Chapter 12
Security and Privacy in 5G-Enabled Internet of Things: A Data Analysis Perspective

S. R. Mani Sekhar, G. Nidhi Bhat, S. Vaishnavi, and G. M. Siddesh

1 Introduction

There is a need to write this chapter to bring awareness about the consequences of the data being transferred every time and how it affects our privacy and security. This works on the measures which are taken and the new technologies which are blooming in the industries in order to protect the data from malicious activities. After that, the author tells well the innovative ideas that could be implemented along with their advantages and disadvantages. In this chapter, the authors have tried to acknowledge the severities in data transfer in 5G-enabled IoT and also have included a few innovations in this field and a comparative study which has helped in securing data.

In this era of advanced technology, connectivity is the utmost requirement for all activities. There has been a continuous exponential development in the field of networking as shown in Fig. 12.1. 2G, 3G, 4G, and 4G LTE have been able to help us connect with people all over the world and now have stepped into the next generation of networking that is 5G. It is a wireless standard where everything including objects and machines is connected. It reduces a lot of drawbacks imposed by the previous networks by providing peak data speeds, low latency, high network capacity, and availability; it explores user experiences and is highly effective. It is estimated that 5G technology is ten times faster than 4G LTE. Its ability is immense. Fields where 5G is most important include autonomous vehicles, improved broadband, healthcare, remote device controller, public protection and infrastructure, and IoT.

In the upcoming section of the chapter, the authors discuss the various security-related issues and their possible solutions followed by privacy section which

S. R. Mani Sekhar (✉) · G. Nidhi Bhat · S. Vaishnavi · G. M. Siddesh
Department of Information Science & Engineering, Ramaiah Institute of Technology, Bangalore, India
e-mail: manisekharsr@msrit.edu

S. Tanwar (ed.), *Blockchain for 5G-Enabled IoT*,
https://doi.org/10.1007/978-3-030-67490-8_12

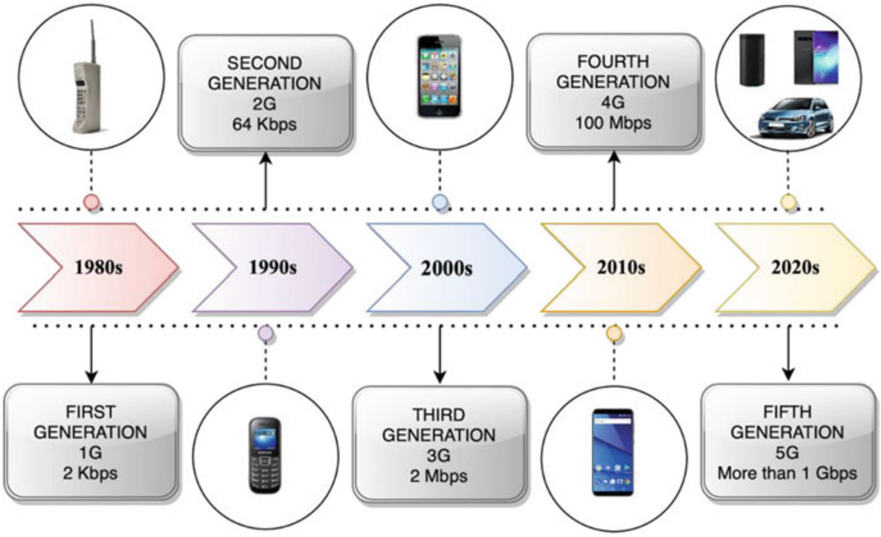
SECOND GENERATION 2G 64 Kbps
FOURTH GENERATION 4G 100 Mbps
1980s
1990s
2000s
2010s
2020s
FIRST GENERATION 1G 2 Kbps
THIRD GENERATION 3G 2 Mbps
FIFTH GENERATION 5G More than 1 Gbps

Fig. 12.1 Timeline for evolution from 1G to 5G

discusses the privacy issues and their possible mitigations. Further, the author discusses the various case studies which help in understanding the different approaches to security and privacy issues.

1.1 IoT Devices Working with 5G Networks

IoT devices use a variety of wireless technologies which include Wi-Fi, Bluetooth ZigBee, Z-Wave, GSM, 4G-LTE, and even 5G. Other alternatives like cellular technologies are also used by IoT devices. This offers global connectivity, security, and performance. Connectivity is the heart of IoT devices. With IoT devices having this level of connectivity as in 5G networks, there would be no need for any manual attempt to switch on lights. Although 5G provides a lot of benefits, it still does come with its costs. The case studies help us learn about how privacy and security issues are being tackled in vast areas like transport, communication aids, etc. A lot of data which could be used to do great harms is too easy to reach. A few challenges regarding privacy and security threats are explained with some solutions which would secure our data.

In 2011, the US military lost its national secret data due to a mission over Afghanistan which was contained in American sentinel unmanned aerial vehicle (UAV) to Iranian forces. The theft of such national secret data could cause severe catastrophes which are unimaginable. In such cases, erasure of data is one solution as designed in the paper [1], but it might not be enough at all times.

A wide range of research has been happening to fill in the gap between IoT practical usage and privacy concerns. Various protocols and architectures are being studied to maintain our data in secure hands.

2 Security in 5G-Enabled IoT

Security concerns must be dealt with utmost attention, and this has been a challenge in 5G-enabled IoT. With a number of IoT devices gaining popularity, the significance of dealing with security issues cannot be overlooked. These issues are not only considered to be damaging to the cost but are also causing other pressing issues such as loss of consumer confidence, social trust, and personal safety.

IoT integrates and implements various tools, advancements, and infrastructure. The threats imposed by these network technologies which are utilized in IoT expose the layers of IoT architecture to security challenges [2, 31]. IoT systems raise security concerns, unlike the conventional networks where the security issues can be handled with much ease. The physical layer of the IoT system contains less executing power and less data storage due to which conventional security solutions like encryption and spread-spectrum methods cannot be implemented [3] at all ends. Subsequently, IoT systems are heterogeneous, and hence they have different defense mechanism capabilities; hence, the most vulnerable layer determines the security level of the system.

2.1 Security Issues and Threats of a Layered IoT Architecture

The below section discusses the various security issues of a 5G IoT architecture [4, 5].

2.1.1 The Architecture of 5G-Enabled IoT

Since there is no proper organized layered structure for IoT devices despite the emerging number of IoT applications, let's consider the most common approach using mainly three layers [6]:

(i) Physical layer: It usually includes sensors and actuators to gather information from the environment.
(ii) Network layer: It helps in connecting various smart things, network devices, and servers. Subsequently it is used for sending and processing sensor data.
(iii) Application layer: It is used to deliver application-specific facilities to the end users.

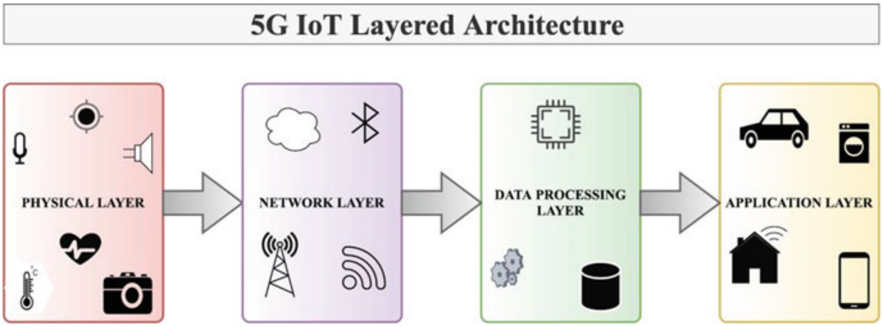

Fig. 12.2 5G IoT layered architecture [32]

Some approaches could consist of a data processing layer which classifies all cloud-based service-related issues [7]. Figure 12.2 represents these layers of the 5G IoT architecture.

2.1.2 Security Issues

(i) Physical Layer

The sensors and actuators of the physical layer are considered to be prone to security breach since they operate where devices can be accessed physically. This means that the devices can be physically tampered and firmware can be replaced or can even be destroyed [8]. Unauthorized access and cloning of the tag can also occur in sensors which may allow the malicious attacker to reprogram the data or provide fake information.

Tampering can also be the initial stage of implementing a denial-of-service (DoS) attack alongside extra nodes in the grid. Closed systems are also subjected to attacks by jamming in the physical layer.

(ii) Network Layer

IoT systems are heterogeneous, and hence in the network layer, it is observed that the security threats differ remarkably. Edge devices and the endpoints in the cloud are more influential devices and hence can adapt to traditional security measures, whereas the nodes lack features like public-key cryptographic methods [9], thus often limiting the defending capabilities of the whole network.

A common attack through networks is a DoS attack. In an edge computing scenario, distributed DoS attack and wireless congestion are dangerous. The other most prevalent form of attack is a man-in-the-middle attack as it violates the discretion, honesty, and privacy of the delimited data. Such attacks are executed in various ways such as eavesdropping on the messages or misusing them; privacy and quality of service are deteriorated by altering unencrypted routing data [10].

The other forms of attacks could be IP theft, counterfeit attack, packet sniffing, and so on.

(iii) Data Processing Layer

The main security threats in the cloud are DoS attacks that can shut down the cloud system and deny the services. With the rise in the 5G-enabled IoT application and 5G wireless speed, DoS attacks are higher-risk factors since the previous detection methods cannot handle the high volume data traffic. System vulnerabilities may also allow attackers to easily damage the cloud computing system [5].

(iv) Application Layer

The application layer clubs different interfaces like web applications, service organization tools, and middleware [11]; in this layer, the major security concern is the traditional software attacks involving a lot of risks. DoS attack and malicious code injection are common security concerns. It is easy to attack and shut down a service if there is no secure authentication and key agreement. At situations where data is not validated enough, attackers would find it a loophole to inject malicious data which as a consequence they get easy access to perform various actions, such as stealing records, negotiating database integrity, or bypassing validation [12].

2.2 Possible Mitigations for Security Issues

Some possible mitigations for security issues concerning each layer are mentioned below [7].

(i) Physical Layer

Tamper-resistant packaging can be used to provide maximum security against tampering of the IoT devices. Although there is very little cure for DoS attacks [7], spread-spectrum procedures can be a structured defense mechanism, but this cannot be put into action due to their constraints on computational volume and power consumption [3].

(ii) Network Layer

Passive monitoring (probing), active firewalls, bidirectional link authentication, traffic admission control, encryption, and authorization can be used to prevent eavesdropping and DoS attacks. The edge data centers are to be protected to prevent the attackers from accessing the data.

(iii) Data Processing Layer

Malware detection, traffic monitoring, and appropriately organized firewalls on all system entry points could help prevent various attacks on the cloud system.

(iv) Application Layer

Proper authentication, anti-virus filtering, integrity verification testing, authorization, validation of the inputs, traceability of the data, and process planning and design are some of the possible mitigations to reduce security risks in the application layer.

2.3 Security in IoT Considering 5G

The security issues of software-defined network (SDN)/virtual network functions (VNF)-built network fundamentals on the control plane outweigh the benefits they provide which include low latency and high speeds, especially when the authors relate to the nature of communication. A number of proposed solutions for these security issues are emerging, and hence 5G will be a preferred communication platform for IoT. Another major benefit of 5G-enabled IoT is the elasticity of its devices which leads to well-organized, use-case definite solutions which can be useful to the less standardized issues such as low-powered nodes and sensors. Regarding the less-energy nodes which contribute to IoT, an effective technique to advance security is using physical layer security (PLS) solutions and lightweight cryptography systems. Security threats and possible solutions in layered 5G IoT architecture [7] are summarized in Table 12.1.

3 Privacy in 5G-Enabled IoT

5G technology has helped in gaining momentum for IoT directly or indirectly. IoT has gained a lot of popularity through network connectivity and scope provided by 5G technology. 5G assures a faster lifestyle by reducing the downloading and uploading time durations, lowering the latency, and providing more connection density.

Before going ahead with what changes have been made in 5G IoT devices, it is important to note that the basic underlying physical infrastructure of the Internet is kept intact. In other words, the fiber-optic cables run by the service providers are connected with other ISPs and the broader Internet [13]. And hence, in 5G IoT devices, the risk of losing our privacy is still intact. This includes the exploitation of our communication surveillance, data retention, information sharing, and a lot more.

The amplified usage of IoT and the advancement in technology have led to zero private space. For instance, Equifax, a major credit reporting agency, had leaked 143 million American citizens' data such as name, social security number, birth date, address, and a lot more. Similarly, Facebook also was sued for harvesting over 5 million Facebook users' data without permission. This was a major setback in the

Table 12.1 Security threats and possible solutions in layered 5G IoT architecture

Layers/solution	Physical layer	Network layer	Data processing layer	Application layer
Function	Senses and gathers information from physical devices and sensors	Transmits the sensor data	Processes the collected data	Delivers applications based on the processed information to end users
Security threats	Tampering, DoS attacks	DDoS attacks, man-in-the-middle attack, eavesdropping, IP theft, counterfeit attack, packet sniffing	DoS attacks	DoS attack, malicious code injection
Possible solutions	Spread-spectrum procedures, tamper-resistant packaging	Probing, firewalls, encryption, traffic admissions control, authorization	Malware detection, traffic monitoring	Anti-virus filtering, testing, authentication, authorization, traceability

stock prices of Facebook as well as other social media platforms. The 4G-enabled IoT is cloud-based which could impose a lot of security and privacy threats. It comes to the fact that in 5G technology, more data is generated and more network traffic emerges because of features of the edge paradigms and therefore it is prone to more security and privacy concerns [11].

3.1 Privacy Challenges in 5G Networks

The below section illustrates the various privacy challenges in 5G networks [30].

3.1.1 Location Privacy

Semantic information attacks are very common. They can be defined as the usage of incorrect data to cause harm. Each time a user joins a 5G antenna, mobile networks can track the location data of the user, and this can also be done by access point selection systems in 5G.

The international mobile subscriber identity (IMSI) keeps an account of the identities of the mobile device subscribers. By seizing the IMSI of a subscriber's mobile device, an attacker may interrupt his activity like ongoing calls and texts and monitor them. The purpose of these measures is only to improve the quality of life, but the harms seem to be much bigger [14].

3.1.2 Correlation Privacy

At places where our private and sensitive information is being collected like in hospitals, database encryption might still not serve as a solution. Attackers would be able to integrate and analyze the encrypted information from different devices by specifying time and location where the data is fragmented. Hence, attackers would be able to access unauthorized records of the organization [3].

3.1.3 Broad Sensitive Information

As a part of this huge network, users knowingly or unknowingly share a lot of information. This compromises our broad data (like the information we leak every day) privacy because the attackers are given easy access to the information regarding an individual. Various devices which are connected to the Internet collect a lot of information which could be personal and sensitive.

3.1.4 Identity and Authentication

In previous technologies like 3G and 4G, the security and privacy protocols for preserving identity were based on the single server environment which does not suit the trends in 5G technology. The challenge is to design protocols to build trust and privacy between cloud users and the service. Although there were a few protocols designed like SSL Authentication Protocol (SAP) and Identity-Based Authentication for Cloud Computing (IBACC), there were complaints of their data being digitized.

3.1.5 Radio Communications in High-Frequency Bands

With 5G technology being used, the authors see an integration of radio access technologies which are easily able to tap into licensed, licensed shared, and unlicensed spectrum beyond frequency ranges which are in use. A massive antenna array to optimize the frequency ranges with new technology will be used. The more the number of antennas used, the more the signal paths created, and hence, our data is more vulnerable in the hands of the attackers [15].

3.2 Solutions to Privacy Threats

Transparency and consistency have to be maintained in IoT devices. Transparency is letting the user know about what is happening to the data being collected and how it is being used, and consistency is about how consistent the device serves its purpose. The two criteria of any IoT device help in maintaining our privacy [5].

A few common steps which could be taken to protect from the common attacks are:

(i) Selecting manufacturers who provide software support and updates for devices.
(ii) Using software which is updated so that it could show the vulnerabilities so they could manage them appropriately.
(iii) The behavior of the devices has to be monitored; any deviations from the norms have to be taken seriously [17].

End-to-end encryptions in 5G IoT devices must take care of radio transport, IoT and devices Telco cloud, security operations, and slicing security. Reducing the time a hacker stays undetected at cyber-attack approaches can help to secure privacy to some extent.

4 Case Studies

This section illustrates various case studies on IoT-based 5G networks.

4.1 Secure Network Architecture for Smart Grids in 5G Era [18]

Telecommunications and electric energy are two important factors to fuel the future smart cities and economy. With 5G network, the smart grid era presents a multitude of promising applications, particularly demand response, advanced metering infrastructure (AMI), smart house, and so on. The smart grid brought about immense changes on how electricity is manufactured, communicated, or consumed. It associates a two-way information and power flow between the end users and the grid. Smart grid requires the expansion of communication infrastructures and legacy control, supporting the transmission and generation systems, the network boundaries, and the distribution networks to join the complete supply network of the industry. AMI is distributed globally to bridge the gap between end consumers and utilities, establishing two-way communication links that will allow automatic and efficient load management and the adaptation of auspicious smart grid solutions, particularly DER, V2G, DR programs, and so on.

However, the introduction of AMI widens the attack surface and causes the grid to be susceptible to cyber-attacks from malicious attacks. For example, an attacker may initiate a DoS attack against the Supervisory Control and Data Acquisition (SCADA) system or parts of the AMI, like the neighborhood area networks (NAN), wide area network (WAN), and home area networks (HAN). The smart grid lays the foundation for a reasonable electricity marketplace. Hence, value integrity attacks can severely damage the product demand and supply balance, causing grid uncertainty, and can lead to an economy down. Subsequently this could damage the physical components of the grid or cause blackouts over a large geographic region.

To address these security concerns and in order to safeguard the grid against load alteration or price integrity attacks, a secure network framework was proposed. The major part of this network architecture is the intrusion detection system (IDS) scattered across the various places of the information network.

Depending on resource availability, an intruder may target only specific parts of the AMI or a restricted number of links, that is, the attacker may direct the attack at the access links of NAN, HAN, or backhaul links. These contact associations could cause the pricing information to be transmitted from utility companies to HANs and carry back the amount of electricity spent by these households.

WAN, NAN, or HAN could be provided with an IDS that would enhance application security by recognizing intrusions. An IDS is responsible for detecting any security breach. The signature-based systems depend on identified or familiar patterns in the communication packets based on an initial couple of bytes and are mainly used by proprietary-based solutions. Here, an updated record of signatures is maintained for any previously known security attack, and the signature of any given packet is always compared against these maintained signatures. Moreover, these methods experience trouble from two main disadvantages:

(i) Due to checking packet payloads, these techniques may violate the user's privacy.
(ii) As signature lacks in the database, they may be at the risk of new attacks.

ML and statistical learning techniques are merged by IDSs to reduce these problems. These methods can also be utilized for studying the voltage of AC statistics at different circulation buses to notice any peculiarity in the system. Therefore, IDS screens and checks the demand and supply stability in real time and inspects if there is any unexpected rise in the request. This, in turn, can lead to load or price attacks in the AMI. Different IDS organizations could be developed for different components of an AMI; later these mechanisms can be integrated for additional performance enhancement. For example, when an abnormality is noticed in a certain place of the network, the corresponding IDS can communicate it to the IDSs to take suitable actions at the various layers of AMI, that is, WAN, NAN, and HAN.

4.2 Secure D2D Communication [19]

D2D technique is a point-to-point communication system without a middle node between devices. In mobile networks, D2D communication has numerous advantages:

(i) A communication bridge could be established for data transmission in a cellular network to expand the coverage of each cell and transmit data to a node inside cell coverage.
(ii) By transmitting data directly between devices, D2D communication reduces the base station energy consumption.
(iii) There is an increase in the efficiency of the same radio frequency being reused.

In D2D communication, the distance between devices is shorter than the distance between a base station and a device which implies that in D2D communication scenario, the interference of radio frequency decreases; therefore, using the same radio frequency allows to transmit multiple data. Furthermore, D2D communication is a fundamental method of 5G vehicle-to-everything (V2X), which is a vital method for self-directed driving.

Typically, in a mobile network, D2D communication has a few security issues. The D2D communication involves mainly two measures, namely, device discovery and data communication. During this procedure, there are no verification steps in authenticating the identity of the device. A device sends in a request for a setup link, after which a node responds with an acknowledgement message. Additionally, D2D communication does not authenticate messages nor maintain integrity. This allows the attacker to direct various attacks like privacy sniffing, eavesdropping, location spoofing, impersonation, and free riding.

To address the service demands, IoT technology collaborates with the 5G network, and this corresponds to Ultra-Reliable Low-Latency Communication (URLLC) and Massive Machine-Type Communication (mMTC). IoT applications handle a considerable amount of sensitive data, but the devices have limited properties in terms of memory, power, and performance intake. Security concerns could be difficult to be processed due to these properties of IoT devices, and it makes it critical to find solutions to these issues. Therefore, there is an essential demand for a secure D2D system that consists of a correct validation process among the IoT devices. It has to be made lightly with the resource-constrained environment in mind.

To address the security concerns, a secure D2D communication is designed. For effectiveness in 5G use-cases equivalent to IoT scenarios, URLLC and mMTC, a lightweight authenticated encryption with associated data (AEAD) cipher and an elliptic-curve cryptography (ECC)-based public-key cryptosystem are used as groundwork for this design.

According to this approach, before the D2D communication is carried out, based on the 5G-AKA given by the 5G network, the identity of the user equipment (UE) is verified, and then a token is generated which is used as the key for the Elliptic Curve Digital Signature Algorithm (ECDSA). The produced token could validate the authenticity of the associated UE in the link setup. This can be achieved without linking to the central network. Also in the secure data communication step, the encrypted communication is done through frivolous AEAD cipher; meanwhile, the authentication of the UE can be accomplished, and integrity/confidentiality of the data can be maintained in each transmission process.

This technique can generate greater energy efficiency and performance, compared to the purpose AEAD cipher-based communication application, and can also ensure protection from eavesdropping, impersonation, site spoofing, privacy sniffing, etc.

4.3 UAV IoT Framework [20]

UAVs contribute in various fields including areas related to military, civilian, governmental, and commercial sectors. Some of the applications include environmental monitoring (pollution, industrial accidents), distribution, and surveillance requests intending on seeking or providing data at locations after an attack or a disaster. This information can be used to deliver medicine and other necessities. The commercial applications include distributing goods and products in rural and urban areas. UAVs are reliant on antennas, sensors, and embedded software; hence, they are considered as a part of the IoT. They provide two-way messages for applications linked to monitor and for remote control.

Considering that UAVs are a part of IoT, it mainly consists of similar security issues as that of mobile communication networks, sensor networks, the Internet, and specific privacy-protection problems. They have to deal with enhanced security concepts, like access control, verification, secrecy, cyber-attack anticipation, data protection, and high authorization, to prevent signal jamming, spoofing, RF and mobile application hacking, physical attacks, firmware hacks/sabotage, and protocol abusing.

The proposed framework incorporates cutting-edge comprehensive advances for approaching the present privacy and security level into a robust, highly protected, and principal environment by integrating dissimilar vision-based methods for scene study. Accordingly, a hybrid centralized-distributed system controls UAV flights and handles the operations such as registration, ranking, identification, and organization of moving objects.

A few solutions the framework proposes in order to solve the abovementioned security challenges are (a) vision-based techniques, (b) privacy anticipation and anonymity methods for mobile things, and (c) a lightweight safety toolbox.

The framework supports multi-domain and multilevel defense mechanisms in safeguarding IoT objects. Here privacy is achieved by an active "crowd of things" approach. Vision techniques aim to strengthen the security of IoT by encouraging machine learning and computer vision solutions.

4.4 Intelligent Transportation System

Traffic monitoring has become a major concern to maintain road safety. Intelligent transportation system (ITS) is one such system which works by the fixed transmission of information between vehicles and subsequently with back-end servers. With the exponential usage of IoT devices in vehicles, personal data is captured and processed. A balance between technology and measures to maintain privacy has to be kept to maintain confidence in digital economy services to further enable societal opportunities for innovation [21].

IoT sensors are widely used in the field of transport to support connected and autonomous vehicles (CAV) and ITS. CAV and ITS have technical and legal challenges in protecting the privacy of commuters. A few problems related to privacy are:

(i) Misuse of data
(ii) Malpractice
(iii) Communication overhead information being tracked, for example, IP address of the sender and receiver

The main focus of this system is maintaining the following:

(i) Anonymity: a person must not reveal his/her identity to use resource.

(ii) Unobservability: a third person should not get to know that a resource is being utilized.
(iii) Pseudonymity: the person using a resource should not reveal his/her identity which is still accountable for it.
(iv) Unlinkability: a person must be able to make several uses of resources without others being able to link with it.

Many security and privacy schemes have been structured to prevent privacy problems [22].

Group/Ring Signature-Based Privacy Schemes It is better when only a single person or a group manager has all the users' information rather than anyone who has access to the Internet, and this feature can be made possible by a cluster sign. Asymmetric cryptography is used here where the group members are given private keys and asymmetric keys. This key is used to generate signs and send communications over the network. Later, at the receiving side vehicle, a set of asymmetric keys are used. There are other schemes, but all of them demand high computational overhead and intermediate security; meanwhile, low computational overhead devices provide low security.

Pseudonym-Based Privacy Schemes Several techniques can be used in this scheme which fall under the two categories of symmetric cryptographic schemes and asymmetric cryptographic schemes. In these approaches, to maintain anonymity, fictitious names are assigned. A few of them are public-key cryptographic and secret key cryptographic methods.

A lot of researchers have come up with several schemes under asymmetric and systematic schemes, but the latter proves to be more efficient when it comes to computation.

4.5 End-to-End Network Slicing for 5G Communication

5G network slicing is one concept which has taken a big leap in the future of technology; it depends on the principles of network functions virtualization (NFV) and SDN. In network slicing, one physical network alone can be partitioned from numerous simulated networks, and each slice signifies an autonomous virtualized end-to-end network. The allocate resources is collected from a physical network; this concept is similar to that of the city transportation system where the authors find many modes of transportation by allocating infrastructure resources like roads, rail tracks, etc. This, in turn, reduces latency and high reliability [23].

With the growth of the IoT, network demands increase immensely, at almost 1000 times more data accumulation and more number of devices, lower latency, and higher bit rates. Network slicing provides a cost-effective solution for these demands. Although this proves as a key technology for simplified networking and has a lot of advantages, security and privacy challenges are a major concern [24].

Shielding, a feature of network slicing, refers to the non-interference of each slice from one another though they share the same infrastructure.

Users are not limited to just a single slice rather than a connection with many slices. Customer can expect more security vulnerabilities in end devices. A lot of distributed DoS are prone to happen. Confidentiality, authentication, authorization, availability, and integrity are the most important security principles which have to be followed. Network slice manager (NSM) should track interactions across slices, and it is responsible for interacting and virtual network function.

A few solutions are proposed to protect the data flow among base stations and devices. Here the authors use the concept of cryptography to focus on privacy preservation and protection of intra-slice ciphers with the help of a stream cipher. To secure communications between 5G networks, public cryptosystems like public key infrastructure (PKI) and certificateless cryptography could be used [24]. The solution provided here is more efficient than the encryption method in which a user encrypts the message before sending it.

Another approach is by using the security controls required for core slice addressing. This is a dynamic, future-proof approach which supports the requirements of network slicing on SDN [25] talks about global security policies. It covers a wide range of issues on network slicing and provides few solutions to meet a secure environment.

4.6 Lip Reading-Driven Secure Hearing Aid

A new approach which makes use of new technology and IoT for audiovisual (AV) aids is used to help people with hearing loss. Lip reading serves as a new efficient method as compared to the already existing audio-only hearing aids [29] has proposed a solution to the challenges on privacy-related aspects as well as low latency. It also provides us with a high data rate and low complexity in computation. 5G cloud-radio access network (C-RAN), IoT, and strong privacy techniques have been integrated to counter cybersecurity attacks like eavesdropping and location of privacy. The information in the form of AV sent by the 5G IoT devices is encrypted using a real-time lightweight encryption method based on piecewise linear chaotic and Chebyshev map, secure hash, and an innovative substitution box method.

There are a few encryption methods which comprise advanced technicalities like Advanced Encryption Standard (AES) and RSA (Rivest-Shamir-Adleman) algorithm that are not compatible with low-power sensor networks. Hence, the authors look into lightweight encryption methods. Generally, there are two stages of encryption: confusion and diffusion. The algorithm used in this study uses piecewise linear chaotic map (PWLCM) in the confusing process to make the decrypting and security attacks very complex. In the model proposed by [29], the encrypted audio signal and video signals are utilized in the cloud designed by the lip reading-driven speech-developed application, complement the concepts of deep learning, and use analytical acoustic modeling.

In the scheme proposed by [29], a system cloud which could enhance speech through lip reading is utilized where a collection of the encrypted audio and video signals takes place. This idea explores the capabilities of deep learning and analytical acoustic modeling. The first level is a deep learning regression model, and the second level is a lip reading enhanced visually derived Wiener filter (EVWF) to estimate the clean audio power spectrum [29] has proposed a lightweight chaotic encryption scheme in his paper which provides an easy enabler for modern digital hearing aids which secures privacy.

4.7 5G AKA Protocols

Authentication and key agreement (AKA) was a protocol designed by the 3rd Generation Partnership Project (3GPP) to standardize 3G, 4G, and 5G technologies in order to establish a secure network with serving networks (SN). AKA works on symmetric cryptography and sequence number (SQN). AKA is used in all 3G and 4G USIM (universal subscriber identity module) which is used in almost all the IoT devices. A few instances of security breach have occurred due to the fake base station attacks like the non-protected identity request mechanism to eavesdrop and inject messages. In 5G AKA protocol, asymmetric encryption is introduced to help in the authentication of identifiers [26].

Table 12.2 represents the key differences in the approaches of 4G and 5G authentication [16].

In [27], 5G AKA protocols have made changes to the protocol to include improving the privacy requirements. Instead of sending the messages directly, the protocol encrypts it using randomized asymmetric encryption. Although this prevents the IMSI attacks, it still is not enough to prevent the attacks applicable to 3G and 4G networks. In IMSI, a commonly observed flaw of AKA protocol in 3G and 4G was that it’s very easy to track subscribers in a geographical region by just broadcasting an identity request in that region to the UEs. Hence, to protect messages carrying identity requests, developer uses stronger cryptographic mechanisms in 5G [28] has proposed a new model to analyze the AKA model called Tamarin Prover which has a high level of automation and equivalence properties to maintain privacy properties.

5G AKA provides a SUPI for users with a randomized key, SUCI. Tamarin model makes sure SUPI remains confidential, without which the active and passive users are not able to decrypt the message. Table 12.3 illustrates the brief tabular summary of the above case studies.

Table 12.2 Difference between 4G and 5G authentication

4G authentication	5G authentication
4G defines 4G EPS-AKA as its authentication method	5G defines three authentication methods. They are 5G-AKA, EAP-TLS, AND EAP-AKA
The authentication vector is generated by the Home Subscriber Server (HSS)	The authentication vector is generated by Unified Data Management (UDM)/ Authentication Credential Repository and Processing Function (ARPF) under 5G-AKA and EAP-AKA protocols
The authentication of the UE is decided by the mobility management entities (MME) and Evolved Node B (eNodeB)	The authentication of the UE is determined by Security Anchor Function (SEAF) and Authentication Server Function (AUSF)
The UE identity before being shared in the 5G network is encrypted with the public key of the home network in clear text which could be stolen by any attacker	Before it is sent to the 5G network, the UE makes use of the public key of the HN to encrypt the UE permanent identity
The HN (e.g., HSS) is utilized during authentication to generate authentication vectors and does not have a say in the decisions of the authentication results	The final decision on UE authentication is done by HN, and its results are also transmitted to UDM for logging
The anchor key hierarchy is comparatively shorter	5G has two intermediate nodes, and hence the key hierarchy is longer
The UE identity from UE to SN is IMSI/ Globally Unique Temporary Identity (GUTI) and from SN to HN is IMSI	The UE identity from UE to SN is Subscription Concealed Identifier (SUCI)/5G-GUTI and from SN to HN is SUCI/ Subscription Permanent Identifier (SUPI)
The SN consists of radio access equipment such as MMEs	The SN consists of the SEAF

5 Conclusion

In this chapter, the author has discussed how 5G technology would be used for the development of smart grids and understanding the role of IDS in providing a secure grid for the customers. The author illustrated various methods to make the D2D connections more secure using AEAD ciphers and an ECC-based public-key cryptosystem. They enumerate about the UAV IoT framework and the different methods which could be implemented to secure data. Next, they discussed about how communication between vehicles can be done in a secure way to avoid traffic and accidents using pseudonym- and group/ring signature-based privacy schemes. Network slicing is one of the key requirements in 5G technology to meet its standards, and this is possible by incorporating end-to-end encryption. Although this is prone to security and privacy issues, a few solutions were mentioned like the PKI and certificateless encryption. Later, the author has discussed how 5G has helped the hearing-impaired individuals by lip reading methods, which send the

Table 12.3 Security and privacy concerns and their proposed solutions in the presented case studies

Name of the case study	Security or privacy concerns	Proposed solution
Secure Network Architecture for Smart Grids in 5G Era	DoS attacks against SCADA system or various parts of the AMI as well as NAN, WAN, and HAN Price integrity attacks Load alterations	IDSs merged with ML and statistical learning techniques Different IDS organizations are developed for different parts of an AMI and integrated
Secure D2D Communication	Privacy sniffing Eavesdropping Location spoofing Impersonation Free riding	AEAD cipher ECC-based public-key cryptosystem
Unmanned Aerial Vehicles IoT Framework	Signal jamming Spoofing RF and mobile application hacking Physical attacks Firmware hacks Protocol abusing	Vision-based techniques Privacy anticipation and anonymity for mobile things A lightweight safety toolbox
Intelligent Transportation System	Misuse of data Malpractice Communication overhead information being tracked	Group/ring signature-based privacy schemes Pseudonym-based privacy schemes
End-to- End Network Slicing for 5G Communication	DDoS attacks Compromise in confidentiality, availability, integrity, and authorization	Cryptography for privacy preservation and protection of intra-slice ciphers using stream cipher PKI and certificateless cryptography to secure communication between 5G networks Using the security controls required for core slice addressing
Lip Reading-Driven Secure Hearing Aid	Eavesdropping Attacks against location privacy	Lightweight chaotic encryption scheme based on piecewise linear chaotic and Chebyshev map, secure hash, and an innovative substitution box method
5G AKA Protocols	IMSI attacks Eavesdropping	Asymmetric encryption Tamarin Prover

information in the form of audiovisuals that are encrypted by advanced encryption and use algorithms like PWLCM for a secure network. Finally, the chapter focuses on the various improvements in 5G AKA protocols to solve the privacy constraints which were absent in 4G protocols, as it is challenging to maintain data security and privacy in the field of connectivity, computation, science, and 5G-enabled IoT. This chapter has discussed the overall security and privacy issues in 5G-enabled IoT. Each of these issues has been debated with presently available and possible solutions. At the end of this chapter, the authors have discussed the various case studies which cover the different security and privacy domains of 5G IoT applications and thus helped the reader to gain an insight of the current fields of research on security and privacy of 5G IoT.

References

1. K. Andersson, I. You, R. Rahmani, V. Sharma, Secure computation on 4G/5G enabled Internet-of-Things. Wirel. Commun. Mob. Comput. **2019**, 3978193–3978191 (2019)
2. I. Andrea, C. Chrysostomou, G. Hadjichristofi, Internet of Things: Security vulnerabilities and challenges, in *2015 IEEE Symposium on Computers and Communication (ISCC)*, (IEEE, Larnaca, 2015), pp. 180–187
3. F.A. Alaba, M. Othman, I.A.T. Hashem, F. Alotaibi, Internet of Things security: A survey. J. Netw. Comput. Appl. **88**, 10–28 (2017)
4. P. Varga, J. Peto, A. Franko, D. Balla, D. Haja, F. Janky, et al., 5G support for industrial IoT applications–challenges, solutions, and research gaps. Sensors **20**(3), 828 (2020)
5. L. Liu, M. Han, Privacy and security issues in the 5G-enabled Internet of Things. 5G-Enabled Internet of Things, 241 (2019)
6. P. Sethi, S.R. Sarangi, Internet of things: Architectures, protocols, and applications. J. Electr. Comput. Eng. **2017**, 1 (2017)
7. P. Varga, S. Plosz, G. Soos, C. Hegedus, Security threats and issues in automation IoT, in *2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS)*, (IEEE, Trondheim, 2017), pp. 1–6
8. R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of things (IoT) security: Current status, challenges and prospective measures, in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, (IEEE, London, 2015), pp. 336–341
9. W. Wei, A.T. Yang, W. Shi, K. Sha, Security in internet of things: Opportunities and challenges, in *2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI)*, (IEEE, Beijing, 2016), pp. 512–518
10. N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Commun. Surv. Tutorials **21**(3), 2702–2733 (2019)
11. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet Things J. **4**(5), 1125–1142 (2017)
12. A. Mosenia, N.K. Jha, A comprehensive study of security of internet-of-things. IEEE Trans. Emerg. Top. Comput. **5**(4), 586–602 (2016)
13. Welcome to 5G: Privacy and security in a hyperconnected world, https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not
14. M. Agiwal, N. Saxena, A. Roy, Towards connected living: 5G enabled internet of things (IoT). IETE Tech. Rev. **36**(2), 190–202 (2019)
15. D.M. West, How 5G technology enables the health internet of things. Brookings Center Technol. Innovation **3**, 1–20 (2016)
16. A comparative introduction to 4G and 5G authentication, https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication#:~:text=EAP%2DAKA’%20is%20another%20authentication,the%20UE%20and%20the%20network

17. Zeljka Zorz: 5G IoT security: Opportunity comes with risks, https://www.helpnetsecurity.com/2019/12/02/5g-iot-security/#:~:text=%E2%80%9CLarge%20numbers%20of%20vulnerable%2C%205G,some%20aspect%20of%20the%20infrastructure.%E2%80%9D
18. F.B. Saghezchi, G. Mantas, J. Ribeiro, M. Al-Rawi, S. Mumtaz, J. Rodriguez, Towards a secure network architecture for smart grids in 5G era, in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, (IEEE, Valencia, 2017), pp. 121–126
19. B. Seok, J.C.S. Sicato, T. Erzhena, C. Xuan, Y. Pan, J.H. Park, Secure D2D communication for 5G IoT network based on lightweight cryptography. Appl. Sci. **10**(1), 217 (2020)
20. T. Lagkas, V. Argyriou, S. Bibi, P. Sarigiannidis, UAV IoT framework views and challenges: Towards protecting drones as "things". Sensors **18**(11), 4015 (2018)
21. D.H. Cruickshank, Security and privacy open issues in 5G connected IoT devices. Guildford, Surrey: Institute for Communication Systems (ICS), http://www.charisma5g.eu/wp-content/uploads/2016/07/Security-and-privacy-open-issues-in-the-5G-connected-IoT-devices.pdf
22. Q.E. Ali, N. Ahmad, A.H. Malik, G. Ali, W.U. Rehman, Issues, challenges, and research opportunities in intelligent transport system for security and privacy. Appl. Sci. **8**(10), 1964 (2018)
23. N. Cranford, Understanding end-to-end network slicing for 5G (2018), https://www.rcrwireless.com/20180404/understanding-end-to-end-network-slicing-for-5g-tag27-tag99
24. V.A. Cunha, E. da Silva, M.B. de Carvalho, D. Corujo, J.P. Barraca, D. Gomes, et al., Network slicing security: Challenges and directions. Internet Technol. Lett. **2**(5), e125 (2019)
25. Z. Kotulski, T.W. Nowak, M. Sepczuk, M. Tunia, R. Artych, K. Bocianiak, et al., Towards constructive approach to end-to-end slice isolation in 5G networks. EURASIP J. Inf. Secur. **2018**(1), 2 (2018)
26. R. Borgaonkar, L. Hirschi, S. Park, A. Shaik, New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. Proc. Privacy Enhancing Technol. **2019**(3), 108–127 (2019)
27. A. Koutsos, The 5G-AKA authentication protocol privacy, in *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, (IEEE, Stockholm, 2019), pp. 464–479
28. D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, V. Stettler, A formal analysis of 5G authentication, in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, (ACM, Toronto, 2018), pp. 1383–1396
29. A. Adeel, J. Ahmad, A. Hussain, Real-time lightweight chaotic encryption for 5G IoT enabled lip-reading driven secure hearing-aid. arXiv preprint arXiv*:*1809.04966 (2018)
30. Privacy international, https://privacyinternational.org/long-read/3100/welcome-5g-privacy-and-security-hyperconnected-world-or-not
31. I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mech. Syst. Signal Process. **135**, 106382 (2020)
32. A.K. Sikder, G. Petracca, H. Aksu, T. Jaeger, A.S. Uluagac, A survey on sensor-based threats to internet-of-things (IoT) devices and applications. arXiv:1802.02041 (2018)