and discussions in 5G

6.1 Coverage issues

5G provides us with higher bandwidth, low latency rate and tremendous speed to communicate, but one of the most significant drawbacks of 5G is less coverage. As we know, the higher rate of frequency spectrum discovers the smaller areas. The 5G frequency spectrum is very high to increase the speed and performance of the network, but there are coverage issues in some areas. We need many base stations in a city, which is very costly.

6.2 D2D communication issues

D2D communication is one of the core technologies in the 5G network. There are many security challenges in D2D communication in 4G telecommunication networks, eavesdropping and sniffing. As IoT emerges in 5G technology with ultra-reliable latency and higher bandwidth, more critical issues are discussed in 5G network D2D communication. In the future, we need the best cryptographic techniques and standards to ensure D2D communication security[28][24].

6.3 5G Frequency Spectrum

The 5G frequency spectrum is much higher than the 3G and 4G networks. A higher frequency can increase the performance of 5G, but there are a lot of issues with higher frequency. A higher frequency cannot cover many areas, so we need many stations every 500m. There are numerous issues with the 5G frequency spectrum in remote areas. According to the World Health Organisation, a much higher frequency is ionising and can damage the human eye [15].

7. Conclusion

The number of threats and challenges in the 5G network increases as the 5G threat landscape evolves. This report highlighted the threats and challenges of the 5G network. I have explored the full investigation of threat analysis on core 5G technologies. I have investigated an IoT-based 5G solution and threats at different layers and applications. I also explained the security mechanism for the SDN-based 5G network to secure SDN devices on the 5G network. I also describe the security and encryption mechanisms to ensure communication and share keys through a secure channel. For IoT devices, it is an important task to share access and provide proper management to communicate with devices through wireless communication networks. Quantum technique of encryption and machine learning approaches of intrusion detection is essential to communicate with devices securely. Finally, I have included a list of future threats and challenges in 5G and explain the future direction of 5G research domains.

8. References

[1] Agarwal, M., Roy, A., and Saxena, N., "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE 6 Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.

[2] Zhang, P., Yang, X., Chen, J., et al., "A Survey of Testing for 5G: Solutions, Opportunities, and Challenges," China Communications, vol. 16, no. 1, pp. 69–85, 2019.

[3] Lineage, M., Ahmad, I., Abro, A. B., et al., A Comprehensive Guide to 5G Security. Wiley Publishing, 2018.

[4] Ahmad, I., Kumar, T., Liyanage, M., et al., "5G security: Analysis of threats and solutions," 2017 IEEE Conf. Stand. Commun. Networking, CSCN 2017, no. September, pp. 193–199, 2017, DOI: 10.1109/CSCN.2017.8088621.

[5] Okwuibe, J., Ylianttila, M., and Gurtov, A., et al., "5G security: Analysis of threats and solutions," 2017 IEEE Conf. Stand. Commun. Networking, CSCN 2017, pp. 193–199, 2017, DOI: 10.1109/CSCN.2017.8088621.

[6] Maier, G., and Reisslein, M., “Transport SDN at the Dawn of the 5G Era,” 2019.

[7] Islam, M. M., and Al-Shaer, E., "Active deception framework: An extensible development environment for

adaptive cyber deception," Proc. - 2020 IEEE Secure. Dev. SecDev 2020, pp. 41–48, 2020, DOI: 10.1109/SecDev45635.2020.00023.

[8] Bonfim, M. S., Dias, K. L., and Fernandes, S. F., "Integrated NFV/SDN Architectures: A Systematic Literature Review," ACM Computing Surveys (CSUR), vol. 51, no. 6, p. 114, 2019.

[9] Bouraga, S., "A taxonomy of blockchain consensus protocols: A survey and classification framework," Expert Syst. Appl., vol. 168, p. 114384, 2021, DOI: 10.1016/j.eswa.2020.114384.

[10] Li, S., Da Xu, L., and Zhao, S., "5G Internet of Things: A Survey," Journal of Industrial Information Integration, 2018.

[11] Lien, S.-Y., Tseng, C.-C., Moerman, I., et al., Recent Advances in 5G Technologies: N ew Radio Access and Networking," Wireless Communications and Mobile Computing, vol. 2019.

[12] Bendale, S. P., and Rajesh Prasad, J., "Security Threats and Challenges in Future Mobile Wireless Networks," Proc. - 2018 IEEE Glob. Conf. Wirel. Comput. Networking, GCWCN 2018, pp. 146–150, 2019, DOI: 10.1109/GCWCN.2018.8668635.

[13] Abdou, A. R., van Oorschot, P. C., and Wan, T., "Comparative Analysis of Control Plane Security of SDN and Conventional Networks," IEEE Communications Surveys & Tutorials, 2018.

[14] Wu, J., Dong, M., Ota, K., et al., "Big Data Analysis Based Secure Cluster Management for Optimized Control Plane in Software Defined Networks," IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 27–38, 2018.

[15] "Everything You Need to Know About 5G - IEEE Spectrum."https://spectrum.ieee.org/video/telecom/wireless/everything-you-need-to-know-about-5g (accessed Dec. 01, 2020).

[16] Kantola, R., Perez, O. L., Itzazelaia, M. U., et al., "Enhancing Security of Software Defined Mobile Networks," IEEE Access, vol. 5, pp. 9422–9438, 2017.

[17] Battula, L. R., "Network Security Function Virtualization (NSFV) Towards Cloud Computing With NFV Over Openflow Infrastructure: Challenges and Novel Approaches," in Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014, pp. 1622– 1628.

[18] Shaik, A., and Borgaonkar, R., "New Vulnerabilities in 5G Networks."

[19] Kumar, R., and Liyanage, M., and Braeken, A., et al. "From Gadget to Gadget-Free Hyperconnected World: Conceptual Analysis of User Privacy Challenges," in 2017 European Conference on Networks and Communications (EuCNC), June 2017, pp. 1–6.

[20] Naikm, N., and Jenkins, P., "Discovering hackers by stealth: predicting fingerprinting attacks on honeypot systems," 4th IEEE Int. Symp. Syst. Eng. ISSE 2018 - Proc., 2018, DOI: 10.1109/SysEng.2018.8544408.

[21] Yu, R., Bai, Z., Yang, L., et al., "A Location Cloaking Algorithm Based on Combinatorial Optimization for Location-Based Services in 5G Networks," IEEE Access, vol. 4, pp. 6515–6527,2016.

[22] Paper, W., "Date: August 2015 Dawn of the 5G Era Immersive Multimedia Experience," no. August, pp. 1–17, 2015.

[23] Liyanage, M., Ylianttila, M., and Gurtov, A., "Analysis of deployment challenges of Host Identity Protocol," EuCNC 2017 - Eur. Conf. Networks Commun., 2017, DOI: 10.1109/EuCNC.2017.7980675.

[24] Hayat, O., Ngah, R., Kaleem, Z., et al., Rodrigues, "A survey on security and privacy challenges in device discovery for next-generation systems," IEEE Access, vol. 8, pp. 84584–84603, 2020, DOI: 10.1109/ACCESS.2020.2991459.

[25] Lam, J., Abbas, R., "Machine learning-based anomaly detection for 5g networks", in arXiv preprint arXiv: 2003.03474, 2020.

[26] Darabseh, A.; Alayyoub, M.; Jararweh, Y. et al., Security: A Software-Defined Security experimental framework. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015.

[27] Liyanage, M., Ahmad, I., Abro, B. A., et al., "A comprehensive guide to 5g security, 2020.

[28] Bisson, P., Waryet, J., "5G PPP phase1 security landscape", in 5G PPP Security Group White Paper,2017