The ISC Int'l Journal of
Information Security
ISeCure

January 2024, Volume 16, Number 1 (pp. 17–35)
http://www.isecure-journal.org

# An Overview of Security Attacks in 5G Enabled Technologies: Applications and Use Case Scenarios

Shadab Kalhoro [1,*], Farhan Bashir Shaikh [1], Anam Kalhoro [2],
Junaid-Ur-Rehman Abbasi [3], and Ramesh Kumar Ayyasamy [1]

[1] *Department of Computer Science, Faculty of Information and Communication Technology, University Tunku Abdul Rahman (UTAR), Perak, Malaysia*
[2] *Department of Computer Science, University of Sindh, Jamshoro, Pakistan*
[3] *Faculty of Engineering and Green Technology, University Tunku Abdul Rahman (UTAR), Perak, Malaysia*

ARTICLE INFO.

*Article history:*
**Received:** August 4, 2022
**Revised:** October 23, 2022
**Accepted:** May 8, 2023
**Published Online:** November 20, 2023

*Keywords:*
5G, Mobile Communication, Security Attacks, Security Models, 5G Usage Scenarios, Intelligent Applications

**Type:** Research Article

**doi:** 10.22042/isecure.2023.354872.829

**dor:** 20.1001.1.20082045.2024.16.1.2.6

ABSTRACT

With the advancement of ICTs, the fifth generation has developed into an emergent communication platform that supports high speed, low-latency, and excellent connectivity to numerous devices with modern radio technology, service-oriented design, and cloud infrastructure. The recent developments in 5G and existing proposed plans are centered on the security model of this study, with authentication, availability, confidentiality, integrity, visibility, and a centralized security policy. However, initiating innovative technologies and enhanced aspects in 5G communication raises new requirements and has presented various security challenges. 5G-based applications face security risks because they use modern technology. This paper presents a study of security attacks and the security risks faced by 5G intelligent applications. This article also investigates the three main 5G usage scenarios (i.e., eMBB, uRLLC, and mMTC). This research recommends reducing the security risks of 5G usage scenarios and intelligent applications.

## 1 Introduction

The evolution of mobile networks has provided new services to meet new demands for better performance, leading to the emergence of modern communication technology in less time [1]. Mobile communication has changed from analog phone calls to more advanced technologies that give end users and communication transmissions faster data speeds [2]. Currently, mobile phones are bandwidth-hungry and demand high data rates on mobile networks, which they were until the development of 4G mobile networks, which enhanced data transmission speed and optimized the performance of smartphone devices [3]. When 4G reaches its limitations, researchers are turning to 5G, which they believe is the future of cellular technology. However, 5G technology changes how new IT technologies are thought of to make a mobile network environment that fits the needs and features of different IoT devices [4].

Due to the abundance of transmissions and technologies, wireless subscriptions are expected to grow. Through the advancement of wireless technology, the increase in bandwidth and transmission speed is the catalyst for designing new wireless technology standards [5]. The 5G wireless standard has this latest push for faster speeds and better coverage. Table 1 [6]

[*] Corresponding author.
Email addresses: shadabkalhoro@1utar.my, , , ,

ISSN: 2008-2045 © 2024 ISC. All rights reserved.

demonstrates the description of different generations throughout the years.

The 5G network is an improvement over the old 4G network and a new structure with several new facilities. 5G technology offers numerous progressive features like high capability, high density of portable broadband consumers, auxiliary device-to-device (D2D) communication, large-scale machine-type communication, less power consumption, and comes with lesser latency in the improved execution of the Internet of Things (IoT) [4]. 5G includes eight progressive characteristics, which are [3]:

- $1-10$ Gbps connections towards endpoints
- 1−millisecond latency
- the bandwidth of 1000−X for each unit area
- 10 to 100−X number of linked gadgets
- 99.999 percent accessibility
- The network is completely handled
- For low-powered devices, the battery has a lifespan of up to ten years
- 90% off for network energy usage

5G permits innovations and gradual changes in all vertical industries, such as smart grids, campuses, homes, and cities [7], IoT, vehicle-to-vehicle and infrastructure, manufacturing automation, and various 5G usage cases [8]. The International Telecommunication Union (ITU) has recognized three new usage scenarios for 5G, namely enhanced mobile broadband (eMBB), ultra-reliability and low delay communications (uRLLC), and massive-scale machine type communication (mMTC) [9].

5G is centered on the most contemporary architecture [10], namely 3GPP (3rd Generation Partnership Project), which specifies the entire structure required for 5G network design [11]. Innovative architecture, modern technologies, the latest usage cases, the latest applications of industry, and many community-connected devices pose new challenges to security and protection in 5G wireless systems [12]. Due to the transmission type and restricted bandwidth of wireless connections, it is a big challenge for service providers to promise confidentiality, integrity, and authentication [13]. Security and privacy are the primary concerns of users and the most pressing issues in today's technological world [14].

5G is one of the most popular research areas among researchers and communication specialists. Several studies on 5G networks have discussed future research opportunities in design, flexibility, traffic control, safety measures, and privacy considerations for 5G networks [15]. These studies have underlined security as the most pressing issue associated with 5G technology [16]. Unfortunately, no single study covers all characteristics of 5G security attacks and application usage scenarios. Hence, the primary motive behind this study is to focus primarily on security attacks associated with 5G technologies. The study also demonstrates the evolution and limitations of privacy protection from 1G to 4G, intelligent 5G applications with use cases, and steps to reduce the security risk of usage scenarios.

The rest of this paper is structured as follows: Section 2 discusses the evolution of mobile communication as well as its limitations, Section 3 presents the security model for 5G communication, Section 4 highlights the common types of security attacks associated with 5G networks, Section 5 describes 5G usage scenarios and the security risks associated with these scenarios, Section 6 explains intelligent 5G applications with use cases, and Section 7 highlights steps to reduce security risk of usage scenarios of 5G, Section 8 presents the conclusion. In contrast, the contribution of the study is elaborated in Section 9.

## 2 Evolution of Mobile Communication Systems (1G−5G)

This part evaluates the evolution discussion from 1G networks to 5G. Each generation has new functionalities, improved performance, and limitations relative to the previous generation [17]. This section briefly examines each generation's major technologies, uses, harms, security attacks, and risks. The evolution of mobile communication has been further explained as follows:

### 2.1 First Generation (1G)

First-generation mobile communications are centered on analog technology. This generation supported reliable voice calls but could have been more costly and insecure. The first-generation maximum speed was 2KBPS [5]. In 1G, the handset only needs to be authenticated at the base station, and if the verification from the base station to the handset fails, it creates serious trouble [6]. The severe security error in 1G is that the user mistakenly believes that the phone service provider is connected to the base station because the attacker may have made himself an authentic channel. If the attacker gets into the antenna, he can use it to build a fake base station [7]. This basic channel can connect targets to the antenna, which can be used to hear discussions or manipulate information [8].

Moreover, the call is not encoded; it is directly programmed into the carrier signal. Due to this shortcoming of the 1G Network, attackers can easily hear the conversation by tapping the signal; which is commonly known as “eavesdropping” [9].

### 2.2 Second Generation (2G−GSM)

Second-generation (2G) mobile communications are vastly improved on 1G. 2G is digital and uses the standard Global System for Mobile Communications (GSM) and offers data transmission rates of at least 500KBPS [17]. To use GSM, the user must have a handset with a SIM card to activate the handset on a network. This permitted the mobile phone to work in various territories, which was impossible with 1G technology [7]. In a decade, the 2G technology advanced from GSM to Global Packet Radio Service (GPRS), EDGE, and EDGE+ [18]. Users of 2G technology could send SMS or MMS messages. Mobile phone calls have become less expensive, which is the core reason for 2G's success globally [5]. The key feature of 2G networks is that calls are encoded between the base station and the terminal device [12]. This encoding is symmetrical, and the source and terminal devices utilizing the SIM card module can find the key used. Many algorithms are used to run this encoding [6]. Unfortunately, those encoding algorithms can be broken easily. The encoding was only possible among the terminal device and base station, not the entire network [19]. The network traffic was forwarded without the use of any encoding. Due to this shortcoming, fake base stations could be created [8]. Attackers may hear or tamper with the data during transmission if the connections to devices interfere with communication between the operator and service provider [9].

### 2.3 Third Generation (3G)

For the third generation, more advancements have been made based on the GPRS and EDGE standards of the second generation [20]. Data rates of at least 2MBPS are allowed for the third-generation cellular networks [21]. 3G has introduced innovative encryption algorithms that still have some susceptibilities but are more reliable than the algorithms utilized in 2G [6]. In addition, it allowed 3G end devices to be authenticated over the network [7]. The newly introduced two-way authentication process has made stingrays challenging but possible. Stingray devices, also known as IMSI (international mobile subscriber identity) catchers, mimic mobile phone towers and transmit signals to track the location of mobile phones. Stingray devices allow for eavesdropping on the targets' communications and monitoring their activities.

Stingray may need a connection from the former 2G specification, known as a downgrade attack [22]. Utilizing this attack, the stingray can exploit old specifications' weaknesses.

### 2.4 Fourth Generation (4G−LTE)

The fourth generation is also called the long-term evolution (4G−LTE) of mobile communication. 4G networks significantly improve download speeds compared to 3G technology [13]. The data transfer speed offered by 4G technology is 100MBPS or 1GBPS [14]. Download speed enabled consumers to utilize their mobile devices for various applications. 4G uses technologies like multiple input, multiple output (MIMO) and orthogonal frequency division multiplexing (OFDM) [15]. Users can watch HD television via mobile networks and make real-time face-to-face calls with high-quality, high-capacity, and high-speed services. The fourth generation's security is improved, and communication is encrypted compared to 3G [5]. There are no known disadvantages of the algorithm for encoding transmissions in 4G, but attacks on 4G networks are still possible [6]. Because 4G terminal devices can communicate with the internet more quickly, traditional attacks such as malware or ransomware should be possible [7].

### 2.5 Fifth Generation (5G)

5G significantly improved the constraints and performance of 4G. It maintains excellent data transfer rates with less latency and higher linked density [11]. It encourages device-to-device communication, improved wireless coverage, and improved battery usage [12]. The data transfer speed of 5G is thirty-five times faster than 4G [13]. Methods and technologies such as “small cell”, “massive MIMO”, “millimeter wave”, and “light fidelity (Li−Fi)” are used to deliver 10GBPS with minor delay. It establishes almost a hundred billion device connections [14]. Table 1 shows the evolution of technology over the last few years.

Figure 1 shows how communication technology has evolved from 1G to 5G.

## 3 The Security Model for 5G

The new architecture, innovative technologies, and use cases in 5G networks bring new features and needs for security services. This section evaluates the six types of security services for 5G: confidentiality (data confidentiality and privacy), integrity, availability, authentication (entity and message authentication), centralized security policy, and visibility. Figure 2 presents the security model of 5G.

### 3.1 Confidentiality

In the security model of 5G, the confidentiality of data is one of the essential security requirements that could be used to protect data during transmission from exposure to unauthorized access and passive at-

**Table 1**. Evolution of technology during the last few years [11]

| Technology | Deployment | Bandwidth | Key differentiator | Technologies | Services | Core Network |
|---|---|---|---|---|---|---|
| **1st Generation** | 1980*s* | 2kbps | Mobility | AMPS, NMT, TACS | Voice | PSTN |
| **2nd Generation** | 1990*s* | 500kbps | Secure, mass Adoption | GSM/GPRS, D-AMPS, cdmaOne | SMS, Digital Voice, Higher capacity packetized data | PSTN |
| **3rd Generation** | 2000*s* | 2Mbps | Better internet experience, applications | WCDMA/HSPA+, CDMA2000/E V-DO, TD-SCDMA | Cohesive high-class audio[24], video, and data | Packet Network |
| **4th Generation** | 2010*s* | 1Gbps | Faster broadband internet, lower latency | LTE, LTE Advanced | Dynamic information access, wearable devices | Internet |
| **5th Generation** | 2020*s* | 20Gbps | Faster internet, wide range of applications, IoT | MIMO, mmWave, Li-Fi, Small cells | Dynamic information access, wearable devices with AI capabilities | Internet |

tacks like eavesdropping [15]. Standard data encryption algorithms are implemented to attain data confidentiality in 5G network applications. A Symmetrical key encoding algorithm is used for encoding and decoding information using a private key distributed amongst communicating parties, for example, the source and receiver [16].

### 3.2 Integrity

This security model is intended to stop data tampering during data transfer. The integrity of 5G new radio (NR) traffic is more secure than 4G [15]. The only significant development in fifth-generation integrity safety is that the NR provides user plane security, whereas the fourth generation did not sustain integrity safety for the user plane [23]. This latest asect is helpful for small information broadcasts and minimal IoT devices. Additionally, this method utilizes signaling to maintain 5G-AKA (authentication and key agreement) integrity. It confirms that the unauthorized party does not access the information transmitted over the air [24].

### 3.3 Availability

Availability ensures legitimate consumers can access network resources when needed, as availability affects service provider reputation [15]. In addition, availability guarantees the high potential effect of the network structure. Several security concerns interrupt the continual availability of network assets. It estimates the active network attacks, for example, denial-of-service (DoS) attacks, which could destroy network performance [25]. Also, jamming attacks have reduced radio access sources; because of this, consumers cannot retrieve cellular customer facilities.

### 3.4 Authentication

Authentication is the basic idea for verifying consumers' identities on the network. Several methods are applied to authenticate data on 5G networks [14]. There are two key components of authentication: primary and secondary authentication. Primary authentication operates on non-3GPP (third-generation partnership project) technologies [26]. Primary authentication has several challenges, including knowledge control and device authentication, which must need to be sufficiently offered [15]. The AKA (authentication and key agreement) and extendible authentication procedures are employed to address these issues. However, secondary authentication allows external networks to authenticate mobile operators and operate on 3GPP. Extensible authentication protocol (EAP) techniques are applied for secondary authentication [27].

### 3.5 Centralized Security Policy

Existing 3GPP security designs for 4G could not be immediately applied to newer 5G, because they are based on the traditional operator-subscriber trust model [15]. Consequently, to endorse the latest advanced and centralized security policy, a management system is required that allows users to retrieve applications and resources. In [28], a policy-based security management framework is integrated to help with the security management for 5G. Researchers in [29] state that mobile operators can safeguard their network structure with the support of policy-based security management. Furthermore, operators can offer Security-as-a-Service (SaaS) solutions for multiple clients.

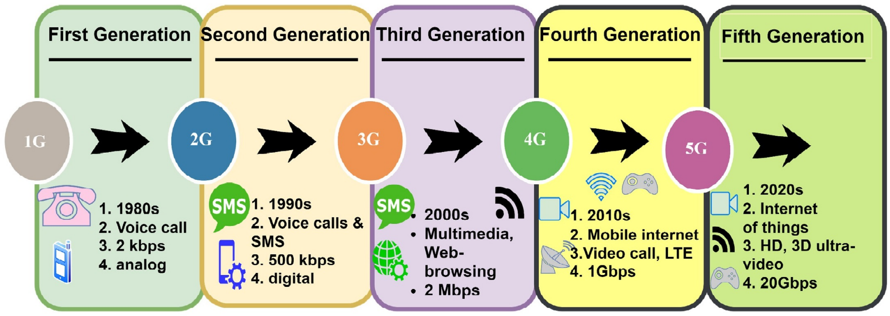

**Figure 1**. Generation of mobile communication from 1G-5G [12]

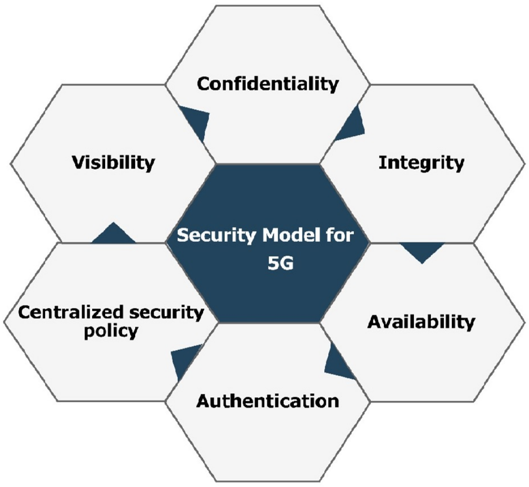

**Figure 2**. The Security model for 5G [14], [15]

### 3.6 Visibility

Visibility allows for the end-to-end perception of the mobile network to the control plane. It could effectively deal with fundamental network problems to guarantee a safe environment [15]. The fifth generation must use specific end-to-end security policies that cover all network layers, including applications, signaling, and data planes [23]. To execute such a specific defense mechanism, operators must have complete visibility, monitoring, and control over all network layers [24]. In this case, on a fifth-generation network, both the software and hardware have reliable security strategies [28].

## 4 Security Attacks in 5G Networks

The primary motive of the 5G network is to offer high bandwidth to consumers [7], along with low-latency communications, and provide comprehensive coverage of signals to support a broad range [10]. Security has been identified as one of the significant needs associated with 5G technologies [11]. As 5G networks link every aspect of life, consumer data is stored and shared online, so providing user confidentiality would be a challenge for the operators [26]. The latest research has revealed that 5G facilities should guarantee consumer security [13]. In 1G wireless networks, handsets and channels were intended for illegal replication [14]. In the 2G era of wireless networks, message spamming was famous not only for widespread attacks but also for broadcasting fake information [16]. In 3G, internet security vulnerabilities and challenges have migrated across the IP-based wireless communication domain [17]. With the growing need for IP-based communications, 4G mobile networks expanded into new services like mobile devices and multimedia traffic in the mobile domain [18]. Wireless communication systems have been vulnerable to security weaknesses since their inception. This growth has led to a more complex and dynamic threat landscape. With the initiation of 5G, threat vectors have become more concerned about security than ever before [19]. As a result, it is critical to emphasize the security threats to technologies. Attacks on 5G networks could be launched from various locations, such as the user equipment, access networks, and core networks of mobile operators [20]. Figure 3 summarizes and helps to understand the security attacks affecting different segments of 5G networks. Below are the types of attacks associated with 5G.

### 4.1 Jamming Attacks

The wireless communication radio interface in 5G is susceptible to jamming attacks, which can degrade system execution. It needs to control channels to work properly [21]. Attackers can disrupt frequency bands by blocking control channels using high-powered attacks [30]. The intensity of the jamming attacks will rise if the attackers can compromise multiple devices and create a botnet. These cooperative mobile devices act as jamming devices [31]. Jamming attacks are classified into three types [32]:

1. *Pilot jamming*: The purpose of pilot jamming is to harm legal communication. It possesses prior information about the pilot sequences. Because the attacker only needs to corrupt the pilot signals and not the entire communication, this

jamming attack can be very energy efficient.

2. *Proactive Jamming*: With proactive jamming, attackers send jamming signals regardless of whether legal data communication is present. Attackers occasionally spread random bits or regular packets into networks to save energy and switch between the sleep and jamming phases.

3. *Reactive Jamming*: The jamming attackers can monitor the activity on the legal channel. If there is activity, the adversary immediately sends a random signal to collide with the existing signal on the channel.

It is, important to use frequency-hopping or spread-spectrum technologies that can make it more difficult for an attacker to disrupt wireless communication. Additionally, implementing signal strength monitoring and intrusion detection systems can help detect and prevent jamming attacks. Other preventive measures include limiting physical access to wireless devices, implementing strong encryption and authentication mechanisms, and maintaining up-to-date security software and firmware [33].

### 4.2 Spoofing Attacks

The vulnerability known as "spoofing" allows an attacker to intercept legitimate conversations on the 5G network [14]. In this attack, the attacker injects malicious messages under false identities, such as denial of service and man-in-the-middle attacks [34]. Spoofing attacks are one of the significant risks in 5G−enabled wireless communications, as there is a potential for physical layer attacks in wireless communications [15]. There are two typical spoofing attacks [32]:

1. *Identity spoofing attacks*: These attacks are simple to launch in networks. An attacker who spoofs identity can claim to be an authenticated device by using a bogus identity. After gaining illegal access to the network, attackers attempt more advanced attacks on the networks and devices.
2. *Sybil attacks*: In this attack type, a malicious node can imitate other nodes and create false identities; the attacker may produce an arbitrary number of additional nodes using only one physical device. In the presence of these attacks, the network may generate incorrect reports, and users may receive spam and lose their privacy.

To prevent spoofing attacks, it's important to use strong authentication mechanisms, such as multi-factor authentication, to verify the identity of users and devices. Additionally, implementing secure network protocols and encryption can help prevent data manipulation in transit. Other ways to stop attacks are to set up access controls, watch network traffic for signs of suspicious activity, and keep antivirus and anti-malware software up-to-date [33].

### 4.3 Man in the Middle Attack (MITM)

In this attack, an attacker creates a tentative scenario that interrupts data communication between user equipment over the network to alter the information. The MITM attack is classified into the following types [35]:

1. *IP spoofing*: In an IP spoofing attack, the attacker spoofs the IP address of a trusted host to gain access to a network or system. It allows the attacker to intercept and modify network traffic.
2. *DNS spoofing*: In a DNS spoofing attack, the attacker spoofs the DNS server used by the victim, which allows the attacker to redirect the victim to a malicious website that intercepts and modifies the victim's DNS requests.
3. *SSL stripping*: In an SSL stripping attack, the attacker intercepts the communication between the victim and the server and downgrades the secure SSL connection to an unencrypted connection. It allows the attacker to eavesdrop on the communication and steal sensitive information.
4. *Email Hijacking*: This is another type of man-in-the-middle attack in which the hacker compromises and gains access to a target's email account. The attacker then silently monitors the communications between the client and the provider and uses the information for malicious purposes.

To prevent man-in-the-middle attacks, it is important to use encryption and strong authentication mechanisms, such as two-factor authentication and digital certificates. Additionally, it's important to keep software and firmware up-to-date, as security patches are often released to address vulnerabilities that could be exploited in a MitM attack. Also, it is important to be cautious when connecting to public Wi-Fi networks and to avoid accessing sensitive information or logging into sensitive accounts while connected to an unsecured network [36].

### 4.4 DoS Attack

In this type, the attacker attempts to send duplicate data to the nodes, creating a network unreachable for consumer authentication. When the network is used to attack without any security measures, many denial-of-service (DoS) attacks could be made [10]. Attackers could launch DoS/DDoS (distributed denial of service) attacks to establish network blocking that can lead to a service breakdown [29]. There are several types of DoS attacks, including [36]:

1. *Ping of Death*: In a Ping of Death attack, the attacker sends oversized packets to the victim's system, causing it to crash or freeze.
2. *Smurf Attack*: In a Smurf attack, the attacker spoofs the victim's IP address and sends a large number of ICMP echo requests (pings) to a network's broadcast address, causing all devices on the network to respond to the victim's IP address and flood it with traffic.
3. *SYN Flood*: In an SYN Flood attack, the attacker sends many TCP connection requests with fake source IP addresses to the victim's system, causing it to become overwhelmed and unresponsive.
4. *UDP Flood*: In a UDP Flood attack, the attacker sends many UDP packets to the victim's system, which uses up all of its resources and makes it unusable.
5. *HTTP Flood*: In an HTTP Flood attack, the attacker sends many HTTP requests to the victim's web server, overwhelming it with traffic and causing it to become unresponsive.

Implementing strong security measures, such as firewalls, intrusion detection and prevention systems, and anti-DDoS services, is important to prevent DoS attacks. Additionally, it is important to keep software and firmware up-to-date, as security patches are often released to address vulnerabilities that could be exploited in a DoS attack. It is also important to monitor network traffic and configure systems to limit the number of connections that can be made to the system at any time [37].

### 4.5 Eavesdropping Attacks

In this case, when the attacker controls the transmission channel, the attacker struggles to hear or read the messages over the network channel without the user's permission and proposes numerous suggestions to protect against eavesdropping [12]. This is one of the possible attacks on 5G, as it helps the attacker to make more attacks [38]. Here are the most common types of eavesdropping attacks [32]:

1. *Passive attack*: In this attack, the attacker listens to the communication between two parties without modifying or disrupting the communication.
2. *Active attack*: In this type of attack, the attacker intercepts and modifies the communication between two parties in real time, allowing them to manipulate the communication or access sensitive information.
3. *Wireless eavesdropping*: This attack targets wireless networks and captures wireless signals to intercept and read the data sent over the web.

To protect against eavesdropping attacks, it is important to use encrypted communication channels, such as HTTPS, SSL, and VPNs. Additionally, strong authentication measures and implementing access controls can help prevent unauthorized access to sensitive data [33].

### 4.6 Tampering Attacks

Attackers may delay or alter data transmitted over a network channel without the user's permission. An attack could destroy the capabilities and performance of fog computing [25]. Such attacks could delay or create failures in data packet transmission due to the wireless network and consumer mobility. These attacks are difficult to detect. Some common types of tampering attacks are [39]:

1. *Data modification*: In this attack, the attacker personally modifies data in transit or at rest, resulting in unauthorized changes to sensitive information.
2. *Session hijacking*: In this type, an attacker takes control of a user's session by stealing the user's session ID or cookie and using it to access to the user's account or data.
3. *Code injection*: It is a type of attack in which the attacker puts malicious code into software or application that is supposed to be safe. This lets the attacker change how the software or application works.

To protect against tampering attacks, it is essential to implement security measures such as data encryption, digital signatures, secure coding practices, and access control that limits access to sensitive information. Additionally, monitoring network traffic and system logs for suspicious activity can help detect and prevent tampering attacks [37].

### 4.7 Privacy Leaks

Privacy leaks, or privacy breaches, occur when sensitive or personal information is unintentionally or intentionally released to unauthorized parties. Here are some of the most common types of privacy leaks [14]:

1. *Data breaches*: In a data breach, an attacker gains unauthorized access to sensitive data, potentially compromising personal information such as names, addresses, social security num-

bers, and credit card information.

2. *Phishing attack*: In this type of attack, the attacker sends an email or message that appears to be from a trusted source, tricking the recipient into providing sensitive information such as passwords, and credit card numbers.
3. *Metadata leaks*: In this attack, information about a user's online activity, such as browsing history or location data, is inadvertently released to unauthorized parties.

Privacy leaks can have serious consequences, including identity theft, financial loss, and reputational damage. To protect against privacy leaks, it is essential to implement security measures such as data encryption, access controls, and employee training programs to raise awareness about the risk of privacy breaches. Additionally, monitoring systems for suspicious activity and promptly reporting and responding to privacy breaches can help mitigate their impacts [33].

### 4.8 Hijacking Attacks

This attack utilizes controller resources (i.e., data-to-control plane). The attackers aim to slow down certain network parts or make them inaccessible using controller reserves [24]. Some types of hijacking attacks are:

1. *Cross-site scripting (XSS)*: In an XSS attack, the attacker injects malicious code into a legitimate website, allowing them to steal user information or take control of the user's session.
2. *Clickjacking*: In this attack, the attacker tricks the user into clicking on a link or button that performs an unintended action, such as granting the attacker access to the user's account or downloading malware.
3. *Password cracking*: In a password cracking attack, the attacker uses automated tools to guess a user's password or steal a password through phishing or other means.
4. *Brute-force attacks*: In a brute-force attack, the attacker attempts to gain access to a user account by repeatedly guessing the password or other authentication information.

To protect against hijacking attacks, it is crucial to implement security measures such as multi-factor authentication, data encryption, and access control to limit access to sensitive information. Additionally, monitoring systems for suspicious activity and promptly reporting and responding to hijacking attacks can help mitigate their impact.

### 4.9 Side-Channel Attack

In 5G networks, the physical infrastructure and reserves are shared across multiple slices, enabling side-channel attacks on 5G network slices [12]. This attack arises when the transducer considers specific physical patterns and features, such as power consumption, to obtain sensitive data [31]. While 5G is based on network slicing, the attacker could effortlessly select a slide from it and study its performance [34]. The following are some examples of side-channel attacks:

1. *Power analysis attacks*: These attacks involve measuring the power consumption of a device during cryptographic operations to extract sensitive information.
2. *Timing attacks*: These attacks involve analyzing a system's time to perform a cryptographic operation to deduce information about the secret keys.

To prevent side-channel attacks, system designers can use various techniques, such as implementing countermeasures like adding noise to the system or using a constant-time algorithm. Reducing information leakage through proper system design and using physical security measures to prevent unauthorized access to the system [32].

### 4.10 HX-DoS Attack

This attack combines HTTP and XML messages that the attacker deliberately sends into the flood script and demolishes the cloud service provider's communication channel capability [39]. These attacks can overwhelm the web server's resources, making it unavailable to legitimate users. Here are some common types of HX-DoS attacks [33]:

1. *HTTP GET flood attacks*: This attack involves sending many HTTP GET requests to a web server, which can cause the server to consume significant resources attempting to respond to each request.
2. *HTTP flood attack*: The attacker floods the server with many HTTP requests, causing the server to consume significant resources attempting to respond to each request.
3. *HTTP fragmentation*: This attack involves sending broken HTTP requests to a web server, which can use up many resources as the server tries to back together each request and process it.

To prevent HX-DoS attacks, web server administrators can use various techniques, such as implementing rate limiting, blocking suspicious IP addresses, using content delivery networks (CDNs) to distribute traffic, and using DDoS mitigation services [40].

### 4.11 Malware Attack

At times, the enemy performs mischievous scripts on the remote system to carry out several illegal behaviors like theft, deletion, update, and encoding of important material [12]. Malware comes in many forms, including viruses, worms, keyloggers, spyware, ransomware, and Trojan horses [41]. They are also used to observe customer behavior without their knowledge. Here are some examples of malware attacks [36]:

1. *Virus*: A virus is malware designed to replicate itself and infect other files or systems. Viruses can damage the system, steal private information, or open a back door for different types of malware to get in.
2. *Trojan*: A Trojan, or Trojan horse, is a type of malware disguised as a legitimate program or file. When the Trojan runs, it can give the attacker remote access, steal sensitive information, or change the system's settings.
3. *Worm*: A worm is malware designed to self-replicate and spread to other systems, often through network vulnerabilities. Worms can do much damage to systems and networks because they can use up many resources and overload servers.
4. *Ransomware*: Ransomware is malware that encrypts a victim's files or locks them out of their system, demanding payment in exchange for access to their files or system. Ransomware attacks can be highly disruptive and costly to businesses and individuals.

1. *Spyware*: Spyware is malware designed to monitor a user's activity and steal sensitive information, such as login credentials or financial data. It can be used for identity theft, corporate espionage, or other malicious activities.
2. *Rootkit*: A rootkit is malware designed to hide its presence and activity from the user and security software. It can give attackers remote access to the system, which means they can do bad things without being caught.

To prevent malware attacks, users and organizations can implement various measures, including anti-malware software, keeping software and systems up-to-date, practicing safe browsing and email habits, and using strong and unique passwords [37].

### 4.12 Botnet Attack

A botnet is a type of malware that could influence a set of internet-linked gadgets [42]. Mobile botnets can automate multiple mobile ends to execute several attacks, i.e., DoS on 5G systems. The threat is growing as 5G networks interconnect high-powered mobile phones. Here are some common types of botnet attacks [14]:

1. *Spamming*: A botnet can send large volumes of spam emails, often promoting fraudulent products or services.
2. *Click fraud*: A botnet can make fake clicks on online ads, which makes it more expensive for real businesses to advertise.
3. *Credential stuffing*: A botnet can make credential stuffing attacks, in which stolen login information from one website is used to try to get into other websites and services without permission.
4. *Cryptocurrency mining*: A botnet can be used to mine cryptocurrencies. It makes money for the attackers by using the computing power of the compromised computers.

To prevent botnet attacks, users and organizations can take various measures, including keeping software and systems up-to-date, using strong and unique passwords, and anti-malware software, and implementing network segmentation and access controls. Organizations can also implement DDoS mitigation strategies, such as using content delivery networks (CDNs) or working with DDoS mitigation service providers [36].

### 4.13 Insider Attack

An insider attack is initiated by an internal user authorized to use the attacked system. In this malign action, the authorized user manipulates the stored information to reveal other severe attacks like session key computation and password guessing attacks [11]. The following are the common types of insider attacks:

1. *Malicious insider attacks*: These attacks are carried out by insiders who intentionally cause harm to the system or organization. Malicious insiders can use their access to steal sensitive information, introduce malware, damage systems, or sabotage operations.
2. *Compromised insider attack*: This attack occurs when an insider's credentials or access are stolen or compromised by an external attacker. It can happen through phishing, social engineering, or other tactics, allowing the attacker to carry out malicious activities using the compromised credentials.
3. *Third-party insider attack*: This attack occurs when an insider from a third-party organization, such as a vendor or contractor, uses their access to cause harm to the system or organization. Third-party insiders have access to sensitive data or systems, and their actions can be challenging to monitor and control.

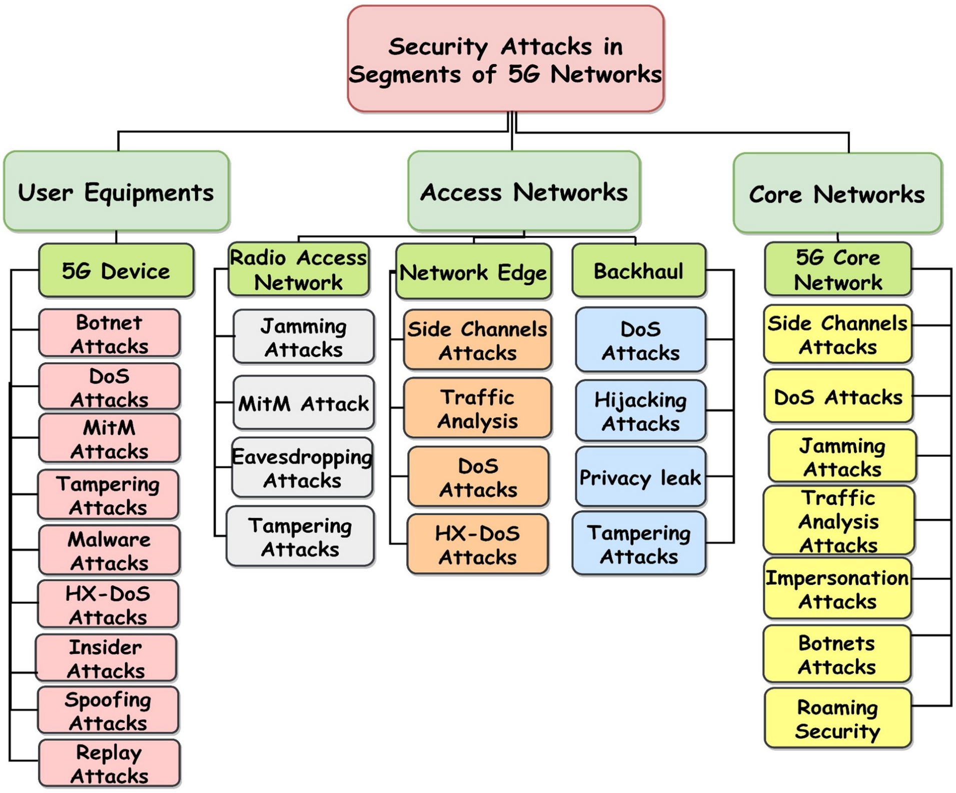

**Figure 3**. Security attacks in segments of 5G networks

Organizations can implement various measures to prevent insider attacks, such as access controls, monitoring and logging of user activities, employee training, awareness programs, and security audits and assessments. It is also essential to maintain a security culture and foster open communication between employees and security teams to identify and address potential insider threats [33].

### 4.14 Traffic Analysis Attack

This attack is similar to the eavesdropping attacks. In this attack, the attacker intercepts and substitutes messages [12]. The attacker listens to network traffic to perform traffic analysis and determines the location of key nodes, routing structure, and application behavior forms [15]. There are several types of traffic analysis attacks, including [5]:

1. *Timing analysis*: This type of attack involves analyzing the timing of network traffic to determine communication patterns. For instance, an attacker could determine when a specific user is likely to be online by looking at when they talk.
2. *Protocol analysis*: This type of attack involves analyzing the protocols used to transmit network traffic to determine the type of communication that is taking place. An attacker could, for example, find out if a user is going to a website or using a messaging app.
3. *Flow analysis*: This type of attack involves analyzing the flow of network traffic to determine which devices are communicating with each other. An attacker could, for example, find out which devices are talking to a specific server or network.
4. *Encrypted traffic analysis*: This type of attack involves analyzing encrypted network traffic to determine the content of the communication. For example, an attacker could use timing analysis to determine when encrypted traffic is being transmitted and protocol analysis to determine the type of communication taking place.

Preventing traffic analysis attacks can be challenging, as these attacks often rely on analyzing patterns and behaviors inherent to network traffic. However, several steps can be taken to reduce the risk of being a victim of a traffic analysis attack, like using encryption, traffic obfuscation techniques, limiting the amount of data you share, using network segmentation, regularly updating and patching software, and using a network monitoring tool. It can help prevent further damage to the network [40].

### 4.15 Replay Attack

Replay attacks occur when a cybercriminal listens to a secure network connection, intercepts it, and then fraudulently delays or mislead the receiver [13]. It happens when the attacker exchanges messages and fraudulently delays the recipient by confusing them [25]. There are several types of replay attacks, including [5]:

1. *In a simple replay attack*: An attacker records a data packet and then sends it again later to reach a particular goal, like getting into a network or stealing information.
2. *Man-in-the-middle (MitM) replay attack*: In a MitM replay attack, an attacker intercepts data packets between two devices and then replays them to one or both devices. The attacker can then use the response from the device to gain unauthorized access or steal information.
3. *Sequence number replay attack*: In a sequence number replay attack, the attacker intercepts and records a data packet, including its sequence number. The attacker then sends the same packet with the recorded sequence number to the destination, potentially causing the destination device to accept the packet as a valid and authentic message.

It is important to use secure communication protocols that protect against replay attacks, such as Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP). Network security tools like firewalls and intrusion detection systems can also help find and stop replay attacks [43].

### 4.16 Impersonation Attack

In this malicious activity, the attacker effectively verifies the uniqueness of the actual party communicating, generates a message, and transmits it to the receiver on behalf of the actual communicating party [14]. There are several types of impersonation attacks, including [32]:

1. *Phishing*: In a phishing attack, an attacker sends an email or other communication that appears to come from a legitimate source, such as a bank or a social media site. Usually, the message has a link to a fake website or a malicious attachment that can be used to steal login information or other sensitive data.
2. *Spear phishing*: This is a more targeted form of phishing attack directed at a specific individual or group. The attacker will usually look up information about the target to make the message seem more real, like using the person's name, job title, or other personal information.
3. *Whaling*: This is a type of spear phishing attack that is directed at high-level executives or other senior personnel within an organization. The attacker will typically use social engineering tactics to gain the target's trust and then use this to trick them into revealing sensitive information or authorizing fraudulent transactions.

It is essential to use robust authentication mechanisms, such as multi-factor authentication, to verify the identity of users and devices. Additionally, security awareness training can help employees recognize and avoid phishing and other types of impersonation attacks. Other preventive measures include implementing access controls, monitoring network traffic for suspicious activity, and maintaining up-to-date antivirus and anti-malware software [43].

## 5 Usage Scenarios for 5G and Security Risk of 5G Usage Scenarios

ITU-R defined three usage scenarios for 5G. These involve enhanced mobile broadband, ultra-reliable and low-latency, and massive machine-type communications [44].

### 5.1 Enhanced Mobile Broadband (eMBB)

eMBB use cases were utilized to arrange smooth coverage and high flexibility scenarios with significantly increased data rates, higher user density, hotspots, and enhanced data rates [45]. It concentrates on applications with significantly higher bandwidth needs. Presently, 4K/8K higher classification video and mobile roaming facilities centered on virtual reality (VR) and augmented reality (AR) have been developed in the eMBB application type [46]. The significant security risks for eMBB are as follows:

#### 5.1.1 The Collapse of Monitoring Means

eMBB applications generate enormous amounts of traffic, creating particularly challenging situations for safety devices [5], such as firewalls and intrusion detection. These safety features are added to existing systems to ensure that traffic recognition, radio coverage, and information storage have enough security [47].

#### 5.1.2 Privacy Leakage

5G contains many of personal information, such as personal data, device information, and address information. The openness of 5G networks has increased the probability of the leakage of private information.

### 5.2 Massive Machine-type Communications (mMTC)

mMTC is employed for IoT and requires lower power utilization and data rates for many linked devices [44]. This landscape of 5G adopts IoT applications that connect large-scale devices used in intelligent transport, grids, and cities [45]. mMTC experienced lower costs, large-scale expansion [40], and insufficient IoT resources [5]. The significant security risks of mMTC are the following:

#### 5.2.1 Remote Controls

Attackers can remotely access and control IoT terminals via software and hardware interfaces and then capture terminals to initiate network attacks by taking advantage of their simplicity and vulnerable security capabilities [48].

#### 5.2.2 Fake Terminals

IoT terminals have inadequate resources and ineffective processing and computing abilities. Hence, authentication may not occur, which could lead to the same terminals and confuse the operation of IoT applications [49].

#### 5.2.3 Eavesdropping and Data Tempering

Attackers interfere with the data by accessing the terminals remotely. Weak transmission paths lead to privacy threats by controlling the data at the terminals.

### 5.3 Ultrareliable and Low-Latency Communications (uRLLC)

uRLLC accommodates security and mission-critical applications of 5G [44]. It focuses on the delay, which is susceptible to a 5G network. uRLLC services need a higher degree of protection with no communication delays. There must be no delay and greater consistency for autonomous driving, remote controls, and industrial internet [46].

#### 5.3.1 Data Security Risk

Attackers exploit vulnerabilities in devices and protocols via network information broadcast routes (air interfaces, the core networks of (5G)) to interfere by replaying application information [5], causing data transmission vulnerabilities and disrupting regular application operations [14].

#### 5.3.2 DDoS Attacks

Attackers may utilize DDoS attacks to cause network or communication congestion, causing the failure of services.

## 6 Intelligent Applications of 5G and Specific Use Cases of These Applications

The fifth generation allows for various intelligent applications, including smart manufacturing, traffic, grids, IoT, and campuses. This section includes specific 5G applications and the usage case scenarios described in [5]. Figure 4 elaborates on 5G applications and the usage case scenarios of these scenarios.

### 6.1 Smart Manufacturing Enabled by 5G

Smart manufacturing can potentially maintain and improve performance in response to changing environments [50]. Listed below are 5G technology usage cases in the intelligent manufacturing sector.

#### 6.1.1 Services (VR/AR and HD Video) to the Cloud: eMBB Scenario

The advent of eMBB allows for digital life. It describes bandwidth-intensive facilities like high-definition video and virtual or augmented reality (VR or AR), higher bandwidth characteristics, and edge computing technology [5]. It can integrate terminal-side video into the cloud for in-depth evaluation, error recognition, optical character recognition deciphering, AR support, VR complicated assembly, and manufacturing security behavior assessment [46].

#### 6.1.2 Automatic Driving, Industry 4.0 and Remote Control: uRLLC Scenario

uRLLC is a compilation of ultra-latency-sensitive services, like automated driving and remote control [5]. The arrival of uRLLC indicates an intelligent future for the digital industry [42]. Low-latency characteristics, network slicing, and edge computing ensure precise network value in this scenario. It works as a remote control, like a robot, for remote engineering machinery and on-site construction line equipment [44].

#### 6.1.3 High Bandwidth Characteristics: mMTC Scenario

mMTC is well suited for complex connectivity scenarios such as intelligent transportation, grid, and manufacturing [5]. Digital society is shaping up with the help of mMTC. In this application, mass connection, higher bandwidth features, and edge computing technology gather sensor records at the factory and then transfer them to the cloud for in-depth investigation [45]. It links several kinds of traffic sensors and other IoT gadgets to evaluate the position of traffic infrastructure. It also generates timely warnings of traffic situations like monitoring, maintenance, inspection, and warning of smart road structures [46].

## 6.2 Smart Traffic Enabled by 5G

It includes automobiles, road structures, managing traffic services, transport scheduling, digital transport platforms, and multiple transport-centered applications [51]. Following are usage cases of 5G technology in the transport industry.

### 6.2.1 High-definition Video Capture for Face Recognition: eMBB Scenario

This application is centered on the capabilities of 5G, such as higher bandwidth communication, higher definition video capture, performing facial detection like security evaluation, and passenger exit with smart train station awareness [52].

### 6.2.2 Observe and Inspect Traffic Infrastructure with Sensor: mMTC Scenario

This application is centered on massive 5G connection features, attached to numerous traffic sensors [52] and other IoT gadgets to examine the position of traffic structures. This scenario creates timely awareness about situations by looking at information received, such as intelligent road monitoring, organization reviews, smart metro inspections, maintenance, and warnings [53].

### 6.2.3 Explore Pedestrian Flow and Accurate Positioning Facility: mMTC Scenario

This scenario analyzes pedestrian flow centered on operator access to the 5G base station [5]. It provides automobiles and individuals with precise positioning services such as high-precision position and indoor navigation [52]. The smart train station and metro traveler flow evaluation are based on the precise position of the 5G base station.

### 6.2.4 Remotely Controlled Driving: uRLLC Scenario

They are centered on 5G higher bandwidth, low-latency, and heavy link features. The latest technologies, like network slicing and edge computing, are utilized to meet the higher demands of remotely operated driving, such as autonomous driving [53].

## 6.3 Smart Grid Enabled by 5G

Smart grids use the two-way flow of power and data to generate broadly dispersed automated energy networks. Below are 5G technology usage cases in the smart grid industry [5].

### 6.3.1 Urgent Reply of the Power Grid: uRLLC Scenario

It is centered on the low-latency characteristics of 5G. It confirms the power net grid's emergency response, distribution network safety, and accurate load control based on slicing, edge computing, and other latest technologies [54].

### 6.3.2 Smart Inspection Videotape: mMTC Scenario

Based on 5G mass connection, higher bandwidth features [5], assemble inspection video and stream it to the cloud for in-depth evaluation such as distribution automation, progressive metering, intellectual assessment, and power grid backup transmissions [55].

## 6.4 Smart Campus Enabled by 5G

The smart campuses established on the IoT integrate daily activities and surveys. This application incorporated service procedures such as tutoring, scientific study, administration, and campus life [5].

### 6.4.1 Distance Dducation, Friend Robots and Early Child Education: eMBB Scenario

To distribute distance learning, 5G utilizes higher bandwidth characteristics [46]. Campuses can implement applications using the slicing technology of 5G, such as youth learning, friendly robots, and child development evaluation [5].

## 6.5 Internet of Things (IoT) Enabled by 5G

IoT is a term used by smart sensors in several specific applications. These sensors are linked to the controller via ethernet, cellular network, Bluetooth, or communication standards [12]. It will benefit 5G as it can communicate with various devices simultaneously, without delay, and with much greater convenience than before [35]. These gadgets can convey without the demand for a cable or Wi-Fi connection to link to the network [40].

### 6.5.1 5G Services to IoT: eMBB Scenario

This eMBB scenario endorses high-definition consumer video (for example, TV and gaming), deliver-

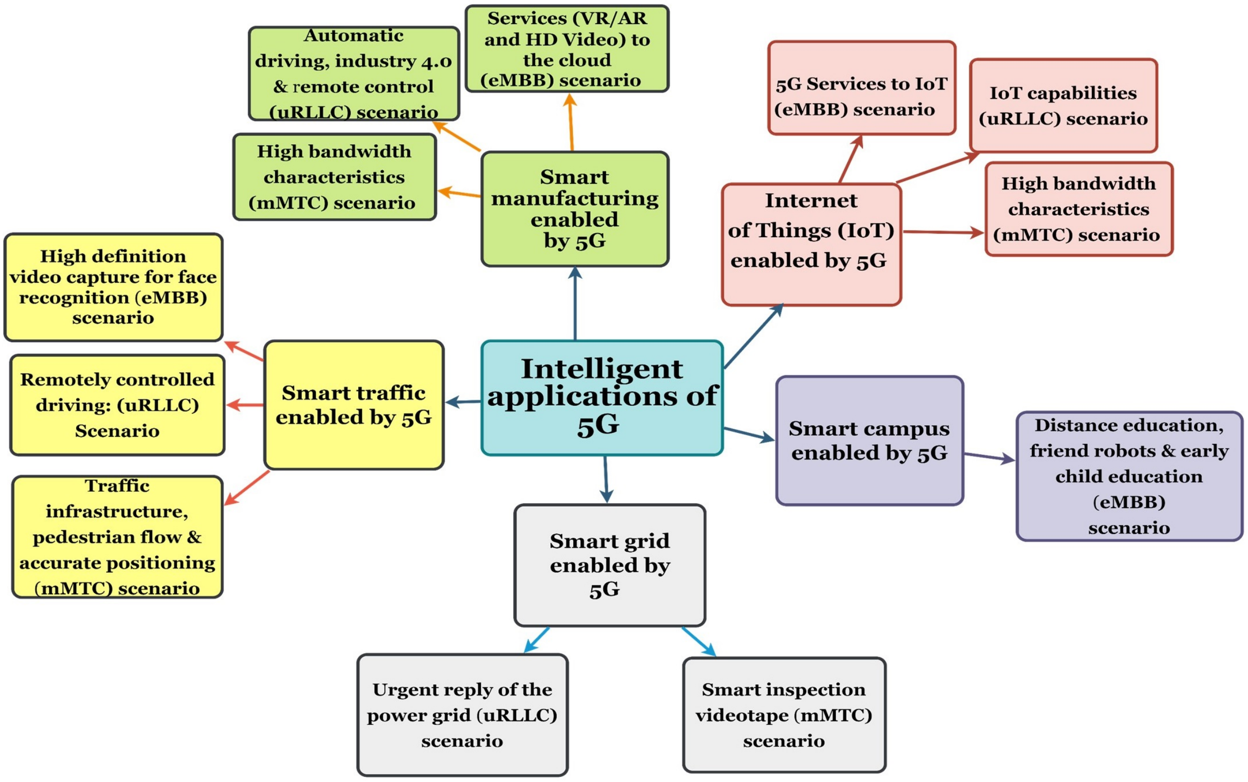
Automatic driving, industry 4.0 & remote control (uRLLC) scenario
Services (VR/AR and HD Video) to the cloud (eMBB) scenario
5G Services to IoT (eMBB) scenario
IoT capabilities (uRLLC) scenario
High bandwidth characteristics (mMTC) scenario
Smart manufacturing enabled by 5G
Internet of Things (IoT) enabled by 5G
High bandwidth characteristics (mMTC) scenario
High definition video capture for face recognition (eMBB) scenario
Remotely controlled driving: (uRLLC) Scenario
Smart traffic enabled by 5G
Intelligent applications of 5G
Smart campus enabled by 5G
Distance education, friend robots & early child education (eMBB) scenario
Traffic infrastructure, pedestrian flow & accurate positioning (mMTC) scenario
Smart grid enabled by 5G
Urgent reply of the power grid (uRLLC) scenario
Smart inspection videotape (mMTC) scenario

**Figure 4**. Intelligent applications and use case scenario of 5G networks.

ing high-speed, immersive communications such as video calling and conferencing and virtual reality [35]. It also offers smart city services such as monitoring IoT video cameras, high output IoT services, and reliable and secure (eMBB) [46]. It poorly updates the policies of suppliers and IoT devices, which makes the devices vulnerable and easy targets for attackers [47].

### 6.5.2 IoT Capabilities: uRLLC Scenario

uRLLC scenario is essential for enterprise IoT usage cases, the customer segment's smart city, and home products. Smart cities can use uRLLC IoT tools to manage traffic more efficiently, avoid overcrowding, alert accidents, and benefit road users [40]. In smart homes, uRLLC capabilities bring many profits when supporting online gaming and AR/VR gadgets [35]. Faster response times and higher consistency decrease transmission delays, giving a more immersive experience [34]. Less uncertainty in connectivity is essential for machines that perform complex tasks, such as autonomous vehicles [46]. The key challenge with IoT device security is the number of devices linked to the network. These devices are exceedingly small and have constrained computational power; the computational power decreases concerning energy utilization [47]. With the rest of the computing power, it is hard to employ reliable algorithms for information broadcast and more protection mechanisms [40].

### 6.5.3 High Bandwidth Characteristics: mMTC Scenario

IoT devices are often utilized in environments that are not autonomous. It gives a chance to the attacker, who obtains physical entry to the device, which can be damaged or tampered with [34]. Many IoT devices with limited security attract attackers [35]. Attackers can utilize IoT to generate a botnet of small sensors and comparable gadgets that launch destructive DDoS attacks under the botnet command [46]. One more dangerous type is a false data injection (FDI) attack [12]. In FDI attacks, truthful information is distorted, leading to a fake response by the IoT controller [40].

## 7 Steps to Reduce the Security Risk of Usage Scenarios in 5G and Intelligent Applications of 5G

Significant security risks of 5G usage scenarios include the collapse of monitoring means, privacy leakage, data security risks, unauthorized terminal access, and remote controls. The eMBB scenario focuses on applications with extremely high bandwidth require-

**Table 2**. Security risk and steps to reduce risk in usage scenarios of 5G [5], [40], [46].

| 5G usage scenarios | The security risk of 5G usage scenarios | Steps to Mitigate Risks |
|---|---|---|
| eMBB scenario | The collapse of monitoring means | • Use traffic-supervising applications at nodes of edge computing to interrupt higher-risk facilities. |
| | Privacy leakage | • The application and terminal platform maintain secondary identity authentication and approval. |
| | | • Manage the security key to encrypt and protect user data. |
| uRLLC scenario | Data security risk | • Use edge computing safety features such as information security reliability and serial numbers. |
| | DDoS attack | • Use 2-way identity verification among the operator endpoint and the application servers. |
| | | • Utilize anti-DDoS facilities. |
| mMTC scenario | Fake terminal | • Utilize practical algorithms for safety measures to execute two-way authentication. |
| | Remote controls | • Use techniques to monitor security, intelligently identify, and prevent large IoT devices from being controlled. |
| | Eavesdropping and data tampering | • Encode and defend the reliability of confidential information generated at the IoT endpoint. |

ments, mainly including the following security risks; the collapse of monitoring means and privacy leakage. As 5G contains a large amount of personal information, the openness of 5G networks has increased the probability of leakage of private information. Massive traffic volumes make it extremely difficult for security devices to protect data. The uRLLC scenario focuses on services sensitive to delays and highly reliable, mainly including data security risk and DDoS attacks. On the network side of 5G, attackers use insecure devices and protocols, resulting in decreased data transmission reliability and network harm. The mMTC scenario includes a fake terminal and remote controls. Weak transmission leads to privacy breaches by manipulating the data at the terminals. Also, attackers interfere with the data by controlling and accessing the terminals remotely. Based on the above description, this research section discusses the specific security risks and steps to reduce the security issues of 5G intelligent applications. Table 2 shows the description of security risks and proposed steps to mitigate these risks in usage scenarios of 5G.

Table 3 displays security risks and steps to reduce security risks in specific use cases of intelligent applications based on the above reviews.

## 8 Conclusion

As communication technology develops and moves toward the future, there is a need to increase and secure communication. 5G is profoundly incorporated into social life and vertical industries. The security of 5G is affected by application designers, service contributors, network operatives, and device providers [4]. This research examines major security attacks on 5G and particular 5G applications like smart manufacturing, transport, grids, IoT, and campus. This article evaluates security risks and specific usage scenarios for user equipment, access networks, and core networks. This research also examined the security risks of 5G applications in the eMBB, uRLLC, and mMTC and proposed steps to mitigate usage scenarios for 5G. Overall, this study provides a thorough report on security risks associated with 5G applications, improves readers' knowledge about security risks, and positively influences the healthy and viable growth of several applications in the 5G era. The main contributions of this study are listed below:

- *Study of the Evolution of Mobile Networks*: The study discussed the evolution of mobile networks and their respective security constraints.

**Table 3**. Security risk and steps to reduce the security risk of specific use cases of intelligent applications [5].

| Intelligent applications of 5G | Specific use cases of 5G intelligent applications | The security risk of specific use cases of intelligent applications | Steps to reduce risk |
|---|---|---|---|
| Smart manufacturing enabled by 5G. | AR assistance, VR complex assembly | Fake terminals and the collapse of monitoring means. | Utilize efficient algorithms; encode data; two-way verification process and anti-jamming methods. |
| | High bandwidth characteristics of sensor data | Data tampering and eavesdropping, jamming | |
| | Automatic driving, Industry 4.0 and Remote control | DDoS attacks and remote control | |
| Smart traffic enabled by 5G. | Using high-definition video capture for face recognition and remotely controlled driving | DoS attacks and data security risks | Utilize traffic observing applications to find high-risk services; use methods to monitor the security and distantly control driving. |
| | Observe and inspect traffic infrastructure (pedestrian flow and positioning facility) with sensor. | Roaming security, the collapse of monitoring means | |
| Smart grids enabled by 5G. | Smart inspection videotape | DoS attacks<br>Fake terminals | Use the process of two-way verification and anti-DDoS facilities |
| | Urgent reply of the power grid | The collapse of monitoring means | |
| Smart campus enabled by 5G. | Distance education, friend robots and early child education | The collapse of monitoring means, spoofing, Jamming, malware, and privacy leakage | Use efficient algorithms, secondary identity authentication, use techniques to monitor and identify malicious attacks |
| IOT enabled by 5G | High-definition consumer video | DoS attacks and data security risks, jamming, spoofing | Maintain secondary identity authentication; |
| | High bandwidth characteristics | Data tampering and data eavesdropping, malware | encode user information for security; use efficient algorithms and methods to detect malevolent attacks. |
| | IoT capabilities | Fake terminals, MITM | |

- *The security model for 5G*: The study examined the security model of 5G communication.
- *Attacks on 5G security*: The study looked at the different security problems that can happen with 5G communication.
- *Highlight the key use cases*: The study identified usage scenarios for 5G communication.
- *Security risk according to the usage scenarios of the 5G network and applications*: The study identified and discussed security vulnerabilities in 5G networks with different segments, such as user equipment, access networks, and core networks. Intelligent applications of 5G and specific usage cases of these applications are also discussed about smart manufacturing, traffic, the grid, and campuses. Further, the study proposes steps to reduce risk in usage scenarios and applications of 5G.

## References

[1] M. Taheribakhsh, A. H. Jafari, M. M. Peiro, and N. Kazemifard. 5G Implementation: Major Issues and Challenges. In *2020 25th International Computer Conference, Computer Society of Iran, CSICC 2020*, pages 1–6, 2020. doi:10.1109/CSICC49403.2020.9050110.

[2] S. Sicari, A. Rizzardi, and A. Coen-Porisini. 5G In the internet of things era: An overview on security and privacy challenges. In *Computer Networks*, vol. 179, papes 1–19, 2020. doi:10.1016/j.comnet.2020.107345.

[3] D. Fang, Y. Qian, and R. Q. Hu. Security for 5G Mobile Wireless Networks. In *IEEE Access*, vol. 6, pages 4850–4874, 2017. doi:10.1109/ACCESS.2017.2779146.

[4] S. Adhikari. Intelligent Cyber Defense in 5G Augmented Aviation Cybersecurity Framework. In *AIAA Scitech 2021 Forum*, page 0661, 2021. doi:10.2514/6.2021-0661.

[5] Q. Qiu, S. Liu, S. Xu, and S. Yu. Study on Security and Privacy in 5G-Enabled Applications. In *Wirel Commun Mob Comput*, vol.2020, pages 1–15, 2020. doi: 10.1155/2020/8856683.

[6] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5G Security Challenges and Solutions. In *IEEE Communications Standards Magazine*, vol.2, no.1, pages 36–43, 2018. doi:10.1109/MCOMSTD.2018.1700063.

[7] C. Benzaïd, and T. Taleb. AI for beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?. In *IEEE Netw*, vol. 34, no. 6, pages 140–147, 2020. doi:10.1109/MNET.011.2000088.

[8] R. Ahmed, and M. A. Matin. Towards 6G wireless networks-challenges and potential technologies. In *Journal of Electrical Engineering*, vol. 71, no. 4, pages 290–297, 2020. doi:10.2478/jee-2020-0040.

[9] M. Agiwal, A. Roy, and N. Saxena. Next generation 5G wireless networks: A comprehensive survey. In *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3. Institute of Electrical and

Electronics Engineers Inc., pages 1617–1655, 2016. doi:10.1109/COMST.2016.2532458.

[10] Y. E. Kim, Y. S. Kim, and H. Kim. Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network. In *Sensors*, vol. 22, no. 10, pages 1–21, 2022. doi:10.3390/s22103819.

[11] S. Khan Tayyaba, and M. A. Shah. 5G cellular network integration with SDN: Challenges, issues and beyond. In *Proceedings of 2017 International Conference on Communication, Computing and Digital Systems*, pages 48–53, 2017. doi:10.1109/C-CODE.2017.7918900.

[12] M. Wazid, A. K. Das, S. Shetty, P. Gope, and J. J. P. C. Rodrigues. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges and Future Research Roadmap. In *IEEE Access*, pages 4466–4489, 2020. doi:10.1109/ACCESS.2020.3047895.

[13] D. Soldani. 5G and the Future of Security in ICT. In *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–8, 2019.

[14] S. Kwon, S. Park, H. J. Cho, Y. Park, D. Kim, and K. Yim. Towards 5G-based IoT security analysis against Vo5G eavesdropping. In *Computing*, vol. 103, no. 3, pages 425–447, 2021. doi:10.1007/s00607-020-00855-0.

[15] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. In *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1. Institute of Electrical and Electronics Engineers Inc., pages 196–248, 2020. doi:10.1109/COMST.2019.2933899.

[16] A. Gupta, and R. K. Jha. A Survey of 5G Network: Architecture and Emerging Technologies. In *IEEE Access*, vol. 3. Institute of Electrical and Electronics Engineers Inc., pages 1206–1232, 2015. doi:10.1109/ACCESS.2015.2461602.

[17] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila. Security for 5G and beyond. In *IEEE Communications Surveys and Tutorials*, vol. 21, no. 4, pages 3682–3722, 2019. doi:10.1109/COMST.2019.2916180.

[18] A. Gohil, H. Modi, and S. K. Patel. 5G technology of mobile communication: A survey. In *2013 International Conference on Intelligent Systems and Signal Processing (ISSP 2013)*, pages 288–292, 2013. doi:10.1109/ISSP.2013.6526920.

[19] N. Panwar, S. Sharma, and A. K. Singh. A survey on 5G: The next generation of mobile communication. In *Physical Communication*, vol. 18, pages 64–84, 2016. doi:10.1016/j.phycom.2015.10.006.

[20] M. Jaber, M. A. Imran, R. Tafazolli, and A. Tukmanov. 5G Backhaul Challenges and Emerging Research Directions: A Survey. In *IEEE Access*, vol. 4. Institute of Electrical and Electronics Engineers Inc., pages 1743–1766, 2016. doi:10.1109/ACCESS.2016.2556011.

[21] R. N. Mitra, and D. P. Agrawal. 5G mobile technology: A survey. In *ICT Express*, vol. 1, no. 3, pages 132–137, 2015. doi:10.1016/j.icte.2016.01.003.

[22] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. 5G security: Analysis of threats and solutions. In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 193–199, 2017. doi:10.1109/CSCN.2017.8088621.

[23] 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. In *Journal of Network and Computer Applications*, vol. 101. Academic Press, pages 55–82, 2018. doi:10.1016/j.jnca.2017.10.017.

[24] P. Gandotra, and R. K. Jha. A survey on green communication and security challenges in 5G wireless communication networks. *Journal of Network and Computer Applications*, vol. 96. Academic Press, pages 39–61, 2017. doi:10.1016/j.jnca.2017.07.002.

[25] J. G. Andrews *et al.*. What will 5G be?. In *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pages 1065–1082, 2014. doi:10.1109/JSAC.2014.2328098.

[26] J. Qiao, X. Shen, J. Mark, Q. Shen, Y. He, and L. Lei. Enabling device-to-device communications in millimeter-wave 5G cellular networks. In *IEEE Communications Magazine*, vol. 53, no. 1, pages 209–215, 2015. doi:10.1109/MCOM.2015.7010536.

[27] S. Gupta, B. L. Parne, and N. S. Chaudhari. Security Vulnerabilities in Handover Authentication Mechanism of 5G Network. In *ICSCCC 2018 - 1st International Conference on Secure Cyber Computing and Communications*, pages 369–374, 2018. doi:10.1109/ICSCCC.2018.8703355.

[28] T. Q. Thanh, S. Covaci, and T. Magedanz. VISECO: An Annotated Security Management Framework for 5G. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11005 LNCS, pages 251–269, 2019. doi:10.1007/978-3-030-03101-5_21.

[29] H. -C. Chen, and S. -S. Kuo. Active Detecting DDoS Attack Approach Based on Entropy Measurement for the Next Generation Instant Messaging App on Smartphones. In *Intelligent Automation & Soft Computing*, vol. 25, no. 1, pages 217–228, 2019.

[30] C. R. Kumar, and V. E. Jayanthi. A Novel Fuzzy

Rough Sets Theory Based CF Recommendation System, 2019.

[31] B. Xiong, K. Yang, J. Zhao, and K. Li. Robust dynamic network traffic partitioning against malicious attacks. In *Journal of Network and Computer Applications*, vol. 87, pages 20–31, 2017. doi:10.1016/j.jnca.2016.04.013.

[32] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. In *IEEE Internet Things J*, vol. 6, no. 5, pages 8169–8181, 2019. doi:10.1109/JIOT.2019.2927379.

[33] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover. 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation. In *2018 IEEE International Conference on Communications Workshops, ICC Workshops 2018 - Proceedings*,pages 1–6, 2018. doi:10.1109/ICCW.2018.8403769.

[34] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. In *Mech Syst Signal Process*, vol. 135, pages 1–21, 2020. doi:10.1016/j.ymssp.2019.106382.

[35] A. J. Akinyoade, and O. T. Eluwole. The internet of things: Definition, tactile-oriented vision, challenges and future research directions. In *Advances in Intelligent Systems and Computing*, vol. 797, Springer Verlag, pages 639–653, 2019. doi:10.1007/978-981-13-1165-9_59.

[36] J. H. Park *et al.*. A Comprehensive Survey on Core Technologies and Services for 5G Security: Taxonomies, Issues, and Solutions. In *Human-centric Computing and Information Sciences*, vol. 11, 2021. doi:10.22967/HCIS.2021.11.003.

[37] . A. Dutta, and E. Hammad. 5G Security Challenges and Opportunities: A System Approach; 5G Security Challenges and Opportunities: A System Approach, 2020.

[38] A. Chonka, and J. Abawajy. Detecting and mitigating HX-DoS attacks against cloud web services. In *Proceedings of the 2012 15th International Conference on Network-Based Information Systems, NBIS 2012*, pages 429–434, 2012. doi:10.1109/NBiS.2012.146.

[39] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park. IoMT Malware Detection Approaches: Analysis and Research Challenges. In *IEEE Access*, vol. 7, pages 182459–182476, 2019. doi:10.1109/ACCESS.2019.2960412.

[40] S. Xu, Y. Qian, and R. Q. Hu. Privacy-Preserving Data Preprocessing for Fog Computing in 5G Network Security. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6, 2018. doi:10.1109/GLOCOM.2018.8647912.

[41] B. P. Kumar, G. Rampalli, P. Kamakshi, and T. Senthil Murugan. DDoS Botnet Attack Detection in IoT Devices. pages 21–27, 2023. doi:10.1007/978-981-16-9967-2_3.

[42] W. Xiang, K. Zheng, and X. S. Shen. 5G Mobile Communications, 2017. doi:10.1007/978-3-319-34208-5.

[43] C. R. Kumar, and V. E. Jayanthi. A Novel Fuzzy Rough Sets Theory Based CF Recommendation System, 2019.

[44] X. Shen. Device-to-device communication in 5G cellular networks. In *IEEE Network*, vol. 29, no. 2. Institute of Electrical and Electronics Engineers Inc., pages 2–3, 2015. doi: 10.1109/MNET.2015.7064895.

[45] M. A. Siddiqi, H. Yu, and J. Joung. 5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices. In *Electronics (Switzerland)*, vol. 8, no. 9. MDPI AG, pages 1–18, 2019. doi:10.3390/electronics8090981.

[46] M. El-Moghazi, and J. Whalley. IMT-2020 Standardization: Lessons from 5G and Future Perspectives for 6G, 2021. Available: https://ssrn.com/abstract=3901148.

[47] B. B. Haile, E. Mutafungwa, and J. Hämäläinen. A data-driven multiobjective optimization framework for hyperdense 5G network planning. In *IEEE Access*, vol. 8, pages 169423–169443, 2020. doi:10.1109/ACCESS.2020.3023452.

[48] D. Wang, and P. Wang. Two Birds with One Stone: Two-Factor Authentication with Security beyond Conventional Bound. In *IEEE Trans Dependable Secure Comput*, vol. 15, no. 4, pages 708–722, 2018. doi:10.1109/TDSC.2016.2605087.

[49] D. Wang, X. Zhang, Z. Zhang, and P. Wang. Understanding security failures of multi-factor authentication schemes for multi-server environments. In *Comput Secur*, vol. 88, pages 1–8, 2020. doi:10.1016/j.cose.2019.101619.

[50] T. Yoshizawa, S. B. M. Baskaran, and A. Kunz. Overview of 5G URLLC System and Security Aspects in 3GPP. In *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*, pages 1–5, 2019. doi:10.1109/CSCN.2019.8931376.

[51] M. A. Abu-Rgheff. 5G enabling technologies: Narrowband Internet of Things and smart cities, 2019.

[52] J. Salo, and M. Liyanage. Regulatory impact on 5G security and privacy. In *A Comprehensive Guide to 5G Security*, wiley, pages 399–419, 2018. doi:10.1002/9781119293071.ch17.

[53] N. Saxena, A. Roy, and H. Kim. Efficient 5G

Small Cell Planning With eMBMS for Optimal Demand Response in Smart Grids. In *IEEE Trans Industr Inform*, vol. 13, no. 3, pages 1471–1481, 2017. doi:10.1109/TII.2017.2681105.

[54] R. Sachan, N. Saxena, and A. Roy. An efficient hybrid scheduling scheme for impatience user in eMBMS over LTE. In *2013 International Conference on Computer Communication and Informatics*, pages 1–5, 2013. doi:10.1109/ICCCI.2013.6466266.

[55] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani. Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations. In *IEEE Communications Surveys and Tutorials*, vol. 21, no. 3, pages 2702–2733, 2019. doi:10.1109/COMST.2019.2910750.

**Shadab Kalhoro** received her B.S. degree in Telecommunication Department from Mehran University of Engineering and Technology (MUET) Jamshoro, Pakistan, and M.S. degree in Information Technology Department from MUET. She is currently pursuing his Ph.D. in Computer Science from Universiti Tunku Abdul Rahman, Kampar, Malaysia (UTAR), Perak, Malaysia. Her research interests include Cyber Security, Cyber Security Behavior, Wireless Communication, Wireless Sensor Network, and Cognitive Radio networks.

**Farhan Bashir Shaikh** is working as assistant professor at University of Sindh Larkana campus, Sindh, Pakistan. He has served as head of computer science department at Sindh university campus Dadu and Larkana. He received his B.S. degree from MUET Jamshoro, Pakistan and received M.S. degree from SZABIST, Islamabad, Pakistan. He is currently pursuing his Ph.D. in Computer Science from UTAR, Perak, Malaysia. His research interests include Information Systems, IT Security, Cyberbullying, Cloud Security, Human-Computer Interaction, and Information Systems Security.

**Anam Kalhoro** received her B.S. degree in the Department of Computer Science from Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST) Larkana Campus, Larkana, Pakistan. She is currently pursuing master of philosophy in department of Computer Science from University of Sindh, Jamshoro, Pakistan. Her research interests include Wireless Communication, Computer Networks, Artificial Intelligence, and Wireless Sensor Networks.

**Junaid-Ur-Rehaman Abbasi** received his B.S. degree in the department of Environmental Engineering from Mehran University of Engineering and Technology (MUET) Jamshoro, Pakistan, and M.S. degree in Environmental Engineering from (MUET). He is currently pursuing his Ph.D. in Environmental Engineering, Faculty of Engineering and Green Technology from Universiti Tunku Abdul Rahman, Kampar, Malaysia (UTAR), Perak, Malaysia. His research interests include Wastewater Treatment, Renewable Energy, Green Technology, Solid Waste Management, Climate Change, and Smart Cities.

**Ramesh Kumar Ayyasamy** (Senior Member, IEEE) received the Ph.D. degree in Information Technology from Monash University, Australia, in 2013. Starting from 2003 to 2008 and from 2013 to 2014, he worked as a Lecturer in Tamil Nadu, India, and Monash University, Malaysia, consecutively. Since 2015, he has been working as an assistant professor with the Faculty of Information and Communication Technology, Universiti Tunku Abdul Rahman, Malaysia. His research interests include Artificial Intelligence, Big Data Analytics, Cyberbullying, Deep Learning, Machine Learning, and Text Mining. He serving as a reviewer for different journals and conferences and a member of editorial boards.