5G SECURITY CHALLENGES AND RECOMMENDATIONS

BY

MD. SHORIFUZZAMAN
ID: 201-25-873

This report presented in partial fulfillment of the requirements for the degree of Master of Science in Computer Science and Engineering.

Supervised By

Md. Zahid Hasan
Associate Professor
Department of CSE
Daffodil International University

Co-Supervised By

Dr. Md. Ismail Jabiullah
Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

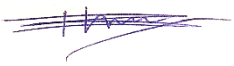
DHAKA, BANGLADESH

JANUARY 2022

APPROVAL

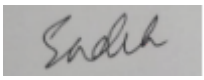
This Project/internship titled **"5G SECURITY CHALLENGES AND RECOMMENDATIONS"**, submitted by Md. Shorifuzzaman, ID No: 201-25-873 to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 22-Jan-2022.

BOARD OF EXAMINERS



Chairman

Dr. Touhid Bhuiyan
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Internal Examiner

Md. Sadekur Rahman (SR)
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Moushumi Zaman Bonny
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Shamim H Ripon
Professor
Department of Computer Science and Engineering
East West University

DECLARATION

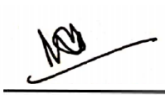
I hereby declare that this thesis has been done by me under the supervision of **Md. Zahid Hasan, Associate Professor, Department of CSE,** Daffodil International University. I am also declared that neither this thesis nor any part of this thesis has been submitted elsewhere for an award of any degree or diploma.

Supervised by:

Md. Zahid Hasan

Associate Professor
Department of CSE
Daffodil International University

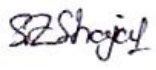
Co-Supervised by:



Dr. Md. Ismail Jabiullah

Professor
Department of CSE
Daffodil International University

Submitted by:



Md. Shorifuzzaman

Student
ID: 201-25-873
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I would like to express my special thanks and gratefulness to Almighty Allah for His divine blessing makes me possible to complete the final year thesis successfully.

I have taken efforts in this thesis. However, it would not have been possible without the kind support and help of many individuals. I would like to extend my sincere thanks to all of them.

I am highly indebted to Daffodil International University for their guidance and constant supervision as well as for providing necessary information regarding the thesis & also for their support in completing the thesis.

I would like to express my gratitude towards my supervisor **Md. Zahid Hasan, Associate Professor, Daffodil International University** for her kind cooperation and encouragement which helped me in the completion of this thesis**.**

ABSTRACT

5G will make it possible for everyone to have access to high-speed internet everywhere, and it will also make it possible for a huge number of devices (e.g. IoT) to be connected in an ultra-reliable and cheap way. Cloud computing, Software Defined Networking (SDN) and Network Function Virtualization (NFV) are the primary technological enablers maturing for use in 5G. However, these technologies face significant security challenges in addition to growing concerns about user privacy. In this work, I discuss the security and privacy issues surrounding 5G technologies. I also discuss security solutions and future approaches for secure 5G systems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

FIGURES **PAGE NO**

LIST OF ABBREVIATIONS

5G	5th Generation
IMT	International Mobile Telecommunications
QoS	Quality of service
D2D	Device-to-Device
MIMO	Multiple-input and multiple-output
V2I	Vehicle-to-Infrastructure
HTTP	Hypertext Transfer Protocol
API	Application programming interface
IPsec	Internet Protocol Security
VMNOs	Virtual Mobile Network Operators
HIP	Host Identity Protocol
CapEx	Capital expenditure
OpEx	Operating expenditure
SDN	Software-defined networking
NFV	Network functions virtualization
IDS	Intrusion Detection Systems
IoT	Internet of Things
HetNet	Heterogenous networks
VM	Virtual machine
mmWave	Millimeter wave
LTE	Long Term Evolution
WAN	Wide area network
SASE	Secure Access Service Edge
DoS	Denial of service
3GPP	3rd Generation Partnership Project
CSPs	Communication Service Providers
IP	Internet protocols
LBS	Location-Based Services
TLS	Transport Layer Security
NFs	Network File System
NGMN	Next Generation Mobile Networks

NAS	Non-Access Stratum
ONF	Open Networking Foundation
MCC	Mobile cloud computer
RATs	Radio access technologies
C-RAN	Cloud Radio Access Network
IMSI	International Mobile Subscriber Identity
SDH	Synchronous Digital Hierarchy

CHAPTER 1
INTRODUCTION

1.1 Introduction

5G, or fifth-generation wireless technologies, are the next generation of mobile telecommunications technology, after 4G. New service capabilities and an evolution of 4G networks make the 5G wireless system better than previous system. I will present and discuss 5G networks in this chapter, covering motives and goals, thesis outline, and Research objectives. Base station density deployment, capacity expansion, significant QoS improvement, as well as ultra-low latency are all goals of the 5G. 5G will need the development of new types of networks, services, storage, and processing infrastructure. Data, services and applications can be managed effectively using cloud computing without a dedicated infrastructure. Thus, the mobile cloud using the same concept will integrate technically different systems into one domain, allowing for greater flexibility and usability. The softwarization of network functions will make network systems and services easier to transplant and have higher flexibility. Innovative networks and simplified network management are other benefits of SDN. As a result, they are regarded as crucial for future networks. However, future network security and user privacy risks exist.

Wireless communication systems have security flaws from the beginning. Mobile phones and wireless channels in the first-generation wireless network(1G) became targets for illegal cloning and disguise. Spam has proliferated not just via large-scale assaults, but also through the dissemination of misleading information or unwelcome commercial content across second-generation wireless networks (2G). Third-generation wireless networks (3G) are vulnerable to flaws and vulnerabilities that may be transferred to the internet through IP-based communications. Because of the increasing demand for IP-based communications, fourth-generation wireless networks (also known as 4G) have been introduced, ushering in a slew of smart gadgets, multimedia traffic, and innovative services. As a consequence of this growth, the threat scenario has become more complicated and dynamic. Fifth-generation wireless networks(5G) will introduce new security challenges and raise concerns about user privacy.

As a result, it's important to note that not only mobile wireless networks, but also technologies that can be used for 5G can be dangerous. In this work, we underline the security risks of 5G and urgently require safety solutions. I also discuss potential solutions to the security challenges in this work.

1.2 Motivation

The goal of 5G research and development is higher capacity than current 4G, device-to-device (D2D) communication, large numbers of mobile broadband users, as well as a large number of machine-type interactions. Also, 5G planning intends to lower latency and power consumption in order to facilitate the implementation of IoT technology.

There are also some specific motives in this work:

- Finding 5G Security and Privacy Challenges.
- Recommendation with potential security solutions for 5G.

1.3 Objectives

There is no single survey that addresses 5G security across all key 5G technologies. In future 5G networks, this effort aims to broaden the scope of possible network security interdependencies.

This work's objectives are noted below:

- The overall 5G Security Threats and current solutions are studied.
- Highlight the security issues that arise from the core technologies of 5G.
- Define the critical security areas for 5G.
- Comprehensive overview of 5G security challenges and solutions.
- Future research directions.

1.4 Thesis Outline

This thesis is arranged as follows:

Chapter 1 **:** Introduction

Chapter 2 **:** Literature Review

Chapter 3 **:** Key security challenges in 5G

Chapter 4 **:** Discussion & Recommendation

Chapter 5 **:** Conclusions & Future Scope

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

The fifth generation of cellular networks is known as 5G. It is the 4G LTE's replacement (Long Term Evolution). 5G includes new technology such as massive MIMO, beamforming, mmWaves, and compact base stations, as well as multi-gigabit transmission speeds, larger bandwidth, and lower latency. 5G is a prominent topic in today's tech world. 5G, which is still in its development phase, can change the way people incorporate technology in their lives and provide a platform to launch several new technologies that could not have been launched with 4G LTE or its predecessors. 5G is expected to connect 1 million devices per 38 square miles where 4G could connect only 2000 devices per 38 square miles. Connecting more devices and transferring more data will be possible with 5G. Given the competitive age we live in, countries and organizations across the world are competing against each other to be the first one to deploy 5G nationwide and are expecting several new technologies to be launched with the deployment of the best cellular network yet.

2.2 Related Works

The authors of [36] offer broad strategies for improving 5G security. In [36], the author outlined the security needs for 5G by evaluating the LTE security criteria. The paper [7] discusses various security mitigation measures as well as efforts to standardize 4G and previous generations. You may find an excellent article on security of 4G and 5G technology in [4]. WiMAX, LTE, Bluetooth, and other types of wireless LAN connectivity are also explored in the research [36]. The paper also discusses the inherent security limitations of each technology as well as prospective trends for enhancing its security. The article [10] focuses on 4G and 5G network authentication and privacy protection technologies. In [4], security threats and assaults against mobile networks were discussed. This article [7] discusses the security vulnerabilities associated with mobile access, as well as core networks. Some research problems are presented in [52] in an effort to give a thorough knowledge of mobile network security. The articles referenced in the linked work are all on certain topics. In [65], usability, secrecy, key management, and privacy identity verification were investigated in respect to existing

or conventional mobile networks. For example, [4][9] and [1][5] respectively address physical layer & air interface security, [7] offers access & core network security, & [8] suggests LTE security. The privacy issues of future networks are discussed in [36]. The 4G network's architecture is the main roadblock to overcoming this challenge. All of these new technologies offer significant power and total cost efficiency improvements, yet they all have security flaws [36][7]. However, new concepts and the integration of large-scale IoT will make 5G's security challenges more diverse than ever. The table 2.2 below shows how security has changed from 1G to 4G. Using data from [10], it has been altered.

Table 2.2: A SYNOPSIS OF SECURITY DEVELOPMENT FROM 1G TO 4G

Network	Security Challenges	Advantages	Disadvantages
1G	Eavesdropping, call interception, and no privacy mechanisms.	Simpler network components	Background interference, limited capacity, insecure, bad battery life, huge phone size
2G	Fake base station, one way authentication, radio link security & spamming.	MMS, SIM introduced and internet access.	Poor coverage and sluggish data transfer rates
3G	IP traffic security vulnerabilities, roaming security, encryption keys security.	Strict security, global roaming	High energy usage, limited network coverage, and high spectrum costs
4G	DoS attacks and long-term key eavesdropping.	MIMO tech, worldwide technology, rapidity and rapid handoffs	Complicated hardware is required, which is difficult to implement.

2.3 Scope of the problem

Increased attack surface:

5G allows for larger and more dangerous attacks because of the increased number of connected devices. Vulnerabilities in the existing internet infrastructure, both present and future, are exacerbated. 5G may increase the risk of sophisticated botnets, privacy violations, and data extraction.

More IoT, more problems:

Inherently insecure, IoT devices are frequently not designed with security in mind. Insecure IoT devices on an organization's network represent a new vulnerability for an attacker to exploit.

Decreased network visibility:

With 5G, our networks will continue to grow and become more accessible to mobile users and devices. This means more network traffic. Companies may not be able to identify abnormalities or attacks without a robust WAN security solution like Secure Access Service Edge (SASE).

Increased supply chain and software vulnerabilities:

Currently, and for the foreseeable future, the number of 5G supply chains is very limited. 5G is also more dependent on software, which raises the risk of the network infrastructure being exploited.

2.4 Most Significant Security Challenges in 5G

A list of most significant security challenges of 5G is given below:

- **Security Challenges in Cloud**

With cloud-based cyber-physical systems, it is possible to virtualize the components of a network.

- HTTP and XML DoS (HXDoS) attacks are common in this environment.
- Virtualized systems can benefit from the use of firewall proxies to mitigate networked denial-of-service (DoS).

Cloud intrusion: Building IDSs that work with other cloud control mechanisms helps mitigate cloud intrusion.

- **Security Challenges in SDN**

By separating control and forwarding planes, software-defined networking (SDN) allows for greater control over networks.

- Attackers can target the control platform because it has centralized network control.

Network control and management will be easier, and new network features will be added faster, because this will make it easier to control the network.

- Security risks can arise if critical APIs are made available to unapproved software. Since OpenFlow's inception, new security threats have emerged.

- **Security Challenges in NFV**

With virtualization, the service model for a system can be separated from its physical implementation, allowing logical copies of the hardware to be used for various purposes. Virtualization can significantly improve user, service, and network security. Slices can be used to separate traffic based on security priorities for different services or networks.

- **Security Challenges in Communication Channels**

The introduction of 5G networks replaced prior-generation mobile networks' use of GTP and IPsec tunnels for dedicated communication channels. Attacking mobile network communication interfaces like X2, S1, S6, and S7 requires a high degree of expertise.

  - These interfaces will be absent from SDN-based 5G networks, which instead use standard SDN protocols. Because these interfaces are open, the number of potential attackers grows.

- **Security Challenges in Network slicing**

Network slicing is an important technology in the next-generation networks that are made possible by software-defined networks and network functions virtualization. Networks that allow multiple tenants to share resources must also meet the security requirements for the situations in which they are used.

- **Privacy Challenges in 5G**

Customers' personal information may be accessed by participants in the process, with or without their consent. It is expected that users and other stakeholders will face greater risks to their privacy as a result of the introduction of new architecture, technology, and services on the 5G network. 5G ecosystems will also be exposed to more serious privacy issues as SDN, NFV, cloud and edge computing are integrated.

- **Security Challenges in massive MIMO**

It is commonly accepted that Massive MIMO is a disruptive and forward-looking 5G technology. Massive MIMO uses antenna elements to serve a huge number of users in

the same frequency band. Multiple antenna elements can be used to improve data rate, reliability, coverage, and energy efficiency.

- **Carryover of 3G/4G security loopholes**

Until the transition from 4G to 5G is complete, the vulnerabilities in 4G networks will persist in 5G networks. Previous-generation networks are particularly vulnerable to SMS and call interceptions, illegal geotracking and denial of service (DoS) attacks.

- **Privacy by design challenge**

The infrastructure operators who realize the total service are responsible for ensuring data management and ownership policies correspond with the need for private communication and ensuring responsibility within the communication substrate.

- **Risks and costs when provisioning 5G equipment**

Since 2019, several countries — including Germany, India, Britain, Australia, the U.S. and various countries in Eastern Europe and Scandinavia — have restricted the import or usage of 5G technology from untrusted suppliers.

- **Multi-tenancy challenge**

Ensure seamless interoperability across wireless and backhaul domains, even if the infrastructure isn't IP-based, by delivering service solutions that span multiple infrastructure owners.

- **Simplicity challenge**

Provide the greatest network services to 5G users in the most frictionless manner possible without requiring lengthy customer visits (e.g. for inter RAT switching).

- **Insecure by association**

Security issues in related technologies have an impact on 5G security.

- **Network vulnerabilities**

Previous-generation networks relied primarily on SS7 and Diameter protocols. IP protocols such as HTTP and TLS are used by 5G networks, which is a common internet protocol (IP). These open-web protocols make it easier for both operators and hackers to get in.

- **Decentralized security**

A swarm of software-defined digitized routers has replaced conventional hardware-based security checkpoints in 5G networks, making them difficult to examine and monitor.

- **Reduced isolation**

Physical appliances are replaced by virtualized network operations in 5G networks. NFs reduce network component isolation as NVFs communicate with each other directly and may share resources. Edge appliances in SD-WANs broaden the attack surface and are often overlooked during patching routines.

- **Privacy and personal risk**

The risk to 5G networks comes from a multitude of devices, including seemingly innocuous home network appliances like smart thermometers and intelligent thermometers that may provide security chinks in network armor.

- **User and signaling confidentiality holes**

Enhanced encryption of user and signaling data between a user device and a base station, itself an increasingly sensitive entity in 5G architecture, is mandatory to ensure data integrity but it is an optional feature to protect user confidentiality in the 5G specification. This confidentiality security chink could allow attackers to intercept status and authorization data and track a user's location.

- **Security challenges for Transition**

5G is not backwards compatible with previous-generation networks; transitioning to 5G requires the replacement or addition of physical devices and software. There are two main security concerns associated with the transitioning process: the carryover of existing 3G/4G security problems; and the risks associated with equipment from untrusted suppliers.

CHAPTER 3
KEY SECURITY CHALLENGES IN 5G

3.1 Introduction

5G will require additional security measures to protect both critical infrastructure and society. As for electrical and electronic equipment, a breach in online power systems could be very dangerous. A similar concern is that, while we understand the importance of data in making decisions, what happens if the data itself is corrupted during transmission over 5G networks? To ensure the safety of 5G networks, it's essential to look into and identify the most pressing security issues and possible solutions. In the literature, there are a lot of problems with 5G that people talk about a lot. These are the main problems:

- **Flash network traffic:** Many new devices and many new items (the Internet of Things) are being added to the network every day.
- **Radio interface security:** Unsecured channels deliver radio encryption keys.
- **User plane security:** The user data plane's cryptographic integrity is unprotected.
- **Mandatory network security:** Constrictions on security provided by service providers that lead to additional security measures being offered as an option.
- **Roaming security:** When a user switches networks, their security settings do not update, which could lead to security vulnerabilities while roaming.
- **Denial of service attacks:** DoS attacks can happen because network control elements can be seen and control channels are not encrypted, which makes the infrastructure vulnerable.
- **Signaling storms:** Distributed control systems that require coordination, such as the 3GPP protocols' Non-Access Stratum layer.
- **End-user device DoS attacks:** Operating systems, programs, and configuration data have no security measures.

The 3GPP Working Group (SA) is actively engaged in establishing WG3 security and privacy criteria, as well as outlining the 5G security architecture and protocols. The Open Networking Foundation publishes technical standards for SDN & NFV with the goal of increasing their adoption and assuring their long-term viability. Beyond Radio

Efficiency's 5G design ideas include the following: establishing a single composable core and simplifying operation and administration through the use of new computer and networking technologies. As a result, we concentrated on securing the technologies that would match the NGMN design criteria, including Mobile Cloud, SDN, and NFV, as well as the communication connections utilized by or amongst these technologies. I also talked about possible privacy issues because people are becoming more concerned about their privacy. Figure 3.2 and Table 3.2 show the security challenges. Table 3.2 summarizes the most vulnerable technologies, network components, and threats. These security concerns are summarized below.

3.2 Security Challenges in Mobile Clouds

Due to the centralized nature of cloud computing resources, malicious traffic generated by one user can readily propagate to other users. Because each location in a multi-tenant cloud network has its own control system, when they interact, they have the potential to generate network setup issues. The fundamentals of cloud computing will be applied to the 5G eco-system in a mobile cloud computing system. This creates a slew of security concerns, the majority of which stem from 5G's architectural and infrastructure changes. Because the MCC is open and mobile terminals are so flexible, there are places where attackers could try to get into the mobile cloud and get their hands on private information.

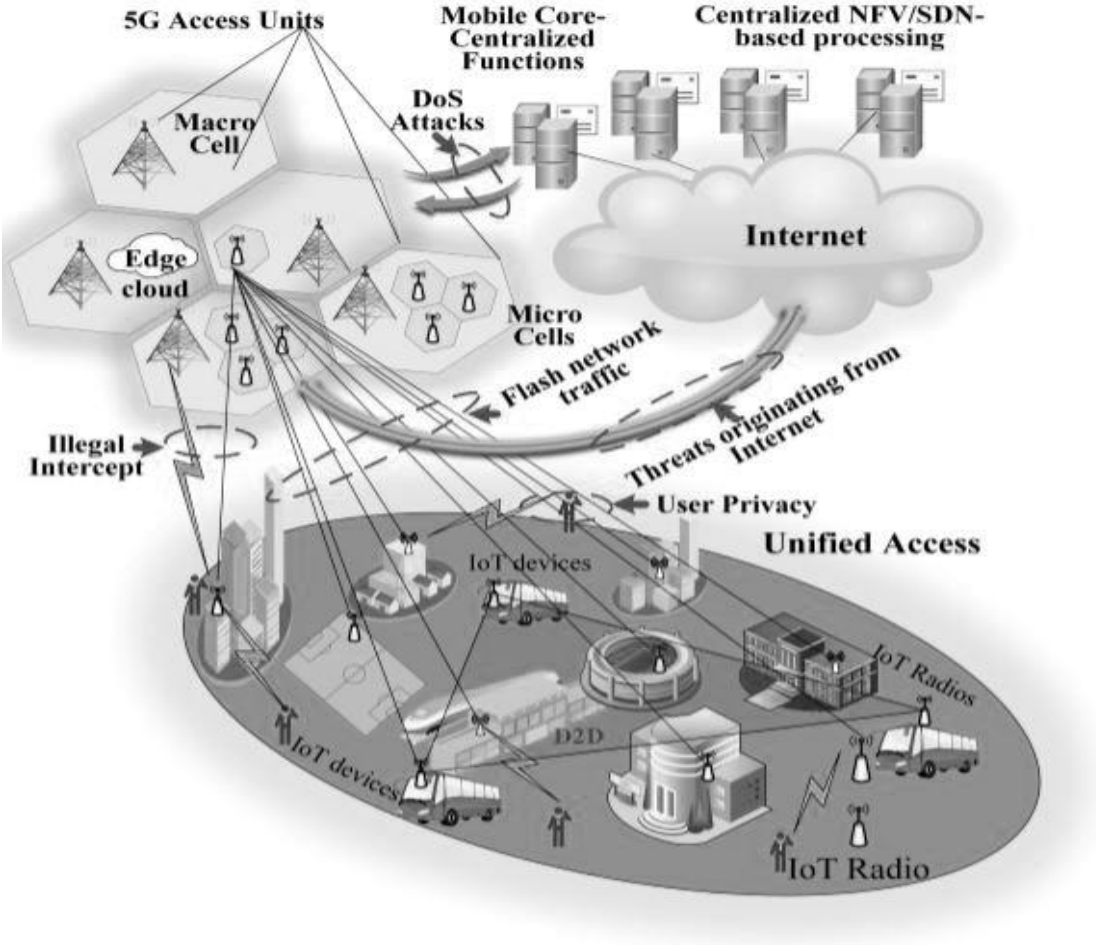


Figure 3.2: 5G NETWORK AND THE THREAT LANDSCAPE [6]

MCC threats are divided into three cloud areas in this work: front, back, and rear security risks. At the heart of MCC design is a customer platform that has a portable space that contains the resources and communication infrastructure necessary to access the cloud capabilities. In application-based attacks, adversaries utilize malware, spyware, and other harmful software to interrupt user apps or acquire sensitive user information. Servers and storage systems for the back-end platform, as well as virtual machines, a hypervisor and protocol software, make up this part of the cloud service platform. There are a lot of security threats to mobile cloud servers in this discussion group. These threats include data duplication and HTTP/XML DoS (HX-DoS) attacks.

Table 3.2: SECURITY CHALLENGES IN 5G TECHNOLOGIES

Security Threat	Target Point/Network Element	Effect Technology				Privacy
		SDN	NFV	Channels	Cloud	
Denial-of-service attack	Control aspects that are centralized	✓	✓		✓	
Penetration attacks	Virtual resources, clouds		✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Theft of user identities	Data bases of user information				✓	✓
Storms of signaling	5G key network aspects			✓	✓	
Stealing resources	Hypervisor, shared cloud		✓		✓	
Attacks on configuration	Virtual SDN switches and routers	✓	✓			
Attacks at the TCP level	Controller-to-switch communication in SDN	✓		✓		
Attacks of saturation	Controllers and switches for the SDN	✓				
IP spoofing and reset	Channels de command			✓		
Scanning for threats	Interactions in the open air			✓		✓
Timing attacks	Location of the subscriber				✓	✓
Boundary attacks	Location of the subscriber					✓
IMSI catching attacks	Identity of the subscriber	✓		✓		✓
Man-in-the-middle attack	SDN controller communication			✓		✓

In an effort to gain access to mobile devices, cybercriminals are focusing on radio access technologies (RATs). Wi-Fi, 4G LTE, and other new radio access technologies (RATs) will be supported by 5G. This type of attack includes Wi-Fi surveillance, denial-of-service attacks, impersonation attacks, and session hijacking. Cloud Radio Access Networks are another popular issue in the investigation of security risks in the 5G mobile cloud. C-RAN can be used to boost industrial capacity in 5G mobile communication networks. In addition, the system is under constant threat from unauthorized intrusion attempts that allow attackers to examine or modify the platform's viewable area.

3.3 Security Challenges in SDN and NFV

It is possible to program a communication network using SDN since it centralizes network control systems. Crushing and hacking of networks are made easier by these two disruptive qualities. For example, DoS attacks may benefit from centralized controls, and undesirable applications can breakdown the whole network by exposing

the critical APIs. Changes in data flow regulations are made by the SDN controller, which makes it easier to identify traffic. For DoS attacks to succeed, the controller must be visible on the network, which makes it an obvious target. Because of saturation assaults, centralizing network control might turn the controller into a network bottleneck. Viruses and other malicious software can take over a network if malicious applications are given access to the SDN infrastructure.

Security problems related to network functions virtualization include confidentiality, integrity, authenticity and non-repudiation. It has been shown that existing NFV systems do not offer enough security and isolation for virtualized telecommunications services when used in mobile networks. Table 3.2 highlights some of the challenges, but the most pressing concern is that if a hypervisor is hijacked, the entire network may be disrupted.

3.4 Security Challenges in Communication Channels

In addition to drones, cloud-based reality, linked vehicles, cloud-based robotics, transportation and health will all be part of the 5G ecosystem. As a result, apps need secure communication technologies that enable authentication and data transmission. More service providers will enter the market, such as mobile network carriers and cloud service providers. For both network access and service levels, there must be a lot of integrated authentications, as well as standard checks. This is true for both the network and the service levels.

Mobile networks depended on specialized communication channels designed around GTP & IPsec tunnels prior to the introduction of 5G networks. Attacking mobile network communication interfaces like X2, S1, S6, and S7 requires a high level of skill. SDN-based 5G networks, on the other hand, will use standard SDN interfaces rather than dedicated interfaces. The number of possible attackers grows as these APIs become more exposed. The communication channels in a 5G mobile network based on SDN are classified as follows: data channels, control channels, and inter-controller communication channels. Current SDN systems encrypt these channels with TLS or SSL sessions. However, insufficient authentication mechanisms and IP layer attacks make TLS/SSL sessions highly vulnerable.

3.5 Privacy Challenges in 5G

As a user, you may be concerned about the privacy of your data, location, and even your identity. Most smartphone apps demand personal information from the user before installation. Data is seldom disclosed by application developers or organizations as to how it is kept or for what reasons it will be utilized. Subscriber location privacy is threatened by semantic information, timing and boundary breaches. The physical layer of 5G mobile networks may expose location privacy via access point selection mechanisms. Attacks that capture a subscriber's User Equipment's (UE) International Mobile Subscriber Identifier (IMSI) may be used to deduce the subscriber's identify. It is possible that the IMSI associated with the victim will be utilized to evade detection by establishing a false base station as the result of these assaults.

In addition to VMNOs, CSPs, and network infrastructure providers, 5G networks employ a wide range of professionals. Each of these actors is concerned with distinct aspects of security and privacy. An issue with 5G networks is that different groups of people have different privacy policies. All system components were under direct control of mobile operators in the past generation. Carriers would lose total control of the system if 5G relied solely on new participants like CSPs. This would result in the full loss of security and privacy for 5G service providers. Each of these actors is concerned with distinct aspects of security and privacy. Sharing infrastructure between actors, such as VMNO and competitors, compromises user and data privacy. Because of the properties of cloud data storage & network functions virtualization (NFV), 5G networks have no physical limits. There is no direct control over how much data storage space the cloud has for 5G operators, so this means that they don't have a lot of control over this. Having user data stored in the cloud in a separate nation poses a privacy risk because of the differing degrees of data protection in different countries.

CHAPTER 4
DISCUSSION AND RECOMMENDATION

4.1 Introduction

In this section, I will discuss the security measures that were put in place to address the issues mentioned in the previous section. Adding resources or technology can help overcome the challenges of flash network traffic. I think that emerging technologies like SDN and NFV may help tackle these problems at a lower cost. Operating time resources, such as bandwidth, can be allocated to specified areas of the network using SDN. Network data can be collected from network equipment using the southbound API in SDN to see whether traffic levels rise. Services from the core network cloud may be routed to satisfy user requirements using NFV. To deal with flash network traffic, visual network fragments can only be dispersed in places with a IoT of UE.

The security of radio interface keys remains an issue, necessitating the safe exchange of encrypted keys, such as the Host Identity Protocol (HIP). Similar to this, the end-to-end encryption approaches mentioned in these can be used to ensure the integrity of the user aircraft being used. Using centralized systems with worldwide visibility of user actions and network traffic behavior, extensive network-enabled security controls can be implemented. Signing storms will be difficult due to SDN's over-the-top UE connections, tiny built-in channels, and significant user traffic. C-RAN & edge-computing can help solve these issues, but they need be developed with increased signature traffic in mind, as stated by NGMN. The security solutions discussed in this section are listed in Table 4.2, which is located below.

4.2 Security Solutions for Mobile Clouds

It's a good idea to use virtualization techniques strategically, change encryption methods, and move data processing points around to keep your data safe. There are many ways that you can secure cloud services via virtualization, such as by connecting each endpoint to a separate virtual machine (VM). The visual link between each user and the other users is isolated, ensuring their safety. Similarly, the service-based limitation ensures the safe usage of cloud computing technology. The paper proposes a "secure sharing and search of real-time video data in the mobile cloud" system that

integrates cloud platforms with 5G technology to secure cloud services. Unlike existing systems, which allow anyone with a shared link to view online video broadcasts, this research only impacts approved viewers. Certain solutions, like as learning programs, are more beneficial than traditional techniques when dealing with security concerns like HX-DoS. A learning-based system, for example, collects a set amount of packet samples and compares them to various known signals in order to detect and decrease threats.

Table 4.2: SECURITY TECHNOLOGIES AND SOLUTIONS

Security Technology	**Primary Focus**	**Target Technology**				**Privacy**
		SDN	**NFV**	**Channels**	**Cloud**	
Detection of DoS and DDoS	The central control point's security	✓	✓			
Configuration verification	Flow rules are checked in SDN switches.	✓				
Access control	Control access to software-defined networking and critical network elements	✓	✓		✓	
Isolate traffic	Ensures virtual slice and VNF separation		✓			
Link security	Control channels should be secure.	✓		✓		
Identity verification	Verifying a user's identity for services like roaming and cloud storage					✓
Identity security	Assure user identity protection					✓
Location security	User location must be kept secure					✓
IMSI security	Encryption protects subscriber identity					✓
Mobile terminal security	Securing mobile terminals with anti-malware					✓
Integrity verification	Security of data and storage systems in clouds					
HX-DoS mitigation	Security cloud web service					
Service access Control	Cloud security via service-based access control					

Anti-malware can be used to protect mobile devices from malware attacks. This may help them become more malware-resistant. Anti-malware software may be installed on a mobile device or can be hosted and delivered via the cloud. Effective power procedures in the security architecture will secure MCC data and storage. These mechanisms will make sure that data and storage services are safe when they are used with public information systems and when unstable storage is released. Protecting

expandable programs on cloud computing mobile devices is one of the frameworks presented for app security, along with other ideas such as an unencrypted user authentication protocol, a private privacy device, and the cloud computing.

4.3 Security Solutions for SDN and NFV

SDN gathers intelligence from logically centralized network resources, states, & flows to swiftly identify threats. It also makes it easier for network forensics, policy changes, and new security services to be added. These systems are highly responsive and proactive in nature because of the SDN architecture's ability to monitor and respond to traffic in real time. By updating the flow table of software-programmable network switches, traditional network security rules can be applied across the network. Security solutions such as firewalls and intrusion detection systems can be used for specific traffic. Security for VNFs is addressed in [55] using a security orchestrator that adheres to the ETSI NFV design. In a communications network, the proposed design protects both virtual and physical entities. Virtual systems and hypervisors may be protected by using trusted computing, remote verifying, & integrity checks, according to a paper published in [56].

4.4 Security Solutions for Communication Channels

5G demands robust communication channel security while keeping SDN features like centralized policy administration, programmability, and global network state visibility. Today's communication systems, such as 4G-LTE [57], employ IPsec to protect communications channels. With minor modifications, IPsec tunneling can be used to protect 5G communication channels, as shown in [22] and [24]. Furthermore, several security techniques, such as authentication, integrity, and encryption, are integrated to ensure security for LTE communications. However, the main problems with current security schemes are that they use a lot of resources, have a lot of overhead, and don't work well together. As a result, these technologies aren't suitable for 5G critical infrastructure connectivity. RF fingerprinting, asymmetric schemes, & dynamically changing security settings can all be used to improve the level of security for important communication. In addition, as mentioned in [60], cryptographic protocols like HIP can secure user communication.

4.5 Security Solutions for Privacy in 5G

This means that 5G must be designed with privacy in mind from the start, and that many key protections must be built-in to protect users' data. For high-sensitive data, mobile operators should keep and process it on their own servers, whereas less-sensitive data should be processed on public cloud servers. This will allow operators to make better informed judgments regarding how and whom they share their data in the future. Furthermore, 5G service-oriented privacy would provide more viable solutions for the preservation of personal information [61].

There will need to be better ways to be accountable, keep data to a small amount, be transparent, open, and control who has access to it in the future. The standardization of 5G should thus take into consideration stringent privacy standards and legislation [29]. There are three sorts of regulatory approaches [62]. For starters, governments regulate privacy at the national level, and multi-national organizations like the UN and the EU regulate privacy globally (EU). In the second level, different industries and groups like 3GPP, ETSI and ONF work together to come up with the best practices and principles to keep your privacy safe. Third, consumer-level restrictions are in place to ensure that consumers have the privacy they desire.

Anonymity-based techniques, in which the subscriber's genuine identity is concealed and replaced by pseudonyms, are required for location privacy [63]. Before sending a message to someone who provides Location-Based Services (LBS), the message can be encrypted. This way, no one can read it. Techniques like obfuscation protect location privacy by lowering data quality [65]. Also, location cloaking algorithms can handle important location privacy assaults including timing and boundary attacks [26].

CHAPTER 5
CONCLUSIONS AND FUTURE SCOPE

5.1 Conclusion

5G will use SDN, NFV, and mobile clouds to address significant connectivity, flexibility, and cost issues. Even though these technologies have a lot of good things going for them, they can also be dangerous. As a result, I've highlighted some of the most serious security concerns that 5G could face. I also talk about security measures and how to deal with these issues. Security threats cannot be fully realized due to the limited deployment of 5G technology. Similarly, when more consumer gadgets (such as IoT) will be linked, security and privacy issues will become more obvious. In other words, the deployment of new 5G technology and services is expected to bring forth new dangers and security issues. To ensure the safety of 5G networks, it's essential to look into and identify the most pressing security issues and possible solutions. Considering these issues from the start can be reduced privacy issues and security challenges.

5.2 Future Scope

For the security and protection of a huge system, it does not work after 5G the different parts of the system configuration have just been completed. Instead, security in addition, protection features should be included in the system plan. This goal requires Security and protection between the dynamic discourse between the network and every other party who Contribute to 5G innovation. Now, many parts of 5G are still unverifiable but there is still some abnormal state. Choices about safety and protection standards can now be agreed upon partner. For example, whether you have 5G security or not, you can agree the security device will still cover the management layer despite the entry-level. The time is generally correct to determine whether to extend the end-to-end portion. Therefore, it may now be agreed whether to expand security. If you receive each of these standards, it will affect the 5G system outline and they can be considered in the early stages of planning, and Words can begin. All the issues we discuss in this article will be understood as some stage of the discourse, once started. Safety and protection prerequisites are often seen as obstacles. However, in the long run, the system configuration will ignore them anyway. The features included since

then are less successful and are usually more expensive than including it. In the long run, security is a driving factor in Management and system development. Management and systems engineering from 5G is undergoing a sensational redesign that will enhance elements and concentration if safety insurance and protection ideas are incorporated on time, the quality of 5G. 5G will be able to do things that aren't possible yet now. This could have a huge impact on the world as a whole. But it will also open up new opportunities for people who want to use this new technology. For the most critical infrastructure, it must be the most secure and safest possible. To begin, it's important to realize how vastly different the security challenges of 5G are from those of previous generations. Technologists, educators, vendors, operators and the government are working to better understand how 5G will work, what its security concerns and how it will be used around the world. 5G is supposed to solve a lot of problems by having a lot of new features, like super high-speed internet and smooth, always-on service. Wireless communication systems have security flaws from the beginning. With 4G/3G still under development, and 5G not yet begin in many places, what is the future of 5G? Unrestricted call volumes and unfathomable data broadcasting are incorporated into the most modern mobile operating system. So, in the near future, more intelligent technology will be used to connect the whole world with no borders. Similarly, unrestricted access to information, communication, and entertainment will give our lives a new dimension and change our lifestyles. Moreover, governments and regulators need to work together to address the 5G security challenges so that the full benefits of 5G can be realized in the future.

REFERENCES

[1] R. F. Olimid and G. Nencioni, "5G Network Slicing: A Security Overview," *IEEE Access*, vol. 8. 2020, doi: 10.1109/ACCESS.2020.2997702.

[2] S. Fonyi, "Overview of 5G security and vulnerabilities," *Cyber Def. Rev.*, vol. 5, no. 1, 2020.

[3] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 4, 2019, doi: 10.1109/COMST.2019.2916180.

[4] A. Dutta and E. Hammad, "5G Security Challenges and Opportunities: A System Approach," 2020, doi: 10.1109/5GWF49715.2020.9221122.

[5] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G Mobile Wireless Networks," *IEEE Access*, vol. 6, 2017, doi: 10.1109/ACCESS.2017.2779146.

[6] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," 2017, doi: 10.1109/CSCN.2017.8088621.

[7] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," *IEEE Access*, vol. 9. 2021, doi: 10.1109/ACCESS.2021.3105396.

[8] L. T. Sorensen, S. Khajuria, and K. E. Skouby, "5G visions of user privacy," in *IEEE Vehicular Technology Conference*, 2015, vol. 2015, doi: 10.1109/VTCSpring.2015.7145587.

[9] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A comprehensive guide to 5G security*. 2018.

[10] X. Ji *et al.*, "Overview of 5G security technology," *Science China Information Sciences*, vol. 61, no. 8. 2018, doi: 10.1007/s11432-017-9426-4.

[11] V. Sucasas, G. Mantas, and J. Rodriguez, "Security Challenges for Cloud Radio Access Networks," in *Backhauling/Fronthauling for Future Wireless Systems*, 2016.

[12] S. Shin and G. Gu, "Attacking software-defined networks: A first feasibility study," 2013, doi: 10.1145/2491185.2491220.

[13] A. Chonka and J. Abawajy, "Detecting and mitigating HX-DoS attacks against cloud web services," 2012, doi: 10.1109/NBiS.2012.146.

[14] A. Khurshid, W. Zhou, M. Caesar, and P. B. Godfrey, "Veriflow: Verifying network-wide invariants in real time," in *Computer Communication Review*, 2012, vol. 42, no. 4, doi: 10.1145/2377677.2377766.

[15] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," 2010, doi: 10.1109/LCN.2010.5735752.

[16] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," 2013, doi: 10.1109/IWCMC.2013.6583635.

[17] I. Ahmad, M. Liyanage, M. Ylianttila, and A. Gurtov, "Analysis of deployment challenges of Host Identity Protocol," 2017, doi: 10.1109/EuCNC.2017.7980675.

[18] W. Yang and C. Fung, "A survey on security in network functions virtualization," 2016, doi: 10.1109/NETSOFT.2016.7502434.

[19] G. Baldini, R. Giuliani, and E. Cano Pons, "An Analysis of the Privacy Threat in Vehicular Ad Hoc Networks due to Radio Frequency Fingerprinting," *Mob. Inf. Syst.*, vol. 2017, 2017, doi: 10.1155/2017/3041749.

[20] S. S. Vikas, K. Pawan, A. K. Gurudatt, and G. Shyam, "Mobile cloud computing: Security threats," 2014, doi: 10.1109/ECS.2014.6892511.

[21] I. Ahmad, S. Namal, M. Ylianttila, S. Member, A. Gurtov, and S. Member, "Security in Software Defined Networks: A Survey - IEEE Journals & Magazine," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, 2015.

[22] K. Norrman, M. Näslund, and E. Dubrova, "Protecting IMSI and User Privacy in 5G Networks," 2016, doi: 10.4108/eai.18-6-2016.2264114.

[23] J. Cao *et al.*, "A survey on security aspects for 3GPP 5G networks," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1. 2020, doi: 10.1109/COMST.2019.2951818.

[24] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," 2015, doi: 10.1109/CNS.2015.7346836.

[25] NGMN Alliance, "5G security recommendations Package #2: Network Slicing," *Ngmn*, 2016.

[26] NGMN Alliance, "NGMN 5G White Paper," 2015.

[27] B. Jaeger, "Security orchestrator: Introducing a security orchestrator in the context of the ETSI NFV reference architecture," in *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, 2015, vol. 1, doi: 10.1109/Trustcom.2015.514.

[28] S. Namal, I. Ahmad, A. Gurtov, and M. Ylianttila, "Enabling secure mobility with OpenFlow,"

2013, doi: 10.1109/SDN4FNS.2013.6702540.
[29] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, “Towards software defined cognitive networking,” 2015, doi: 10.1109/NTMS.2015.7266528.
[30] J. H. Lam, S. G. Lee, H. J. Lee, and Y. E. Oktian, “Securing distributed SDN with IBC,” in *International Conference on Ubiquitous and Future Networks, ICUFN*, 2015, vol. 2015-Augus, doi: 10.1109/ICUFN.2015.7182680.
[31] A. N. Khan, M. L. Mat Kiah, S. U. Khan, and S. A. Madani, “Towards secure mobile cloud computing: A survey,” *Futur. Gener. Comput. Syst.*, vol. 29, no. 5, 2013, doi: 10.1016/j.future.2012.08.003.
[32] M. Johansson, M. Karreman, and A. Foukaki, “3rd Generation Partnership Project: Coopetition in a Developmental Standardisation Setting,” *Acad. Manag. Proc.*, vol. 2017, no. 1, p. 11281, Aug. 2017, doi: 10.5465/AMBPP.2017.11281abstract.
[33] T. Dierks and E. Rescorla, “RFC 5246 - The transport layer security (TLS) protocol - Version 1.2,” 2008.
[34] Q. Qiang, G. Wu, K. Huang, S. Hu, and S. Li, “Survey on research and standardization of 5G security technology,” *Scientia Sinica Informationis*, vol. 51, no. 3. 2021, doi: 10.1360/SSI-2020-0225.
[35] Z. Yan, P. Zhang, and A. V Vasilakos, “A security and trust framework for virtualized networks and software-defined networking,” *Secur. Commun. Networks*, vol. 9, no. 16, 2016, doi: 10.1002/sec.1243.
[36] M. Agiwal, A. Roy, and N. Saxena, “Next generation 5G wireless networks: A comprehensive survey,” *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3. 2016, doi: 10.1109/COMST.2016.2532458.
[37] C. Zhao, L. Huang, Y. Zhao, and X. Du, “Secure machine-type communications toward LTE heterogeneous networks,” *IEEE Wirel. Commun.*, vol. 24, no. 1, 2017, doi: 10.1109/MWC.2017.1600141WC.
[38] N. Lal, S. M. Tiwari, D. Khare, and M. Saxena, “Prospects for handling 5G network security: Challenges, recommendations and future directions,” in *Journal of Physics: Conference Series*, 2021, vol. 1714, no. 1, doi: 10.1088/1742-6596/1714/1/012052.
[39] M. Liyanage, A. Gurtov, and M. Ylianttila, *SoftwareDefined Mobile Networks (SDMN): Beyond LTE Network Architecture*. 2015.
[40] T. Kumar, M. Liyanage, A. Braeken, I. Ahmad, and M. Ylianttila, “From gadget to gadget-free hyperconnected world: Conceptual analysis of user privacy challenges,” 2017, doi: 10.1109/EuCNC.2017.7980650.
[41] M. Liyanage, A. Braeken, A. D. Jurcut, M. Ylianttila, and A. Gurtov, “Secure communication channel architecture for Software Defined Mobile Networks,” *Comput. Networks*, vol. 114, 2017, doi: 10.1016/j.comnet.2017.01.007.
[42] J. H. Jafarian, E. Al-Shaer, and Q. Duan, “OpenFlow random host mutation: Transparent moving target defense using software defined networking,” 2012, doi: 10.1145/2342441.2342467.
[43] ONF, “SDN Security Considerations in the Data Center,” *ONF Solut. Br.*, 2013.
[44] A. Cleeff, W. Pieters, and R. Wieringa, “Security implications of virtualization: A literature study,” in *Proceedings - 12th IEEE International Conference on Computational Science and Engineering, CSE 2009*, 2009, vol. 3, doi: 10.1109/CSE.2009.267.
[45] Z. Riaz, F. Dürr, and K. Rothermel, “Location Privacy and Utility in Geo-social Networks: Survey and Research Challenges,” 2018, doi: 10.1109/PST.2018.8514193.
[46] C. Yu Hunag, T. Min Chi, C. Yao Ting, C. Yu Chieh, and C. Yan Ren, “A novel design for future on-demand service and security,” 2010, doi: 10.1109/ICCT.2010.5689156.
[47] H. Kim, “5G core network security issues and attack classification from network protocol perspective,” *J. Internet Serv. Inf. Secur.*, vol. 10, no. 2, 2020, doi: 10.22667/JISIS.2020.05.31.001.
[48] E. Maccherani *et al.*, “Extending the NetServ autonomic management capabilities using OpenFlow,” 2012, doi: 10.1109/NOMS.2012.6211961.
[49] P. Kulkarni, R. Khanai, and G. Bindagi, “Security frameworks for mobile cloud computing: A survey,” 2016, doi: 10.1109/ICEEOT.2016.7755144.
[50] M. Liyanage, I. Ahmad, M. Ylianttila, A. Gurtov, A. B. Abro, and E. M. De Oca, “Leveraging LTE security with SDN and NFV,” 2016, doi: 10.1109/ICIINFS.2015.7399014.
[51] M. Liyanage, M. Ylianttila, and A. Gurtov, “Securing the control channel of software-defined mobile networks,” 2014, doi: 10.1109/WoWMoM.2014.6918981.
[52] M. Liyanage and A. Gurtov, “Secured VPN models for LTE backhaul networks,” 2012, doi: 10.1109/VTCFall.2012.6399037.

[53] S. Sezer *et al.*, "Are we ready for SDN? Implementation challenges for software-defined networks," *IEEE Commun. Mag.*, vol. 51, no. 7, 2013, doi: 10.1109/MCOM.2013.6553676.
[54] M. Monshizadeh, V. Khatri, and A. Gurtov, "NFV security considerations for cloud-based mobile virtual network operators," 2016, doi: 10.1109/SOFTCOM.2016.7772161.
[55] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101. 2018, doi: 10.1016/j.jnca.2017.10.017.
[56] A. Checko *et al.*, "Cloud RAN for Mobile Networks - A Technology Overview," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, 2015, doi: 10.1109/COMST.2014.2355255.
[57] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 446–471, 2013, doi: 10.1109/SURV.2012.013012.00028.
[58] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, "NFV: State of the art, challenges, and implementation in next generation mobile networks (vEPC)," *IEEE Netw.*, vol. 28, no. 6, 2014, doi: 10.1109/MNET.2014.6963800.
[59] M. A. S. Santos, B. T. De Oliveira, C. B. Margi, B. A. A. Nunes, T. Turletti, and K. Obraczka, "Software-defined networking based capacity sharing in hybrid networks," 2013, doi: 10.1109/ICNP.2013.6733664.
[60] M. Liyanage, A. B. Abro, M. Ylianttila, and A. Gurtov, "Opportunities and Challenges of Software-Defined Mobile Networks in Network Security," *IEEE Secur. Priv.*, vol. 14, no. 4, 2016, doi: 10.1109/MSP.2016.82.
[61] K. Kaska, H. Beckvard, and T. Minárik, "Huawei, 5G and China as a security threat," 2019.
[62] A. N. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Security and Privacy*, vol. 11, no. 2. 2013, doi: 10.1109/MSP.2012.136.
[63] E. Al-Shaer and S. Al-Haj, "FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures," 2010, doi: 10.1145/1866898.1866905.
[64] Huawei Technologies Co., "5G Security: Forward Thinking Huawei White Paper," *Huawei.Com*, 2015.
[65] A. Nayak, A. Reimers, N. Feamster, and R. Clark, "Resonance: Dynamic access control for enterprise networks," 2009, doi: 10.1145/1592681.1592684.
[66] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," 2013, doi: 10.1145/2508859.2516684.
[67] R. Yu, Z. Bai, L. Yang, P. Wang, O. A. Move, and Y. Liu, "A Location Cloaking Algorithm Based on Combinatorial Optimization for Location-Based Services in 5G Networks," *IEEE Access*, vol. 4, 2016, doi: 10.1109/ACCESS.2016.2607766.
[68] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, 2013, doi: 10.1109/SURV.2012.013012.00028.
[69] D. Kreutz, F. M. V Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," 2013, doi: 10.1145/2491185.2491199.
[70] F. Kemmer, C. Reich, M. Knahl, and N. Clarke, "Software defined privacy," 2016, doi: 10.1109/IC2EW.2016.34.
[71] P. Fonseca, R. Bennesby, E. Mota, and A. Passito, "A replication component for resilient OpenFlow-based networking," 2012, doi: 10.1109/NOMS.2012.6212011.

5G SECURITY CHALLENGES AND RECOMMENDATIONS

ORIGINALITY REPORT

29%	26%	21%	23%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	3%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	3%
3	www.researchgate.net Internet Source	2%
4	jultika.oulu.fi Internet Source	2%
5	zenodo.org Internet Source	1%
6	arxiv.org Internet Source	1%
7	Submitted to Staffordshire University Student Paper	1%
8	Submitted to Melbourne Institute of Technology Student Paper	1%
9	www.hindawi.com Internet Source	1%