International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

5 G Enabled Applications: Security and Privacy

Ayan Dhanda

Undergraduate Student, Computer Science Engineering, International Centre for applied Sciences (ICAS), Manipal Academy of Higher Education (MAHE)
Email: *ayandhanda74[at]gmail.com*

Abstract: ***5G applications face security risks due to the new technology used and the performance requirements of the specific application scenario. This paper analyzes the security requirements and presents hierarchical solutions for stakeholders to build secure 5G applications. Firstly, the technical characteristics and typical usage scenarios of 5G is summarized and then, the security and privacy risks faced by 5G applications and related security standards and research work is analyzed. In addition, the system reference architecture and overall security and privacy solutions for 5G applications has been elaborated upon. Finally based on the three major application scenarios of eMBB, uRLLC, and mMTC, specific suggestions for security and privacy risks along with a use case of industrial terminal access control have been presented before concluding the paper.***

Keywords: Enhanced Mobile Broadband (eMBB), Ultra Reliable and Low Latency Communications (uRLLC), Massive Machine type Communications (mMTC), Extensible Authentication Protocol, Network slicing

1. Introduction

The fifth-generation mobile network (5G) is a new generation mobile network that enables innovations and progressive changes across all vertical industries like smart grids and smart campus. 5G mobile communication technology is based on a new architecture. The 3rd Generation Partnership Project (3GPP) has provided complete system specifications for 5G network architecture (see Figure 1). Components of the core network can be instantiated multiple times to support virtualization technologies and network slicing. The architecture is driven by the motivation to remove the data overlay that has been traditionally used in previous generations of mobile networks. With the introduction of new key technologies such as network function virtualization (NFV), software-defined network (SDN), network slicing, multi access edge computing (MEC), mm-Wave communication, and massive MIMO the network support for various applications has drastically improved.

Based on the technology there are three new usage scenarios of 5G which are enhanced mobile broadband (eMBB), ultra reliable and low latency communications (uRLLC), and massive machine type communications (mMTC). The rich and diverse 5G applications and their broad development prospects initiate a new era of ubiquitous and intelligent internet and thus 5G will become the backbone of functions like energy, transport, banking, health and industrial control systems. As 5G new technology and the performance requirements of specific application scenarios bring about many security risks, security has become a priority when stakeholders develop 5G vertical applications. This paper is to research on the following aspects:

a) Analyzes the technical characteristics of 5G technologies and use cases of 5G applications. Then summarizes typical vertical applications enabled by 5G technologies, involving smart manufacturing, smart traffic, smart grid, and smart campus.

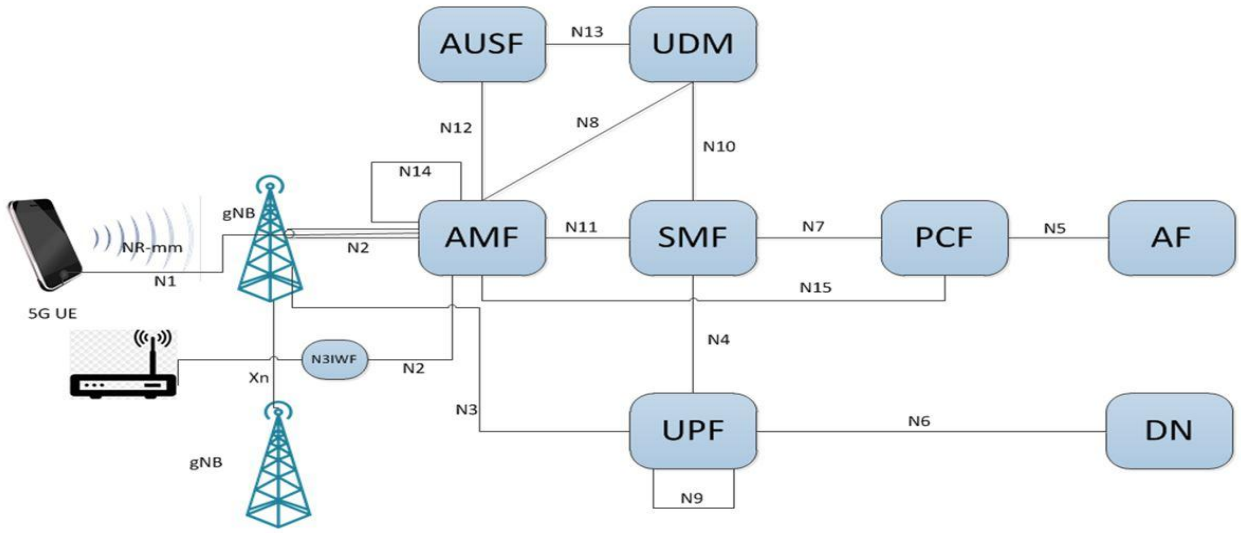

Figure 1: 5G Network Architecture

b) Analyzes the security and privacy risks faced by 5G applications, including privacy leakage in the eMBB scenario, DDoS attacks in the uRLLC scenario, and remote control in the mMTC scenario.
c) Analyzes the existing work for 5G application security, including security standards, security authentication frameworks and protocols, network slicing, and MEC security mechanisms. Particularly, secondary authentications for industry customers and three-factor authentications for mobile lightweight devices are studied.
d) Provides the system reference architecture for 5G applications, including the device layer, network layer, platform layer, and service layer, and summarizes security and privacy goals and corresponding solutions layer by layer.
e) Summarizes some specific suggestions in typical application scenarios, including secure deployment of edge computing node in the eMBB scenario, preventing application data from tampering/falsification/replay attacks in the uRLLC scenario, and lightweight equipment authentication in the mMTC scenario.
f) Provides a use case of industrial terminal access control for 5G application security by triple authentication.

2. Applications Enabled by 5G Related Techniques

5G enables a variety of intelligent applications, including smart manufacturing, smart traffic, smart grids, and smart campus. In Figure 2, the blue points are the typical 5G applications and the grey points are some specific use cases of these applications.

2.1 5G Enabled Smart Manufacturing

Smart manufacturing, today, is the ability to continuously maintain and improve performance, with intensive use of information, in response to the changing environments. The use cases of 5G technology in the field of intelligent manufacturing are listed below.

2.1.1 eMBB Scenario
Using 5G high-bandwidth features and edge computing technology, collecting terminal-side video to the cloud for deep analysis, such as defect detection, OCR decoding, AR assistance, VR complex assembly, production safety behavior analysis, and 5G PLC.

2.1.2 uRLLC Scenario
Utilizing 5G low-latency features, network slice, edge computing, and other new technologies to ensure network quality for remote and precise control, such as engineering machinery remote control, AGV control, robot control, and on-site production line equipment control.

2.1.3 mMTC Scenario
Using 5G mass-connection, high bandwidth characteristics, and edge computing technology, collecting sensor data in the factory and transmitting it to the cloud for deep analysis, such as 5G large-scale data collection.

2.2 5G Enabled Smart Traffic.

Smart traffic covers vehicles, road infrastructure, traffic management facilities, transportation planning, digital transportation platforms, and various transportation-based applications [1]. The use cases of 5G technology in the transportation industry [2] are listed below.

2.2.1 eMBB Scenario
Based on 5G high-bandwidth transmission capabilities, using high-definition video capture and transfer back to the application platform to perform face recognition, such as passenger behavior safety analysis and passengers exit without perception of smart train station.

2.2.2 mMTC Scenario
Based on the 5G massive connection characteristics, connect various types of traffic sensors and other IoT devices, to analyze the health status of traffic infrastructure, and timely alert traffic conditions by analyzing various types of data received, such as infrastructure monitoring and inspection, smart subway inspections and maintenance, and warning and management of smart roads.

2.2.3 uRLLC Scenario. Based on the high bandwidth, low latency, and massive connection characteristics of 5G, new technologies such as network slicing and edge computing are used to meet the high requirements of unmanned and remotely controlled driving, such as autonomous driving, smart ports, and smart airport.

2.2.4 Others
Based on the user's access to the 5G base station, analyze the pedestrian flow within the coverage of the base station, such as smart train station traffic transfer linkage and smart subway passenger flow analysis; based on the 5G base station's precise positioning function, to provide precise positioning services for vehicles and people, such as high precision positioning and high-precision indoor navigation.

2.3 5G Enabled Smart Grid

Smart grid uses two-way flows of electricity and information to create a widely distributed automated energy delivery network [3].

2.3.1 uRLLC Scenario
Based on 5G low-latency features, slicing, edge computing, and other new technologies, ensure emergency response of the power grid, such as distribution network differential protection, distribution network PMU, and precise load control.

2.3.2 mMTC Scenario
Based on 5G mass-connection, high bandwidth characteristics, and network slicing, edge computing technology, collect inspection video and transmit to the cloud for deep analysis, such as distribution automation of FTU, DTU, and TTU, advanced metering, intelligent inspection, and power grid emergency communications.

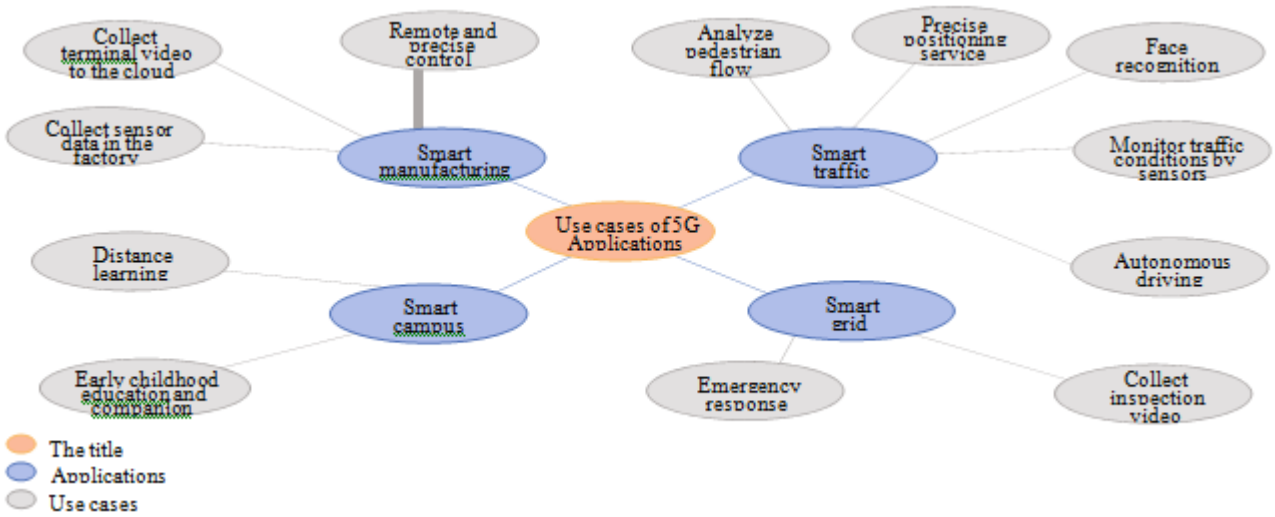

Figure 2: Use Cases of 5G Applications

2.4 5G Enabled Smart Campus.

Smart campus refers to a smart campus based on the Internet of things, which integrates work, study, and life. This integrated environment takes various application service systems as the carrier and fully integrates teaching, scientific research, management, and campus life.

3. Risk Analysis of 5G Applications

3.1 General Risks in 5G Applications

Security risks for general 5G applications mainly come from the device, network, edge, cloud, and centralized security O&M, as seen in Figure 3.

a) Major security risks on the terminal side include unauthorized terminal access, abuse of authorized SIM cards, and attacks and control of authorized terminals
b) Major security risks on the network side include network slicing isolation, misuse of slice resources, and theft and tampering of user-plane information
c) Security risks on the edge MEC side include vulnerabilities on the MEC platform, untrusted applications on the MEC, and attacks on the MEC from the Internet, enterprise cloud, and OM plane
d) (iv)Securityrisks on the enterprise private cloud include MEC-based attacks on the enterprise intranet and enterprise communication theft or tampering
e) Finally, from the perspective of O&M management, there are risks such as security posture awareness failure, unified management of security devices and policies, and lack of O&M audit

3.2 5G Specific Risks in Typical Usage Scenarios

3.2.1 eMBB Scenario

eMBB focuses on applications with extremely high bandwidth requirements. Currently, 4 K/8 K high-definition video and mobile roaming immersive services based on virtual reality (VR) and augmented reality (AR) have become the main application forms of eMBB, which mainly includes the following security risks:

a) Failure of Monitoring Means. eMBB applications produce huge volumes of traffic which would make it extremely difficult for security devices such as firewalls and intrusion detection systems deployed in existing networks to ensure adequate security protection when it comes to traffic detection, radio coverage, and data storage [5].
b) User Privacy Leakage. eMBB services (such as VR/AR) contain a large amount of user privacy information, such as personal information or identification, device identification, and address information, and the openness of 5G networks has increased the probability of leakage of private information [6].

3.2.2 uRLLC Scenario

uRLLC focuses on services that are extremely sensitive to latency, such as autonomous driving/assisted driving, remote control, and industrial Internet. Low latency and high reliability are the basic requirements. For example, if the internet of vehicles is subject to security threats in communications, it may cause danger of life. Therefore, uRLLC services require high-level security without additional communication delays. The main security risks are as follows:

a) DDoS Attacks. Attackers may use DoS/DDoS attacks to cause network congestion or communication interruptions, causing failure of services
b) Data Security Risks. Attackers use vulnerabilities in devices and protocols along network data transmission paths (5G air interfaces, core networks, and the Internet) to tamper with/forge/replay application data, causing the drop of data transmission reliability and harm to normal application operations

3.2.3 mMTC Scenario.

The 5G mMTC scenario supports IoT applications with massive devices being connected, such as smart transportation, smart grids, and smart cities. Due to the low cost, mass deployment, and limited resources (such as processing, storage, and energy) of the

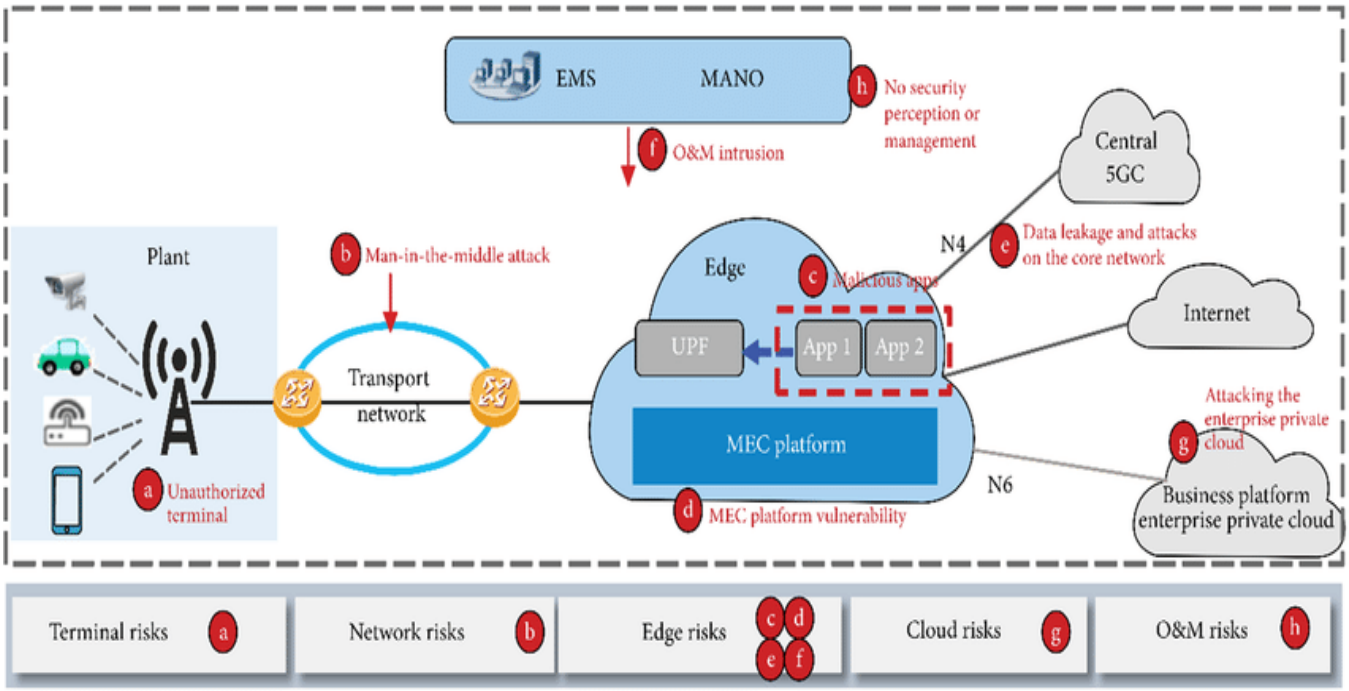

Figure 3: Risks to 5G applications in an end-to-end view.

Internet of things [7], the following security risks are common to IoT devices:

a) Counterfeit Terminals. The IoT terminal has limited resources and weak processing and computing capabilities. Therefore, it is likely that authentication would not be performed or a simple method has to be adopted [8,9], which brings opportunities for counterfeit terminals, causing confusion for the operation of IoT applications.
b) Data Tampering. Attackers may tamper with application data by exploiting weaknesses of the terminal and cloud/edge platform
c) Data Eavesdropping. The data collected by IoT terminals deployed in special environments (such as home environments and medical environments) involves user privacy. Weaknesses along data transmission paths may lead to user privacy breaches.
d) Remote Controls. Attackers may remotely access and control IoT terminals through software and hardware interfaces by taking advantage of the simplicity of IoT terminals and weak security protection capabilities, and then use the captured terminals to launch network attacks.

4. Related Work on Security of 5G Applications

4.1. Security Standards on 5G Applications

For 5G applications, the R16 standard released by 3GPP further enhances the quality and efficiency of 5G applications. For example, for Industrial Internet, new technologies are introduced to support 1 ms synchronization accuracy and 0.5-1 ms air interface delay, which can achieve end-to-end lower latency and higher reliability. For internet of vehicles, it supports the direct connection communication of V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure). By a variety of communication methods such as multicast and broadcast, as well as technologies such as optimized perception, scheduling and retransmission realize V2X (vehicle-to-everything) to support vehicle networking, semiautomatic driving, epitaxial sensors, remote driving, and other IoV (internet of vehicles) scenarios. For industry applications, the introduction of a variety of 5G air interface positioning technologies improves positioning accuracy by more than ten times and reach meter level. 5G applications involve various roles such as communication network providers, industry application providers, and security regulatory agencies. Currently, standards are mainly developed through collaboration between relevant parties to ensure application security. For 5G application security, major international standards organizations and industry associations have carried out research work, are given below:

3 GPP TS 22.261 service requirements for the 5G system:

a) R15 focuses on supporting eMBB services and basic uRLLC services and R16 enhances the ability and efficiency of network to support eMBB
b) R16 focuses on improving support for vertical industry applications, especially uRLLC and mMTC services.
c) 3GPP TS 33.501 security architecture and procedures for 5G system:The application layer access authentication and secure channel establishment in the IoTand the solution of authentication and session key management for upper-layer applications provided by 5G security certificate.

3GPP TR 33.819 study on security enhancements of 5GS for vertical and local area network (LAN) services: The security requirements and solutions of the 5G vertical industry. 3GPP TR 33.814 study on the security of the enhancement to the 5GC (5G core network) location services (LCS): The security threats and requirements and solutions of 5GC LCS. 3GPP TR 33.836 study on security aspects of 3GPP support for advanced V2X services: The security threats and requirements and solutions of IOV. 3GPP TR 33.825 study

on the security of ultra-reliable low-latency communication (URLLC) for 5GS: The security requirements and solutions of the uRLLC scenarios.

ITU-T X.1373 secure software update capability for intelligent transportation system communication devices: The software security update between the remote update server and the vehicle couplet and the process and content recommendations for security update.

ISO Criteria for the assessment of information security of connected vehicles based on ISO/IEC 15408:The security threats and security goals faced by connected vehicles and the security requirements and security function components.

4.2 Authentications in 5G Applications.

Security authentications face higher requirements in 5G applications. On the one hand, in order to protect the application data of power, industry, finance, and other important fields carried by 5G network, the concept of secondary authentication is proposed, that is, the authentication to establish data channel for accessing specific business after user authentication for access network. On the other hand, with the rapid development of 5G applications, mobile lightweight devices including laptops, smartphones, smartwatch, and other wearable devices are increasingly popular. It is necessary to concern the authentication for mobile lightweight devices and guarantee user privacy.

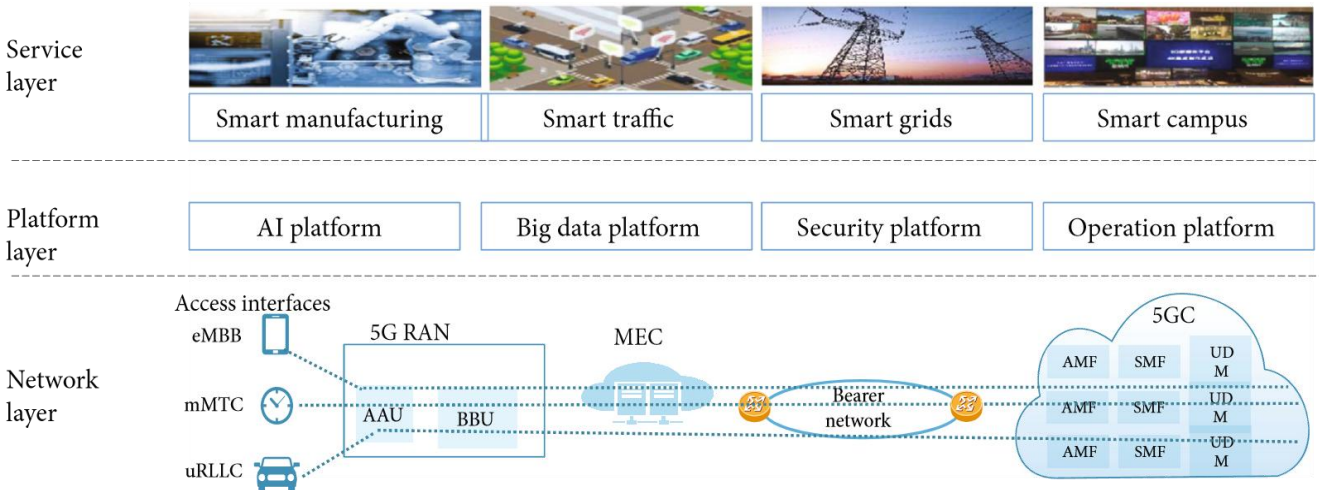

Figure 4: Reference architecture of 5G applications

To consumers			To business sectors			
Mobile phones	VR/AR	……	Instruments	Devices	Sensors	……

4.2.1 Secondary Authentications for Industry Customers.

In the implementation scheme based on the 3GPP standard [11], the protocol stack between the user terminal and the AAA (authentication, authorization, and audit) server is shown in Figure 5. The secondary authentication protocol between the UE and the AAA server is carried by EAP (Extensible Authentication Protocol). During the interaction of the secondary authentication protocol, AN (access network), AMF (Access and Mobility Management Function), SMF (Session Management Function), UPF (User Plane Function), and other network elements will not parse the secondary authentication protocol and can realize end-to-end secondary certification of users in enterprise and industry. Generally, industry customers deploying 5G applications can directly complete the secondary authentication by algorithms and protocols provided by telecommunication operators. 3GPP [11] defines a series of standard secondary authentication protocols, including PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), PPP (Point-to-Point protocol), AKA (Authentication and Key Agreement), and TLS (Transport Layer Security). PAP and CHAP use a relatively simple authentication mechanism. AKA and TLS are based on cryptographic algorithms and have designed a relatively blameless protocol to achieve user access authentication. In addition, based on the openness of 5G network capabilities, the AKMA [12] mechanism was proposed. The mechanism can provide authentication and session key negotiation services for third-party applications based on the access authentication system of the USIM card and carrier network and establish secure transmission channels from terminals to applications. Users with high-security requirements can also take advantage of the openness of 5G network capabilities and the industry-oriented feature and use customized secondary authentication algorithms and protocols to realize the self-controllable secondary identity authentication of the enterprise or industryaccess authentication system of the USIM card and carrier network and establish secure transmission channels from terminals to applications.Chen et al. [13] proposed a customized secondary authentication (Authentication and Key Agreement), and TLS (Transport Layer Security). PAP and CHAP use a relatively simple authentication mechanism. AKA and TLS are based on cryptographic algorithms and have designed a relatively blameless protocol to achieve user access authentication. In addition, based on the openness of 5G network capabilities, the AKMA [12] mechanism was proposed. The mechanism can provide authentication and session key negotiation services for third-party applications based on the access

authentication system of the USIM card and carrier network and establish secure transmission channels from terminals to applications. Users with high-security requirements can also take advantage of the openness of 5G network capabilities and the industry-oriented feature and use customized secondary authentication algorithms and protocols to realize the self-controllable secondary identity authentication of the enterprise or industry. Chen et al. [13] proposed a customized secondary authentication

Table 5: Countermeasures against security and privacy risks in 5G applications

Risks	Countermeasures	Related layer
eMBB scenario		
Failure of effective monitoring means	(i) Application traffic monitoring at edge computing [63] nodes, suspension of high-risk services in specific cases	(i) Network
User privacy leakage risk	i) Perform secondary identity authentication and authorization between the terminal and the eMBB application service platform (ii) negotiate and manage the service layer key to encrypt and protect user data (iii) physical isolation or encryption (iv) network slicing [55] or data dedicated line	(i) Terminal (ii) network (iii) service
uRLLC scenario		
DDoS attack risk	(i) Two-way identity authentication between the user terminal and the application servers (ii) Deploy anti-DDoS capabilities.	(i) Network l (ii) terminal
Data security risk	(i) Security capabilities deployed at edge computing, as well as data integrity protection, timestamp, serial number, etc. [6];	(i) Network
mMTC scenario		
Counterfeit terminal	(i) Using lightweight security algorithms, simple and efficient security protocols to implement two-way authentication	(i) Terminal
Data tampering and eavesdropping	(i) Encrypt and protect the integrity of sensitive application data generated by IoT terminals [6]	(i) Terminal
Remote control	(i) Deploy security monitoring methods to timely detect and prevent massive IoT devices from being controlled	(i) Terminal

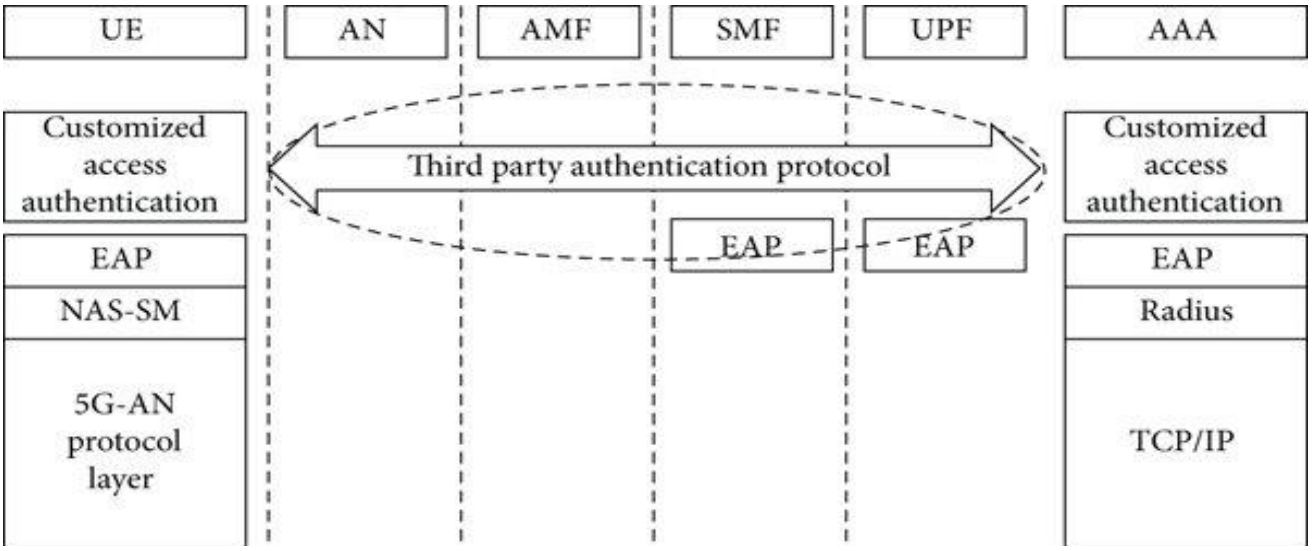

Figure 5: End-to-end protocol stack for secondary authentication

protocol, mainly using mobile terminals to collect biometric information such as fingerprints and irises of users and combined with the challenge-response identity authentication mechanism for identity authentication. Li et al. [14] proposed a secondary authentication protocol based on a symmetric cryptosystem that improves existing protocols such as AKA and provides user identity information protection, message integrity protection, and two-way authentication. Liu et al. [15] proposed an online identification technique with biological characteristic authentication and multimedia signal fast encoding over 5G to deal with the explosive growth in mobile data generated by huge equipment connections and a large number of new business and application scenarios.

4.2.2. Three-Factor Authentications for Mobile Lightweight Devices

Mobile lightweight devices can conveniently access cloud servers for online payment, video chatting, e-commerce, etc. At the same time, the openness of wireless network communication will also bring risks to the security and privacy of user data, so authentication for mobile light devices should be considered. Authentication and Key Agreement (AKA) protocols based on public key technology provide a secure communication mechanism for 5G application environments. It is essential to establish an AKA protocol to protect the conversation between mobile lightweight devices and remote servers. In 2018, Wang et al. [16] described the identity-based AKA protocols for privacy preserving of mobile devices and pointed out corresponding challenges. Moreover, Xiao et al. [17] proposed an improved AKA protocol based on chaotic maps and then a series of

AKA protocols based on chaotic maps [18-20] have been proposed. In addition, it is generally believed that the three-factor AKA protocol has better security performance than single factor and two-factor protocols. Since the existing three-factor AKA protocol cannot meet all the security requirements, it has become a research focus in recent years. Biometrics including fingerprint, face, iris, and others are invariable physiological characteristics that people own, and nowadays more and more mobile lightweight devices have the function of biometric recognition. In the face of stringent security requirements, the combination of traditional AKA protocol and the third authentication factor (i.e., biometrics) can achieve higher security. In order to solve the common security problems in the existing three-factor AKA protocol, Qiu et al. [21] designed a new three-factor AKA protocol by combining biometrics with chaotic mapping, using "Fuzzy Verifiers" and "Honeywords," which can achieve semantic security and meet the security evaluation criteria. Finally, it is proved that the new three-factor AKA protocol is more practical on mobile lightweight devices.

4.3. Other Research Focuses

As for the security architecture of 5G application, GTI (Global TD-LTE Initiative) released the security reference architecture of 5G smart city [22]. Zhou et al. [23] proposed the service architecture, PKI architecture, and multi-PKI mutual trust mechanism for 5G V2X communication security. Wang and Liu [24] analyzed 5G applications for special industries with high security levels and the security enhancement requirements and proposed a design scheme of security architecture based on special industry slices.

4.3.1 MEC

As for key security technologies of 5G application, MEC is the technology most closely related to 5G applications. According to ETSI [25], MEC architecture is divided into system level and host level. There is a remarkable resemblance of risks between MEC and cloud infrastructure, so their security measures are also similar. He et al. [26] proposed to enhance the isolation and access control by standardizing the configuration of infrastructure and application system, so as to improve the security protection ability of MEC nodes. At the same time, strengthen the security control of MEC applications. Zhuang et al. [27] analyzed the security threats, protection framework, and scheme of MEC from aspects of infrastructure, MEC platform, ME app, MEC scheduling and management system, and gateway of data plane.

4.3.2 Network Slicing

Network slicing is another important technology of 5G. Zhou [28] proposed four network slicing deployment schemes according to different requirements of cost, QoS, security levels, and network topology flexibility. Liu et al. [29] elaborated the existing risks of network slicing from the framework, management model, and implementation technology of network slicing and provided differentiated security services for 5G network slicing by establishing a security model. Chen et al. [30] proposed technical solutions to the security threats caused by the introduction of 5G into network slicing and proposed the security isolation of network slices, the secure access of terminal access slices, the security construction of network slices, and the security communication within the slices. The thesis [31] proposes 5G-SSAAC (5G Slice-Specific AAC), which enables 5G networks to provide various AAC mechanisms to the 3rd parties according to their security requirements.

5. Security and Privacy Solutions in a Systematic View

5G applications can be modelled into the terminal layer, network layer, platform layer, and service layer, as shown in Figure 4 above. Each layer has corresponding security goals and solutions. Solutions on Terminal Layer. A large number of 5G terminals have low power consumption, as well as limited computing and storage resources, which makes the deployment of complex security policies and control over the software difficult. Consequently, these limitations make the terminals become easy and likely targets to be hacked.

5.1.1. Prevent and Defend against DDOS Attacks

DDoS attacks may be initiated by hacked terminals or unintentionally caused by software defects or network faults. It is recommended that security defense mechanisms to be built at the network level for attack detection and self-protection to ensure that any DDoS attacks can be detected in time. Besides, active preventive measures are recommended in terminal exception handling and signaling registration.

5.1.2. Prevent Various Damage Caused by Exploited Terminals

For the prevention of risks brought by terminal hacking, it is recommended that certain security capabilities such as SSH security login, TLS transmission encryption, and built-in security chip are being built in terminals in terms of access authentication on the management and O&M plane as well as encryption protection on the signaling/data plane.

5.2 Solutions on Network Layer.

From the perspective of network components, the noteworthy aspects of network layer security include security in the RAN base station air interfaces [32], MECs, 5G Core, bearer networks, and 5G slices.

5.2.1. Base Station Air Interface Security

To prevent user data eavesdropping and tampering, SUCI and air-interface PDCP data packets encryption can be enabled. Besides, a DDoS detection and defense system and a unified rogue base station detection system can be deployed to avoid malicious attacks and interference.

5.2.2. MEC Security

To avoid physical attacks and cross network penetration and infection of network, 5G networks need to focus not only on the physical security control of MEC but also on the isolation between enterprise networks and operator networks. Security facilities such as firewalls and IPS are recommended for network boundary protection.

5.2.3 5GC Security

For MANO, EMS, etc., an access security control system is suggested to avoid unauthorized management and O&M

access. To prevent viruses and OS vulnerabilities caused by O&M terminals, desktop cloud terminals can be used. For the north-south border security of the network, firewalls, sandboxes, WAF, IPS, and anti-DDoS devices can be deployed in the data center. For the east west security, network micro segmentation, whitelist ACL, and network traffic probe ought to be deployed. Finally, it is recommended that host security scanning and hardening are being routinely implemented, and monitoring software is being deployed at the hypervisor level of servers to prevent VM escape [33-36].

5.2.4 Bearer Network Security

For network planning and design, redundancy design needs to be adopted to avoid single points of failure. Permission management and access authentication of accounts and passwords need to be implemented. Security measures such as MD5 authentication or SSL encryption can be configured to avoid possible routing protocol attacks such as BGP routing hijack attacks. Besides, IPsec encryption can be deployed to ensure the integrity of network data packets, to prevent illegal traffic interception or network replay attacks.

5.2.5 5G Slice Security

The security of 5G network slicing needs to be protected by isolation between slices. Besides, secure access and use of slices are also recommended. Access to a corresponding 5G network slice requires dual authentications and authorizations by the slice user (such as a government agency or an industrial mining enterprise) and the operator, ensuring legal access and use of slice resources. Moreover, the privacy protection of Network Slice Selection Assistance Information (NSSAI) needs to be provided.

5.3. Solutions on Platform Layer

The platform layer covers various intelligent analysis and processing AI platforms, big data platforms, and IT middle ground. The security of this layer includes the following aspects.

5.3.1. The Security of Communications Interfaces

In general, communication interface security at the platform layer mainly focuses on the routine maintenance and management of various accounts and passwords, such as regular password changes and password complexity requirements and the encryption of communications interfaces such as TLS.

5.3.2. The Security of Platform Data

The security of data at the platform layer involves the security of various basic data collected and stored by the big data platform, including data availability, integrity, and privacy. Availability is guaranteed by technologies such as data redundancy. Integrity is guaranteed by technologies such as data verification. For privacy, as the data amount is usually huge, more effective access control and security audit are required.

5.4 Solutions on Service Layer

The security of the service layer consists of various application system software security and secure O&M of application systems.

5.4.1. Software Security of the Application

Application system software security mainly involves scans for vulnerabilities and the improvement of software security (including the application software itself, OS databases, and other software systems), software operation logging, and software system high availability (HA) disaster recovery deployment (such as dual-host backup).

5.4.2. O&M Security of the Application

Secure O&M of application systems focus more on the operation and use of application systems and the security constraints and control of information on the operation management personnel, for example, application system login accounts and passwords, multifactor authentication for important and sensitive operations, permission-based operation access control, and physical security control of personnel access of O&M operations offices and equipment rooms.

6. Counter measures against Security and Privacy Risks in 5G Applications

Based on the systematic security and privacy solutions proposed above, the following specific security measures are recommended for 5G application service developers and providers in different application scenarios [37-39]. The related layers in the reference architecture to deploy these countermeasures are also suggested (see Table 5 above).

6.1. eMBB Scenario

Security risks in the eMBB scenario mainly include failure of effective monitoring means and user privacy leakage, and the countermeasures are as follows:-

1) Deploy application traffic monitoring at edge computing nodes and support the suspension of high-risk services in specific cases
2) The secondary authentication and key management mechanism are used to perform secondary identity authentication and authorization between the terminal and the eMBB application service platform to ensure the authenticity of the terminal and platform identity and the legality of the application. At the same time, negotiate and manage the service layer key between the two sides to encrypt and protect user data, thus preventing attackers from eavesdropping.
3) In applications with high-security requirements, the user plane of the 5G network can be protected by physical isolation or encryption to ensure the security of user data transmission between network functions
4) The network slicing or data dedicated line is used between the operator's 5G core network and the eMBB application service platform to establish a secure data transmission channel to ensure the security of user business data transmission.

6.2 uRLLC Scenario

Security risks in the uRLLC scenario mainly include the DDoS attack and the data security risk, and the corresponding countermeasures are as follows:

1) Establish a two-way identity authentication mechanism between the user terminal and the application server to prevent fake users from establishing connections
2) Deploy anti-DDoS capabilities to prevent network congestion, wireless interference, and communication link disruptions
3) Through the security capabilities deployed at edge computing, as well as data integrity protection, timestamp, serial number, and other mechanisms, to prevent application data from being tampered/-falsified/replayed and ensure the reliability of data transmission.

6.3. mMTC Scenario

Security risks in the mMTC scenario mainly include the counterfeit terminal, data tampering and eavesdropping, and remote control, and the corresponding countermeasures are as follows:

1) Using lightweight security algorithms, simple and efficient security protocols to implement two-way authentication between IoT terminals and the network to ensure that the access terminals are secure and reliable
2) Encrypt and protect the integrity of sensitive application data generated by IoT terminals to prevent attackers from eavesdropping, tampering, forging, and replaying business data on the transmission path
3) Deploy security monitoring methods to timely detect and prevent massive IoT devices from being controlled, to prevent these devices from being used maliciously, such as launching DDoS attacks on air interfaces and service platforms, causing network congestion and causing mMTC services to fail.

7. A Use Case of Industrial Terminal Access Control

7.1. Introduction and Security Requirements. This is a case of industrial terminal access control, as shown in Figure 5. The services include industrial machine vision for quality inspection that requires high bandwidth, automatic robot control, crane remote control, and unmanned transportation with real-time control requirement. Considering that the campus coverage area does not need to be large and high security is required when data cannot be transmitted out of the campus, the UPF and MEC are deployed at the local edge, and different service networks are isolated. This case involves several security requirements on terminal access controls.

(i) Prevent terminals such as 5G CPE, AGV, and gantry crane being attacked or illegally controlled (ii) Prevent CPEs being accessed by fake terminals, so that legal terminals (such as PLC) and the central control system would not be attacked

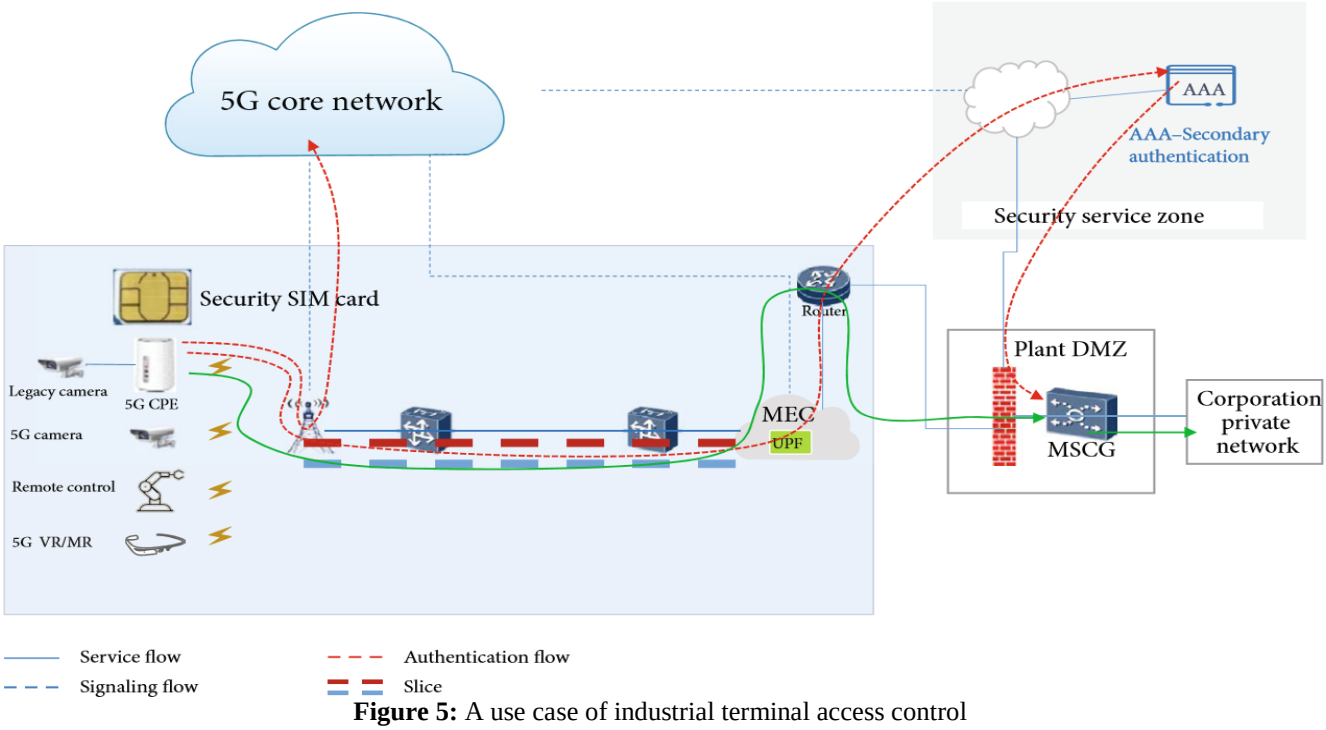

Figure 5: A use case of industrial terminal access control

7.2 Terminal Access Control Solutions

With the purpose that only authorized terminals can access the enterprise private network, the carrier and enterprise jointly provide triple authentication. First, carriers enable 5G AKA-based bidirectional authentications on the RAN side, leading the bidirectional authentication and encryption (5G AKA standard) between the 5G CPE/5G camera and the 5G network to prevent the fake terminals from accessing. Legacy cameras also must pass AAA authentication before accessing the CPE. Besides, configure the terminal whitelist and device-card binding on the core network to prevent unauthorized terminals and legal SIM card abusing. 5G CPE configured with MAC address list that allows access of

traditional cameras. Then, the core network binds the network slice to the terminal identity and the physical location that the terminal can access and also restricts access of specific terminals to slices. The mapping between IMSI and slice S-NSSAI is configured on the 5GC. Only terminals in the campus IMSI list can access slices. Mapping between the TAI (Tracking Area Identifier) list and campus slice SNSSAI configured on the 5GC, and only authorized terminals can access the enterprise private network within the campus. Second, enterprises deploy the AAA system in the security service zone to provide secondary authentication for wireless communication and mobile computing terminals accessing the slice in Username-Password mode. By using AAA system and security SIM card technology, terminals and applications that have high-security requirements can improve secondary authentication strength. Here, the security SIM card is a USIM-based card with a built-in USB key function. It is based on the PKI digital certificate system. The key is stored in the security chip of the SIM card and cannot be copied, repudiated, or tampered with. Third, the enterprise can deploy the multiservice access gateway (MSCG) at the intranet border. The MSCG grants the access rights of terminals to the enterprise private network only after the terminals pass the second authentication. With the implementation of the above schemes, the factory campus has denied 10412 access queries from untrusted terminals during the past 6 months.

8. Conclusions

5G is deeply integrated with social life and vertical industries, and the security and privacy of the 5G ecosystem are largely influenced by application developers and service providers, as well as network operators and equipment suppliers. The achievement of security and privacy in 5G applications requires a comprehensive and systematic design, as well as the deployment of proper security measures according to the specific application scenarios and the needs of the industry. This paper makes contributions in the research of security and privacy in 5G-enabled applications, as shown in Table 6. In view of numerous 5G applications, such as smart manufacturing, smart transportation, smart grid, and smart campus, this paper analyzes general security risks from devices, networks, edges, and other aspects, as well as specific risks in typical usage scenarios. As a result, readers will have a more comprehensive grasp of security risks in 5G applications. Besides, the existing related work for 5G application security is analyzed, including security standards, authentications, network slicing, and MEC. In particular, secondary authentications for industry customers and three-factor authentications for mobile lightweight devices are researched. After that, the reference architecture of 5G applications is analyzed, and security solutions are summarized in a systematic view. In addition, we also analyze the security and privacy risks for 5G applications in eMBB, uRLLC, and mMTC scenarios and summarize corresponding countermeasures. Finally, a use case of industrial terminal access control is studied, which enhances readers' understanding of specific 5G application security risks and solutions. On the whole, this paper conducts a comprehensive study on security and privacy in 5G applications, which strengthens readers' risk awareness and security capabilities and generates a positive impact on the healthy and sustainable development of various applications in 5G era.

References

[1] Z. Bao, "Discussing 5G network technologies in smart traffic construction," China ITS Journal, vol. 226, no. 1, pp. 81-82 +102, 2019.
[2] S. Basudan, X. Lin, and K. Sankaranarayanan, "A privacy preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing," IEEE Internet of Things Journal, vol. 4, no. 3, pp. 772–782, 2017.
[3] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: a survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944–980, 2012.
[4] N. Saxena, A. Roy, and H. S. Kim, "Efficient 5G small cell planning with eMBMS for optimal demand response in smart grids," IEEE Transactions on Industrial Informatics, vol. 13, no. 3, pp. 1471–1481, 2017
[5] CAICT, IMT 2020(5G), Promotion Group, 5G Security Report, The China Academy of Information and Communications Technology (CAICT) and IMT 2020(5G) Promotion Group, 2020.
[6] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes," Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.
[7] K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, "Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G," Security and Communication Networks, vol. 9, no. 16, 3104 pages, 2016.
[8] D. Wang and P. Wang, "Two birds with one stone: two-factor authentication with security beyond conventional bound," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 708–722, 2018.
[9] D. He, D. Wang, and S. Wu, "Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards," Information Technology and Control, vol. 42, no. 4, pp. 170–177, 2013.
[10] 3GPP TS 22 261, Service Requirements for the 5G System, The 3rd Generation Partnership Project (3GPP), 2018.
[11] 3GPP TS 33 501, Security Architecture and Procedures for 5G System R15 TS 33.501, The 3rd Generation Partnership Project (3GPP), 2018.
[12] 3GPP TR 33.835, Study on Authentication and Key Management for Applications Based on 3GPP Credential in 5G, The 3rd Generation Partnership Project (3GPP), 2018.
[13] F. L. Chen, J. Wang, and X. Du, "Primary exploration of 5G secondary identity authentication scheme for enterprise/industry users," Communications Technology, vol. 52, no. 7, pp. 1740–1743, 2019.
[14] C. L. Li, Y. Gu, and J. Wang, "Analysis and design of 5G secondary authentication protocol,"

Communications Technology, vol. 52, no. 7, pp. 1733–1739, 2019.
[15] X. Liu, P. Wang, Z. Lan, and B. Shao, "Biological characteristic online identification technique over 5G network," IEEE Wireless Communications, vol. 22, no. 6, pp. 84–90, 2015.
[16] D. Wang, H. Cheng, D. He, and P. Wang, "On the challenges in designing identity-based privacy-preserving authentication schemes for mobile devices," IEEE Systems Journal, vol. 12, no. 1, pp. 916–925, 2018.
[17] D. Xiao, X. Liao, and S. Deng,"A novel key agreement protocol based on chaotic maps," Information Sciences, vol. 177, no. 4, pp. 1136–1142, 2007.
[18] L. Han, Q. Xie, W. Liu, and S. Wang, "A new efficient chaotic maps based three factor user authentication and key agreement scheme," Wireless Personal Communications, vol. 95, no. 3, pp. 3391–3406, 2017.
[19] Y. Liu and K. Xue, "An improved secure and efficient password and chaos-based two-party key agreement protocol," Nonlinear Dynamics, vol. 84, no. 2, pp. 549–557, 2016.
[20] Q. Jiang, F. Wei, S. Fu, J. Ma, G. Li, and A. Alelaiwi, "Robust extended chaotic maps-based three-factor authentication scheme preserving biometric template privacy," Nonlinear Dynamics, vol. 83, no. 4, pp. 2085–2101, 2016.
[21] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, p. 1, 2020.
[22] GTI, "GTI security consideration for 5G smart city whitepaper," 2020, http://www.gtigroup.org/Resources/rep/2020-03-16/14833.html. [42] W. Zhou, X. T. Zhu, and X. Xia, "Study on 5G V2X communication security service," Application of Electronic Technique, vol. 45, no. 12, pp. 34–37, 2019.
[23] J. P. Wang and G. Q. Liu, "High security level special industry 5G application security architecture," Confidential Science and Technology, vol. 1, pp. 16–21, 2019.
[24] ETSI, Multi-Access Edge Computing (MEC), Framework and Reference Architecture, 2019.
[25] M. He, J. Shen, G. W. Wu, and N. Fan, "Discussion on MEC security," Mobile Communications, vol. 43, no. 10, pp. 2–6, 2019. [27] X. J. Zhuang, B. Yang, X. Wang, and J. Peng, "Approach on mobile edge computing security," Telecom Engineering Technics and Standardization, vol. 31, no. 12, pp. 38–43, 2018.
[26] W. Zhou, "Research on 5G network slicing security technology," Mobile Communications, vol. 43, no. 10, pp. 38–42, 2019.
[27] J. W. Liu, Y. R. Han, B. Liu, and B. Y. Yu, "Research on 5G network slicing security model," Netinfo-Security, vol. 20, no. 4, pp. 1–11, 2020.
[28] S. Chen, W. T. Liang, N. Song, and K. Y. Fan, "Design of secure protection for 5G network slice," Communication Technology, vol. 52, no. 10, pp. 2499–2506, 2019.
[29] S. Behrad, Slice Specific Authentication and Access Control for 5G, Doctoral School of the Polytechnic Institute of Paris, Doctoral Dissertation, 2020.
[30] Y.-J. Ku, D.-Y. Lin, C.-F. Lee et al., "5G radio access network design with the fog paradigm: con fluence of communications and computing, " IEEE Communications Magazine, vol. 55, no. 4, pp. 46 –52, 2017.
[31] ETSI GS NFV-SEC 001 V111, Network Functions Virtualisation (NFV), NFV Security; Problem Statement, 2014.
[32] ETSI GS NFV-SEC 003 V111, Network Functions Virtualisation (NFV), NFV Security; Security and Trust Guidance, 2014.
[33] ETSI GS NFV-SEC 012 V311, "Network functions virtualisation (NFV) release 3," Security; System Architecture Specification for Execution of Sensitive NFV Components, European Telecommunications Standards Institute (ETSI), 2017.
[34] ITU-T X1038, Security Requirements and Reference Architecture for Software-Defined Networking, International Telecommunications Union (ITU), 2019.
[35] B. Zhang, J. Yuan, Q. Qiu, X. J. Li, and F. Zhang, "Research on 5G security technology and development, " in Proceedings of "5G +" China Mobile Science and Technology Association , pp. 1 –5, Beijing, China, 2019.
[36] N. Fan, G. Liu, and J. Shen, "Analysis of mobile network security for operators in the initial stage of 5G commercialization," China Information Security, no. 7, pp. 85 –87, 2019.
[37] A. K. Das, S. Zeadally, and M. Wazid, "Lightweight authentication protocols for wearable devices," Computers & Electrical Engineering, vol. 63, pp. 196 –208, 2017 & Research papers by Qin

Author Profile

Ayan Dhanda, Student CSE in ICAS, Manipal. He has an exceptional record in academics, determined to excel in every sphere of life, technically inquisitive, socially amicable, persevering & a good decision maker, I want to develop a keener awareness of technical aspects and enhance my overall perception towards serving the world. Email: ayandhanda74[at]gmail.com