International Journal of Engineering and Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 12 Issue 10 October 2023 || PP 77-81

Advance Security and Privacy Issues in 5g and 6g Networks

[1] Alumona T.L [2] Okorogu V.N [3] NWEZEEKWUNIFE O. G
[1] *Electronic and Computer Engineering, Nnamdi Azikiwe University Awka, Anambra State Nigeria*
[2] *Electronic and Computer Engineering, Nnamdi Azikiwe University Awka, Anambra State Nigeria*
[3] *Electronic and Computer Engineering, Nnamdi Azikiwe University Awka, Anambra State Nigeria*

ABSTRACT
With the coming of 5G and impending introduction of 6G networks, new prospects for improved connectivity and communication are opening up. These cutting-edge networks, nevertheless, also present fresh privacy and security difficulties. In order to solve the changing security and privacy challenges in 5G and 6G networks, this solution paper investigates cutting-edge tactics and solutions. This work explores several security and privacy threats to the stated networks, as well as proffered solutions to these advance security and privacy issues.

Date of Submission: 01-10-2023 Date of Acceptance: 12-10-2023

I. INTRODUCTION

It is fact that the sixth generation (6G) of mobile communication is already envisioned despite of the fact that 5G specifications are still developing and 5G coverage is not yet fully provided [1]. The most significant driving force in 6G leap is the inherent connected intelligence in the telecommunication networks accompanied with advanced networking and Artificial Intelligence (AI) technologies. In the development and implementation of 5G and 6G networks, security and privacy are top priorities [1]. These networks, which represent the next wave of wireless communication technology, promise greater connectivity, faster speeds, and low latency, but they also bring with them new risks and weaknesses. In 5G and 6G networks, the following cutting-edge security and privacy vulnerabilities exist: Network Slicing Security issues, IoT Vulnerabilities, Massive MIMO and Beamforming Attacks, Quantum Cryptography Needs, AI-Enhanced Threats, Edge Computing Security, Privacy Concerns with Location Data, Supply Chain Security, Authentication and Identity Management, Policy and Regulatory Challenges, Resilience and Disaster Recovery issues and Cross-Domain Security.

In this work, we shall be discussing the above listed issues, in a few to understanding how they affects the network proffer solutions to mitigate them.

The introduction of 6G network is expected to greatly enhance the development, deployment and use of artificial intelligence (AI), but however, the alliance between 6G and AI may also be a double-edged sword in many cases. While we tap into the immense benefits inherent in these networks, we should be ready to deal with the security and privacy issues that will arise from them.

II. SECURITY AND PRIVACY ISSUES IN 5G and 6G NETWORKS

1. IoT Vulnerabilities: The proliferation of Internet of Things (IoT) devices in 5G and 6G networks increases the attack surface. Many IoT devices lack robust security features, making them vulnerable to attacks, which can have cascading effects on the network. Researchers warn that the proliferation of data traffic and mobile IoT connectivity comes with a significant amount of risk that should be addressed by the telecom industry before5G is deployed on a large scale [2]. Designers must foresee and prepare for dangers, incorporating efficient security measures into the design of 5G networks rather than attempting to handle problems as they happen, to ensure the best security for IoT deployments. According to the Author in [2], advanced challenges for IoT on 5G include:
An Evolving Trust Model:

Trust models define standards for how devices assess the security of other devices and systems and determine if a connection is secure. The trust model has changed significantly between 4G and 5G networks. With increasing separation from the network core in a standalone 5G system, trust declines. The universal integrated circuit card (UICC) and the universal subscriber identity module (USIM) serve as a foundation for trust. For hardware and software to operate safely under the new trust paradigm, IoT developers and network operators must collaborate.

Authentication Systems:

Providers employ authentication mechanisms, which have significantly evolved between 4G and 5G, to identify various devices on a 5G network. There are a variety of supported authentication models, all of which can operate, for instance, over Wi-Fi because they are radio access network (RAN) neutral. Strong device authentication is crucial for 5G security because of the vast number of devices collecting data in IoT networks, such as connected municipal infrastructure, medical systems, smart offices, and residences. Investment in safe biometric authentication solutions can stop device hacking and identity theft.

Data Privacy:

While 4G and other technologies have trouble ensuring privacy, 5G expressly addresses this issue. It's simpler to monitor than prior systems because it's mostly software-based and cloud-based, and more data is encrypted. Carriers, integrators, and privacy specialists will need to adapt to a new normal as a result of the infrastructural changes, but they also lay a strong foundation for data protection going forward.

2. Network Slicing Security: Network slicing is a key feature in 5G and 6G networks that allows operators to create multiple virtual networks on a single physical infrastructure. This introduces potential security risks as malicious actors may exploit vulnerabilities in one slice to affect others or gain unauthorized access. According to [3], network slicing is the concept of partitioning the physical network infrastructure into multiple self-contained logical pieces which can be identified as slices. Each slice can be customized to serve and meet different network requirements and characteristics. In terms of security, network slices has allowed for new security vulnerabilities such as Distributed Denial of Service (DDoS) and resource exhaustion. However, slices can be isolated to provide better resource isolation. In addition, each slice is considered an end-to-end virtual network, operators would be able to allocate resources to the tenants which are the service providers. The isolated resources are controlled by the tenants; each tenant has control over how to use them to meet the requirements of the clients. One of the challenges in network slicing is Radio Access Network (RAN) slicing. The target of RAN Slicing is to meet the QoS requirements of different services for each end-user. However, the coexistence of different services is challenging because each service has its requirements. Each slice must estimate its network demands based on the QoS requirements and control the admission to the slice. To solve this issue, we consider the scenario for the enhanced mobile broadband (eMBB) and the ultrareliable-low-latency communication (URLLC) use cases' coexistence, and we slice the RAN based on the priority of the user application.

One of the biggest security challenges for network slicing in 5G is Distributed Denial of Service (DDoS) attacks [4]. These attacks involve targeting services with the goal of overloading them with a large amount of traffic till they are inaccessible to other end-users.

DDoS attacks can also take the form of depriving a target of resources it shares with other hosts. The misappropriation of necessary features in 5G technology, such as overload control metrics, could facilitate these types of attacks.

There are three primary categories of security vulnerabilities [3]:

1. Network slice life-cycle security concerns
2. Intra-slice security concerns
3. Inter-slice security concerns

[3] Suggested some technological solutions towards 5G Network Security, to include:

1. End-to-End Security
2. Isolation

3. Massive MIMO and Beam forming Attacks: 5G and 6G networks rely heavily on technologies like massive multiple-input, multiple-output (MIMO) and beamforming for improved performance. However, these technologies can be exploited for eavesdropping or signal jamming if not adequately secured.

According to [5], mutual authentication and end-to-end encryption are still a challenge and the subject to demand a breakthrough. Absence of these two features is a major source of many notorious attacks such as fake operators, eavesdropping, and traceability attacks. Even 5G is likely to fail to meet these security goals, since implementing these two features faces challenges of high computation and communication overload. Without a breakthrough in processing capacity and management models, a mandate of strong end-to-end encryption and mutual authentication in 6G can impact on many latency-sensitive services. Any delay to have such features in 6G can practically sink the hope of thoroughly fixing the existing security issues.

4. Artificial Intelligent -Enhanced Threats: AI and machine learning are being used both defensively and offensively in cyberattacks. Malicious actors can leverage AI to create more sophisticated and targeted attacks, making it challenging to detect and mitigate threats effectively.

A. Security Issues in Artificial Intelligent

1) Issues: 6G uses AI-enabled functions to create connected intelligence, notably with machine learning (ML) systems that are vulnerable to security risks. A ML system's learning phase is affected by poisoning attacks, which causes the model to learn incorrectly. Examples of poisoning attacks include data injection, data manipulation, and logic corruption. During the inference phase, evasion assaults make use of expertly prepared adversarial samples to try to evade the model. Attacks on ML models based on the API include model extraction, model inversion, and membership inference [5,6].
2) Solutions: Resilient AI systems can be built using potential defenses like adversarial machine learning and moving target defense. Other defense strategies include input validation and strong learning to counter poisoning attacks, adversarial training and defensive distillation to counter evasion attacks, and differential privacy and homomorphic encryption to counter API-based assaults. With these defense systems, it is difficult to strike a balance between enhanced defense and performance degradation [5,6].
B. Privacy Issues in Artificial Intelligence
1) Issues: Due to AI's capacity for large-scale data processing, together with future computing speeds and network automation requirements, privacy can be easily compromised. With billions of gadgets required for 6G, individuals no longer have control over how other systems will treat their data. For instance, the suggested intelligent authentication systems [5, 7] may employ private user data and depend on physical features. Data thieves may target insecure IoT devices (such as weak sensors) feeding AI algorithms with personal information. Attacks on ML using model inversion to retrieve training data have the potential to violate privacy [5, 8].
2) Solutions: By enforcing a physical control to keep data closer to the user, edge-based federated learning protects data privacy [5, 8]. A technical control for privacy preservation is imposed by homomorphic encryption, which permits conducting mathematical operations without decrypting data [5, 9]. To verify that learning with encrypted data yields the same results as learning with plain data, more research on homomorphic encryption is required. Differential privacy approaches can conceal private information from learning models by introducing random noise to the training data [5, 10].

5. Privacy Concerns with Location Data: 5G and 6G networks can provide highly precise location data, which raises privacy concerns. Unauthorized access to this data can lead to stalking, surveillance, or other privacy violations.
[11] Opines that there are also new privacy issues to contend with due to the diversity of business types and application scenarios in 5G networks. The openness of the platform can mean that a user's sensitive information can easily and frequently change from a closed state to an open state. Accordingly, the contact state changes from offline to online, greatly increasing the risk of leaks. Therefore, the privacy issues we will inevitably face with 5G will become a problem that must be faced and solved in the next few years. Fortunately, advancements in data mining and machine learning technologies mean that privacy protection methods have been well trained and will only become more powerful in the future.

6. Quantum Cryptography Needs: With the advent of quantum computing, traditional encryption methods may become vulnerable to attacks. As a result, there's a need to develop and implement quantum-resistant cryptographic algorithms to ensure the long-term security of 5G and 6G networks. According to [12], the 6G system has to get rid of existing asymmetric key encryption techniques since quantum computers will make them insecure. Post-quantum cryptography (PQC) solutions, such as lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based signature, have been the focus of many researchers. As part of its PQC study, the US National Institute of Standards and Technology (NIST) is scheduled to pick the best PQC algorithms between 2022 and 2024. In comparison to Rivest–Shamir–Adleman (RSA), the key length presently under consideration for PQC is projected to be many times larger. PQCs are likely to have a larger computational cost than the current RSA method. As a result, it is essential that PQC be appropriately integrated into the 6Gnetwork's HW/SW performance and service needs [12].

7. Authentication and Identity Management: Ensuring strong authentication and robust identity management is essential to prevent unauthorized access to network resources. This includes implementing multi-factor authentication and biometric security measures. The Author in [13] stated that authentication using biometrics or a password-free service to access control mechanisms has been a long-awaited feature for 6G security. Many applications have relied on password-based security methods for decades. Unfortunately, there are several drawbacks. Some may be easily hacked, expensive to store, and difficult to remember. Brainwave/heartbeat-based authentication might deliver a more secure and improved user experience in the future.

8. Other Security and Privacy issues: We have listed below, other challenges relating to security and privacy in 5G and 6G networks.

a) Edge Computing Security: Edge computing is a fundamental component of 5G and 6G networks, bringing processing closer to the end-users. Securing edge nodes and ensuring data privacy at the edge is crucial to protect sensitive information.
b) Supply Chain Security: Securing the supply chain for network equipment and devices is crucial. Hardware or software components with vulnerabilities can be exploited to compromise the entire network.
c) Policy and Regulatory Challenges: The rapid deployment of 5G and 6G networks often outpaces regulatory and policy frameworks. Establishing comprehensive and up-to-date regulations to address emerging security and privacy challenges is a significant hurdle.
d) Cross-Domain Security: 5G and 6G networks will likely span multiple domains, including telecommunications, healthcare, transportation, and more. Ensuring security across these domains and preventing unauthorized access is a complex challenge.
e) Resilience and Disaster Recovery: Building resilience into 5G and 6G networks is crucial to ensure uninterrupted service during cyber-attacks or natural disasters. Effective disaster recovery plans and redundancy measures are essential.

III. SOLUTIONS TO 5G AND 6G NETWORK ISSUES

Addressing these advanced security and privacy issues in 5G and 6G networks will require collaboration among industry stakeholders, governments, and cyber-security experts. It will also involve continuous research and development of new security technologies and practices to stay ahead of evolving threats. This articles happen to have some solutions to the stated problem, as stated the various subsections in section 2.0 and filtered out in this chapter.

1. AI-Powered Threat Detection: Use AI and machine learning algorithms to quickly identify and address risks as they change. Unusual patterns and probable security vulnerabilities can be found via behavioral analysis and anomaly detection.
2. Network Slicing Security: Secure network slicing is essential for protecting the resources allotted to each slice and isolating vital services. Strict access control and the implementation of security regulations for each network slice aid in preventing unauthorized access.
3. Zero-Trust Architecture: By adopting a zero-trust security paradigm, even within the network, trust is never assumed, security can be improved. Continuous device and user authentication, permission, and validation are crucial components.
4. End-to-End Encryption: By putting strong end-to-end encryption methods in place, you can make sure that data is kept private as it moves throughout the network. To defend against hypothetical quantum attacks in the future, quantum-safe encryption techniques should be investigated.
5. Privacy-Preserving Technologies: Use privacy-preserving technologies to safeguard user data, such as homomorphic encryption and secure multi-party computation. In the processing of data, anonymization techniques can aid in protecting user privacy.
6. Security by Design: Don't add security as an afterthought to the architecture and design of 5G and 6G networks. Conduct extensive security audits and penetration tests while the system is being developed.
7. Blockchain for Security and Privacy: 5G and 6G networks' security and openness can be improved by utilizing blockchain technology. It can be used for decentralized control, secure identity management, and data provenance.
8. Collaborative Threat Intelligence: Create partnerships and information-sharing platforms to promote the sharing of threat intelligence among suppliers and service providers. Early warning systems can support proactive threat management.
9. User Education and Awareness: Inform users about the privacy and security vulnerabilities that may be present with 5G and 6G networks. Users should be encouraged to frequently update their devices and follow best security practices.
10. Redundancy and Resilience: Include failover and redundancy methods in the network to preserve service availability during network outages or cyber-attacks. Implement and frequently test your disaster recovery strategy.
11. Continuous Monitoring and Updates: To stay ahead of evolving threats, update network infrastructure and security controls often. To spot and address new vulnerabilities, keep an eye on network activity.
12. Regulatory Compliance: Comply with national and regional laws governing network security and data protection. The security and privacy of user data can be ensured by adhering to regulations like General Data Protection Regulation (GDPR) and National Institute of Standards and Technology (NIST).
13. Ethical Considerations: To prevent abuse, ethical standards for AI and automation in these networks should be created. Make that user security and privacy are given priority in AI-driven decisions.

In conclusion, addressing advanced security and privacy issues in 5G and 6G networks requires a multi-faceted approach that combines advanced technologies, regulatory compliance, and user education. By adopting these solutions, stakeholders can pave the way for secure and privacy-respecting next-generation networks.

IV. CONCLUSION

In conclusion, a new era of connectedness and technical advancement has been ushered in by the arrival of 5G and the continuous development of 6G networks. These improvements do, however, present important privacy and security problems. As we've seen, as these networks' speed, capacity, and connectedness expand, so do the opportunities and dangers they present.

Network operators, manufacturers, and regulatory agencies must collaborate to create effective security procedures in the context of advanced security. To protect against cyber-attacks, these may incorporate encryption, authentication, and intrusion detection systems, among others. The integrity and dependability of 5G and 6G networks must be guaranteed by the proactive identification and mitigation of vulnerabilities.

In these networks, privacy issues are equally important. Individual privacy is at stake due to the massive amount of data collected and sent via these high-speed networks. The difficulty of finding a balance between data collecting for network performance and user privacy protection calls for considerable thought. The key to addressing these issues is implementing privacy-enhancing technologies and following data protection laws.

Furthermore, to keep ahead of new security and privacy vulnerabilities as these networks develop, continual research and engagement among stakeholders are essential. This includes exchanging threat intelligence and sharing threat intelligence, as well as developing AI-driven security solutions.

In conclusion, 5G and 6G networks have enormous potential to change businesses and improve connectivity globally. But in order for them to reach their full potential, it is crucial to solve sophisticated security and privacy challenges. In an increasingly connected world, we can profit from these networks while protecting our data and privacy by being vigilant, working together, and implementing cutting-edge solutions.

REFERENCES

[1]. P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, M. Ylianttila, "6G Security Challenges and Potential Solutions".

[2]. M. Voicu, "The Risks to 5G IoT: Preparing for the NextGeneration of Cybersecurity Threats", https://www.telit.com/blog/5g-iot-security-issues-solutions, 2021.

[3]. R. J. Alghawi, "Network Slicing in 5G: Admission, Scheduling, and Security", Graduate Theses, Dissertations, and Problem Reports. 11346. https://researchrepository.wvu.edu/etd/11346, 2022.

[4]. D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate ddos attacks on 5g core network slices," in 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019, pp. 82–90.

[5]. Y. Siriwardhana, P. Porambage, M. Liyanage, M. Ylianttila, "AI and 6G Security: Opportunities and Challenges", Centre for Wireless, Communications, University of Oulu, Finland,

[6]. C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?" IEEE Network, vol. 34, no. 6,pp. 140–147, 2020.

[7]. H. Fang, A. Qi, and X. Wang, "Fast Authentication and Progressive Authorization in Large-Scale IoT: How to Leverage AI for Security Enhancement," IEEE Network, vol. 34, no. 3, pp. 24–29, 2020.

[8]. Y. Sun, J. Liu, J. Wang, Y. Cao, and N. Kato, "When Machine Learning meets Privacy in 6G: A Survey," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2694–2724, 2020.

[9]. J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy Preservation for Machine Learning Training and Classification based on Homomorphic Encryption Schemes," Information Sciences, vol. 526, pp. 166–179, 2020.

[10]. T. Zhang, T. Zhu, P. Xiong, H. Huo, Z. Tari, and W. Zhou, "Correlated Differential Privacy: Feature Selection in Machine Learning," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2115–2124, 2020.

[11]. M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, "Security and privacy in 6G networks: new areas and new challenges", Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020.07.003.

[12]. T. C. Clancy, R. W. McGwier, L. Chen, "Post-Qantum Cryptography and 5G Security",

[13]. S. A. A. Hakeem, H. H. Hussein, H. W. Kim, "Security Requirements and Challenges of 6G Technologies and Applications", Yuh-Shyan Chen, Academic Editor, 2022

Alumona T.L , et. al. "Advance Security and Privacy Issues in 5g and 6g Networks". *International Journal of Engineering Science Invention (IJESI)*, Vol. 12(10), 2023, PP 77-81. Journal DOI-10.35629/6734