WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Identity Privacy and Security for 5G Network

Dr. Rangaswamy[1], R Saikrithi[2]

[1,2] Dept. of ECE, SJCIT, Chickaballapur, India

[1]crsecesait@gmail.com, [2]rsaikrithi2002@gmail.com

ABSTRACT—

The Fifth Generation (5G) of wireless communication refers to a more recent generation of mobile networks. Assessments in the area of mobile communication technologies are provided in this article. For these functionalities to be available to all users, the 5G network must ensure extremely high security and privacy standards. A major worry for many academics studying mobile networking is user privacy, specifically with regard to long-term subscription identifiers that are also known as temporary identifiers for international mobile subscribers and short-term subscription identifiers that are also known as temporary identifiers for mobile subscriptions and cell-radio networks. These identifiers are used for paging, location updates, and permanent identification. Additionally, it covers the majority of research on user identification in the context of the 5G network that makes use of temporary identities like TMSI and IMSI in clear text.

I. INTRODUCTION

The field of wireless communication has had remarkable expansion in the last three decades, particularly with the move from 1G to 4G. Smart campuses and smart grids are just two examples of the progressive improvements and advancements made possible by the fifth generation mobile network, which is a new generation network. The foundation of 5G mobile communication technology is a new architecture. For the new wireless communications. Till now this was the most exposed in the world as they are not as the urban and rural there is same as different. As every one can be accessed the network for the purpose of the communication purpose and some good or the bad use.

It goes without saying that security setups and designs from earlier eras might not work with 5G. The standard justification for new security planning and engineering is that it stems from recent administrations and sudden, potentially contradictory organizational structures when an egalitarian and flexible organizational structure was the norm only a few years before. Although the inter-necessities, such as verifying inactivity in vehicular correspondence or "Unmanned Aerial Vehicles" (UAVs), were not as necessary in terms of safety, the security system of the future soon emerged on the refinement anticipated to ensure 5G networks. In addition to the network the security should be improved for the protection of the data and in which they should be highly secured and should be protected and secured in which no one can be accessed the data in which it should be protected.

The transition to 5G is to a superior extent Of a structural move than an advancement od current innovation. These capacities will reinforce extended applications going from HD video spilling to telemedicine to self-driving vehicles and brilliant urban communities under the “web of the things” rubric. The union of substantial variety of IoT devices and arrangements of new administrations, for example, for devoted houses, medical clinics, delivery, and electric matrix framework in 5G will furthermore stimulate the security demanding situations. As if the mobile network is as fast as the it works the users can be increased in advance in which the network.

II.TECHNOLOGY

The configuration of our system.5G cellular network are based on a number of different technologies, which are reviewed by some of them and some of them are mentioned and explained below: Millimeter waves, Small cells, Full duplex, Beamforming, Massive MIMO, Software Defined Network (SDN), Location privacy, and Paging. As there are more and only some of them are been mentioned above and explained.

1. Millimeter waves :

These electromagnetic waves are located in the 30-300 GHz frequency range, as opposed to the band below 6 GHz that is utilized for 4G LTE. 5G networks may employ unlicensed frequencies and transfer massive amounts of data over short distances thanks to the microwave band, which is slightly below millimeter waves. Wi-Fi is now using it. without interfering with Wi-Fi networks by utilizing tiny cells to enhance traditional cellular networks. The extremely high frequency is the international telecommunication union designation for te band of radio frequencies in the electromagnetic spectrum from 30 to 300. Compared to lower bands, radio waves in this band have high atmospheric attenuation they are absorption increases with the frequency.

2. Small cells:

Small cells are low-powered cellular radio access nodes that operate in spectrum that have a range of 10 meters to a few kilometers. They are base stations with low power consumption and cheap cost. They can provide high data rates by being deployed densely to achieve high spatial spectrum efficiency. Their intended use is mainly for dense areas, such as stadiums and indoors. Small cells are available for a wide range of air interfaces.

A point-to-point system made up of two or more linked parties or devices that are capable of bidirectional communication is known as a duplex communication system. Many communications networks use duplex systems, either to enable two connected parties to communicate simultaneously in both directions or to offer a backward path for remote equipment adjustment and monitoring in the field. Duplex communication systems come in two flavors: half-duplex (HDX) and full-duplex (FDX).

3. Beamforming:

In sensor arrays, beamforming, also known as spatial filtering, is a signal processing technique used for directed signal transmission or reception.To do this, an antenna array's components are assembled so that certain signals at specific angles encounter constructive interference while others encounter destructive interference. To achieve spatial selectivity, beamforming can be applied at both the transmitting and receiving ends. The directivity of the array is the enhancement over omnidirectional reception/transmission.

The use of beamforming allows one to deliver high quality signals to receiver. Thus reducing the transfer latency time and the number of errors.

4. Massive MMIO :

MIMO stands for Multiple-input multiple-output. While it involves multiple technologies, MIMO can essentially be boiled down to this single principle: a wireless network that allows the transmitting and receiving of more than one data signal simultaneously over the same radio channel.

Standard MIMO networks tend to use two or four antennas. Massive MIMO, on the other hand, is a MIMO system with it.

A MIMO network has an advantage over a conventional one in that it can increase a wireless connection's capacity without using additional airwaves. There have been significant advances in capacity, which could lead to a 50-fold rise in the future, according to reports.

5. Software Defined Network:

Software-defined networking (SDN) is an approach to network management that enables dynamic and programmatically efficient network configuration to improve network performance and monitoring in a manner more akin to cloud computing than to traditional network management.[1] SDN is meant to improve the static architecture of traditional networks and may be employed to centralize network intelligence in one network component by disassociating the forwarding process of network packets (data plane) from the routing process (control plane). The control plane consists of one or more controllers, which are considered the brains of the SDN network, where the whole intelligence is incorporated. However, centralization has certain drawbacks related to security, scalability and elasticity.[Thus making 5G cellular networks able to meet different application requirements.

III. WORK ON SECURITY OF 5G

1. Security Standards on 5G:

The quality and efficiency of 5G are further improved by the publication of the R16 standard by 3GPP. For instance, new technologies are being launched to allow 0.5-1 ms air interface delay and synchronization accuracy for industrial internet, which can result in end-to-end lower latency and improved dependability. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) direct link communication is supported by the internet of vehicles. reaches meter level and increases positioning accuracy by over ten times using a range of communication techniques. Major worldwide standards organizations and industry associations have conducted study on 5G application security.

2. Authentications in 5G:

Security authentications face higher requirements in 5G applications. On the one hand, in order to protect the application data of power, industry, finance, an other important fields carried by 5G network, the concept of secondary authentication for access network. On the 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.

3. Secondary authentication for industry:

Security authentications face higher requirements in 5G applications. On the one hand, in order to protect the application data of power, industry, finance, an other important fields carried by 5G network, the concept of secondary authentication for access network. On the 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.

4. Three Factor Authentications for Mobile: Cloud servers are easily accessible through lightweight mobile devices for online payments, video chatting, e-commerce, etc. However, the security and privacy of user data would also be at danger due to the open nature of wireless network communication, thus authentications for mobile light devices should be taken into account.

5. Other research focuses:

Regarding the security architecture of 5G applications, the 5G smart city security references architecture was released by GTI (Global TD-LTE Initiative). Wang and Liu conducted security enhancement requirements assessments and 5G application analyses for specific industries with high security levels. They also presented a security architecture design scheme based on industry slices.

6. Network Slicing:

Network slicing is yet another crucial 5G technology. Zhou suggested four development approaches for network slicing based on various needs for network topology flexibility, security levels, and cost.

7. User privacy leakage:

The likelihood of private information leaking has grown due to the eMBB service leak, which comprises a significant amount of user privacy information or identification, device identification and address information, and 5G network openness.

8. Data privacy:

There is a great likelihood that user personal data may leak because 5G technology will connect a vast number of intelligent and heterogeneous gadgets. Without the consent of the customer, service providers and businesses keep and utilize their personal data. Occasionally, the service provider keeps user data for their own product but then distributes it to other businesses so they can examine the data and identify patterns that indicate which of their own products is better suited for the specific users.

IV. WORKING PROCEDURE

1. IMSI Encryption:

In mobile networks, the internet mobile subscriber identification is a long-term subscription identifier. IMSI encryption is essential for safeguarding user identification in 5G.

The network makes sure that this private data is not sent in plain text by encrypting the IMSI. This stops illegal access to user identities and listening in on conversations.

2. Home Network Authentication:

Home network authentication is a step in the 5G network access procedure.

A user's device authenticates with their home network when it connects to the network. This authentication process guarantees that access.

5G guards against identity theft and unauthorized access by confirming the user's identity at the home network level.

3. Privacy Enhanced Fast Mutual Authentication:

PEFMA is an identity-based encryption technique. With this method, the user equipment does not need to be connected to the server network via the home network.

Through network authentication, the UE encrypts its permanent identity.

V. CONCLUSION

Identity privacy in 5G networks is a crucial issue that needs to be carefully taken into account with many different elements. 5G networks can guarantee secure and efficient communication while protecting user privacy by using privacy presentation approaches and following regulatory frameworks.

The security and privacy of the 5G ecosystem are heavily influenced by network operators, equipment vendors, application developers, and service providers. 5G is closely interwoven with social life and vertical businesses. A thorough and methodical design is necessary to ensure security and privacy in 5G applications. Appropriate security measures must also be developed based on industry requirements and the unique application scenarios. Users' privacy, which includes both short-term and long-term subscription identifiers as International Mobile Subscribers Identifiers, is a major concern for many academics studying mobile net working.

From the first generation to 5G, which includes identity and location privacy, there have been issues with user privacy. In this article, user privacy in 5G networks is examined along with earlier generations.

VI. APPLICATIONS

1. 5G is anticipated to advance mission-critical video and data transmission as well as mission-critical push-to-talk (MCPTT).

2. Products and appliances for smart homes are in demand right now. Because the 5G network offers fast speed and low latency, smart homes become more realistic.

3. Very low latency high-speed communication is provided via wireless networks, which is important for autonomous driving.

4. 5G technology will be essential to smart farming and agriculture. Farmers will be able to monitor and swiftly respond to crop threats with the use of 5G sensors and GPS technology.

5. The cellular network does, in fact, include all of the anticipated network security guarantees.

6. In certain places, fixed wireless connections will provide an alternative to fixed line broadband.

7. A real time digital twin of the real object such as a turbine engine, aircraft, wind turbines, offshore platform and pipelines.

8. It is imperative that privacy protocols are incorporated directly into the 5G network's architecture.

VII. FUTHE SCOPE

- Encryption techniques are a viable means of achieving data transmission security. Transmitted data is encrypted to keep message contents secret from prying eyes.
- Since the majority of Internet of Things devices have limited resources, security-enhancing solutions need to be computationally efficient. As a result, with Internet of Things infrastructure, balancing security and performance is difficult.
- The performance and security of many IoT applications are enhanced by the combination of edge computing and IoT technologies.
- Adding machine learning techniques to the fog layer can increase the scalability and energy efficiency of lightweight Internet of Things devices.
- Only information revealed at the intended destination should be disclosed; data transit across various IoT layers needs to be safe. End-to-end security requires the application of security mechanisms at each of the three IoT layers.
- Reliability of data is crucial for important Internet of Things applications like the healthcare system. The data that the Internet of Things devices collect can be analyzed and categorized using machine learning and artificial intelligence algorithms.
- Legal frameworks that reinforce data protection laws and rules, such as the CCPA and GDPR, to guarantee responsibility and openness in identity management and data processing procedures.
- The integration of privacy-preserving technologies and solutions, such as homomorphic encryption, secure multi-party computation, and differential privacy, to safeguard user data and provide insightful and helpful analytics.

VIII. REFERENCES

[1]. Saeed, R.A, Saeed, M.M, Mokhtar, R.A., Alhmuyani, H.,Abdel-Khalek, S.:Pseudonym mutable based privacy for 5G user identity.J.Comput. Syst. Sci. Eng. 29(1), 1-14 (2021).

[2]. Saeed, M.M.,Hasan, M.K.,Hassan,R., Mokhart, R., Saeed,R.,A., Saeid, E., Gupta, M:Preserving privacy of user identity based on pseudonym variable in 5G, CMC- Computers. Comput., Materials & continua (70(3),5551- 5568222).

[3]. Wang,Y.,Zhang,Z., Xie, Y.. :Privacy preserving and standard-compatible AKA protocolfor 5G In: 30th USENIX Security Symposium (2021).

[4]. Hasan,M.,K, et al.: Lightweight cryptographic algorithm for guessing attacks protection in complex internet of things applications. Complexity 2021, 1- 13(2021).

[5]. N. Lindskog and H.Englund, “why side-channel analysis attacks are increasing and how to stop them, “tech. rep.,2023.

[6]. M. S . Khan =, B. Farzaneh, N, Shahariar, N Sahan, and R. Boutbada, “Slicese cure: Impact and detection of dos/ddos attacks on 5G network slices”, in 2022 IEEE Future network world forum (FNWF),pp.639-642,2022.

[7]. NSA and CISA, “ 5G network slicing: security considerations for design, deployment, and maintenance, “ tec. Rep.m 2023.

[8]. R. M. Dhanasekaran, J. Ping, and G. P. Gomez, “End- to-End network slicing across standards organizations,” IEEE Communications Standards Magzine, vol. 7, no. 1,2023.