J Inf Process Syst, Vol.20, No.1, pp.38~52, February 2024
https://doi.org/10.3745/JIPS.03.0192

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

# A Study on the Analysis of Security Requirements through Literature Review of Threat Factors of 5G Mobile Communication

DongGyun Chu[1] and Jinho Yoo[2,*]

**Abstract**

The 5G is the 5th generation mobile network that provides enhanced mobile broadband, ultra-reliable & low latency communications, and massive machine-type communications. New services can be provided through multi-access edge computing, network function virtualization, and network slicing, which are key technologies in 5G mobile communication. However, these new technologies provide new attack paths and threats. In this paper, we analyzed the overall threats of 5G mobile communication through a literature review. First, defines 5G mobile communication, analyzes its features and technology architecture, and summarizes possible security issues. Addition, it presents security threats from the perspective of user devices, radio access network, multi-access edge computing, and core networks that constitute 5G mobile communication. After that, security requirements for threat factors were derived through literature analysis. The purpose of this study is to conduct a fundamental analysis to examine and assess the overall threat factors associated with 5G mobile communication. Through this, it will be possible to protect the information and assets of individuals and organizations that use 5G mobile communication technology, respond to various threat situations, and increase the overall level of 5G security.

**Keywords**

5G Mobile Networks, Security Requirements, Security Threats

## 1. Introduction

The 5G is the 5th generation mobile network that represents a complete generational transition in communication. It provides low-latency communications, massive machine-type communications, and enhanced mobile broadband compared to existing mobile communication. The 5G is an important communication technology that can be used in the era of the 4th Industrial Revolution. It can provide a variety of improved services by utilizing technologies such as multi-access edge computing (MEC), network function virtualization (NFV), and network slicing. The 5G mobile communication is increasingly important due to the development of innovative services in various fields such as autonomous vehicles and smart factories, overcoming the constraints of current communication technologies.

While accelerating the digital transformation of the ICT industry and strengthening competitiveness through 5G technology, the possibility of various attacks and threats is increasing. The 5G communica-



Manuscript received received April 27, 2023; first revision July 31, 2023; second revision September 22, 2023; accepted October 12, 2023.

* **Corresponding Author:** Jinho Yoo (jhyoo@smu.ac.kr)
[1] Division of Business Administration, The Graduate School, Sangmyung University, Seoul, Korea (cdg1608@smu.ac.kr))
[2] Information Systems & Security, Division of Business Administration, Sangmyung University, Seoul, Korea (jhyoo@smu.ac.kr)

tion technology has achieved flexibility due to its high openness, but it also presents a risk of becoming a new target for cyberattacks. In addition, as edge computing is deployed near base stations, there may be a risk of hacking in communication between user equipment (UE) (mobile, Internet-of-Things [IoT] devices, etc.) and various security threats such as information leakage and network failures. These threats may occur against each device attack due to a rapid increase in connectable devices compared to 4G.

These cyber threats are becoming more stealthy and advanced as they are combined and exploited with intelligent technologies such as artificial intelligence and big data. Therefore, it is urgent to prepare a plan to preemptively respond to these threats and attacks and strengthen security.

Edge computing and network slicing, one of the characteristics of 5G mobile communication, are technologies that were not utilized in previous generations of mobile communication. Traffic surges, distributed network attacks, and resource depletion issues can occur. Therefore, there is a need for a comprehensive plan that can encompass the entire 5G mobile communication, not security measures for each threat.

It is necessary to recognize security threats that may arise during the provision, utilization, and operation of 5G mobile communication services, and to systematically respond to and manage these threats. For this systematic response and management, it is important to analyze the system that constitutes 5G mobile communication and identify the security requirements based on security threats.

This study analyzes the overall threat factors of 5G mobile communication and presents security requirements to protect the information and assets of individuals or organizations using 5G mobile communication technology and to cope with various situations that may occur.

The rest of this document is structured as follows. Section 2 raises the need for this study based on previous literature reviews. Section 3 outlines the research methods used to propose 5G security requirements. Section 4 proposes security requirements for the main threat sections (UE, radio access network [RAN], MEC, core network) of 5G mobile communication. Finally, Section 5 presents the conclusion.

# 2. Features and Security Issues of 5G Mobile Communication

## 2.1 Definition of 5G Mobile Communication

The 5G mobile communication technology is a next-generation mobile communication technology that provides low latency, massive machine type, and enhanced mobile broadband compared to 4G. It can provide various services such as smart city, autonomous vehicles, and intelligent CCTV [1].

The International Telecommunication Union has described the representative technical characteristics of 5G into three categories, which can be defined as enhanced mobile broad band (eMBB), ultra-reliable and low latency communications (URLLC), and massive machine-type communications (mMTC) [2].

**Enhanced mobile broad band (eMBB):** It provides much faster data transfer rates ranging from 100 Mbps to 20 Gbps per user and ensures speeds of at least 100 Mbps even in areas with weak signals. It uses a wider frequency band, enabling services that require large-capacity transmission, such as UHD-based augmented reality/virtual reality (AR/VR).

**Ultra-reliable and low latency communications (URLLC):** The latency, which had reached tens of milliseconds in the previous 4G, was maintained at the level of 1ms. Provides services that require real-

time reaction speed and ultra-low latency, such as autonomous vehicle services through the control of various IoT devices like terminals, smart factory devices, and robots, as well as sharing traffic conditions in the vicinity.

**Massive machine-type communications (mMTC):** Massive IoT devices (for home and industrial use) are interconnected for operation and control. Theoretically, one million connections per square kilometer area are available.

## 2.2 Features of 5G Mobile Communication

It has achieved technological evolution to realize eMBB, URLCC, mMTC, which are representative features of 5G mobile communication networks. The representative infrastructure and technical features of the existing 4G mobile communication and other forms can be summarized as follows.

**Network function virtualization (NFV):** The existing mobile communication technology faces the challenge of hardware and software being tightly coupled, requiring a redesign of both whenever new network services and technologies are introduced. To solve these problems, NFV has emerged. NFV is a technology that transforms wired and wireless network equipment into a standardized hardware structure and integrates an independent software structure onto it. In other words, it is a technology that can dynamically provide new services without installing new hardware during network operation. It can also run virtualized services on a regular server, not on its own standard hardware. Through NFV, network functions can be virtualized and provided by software. This allows data to be concentrated in a specific base station and automatically distributed to facilitate smooth communication [3,4].

**Multi-access edge computing (MEC):** In MEC, the explosive rise in the amount of traffic in the mobile environment, the increase in IoT devices, and the demand for personalized services have led to a need for high performance and low latency. Accordingly, it is a technology that provides services such as low latency and high bandwidth through edge computing technology to reduce the traffic burden on the core network. It provides data processing and storage functions to 5G network subscribers through an authorized third party in a location logically adjacent to the base station, that is, near the user. Thus, latency is reduced, and high performance can be provided for high-bandwidth applications. MEC can integrate various services such as video, location services, and virtual reality into a single component. The evolution of application services and verticalization can provide a wide range of coverage and dissemination for 5G networks [5].

**Network slicing:** Within the scope of 3GPP 5G system architecture, network slicing refers to a set of functions that form a complete public land mobile networks (PLMN) for providing services to UE. Network slicing, one of the main features of 5G, can divide a single physical network into several virtual networks according to a specific use case, unlike the previous generation. The advantage of multiple virtual networks is that operators and mobile operators can deliver a controlled composition of PLMNs and specific services. This includes slicing 5G networks and deploying only the functions necessary to support specific customers and market segments. For example, autonomous driving requires ultra-low latency use cases. Therefore, individual PLMNs can be deployed by instantiating only the functions and services necessary to meet customer needs. This includes not providing high throughput. In addition, service-based architecture along with softwareization and virtualization offer advantages that empower operators to respond to customer requirements. The generated slice may vary among different instances based on the system function and service provided [6,7].

## 2.3 The 5G Mobile Communication Technology Architecture

The 5G mobile communication core architecture consists of various network functions and components responsible for end-to-end communication security. It provides authentication functions and various other security functions. The 5G security architecture consists of components that are part of various other architectures and operates horizontally across all other architectures [8,9].

In particular, the security function protects the access of users within the RAN, deals with the security function of the core network and perimeter entities (edge computing), and provides security functions in NFV. Finally, a series of other factors include security management functions, audits and analysis [10].

Fig. 1 shows the architecture of the 5G system as outlined in the 3GPP's 5G mobile communication system technology standard document [11]. First of all, in comparison to LTE, the 4th generation mobile communication system of 3GPP, all components of 5G systems are defined as individual components with connection interfaces in terms of network function. This means that each component can be implemented through virtualization using physical network equipment or network resources.

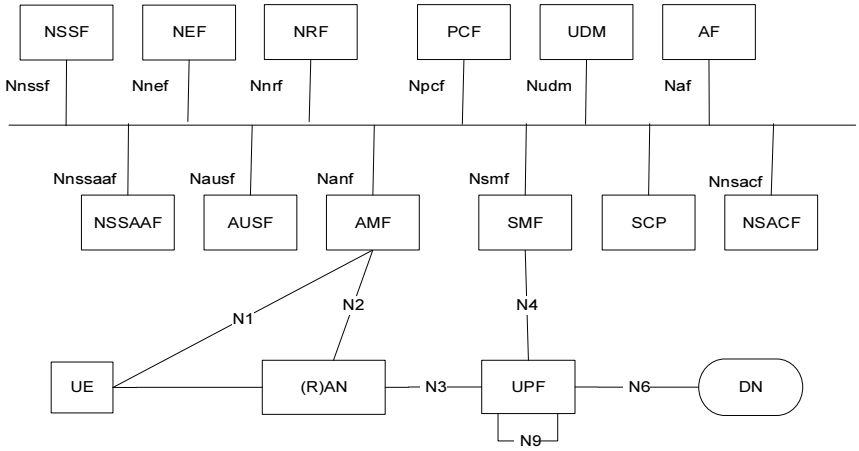


**Fig. 1.** The 5G system architecture.

## 2.4 The 5G Mobile Communication Security Issues

Technical changes such as distributed core network structure, software-defined network (SDN), NFV, MEC, etc., have provided new attack access routes for 5G networks and services to offer openness, scalability, flexibility. Various security issues, such as strict separation requirements, may arise when utilizing network slicing technology [12].

Various research subjects discuss the features and security issues of 5G mobile communication. There are various security issues such as traffic response, data integrity, distributed attacks, and network vulnerability identification. Table 1 summarizes the security issues of major research subjects [11,13-19].

The 5G services play a significant role in various industries such as energy, manufacturing, public safety, healthcare, autonomous driving, and financial services. With the emergence of various 5G services, these services are closely related to safety, human life, etc., and can lead to social and human casualties. As the complexity of 5G networks increases, issues like management risks or malicious attempts by insiders to leak information may arise due to a lack of security expertise in network operation [20-22].

**Table 1.** The 5G security issue

| Study | Year | Description |
|---|---|---|
| NGMN [14] | 2015 | Wireless interface key security, abnormal network traffic, user data plane integrity |
| 5G Americas [16] | 2020 | Edge computing vulnerability identification, network slicing administrator remote access security, distributed attack |
| 3GPP [11] | 2020 | Strengthen subscriber identity information of wireless base stations and strengthen communication-level authentication between terminals and base stations |
| ENISA [13] | 2020 | Authenticate user equipment, isolate resources to prevent virtualization resource depletion |
| Anritsu [15] | 2020 | Strict testing of all elements of the infrastructure and access user equipment, compliance with 5G security protocol standards |
| Bertino et al. [17] | 2020 | Network distributed attack, network slice unauthenticated access |
| Fonyi [18] | 2020 | Identifying vulnerabilities within the network, ensuring confidentiality and availability are important |
| Sullivan et al. [19] | 2021 | Ensuring security and integrity at all levels of 5G |

NGMN=Next Generation Mobile Networks, ENISA=European Union Agency for Cybersecurity.

It is necessary to establish a system capable of handling and managing the information and assets of individuals or organizations utilizing 5G mobile communication technology to address security concerns and potential threats that may arise in a 5G environment.

# 3. Research Method

The purpose of this study is to proactively address security management by analyzing literature related to 5G mobile communication. In 5G mobile communication, smart factories, automobiles, and IoT devices, including user mobile devices, provide services by accessing large quantities of data. 5G data flows communicate with each other through UE, RAN, MEC, and core networks [23]. Especially, MEC is not introduced in previous generations of mobile communications with network slicing, which is very important for 5G mobile communications. MEC is located near the base station and implements ultra-low latency services, which are one of the important features of 5G mobile communication.

## 3.1 User Equipment Threats

One of the key features of the 5G mobile communication system is its ability to support massive connectivity by connecting a large number of smart devices. It is possible to connect with various devices such as smart factories (robots, drones, etc.), autonomous vehicles, VR/AR devices, and intelligent IoT [24]. Therefore, millions of IoT devices connected to the network may be vulnerable to security risks due to weak security management systems. This vulnerability could stem from using outdated IoT devices or being unable to update the operating system firmware because it no longer receives manufacturer updates.

**Stealing administrator authority:** It is possible to obtain administrator privileges by exploiting default or hard-coded passwords on IoT devices that lack support for low-spec or secure algorithms [25].

**Bootloader Replacement:** Low-spec IoT devices receive firmware updates when power is applied. These updates can be vulnerable to mid-size attacks, firmware rollback attacks, firmware replacement attacks, and bootloader replacement attacks [25].

**Low-spec IoT:** Low-spec IoT devices are challenging to install with advanced security features, often leading them to operate with weak passwords and outdated security vulnerabilities. Consequently, they are susceptible to device tampering [26].

**High possibility of personal information leakage:** It is vulnerable to attacks due to improper access by malicious applications and man-in-the-middle attacks. In the case of low-spec IoT devices, there is an increased risk of personal information leakage [12].

**Various types of IoT:** Various types of IoT are likely to cause a number of risks due to different security requirements and standards, making it challenging to design a common standard or architecture [26].

## 3.2 RAN Threats

The 5G RAN technology includes both previous generations (3GPP authorized technologies including generations 2, 3, and 4) and non-3GPP access technologies such as general wired Internet and Wi-Fi technology, and can access 5G networks.

As shown in Fig. 2, there is network flexibility with central unit (CU) and distribute unit (DU). A portion of the gNB (base station) that acts as an antenna is called a radio unit (RU). Since the RU interacts with the gNB and UE, it may be a target for external attacks [13].

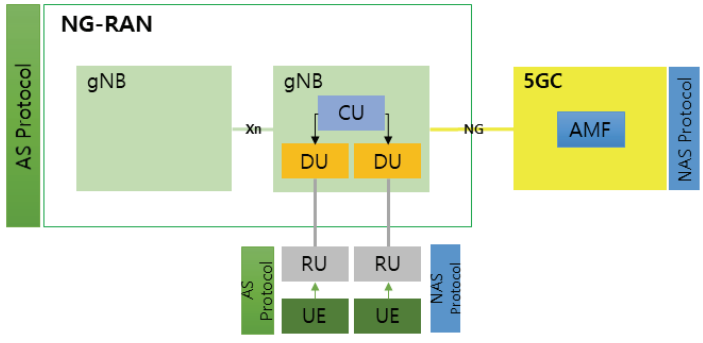


**Fig. 2.** The 5G RAN architecture [13].

The feature of 5G is that it enables various types of wireless access technologies to connect to 5G networks. Protecting base stations is crucial as it allows access to various heterogeneous wireless connections and a multitude of IoT devices. In addition, abnormal traffic caused by millions of user devices connected to the wireless RAN base station can lead to network failures, such as man-in-the-middle attacks and user information theft through impersonation as a legitimate base station by cyber-attackers [27].

**Radio traffic manipulation**: At the base station level, an attacker uses a false base station to manipulate network traffic through a man-in-the-middle attack [4].

**Signal storms:** Affecting networks through signal storms executed by malware or apps that overload cell bandwidth, backbone signaling servers, and cloud servers [28].

**Fake network node:** An attack involving a spoofed base station can compromise a legitimate base station (gnB) through man-in-the-middle attacks, network traffic manipulation, etc. [29].

**Radio frequency interference:** Intentional interruption of network radio frequencies causes service

failure [30].

**Frequency resource abuse:** The unlawful use of resources through malicious dynamic allocation reassignment monopolizes certain frequencies, displacing legal users [22].

## 3.3 MEC Threats

MEC can reduce the traffic burden on the core network by connecting a large number of IoT and mobile terminals in a 5G mobile communication environment and implementing ultra-low latency [13] (Fig. 3).

In addition to ultra-low latency and wide coverage, MEC supports coordination functions, interactions with 5G components, and application lifecycle issues. It could be a new route of attack.

MEC computing connects with the user plane function (UPF) with the mobile operator's 5G edge network, creating a new connection pathway. MEC supports a variety of technologies, including cloud computing and virtualization, and interoperates in an open ecosystem to third-party applications. Therefore, MEC's openness, difference, and diversity can be a major threat to the entire MEC system. [11,31].

**Spoofed or rogue MEC gateways:** Users can set up their own gateways because of the vulnerability of the edge gateway, which can participate even with a user-owned device [8].

**Edge overload:** Traffic surges due to IoT devices experiencing a high volume of authentication requests sent by malicious attackers in a short period [32].

**Edge open API abuse:** This vulnerability enables the exploitation of weaknesses in MEC applications [8].

**Inappropriate API authority:** Sensitive information may be leaked if improper API permissions are granted, as third-party control due to lack of root control [33].

**Traffic transmission of various equipment:** Distributed denial of service (DDoS) attacks induced by traffic generated from a large number of different IoT devices [32].

**Distributed network attacks:** Internal distributed across MEC infrastructure is utilized as a new attack vector by malicious actors [32].

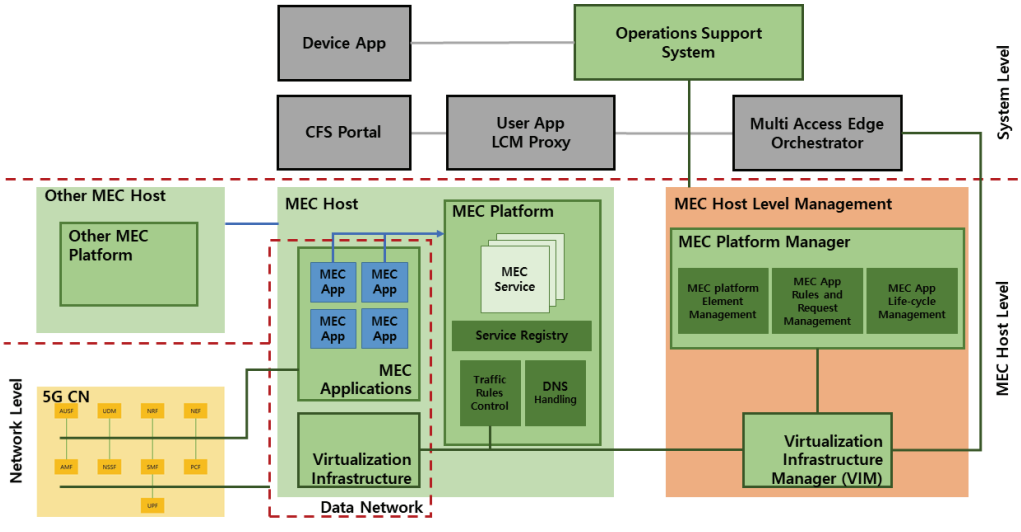


**Fig. 3.** The 5G MEC architecture [13].

## 3.4 Core Network Threats

The core network is an essential component of the 5G infrastructure, offering access network services through the access and mobility management function (AMF) with comprehensive software support [13]. Network slicing and virtualization technologies have accelerated to provide services across all types of networks. The separate authentication functions of the integrated authentication framework offer distinct authentication for each network slice.

NFV and network slicing are critical issues in the 5G core network. It is possible to enhance the flexibility of the technology by segregating the control function using software. Depending on the separation of these control functions, software control is crucial. Using a relatively vulnerable controller can create a point of vulnerability for attackers to exploit the system. Network slicing separates a physical network into several logical networks through virtualization technology, and strict separation by slice is very important. However, if it is not strictly separated, it can be used for slice-to-slice attacks [33].

**Abuse of third-party hosted network functions:** Availability issues and sensitive data breaches may occur as a result of network functions being hosted on systems provided by third-party cloud service providers' systems [13].

**Abuse of remote access:** unauthorized access to critical network components and control of virtual machines [3].

**Authentication traffic surge:** Traffic surge through huge amounts of authentication requests sent by malicious attackers within a short period of time [34].

**Virtualization:** A virtual machine attack can occur through the takeover of administrative rights and side-channel attacks that exploit vulnerabilities in virtualization software [35].

**Network slice resource depletion:** A large number of abnormal connection requests occur in a specific slice, leading to the depletion of resources in other slices [12].

**SDN attack:** DDoS attack on SDN components (controller, controller system, switch memory, etc.) or tampering with the controller [3,8].

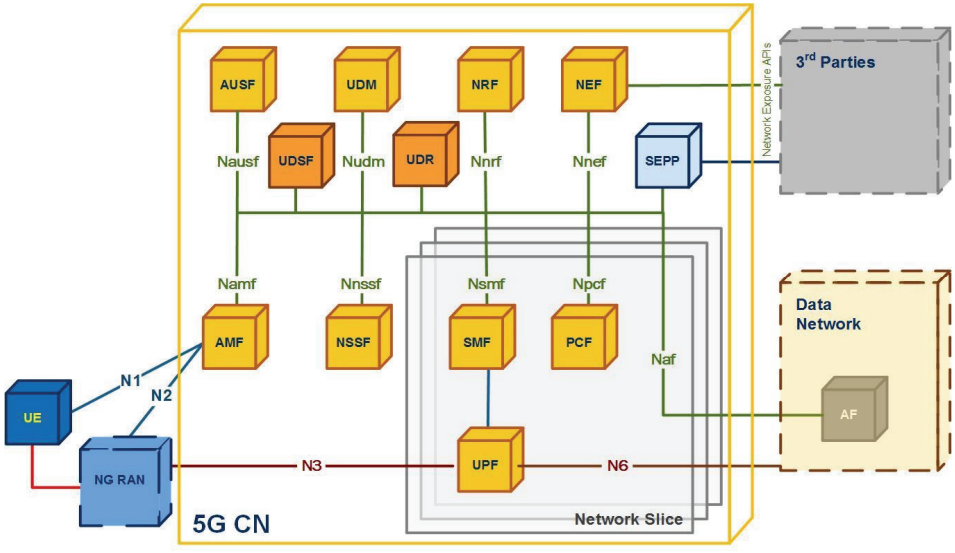


**Fig. 4.** The 5G core network architecture [13].

# 4. 5G Security Requirements Analysis

In this study, we propose security requirements for the main threat sections (UE, RAN, MEC, core network) of 5G mobile communication. The literature on the security requirements of 5G mobile communication threats has been analyzed, and the references cited for each security requirement are presented in the table. In addition, the first word in the security requirements description, followed by a colon (:), represents the security target or provides a compressed representation of each security requirement.

## 4.1 User Equipment Security Requirements

Security hardware and operating system vulnerabilities for various devices connected to 5G mobile communication, data transmission, and other security requirements for the user environment were summarized (Table 2) [11,13-15,23,25].

**Table 2.** UE security requirements

| Description | 3GPP [11] | ENISA [13] | NGMN [14] | Anritsu [15] | Cisco [23] | FSS [25] |
|---|---|---|---|---|---|---|
| Hardware: Remove or protect the debugging port used during the use and development of certified chips and modules. | √ | √ | | | | √ |
| O/S: Conceptual certification code for system drive, setup, upgrade O/S integrity check, system security vulnerability. | √ | | √ | √ | √ | |
| Application data: Security assessment for secure data storage and security assessment for data transfer. | | | √ | | √ | √ |
| Others (such as the environment of use): Periodic security checks, such as central device management, initial settings changes, and enhanced security awareness among users. | | √ | √ | | | |

FSS=Financial Supervision Service.

The biggest security threat to 5G UE is the millions of vulnerable massive IoT devices that are expected to connect to 5G networks. The 5G communications are vulnerable to multiple types of attacks, which could have a widespread effect on the entire 5G network. These attacks are feasible because many interconnected systems depend on each other to function correctly. To stay ahead of these potential vulnerabilities, practitioners must understand the heterogeneous architecture of 5G and the dependencies that govern its performance [36]. Unlike smartphones, IoT devices vary in device types by service (such as smart factory devices, smart city sensors, CCTV, etc.), mounted applications, and supply chain ecosystems. Therefore, it is important to use a certified chip or module and maintain the latest operating system. Because flaws and malware introduced early in development are difficult to detect, lead developers may inadvertently approve them. Malicious actors could exploit these vulnerabilities in the future [37]. The use of devices from unreliable 5G suppliers can expose users to potential risks; therefore, it is crucial to have a dependable supply chain [38]. In addition, there is a need for a system that periodically evaluates and checks security to ensure the safety of data.

## 4.2 RAN Security Requirements

Security requirements that can respond to threats such as wireless encryption, network access authentication, security issues within the base station, and false base stations that may occur during communication between user devices and 5G mobile communication base stations are summarized (Table 3) [11,13,14,16,23,39].

The 5G RAN section can cause DDoS attacks and radio interference due to a large amount of IoT infected with malicious code. Do not create or modify data without proper authorization. In addition, availability must be secured to ensure smooth network operation even if a real cyberattack occurs.

Heterogeneous networks consist of various entities distributed randomly throughout the network, such as legitimate base stations, counterfeit base stations, authorized users, and unauthorized users. Unauthorized users are attackers and eavesdroppers who overhear legal communications. It generates extra lag, delaying the coordination of small cell base stations in such a dense network, which may be exploited for malicious purposes [40].

Therefore, the authentication system for user verification and access should be continuously checked. In addition, since information theft may occur using rogue base stations, it is necessary to establish a monitoring system to detect it.

**Table 3.** RAN security requirements

| Description | 3GPP [11] | ENISA [13] | NGMN [14] | Cisco [23] | 5G Americas [16] | Park et al. [39] |
|---|---|---|---|---|---|---|
| User check and access management: A plan is needed to verify user access rights, including access control and certificate management. | | √ | √ | | | |
| Authentication: Establishment of an authentication system for validating attributes, such as identification. | √ | √ | | | | √ |
| Ensuring integrity: Measures required to prevent unauthorized data creation and modification. | √ | | √ | √ | | |
| Securing availability: Establishing a system that allows network services to operate smoothly even in the event of an attack. | √ | | | | | |
| Establishment of monitoring system: Establishment of a monitoring system involves continuously collecting data to identify the root cause of a problem. | | √ | √ | √ | √ | √ |
| Trust and assurance: Continuing to provide information to the reliability of the system. | | √ | | | | |
| False base station response: Detachment of user location information, modulation of transmission information, and establishment of a defense system against DDoS attacks between users and networks, such as a man-in-the-middle attack through a false base station. | √ | | | | | √ |

**Table 4.** MEC security requirements

| Description | 3GPP [11] | ENISA [13] | NGMN [14] | Cisco [23] | 5G Americas [16] | Kim et al. [31] |
|---|---|---|---|---|---|---|
| Hardware: Control the flow of information in network equipment susceptible to abnormal traffic and detect such traffic. | | √ | √ | √ | √ | √ |
| Software: Provisioning message encryption and validation; introduction of container runtime-based odd symptom detection technology; introduction of container application image integrity and vulnerability verification technology. | | | | | √ | √ |
| Network: Introduction of security threat detection technology and internal access control in MEC system. | | | √ | √ | | √ |
| Management: Establish a crypto technology management system, implement session and authentication security technology, and develop policies. | √ | √ | | | | |

## 4.3 MEC Security Requirements

It presents security requirements for edge computing, a new attack vector for 5G mobile communication. Network management security system, authentication within edge server, and implementation of real-time abnormality detection in cloud containers (Table 4) [11,13,14,16,23,31].

Following the updated design principles of 5G, all components of the MEC are modularized and virtualized on a service basis to build the system in a fully software-based format. MEC requires efficient management systems that can be trusted to exchange trustworthy data among them. Due to the high connectivity across the network, the attack may spread to the central equipment, resulting in service failure and draining resources. Thus, one or more servers or pieces of equipment will be subjected to distributed denial of service attacks, leading to significant security vulnerabilities. In addition to basic hardware traffic management, it is necessary to detect abnormal behavior of software and control unauthorized access.

## 4.4 Core Network Security Requirements

The difference between 5G mobile communication and the mobile communication core network of previous generations is that 5G can provide specialized services to various services with different characteristics by dividing one physical network infrastructure into multiple independent virtual networks based on service type. Accordingly, this study presents the checklist items in three aspects: core network basic security, network virtualization, and network slicing security (Table 5) [13,14,16,17,23,25].

In the 5G core network, network control is managed by software, making it flexible. Software control is crucial because of the segregation of these control functions, and using relatively susceptible controllers can make systems vulnerable to hacking. Network slicing technology separates one physical network into several logical networks. Network slicing supports multiple services and applications with diverse requirements. Each network slice performs a specific service with particular security requirements that

need to be assigned at the creation stage. An attack can spread to other attacks when using shared resources. Attackers also target the communication among slices, which necessitates securing the communication channel between them. Therefore, it is necessary to have a continuous monitoring system to prevent attacks between slices by enforcing strict separation through network slicing.

**Table 5.** Core network security requirements

| Description | FSS [25] | ENISA [13] | NGMN [14] | Cisco [23] | 5G Americas [16] | Bertino et al. [17] |
|---|---|---|---|---|---|---|
| Virtualization: DoS attacks on NFV platforms and measures to effectively monitor security vulnerabilities on known NFV platforms. Prevent remote access to unauthorized individuals' network management interfaces. | | √ | √ | | √ | |
| SDN: Apply appropriate levels of authentication and authorization to all communication interfaces, and ensure the integrity and confidentiality of the packet itself. | √ | | | | √ | |
| Network slicing: Requires strict separation of resource and service traffic within slicing. Establish a real-time monitoring system to detect anomalies indicative of malicious attacks. | | | √ | √ | | √ |

## 5. Conclusion

In this study, technical features, threats, and security requirements were analyzed to protect and ensure safety from malicious cyber-attackers in 5G mobile communication. The overall characteristics of 5G mobile communication were reviewed, and major components according to data flow were analyzed in literature on major security threat factors for four sections: UE, RAN, MEC, and core network. After that, an analysis was conducted to derive security requirements that can respond to threat factors for each of the four sections. In summary, the UE section focuses on security through hardware and operating system updates, the RAN section emphasizes real-time monitoring for false base stations and DDoS attacks, the MEC section involves software vulnerability verification and network access control, and the core network section is strictly separated from NFV vulnerabilities. It is expected that 5G service infrastructure providers, service providers, and related security personnel can use the checklist items outlined in this study to enhance the overall security level.

In addition, this study has the following limitations: as the use of 5G mobile communication technology expands, new threats that are not mentioned in the literature may appear, necessitating continuous updates of security requirements. There is a study suggesting that new security measures using quantum computing can address current classical security issues. Therefore, the implementation of quantum security should also be taken into consideration [41].

In the future, the research can be expanded to develop diagnostic tools that can assess the security level. These tools can be verified by mobile communication experts by developing actual inspection item indicators based on the security requirements identified in this study.

## Acknowledgement

This research was funded by a 2021 research grant from Sangmyung University.

## References

[1] International Telecommunication Union, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond (ITU-R M.2083-0)," 2015 [Online]. Available: https://www.itu.int/rec/R-REC-M.2083-0-201509-I/en.

[2] 5G Americas, "5G Services & Use Cases," 2017 [Online]. Available: https://www.5gamericas.org/5g-services-use-cases/.

[3] M. Geller and P Nair, "5G security innovation with Cisco," 2018 [Online]. Available: https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf.

[4] 5G Americas, "The evolution of security in 5G," 2019 [Online]. Available: https://www.5gamericas.org/the-evolution-of-security-in-5g-2/.

[5] Q. V. Pham, F. Fang, V. N. Ha, M. J. Piran, M. Le, L. B. Le, W. J. Hwang, and Z. Dong, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," *IEEE Access*, vol. 8, pp. 116974-117017, 2020. https://doi.org/10.1109/ACCESS.2020.3001277

[6] J. Hodges, "5G security strategy considerations," 2019 [Online]. Available: https://www.juniper.net/content/dam/www/assets/white-papers/kr/ko/5g-security-strategy-considerations.pdf.

[7] A. Nieto, A. Acien, and G. Fernandez, "Crowdsourcing analysis in 5G IoT: cybersecurity threats and mitigation," *Mobile Networks and Applications*, vol. 24, pp. 881-889, 2019. https://doi.org/10.1007/s11036-018-1146-4

[8] 5GPPP, "View on 5G architecture," 2016 [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-July-2016.pdf.

[9] D. Park and H. Lee, "Standards/test certification technology trend - 5G technology development trend for vertical integration," *TTA Journal*, vol. 168, pp. 61-69, 2016.

[10] P. Song and S. Song, "Trends of standardization activity for 5G RAN architecture," *Electronics and Telecommunications Trend*s, vol. 31, no. 6, pp. 88-96, 2016. https://doi.org/10.22648/ETRI.2016.J.310610

[11] 3GPP, "Security architecture and procedures for 5G system (TS 33.501 version 16.3.0 Release 16)," 2020 [Online]. Available: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf.

[12] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, 2018. https://doi.org/10.1109/MCOMSTD.2018.1700063

[13] European Union Agency for Cybersecurity, "ENISA threat landscape for 5G networks," 2019 [Online]. Available: https://doi.org/10.2824/49299.

[14] Next Generation Mobile Networks, "The NGMN 5G white paper," 2015 [Online]. Available: https://www.ngmn.org/work-programme/5g-white-paper.html.

[15] Anritsu, "A bottom-up approach to 5G network slicing security in user equipment," 2021 [Online]. Available: https://resources.goanritsu.com/white-papers/a-bottom-up-approach-to-5g-network-slicing-security-in-user-equipment.

[16] 5G Americas, "Security Considerations for the 5G era," 2020 [Online]. Available: https://www.5gamericas.org/download/security-considerations-for-the-5g-era-2020-white-paper/.

[17] E. Bertino, S. R. Hussain, and O. Chowdhury, "5G security and privacy: a research roadmap," 2020 [Online]. Available: https://arxiv.org/abs/2003.13604.

[18] S. Fonyi, "Overview of 5G security and vulnerabilities," *The Cyber Defense Review*, vol. 5, no. 1, pp. 117-134, 2020.

[19] S. Sullivan, A. Brighente,S. A. Kumar, and M. Conti, "5G security challenges and solutions: a review by OSI layers," *IEEE Access*, vol. 9, pp. 116294-116314, 2021. https://doi.org/10.1109/ACCESS.2021.3105396

[20] 5GPPP, "5G and the Factories of the future," 2015 [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Factories-of-the-Future-Vertical-Sector.pdf.

[21] 5GPPP, "5G Automotive vision," 2015 [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White-Paper-on-Automotive-Vertical-Sectors.pdf.

[22] 5GPPP, "5G and energy," 2015 [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-White_Paper-on-Energy-Vertical-Sector.pdf.

[23] Cisco, "5G cybersecurity guidance," 2020 [Online]. Available: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-5g-cybersecurity-guidance.pdf.

[24] O. Park, H. Hwang, C. Lee, and J. Shin, "Trends of 5G Massive IoT," *Electronics and Telecommunications Trends*, vol. 31, no. 1, pp. 68-77, 2016. https://doi.org/10.22648/ETRI.2016.J.310107

[25] Financial Security Institute, "Security requirements for 5G-based financial services," *e-Finance and Financial Security*, vol. 2019, no. 17, pp. 33-52, 2019.

[26] Korea Internet & Security Agency, "Home/home appliances IoT security guide," 2017 [Online]. Available: https://www.kisa.or.kr/2060205/form?postSeq=3&page=2.

[27] T. Wan, "False base station or IMSI Catcher: what you need to know," 2019 [Online]. Available: https://www.cablelabs.com/blog/false-base-station-or-imsi-catcher-what-you-need-to-know.

[28] 3GPP, "NR; Radio Resource Control (RRC); Protocol specification (TS 38.331)," 2020 [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3197.

[29] 3GPP, "Study on 5G security enhancement against false base stations (TR 33.809 Release 11)," 2020 [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539.

[30] R. Chirgwin, "Fake mobile base stations spreading malware in China," 2017 [Online]. Available: https://www.theregister.com/2017/03/23/fake_base_stations_spreading_malware_in_china/.

[31] Y. Kim, J. Park, J. Lee, J. Jang, D. Moon, and I. Kim, "Security threat and response technology for multi-access edge computing in 5G environments," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 38, no. 9, pp. 16-24, 2020.

[32] X. Lu, D. Niyato, N. Privault, H. Jiang, and P. Wang, "Managing physical layer security in wireless cellular networks: a cyber insurance approach," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 7, pp. 1648-1661, 2018. https://doi.org/10.1109/JSAC.2018.2825518

[33] S. Vural, S. Revell, M. Shepherd, G. Foster, M, Hawkins, G. Lupton, et al., "5G Network Architecture and Security," 2018 [Online]. Available: https://www.wlep.co.uk/wp-content/uploads/5G_Architecture_and_Security_technical_report_-_04Dec18.pd_.pdf.

[34] 5G PPP Security WG, "5G PPP Phase 1 Security Landscape," 2017 [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf.

[35] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 196-248, 2020. https://doi.org/10.1109/COMST.2019.2933899

[36] B. Curtis, "5G innovations and cybersecurity risk," *ISACA Journal*, vol. 5, pp. 1-6, 2022. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-5/5g-innovations-and-cybersecurity-risk

[37] US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, “Potential threat vectors to 5G infrastructure,” 2021 [Online]. Available: https://www.cisa.gov/resources-tools/resources/5g-potential-threat-vectors.

[38] US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, “Ensuring the security and resilience of 5G infrastructure in our nation,” 2020 [Online]. Available: https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

[39] H. Park, J. Park, B. Kim, and I. Yu, “Analysis of major issues in response to false base stations in 5G security,” *Review of KIISC*, vol. 30, no. 6, pp. 23-30, 2020.

[40] F. Salahdine, T. Han, and N. Zhang, “Security in 5G and beyond recent advances and future challenges,” *Security and Privacy*, vol. 6, no. 1, article no. e27, 2023. https://doi.org/10.1002/spy2.271

[41] C. Mangla, S. Rani, N. M. F. Qureshi, and A. Singh, “Mitigating 5G security challenges for next-gen industry using quantum computing,” *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 6, article no. 101334, 2023. https://doi.org/10.1016/j.jksuci.2022.07.009

**DongGyun Chu** **https://orcid.org/0009-0003-8733-0159**

He received Ph.D. degrees in business administration from Sangmyung University in 2022. He works as a researcher on related projects such as information protection and cyber security. His current research interests include cyber security and management information system.

**Jinho Yoo** **https://orcid.org/0000-0003-4359-8009**

He is a Professor at Sangmyung University. He received his B.S. degree in Mathematics and M.S. in Statistics and Ph.D. degrees in Information Management and Security at Korea University. Prior to joining Sangmyung University, he worked as a director of the Korea Internet and Security Agency, as a managing consultant of CRM and data mining at IBM, and as a researcher of R&D planning at the Electronics and Telecommunications Research Institute. His research interests include issues related to information security & privacy, big data analytics, block-chain and datamining.