E-ISSN: 2997-9382
American Journal of Technology Advancement
https://semantjournals.org/index.php/AJTA

| Research Article

Check for updates

Enhanced Security Features of 6G Network: A Leap Beyond 5G Network

Ayegba Abdullahi
Engineering and Space Systems Department, National Space Research and Development Agency, Abuja, Nigeria

Iruemi Olohimai Juliet
Ground Station and Mission Planning Department, National Space Research and Development Agency, Abuja, Nigeria, Abuja, Nigeria

Ojo Omeiza David
Electrical and Electronics Engineering Department, Federal Polytechnic Idah, Kogi State, Nigeria

Ogundipe Rotimi Josiah
KANMI ALO Interlink Polytechnic, Ijebu, Ijesha, Osun State, Nigeria

Alao Olafunke Janet
Space Regulation and Spectrum Management Department, National Space Research and Development Agency, Abuja, Nigeria

Abstract
The aim of this research work was to examine how 6G is better than 5G in terms of security. The research, which made use of secondary data and qualitative research (descriptive and review research methods), revealed that 6G is more secure than 5G through the use of zero-trust architecture, AI-driven security, quantum-secure communication, network slicing security, enhanced visibility and control, improved authentication, secure multi-party computation, and blockchain integration. In addition to these security features, it was observed from the result that 6G has some advantages over the 5G network, such as advanced AI integration, ultra-low latency, faster speeds, enhanced network capacity, improved security, and real-time applications. From the results, it was concluded that the 6G network has enhanced security compared to the 5G network when the 6G network is being deployed.

Keywords: Artificial intelligence, Encryption, Security, sixth generation (6G), Zero trust Architecture.

1.0 Introduction

The sixth generation (6G) network is wireless communication technology expected to succeed 5G and expected to deliver even faster data speeds and other improved features or properties. 6G is expected to bring in contact or connect trillions of people who are far apart in order to bring the world closer, using some emerging technology like the Internet of Things (IoT), which is currently gaining popularity due to its ability to connect systems and devices that were previously isolated or unreachable (Huang *et al.* 2019, Ajeng *et al.* 2021). Compared to the current 5G generation, 6G is expected to be accessible anywhere, faster, more responsive, reliable, and secure, and have a higher rate of data transferable at any one time and be compatible with various networks such as 5G, Wi-Fi, and satellite (Dylan and Simon, 2024). According to Pavan (2021), radio resource management must become more adaptable and intelligent with the rise of linked devices and technologies like IoT, 5G, and 6G. Presently, the use of blockchain technology and the sixth-generation mobile communication network (6G) has garnered significant attention, as their fusion is poised to profoundly impact the digital economy and society at large (Liu, 2024). In the view of Ahmed (2024), the emergence of blockchain technology and 6G networks has revolutionized service migration, as the dawn of 6G communication networks promises to transform the way communication services are implemented and managed. This new technology will enable a more secure and reliable environment for services to migrate from traditional 4G and 5G networks.

As noted by Thara *et al*. (2025), the rising implementation of sixth-generation (6G) technology allows systems to achieve ultra-state data rates, ultra-low latency, massive connectivity, and intelligent communication capabilities. As part of this shift towards 6G, various distributed ledger technologies are becoming increasingly important for providing a secure platform for data storage and management [Lu *et al.,* 2021]. Very importantly, the transition from 5G to 6G networks introduces significant advancements in speed, latency, and connectivity, but also raises critical security concerns. The increasing number of devices that need to be plugged into the network makes the demand for enhanced security and efficiency paramount (Mengxu and Yubo, 2025).

2.0 Materials and Method

2.1 Materials: The materials used for the work are secondary data. This comprises online materials relating to the topics. It also made use of library materials such as textbooks and journals.

2.2 Method: The research made use of the quantitative research method. It adopted descriptive and review research approaches of qualitative research methods. Descriptive research aims to accurately describe and document the characteristics, behaviors, or phenomena of a particular population, group, or situation without explaining or interpreting the findings, while a review research method synthesizes and summarizes existing research findings on a specific topic to provide an overview of the current state of knowledge and identify gaps or areas for further research.

2.3. Features of 6G Network

Below are some features of the 6G network.

2.3.1. Energy Efficiency

Energy efficiency deals with the use of technology that reduces the amount or quantity of energy needed to carry out a particular role or function. Energy efficiency is one of the features of 6G, as it will minimize energy consumption as a result of the improved technology while maintaining an improved communication network. Through the optimization of network infrastructure and carrying out the implementation of intelligent power management techniques, 6G networks will aim to minimize energy consumption while delivering high-performance connectivity.

2.3.2. Very High Data Rates

Data rate deals with the amount of data that can be transmitted over a communication network at a given time. It is also called bit rate or throughput. The amount of data that can be transmitted over a 6G communication network is extremely high compared to the existing 5G network. 6G has a data rate of 1 Tbps and a higher spectral efficiency, thus providing many users instantaneous access to the network and at a higher speed of download and upload as well as the general connectivity.

2.3.3. Massive Connectivity

Massive connectivity deals with the ability of a communication network to support a large number of devices or connections at the same time. 6G will provide massive connectivity to support the numerous devices that will be connected in the future as the world continues to experience the continuous increase in the Internet of Things (IoT). In a way, it will involve advancements in network architecture, spectrum utilization, and device-to-device communication, which will result in seamless connectivity for a wide range of IoT applications.

2.4.4. Ultra-low latency

Ultra-low latency deals with the ability of the network to experience very minimal delay in signal transmission, processing, or response time. 6G is known to have a higher data rate, and this makes it have a very low latency. This high data rate and low latency will lead to the increase in the performance of many real-time applications as a result of the ultra-low latency. In addition, decreased latency will allow emergency response, remote surgical procedures, and industrial automation, as well as facilitation of seamless execution of delay-sensitive real-time.

2.5.5. AI Integration: AI integration as a feature of 6G is the process of integrating artificial intelligence (AI) into 6G or already existing systems of communication to improve their performances or operation. Artificial Intelligence (AI) was not involved in 4G or any previous generations. It is partially supported by 5G, making a difference in the telecommunications world, opening the doors for emerging remarkable applications (Ajeng, *et al*, 2021) & (Allaw *et al*, 2025), and will be greater in the case of the 6G network.

Therefore, it is expected to play a significant role in 6G networks, such as its implementation in various network components, network levels, and network services. AI integration involves the use of AI algorithms and machine learning techniques, with 6G to enable intelligent network management, resource allocation, and optimization. This integration of AI will increase or improve the overall performance and efficiency of the 6G network.

3.0 Results and Discussions

3.1 Why 6G is more secure than 5G networks

The following are some mechanisms or attributes that make the 6G network more secure than the 5G network.

3.1.1. AI-Driven Security

AI-driven security deals with a proactive defense mechanism that makes use of machine learning algorithms to detect, analyze, and respond to security threats in real time. AI-driven security for 6G networks can be designed using machine learning algorithms and predictive analytics to detect and respond to real-time threats, anomalies, and vulnerabilities. This will enable proactive defense and automated incident response, thus providing a more robust and adaptive security framework compared to 5G networks. Understandably, 6G networks usually incorporate Internet of Things (IoT) nodes, which assume critical roles in essential infrastructures. These devices help to facilitate real-time data collection, analysis, and decision-making, thus enhancing operational efficiency and enabling innovative services, and this can be achieved only through the use of artificial intelligence (Letaief *et al.,* 2021; Oztoprak *et al.,* 2023; Helena et al., 2024). In the

context of the radio interface, intelligent radios that integrate AI capabilities into radio frequency technologies are used, and this integration will enable radios to become more adaptive, perceptive, and self-aware, allowing them to sense, understand, and respond to changes in the radio frequency spectrum and supersede situations of different wireless problems, like fading and interference (Letaief *et al.*, 2019; Helena *et al*., 2024).

3.1.2. Network Slicing Security

Network slicing security deals with the partitioning of a single physical network infrastructure into multiple virtual networks, each optimized for specific applications or services. It is a mechanism that ensures the isolation and security of each network slice, implementing robust security controls and policy enforcement. Network slicing security for 6G networks can be designed through the implementation of robust isolation, encryption, and authentication mechanisms for each slice, thus ensuring that sensitive data or information and applications are segregated and protected. This helps to provide enhanced security and flexibility compared to 5G networks. Network slicing enables the creation of isolated virtual networks on shared infrastructure, each customized for specific services (Ordonez, 2017; Allaw *et al.,* 2025). It divides a single physical network into multiple isolated virtual networks (slices), each optimized for specific service requirements. Each slice operates independently with dedicated traffic flow, architecture, and resource provisioning, allowing providers to deliver customized services while optimizing resource utilization (Li *et al*., 2017; Allaw *et al.,* 2025).

3.1.3. Quantum-Secure Communication

Quantum-secure communication is defined as a method of securing a communication network using quantum-resistant cryptography to protect data transmission against quantum computer attacks. Quantum-secure communication for 6G networks can be designed through the integration of quantum key distribution (QKD) and post-quantum cryptography (PQC) to provide unbreakable encryption keys and secure data transmission. Quantum Key Distribution is a secure communication method that uses quantum mechanics to encode and decode cryptographic keys, enabling two parties to share a secret key while detecting any eavesdropping attempts, thereby ensuring secure data transmission, while Post-Quantum Cryptography refers to cryptographic algorithms and protocols designed to be secure against potential threats from both classical and quantum computers, ensuring long-term data protection and security in a future where large-scale quantum computers may compromise current encryption methods. This helps in ensuring unconditional security and protection against quantum attacks, which is higher than the security capabilities of 5G networks. The emergence of 6G networks initiates significant transformations in the communication technology landscape. Yet, the melding of quantum computing (QC) with 6G networks, although promising an array of benefits, particularly in secure communication (Muhammad et al., 2024). While 5G has already begun to revolutionize connectivity, 6G will build on this foundation by offering even faster data transmission, lower latency, and higher reliability. 6G aims to provide data speeds exceeding 1 Tbps, which will support an even wider range of applications, from immersive holographic communication to real-time AI-driven systems. Also, its exponential increase in bandwidth will allow for the seamless integration of advanced technologies like artificial intelligence (AI), machine learning (ML), and quantum computing into everyday life (Mengxu Zheng and Yubo, 2025).

3.1.4. Improved Authentication

Improved authentication is defined as a security measure that utilizes advanced methods, such as biometrics or behavioral authentication, to provide stronger verification of user identity. Improved authentication in 6G involves advanced methods, such as biometric authentication or behavioral authentication, to provide stronger verification of user identity and prevent unauthorized access.

According to Ahmed et al. (2024), Advanced Encryption Standard (AES)-based schemes are widely suggested for privacy-preserving and authentication protocols in 6G networks. In combination with AI-based QoS, Advanced Encryption Standard provides joint network optimization in 6G. Also, the use of a digital signature-based authentication key exchange protocol with provable reliance against several attacks in 6G Cybertwin network architecture.

That is why Kazmi et al. (2023) stated that the authentication techniques for 6G cellular networks. They went further to categorize the authentication techniques into eight types, such as handover authentication, mutual authentication, physical layer authentication, deniable authentication, token-based authentication, certificate-based authentication, key agreement with privacy, and multi-factor authentication. Handover Authentication takes care of secure and seamless mobility of devices in a cellular network, Physical Layer Authentication takes care of modulation on waveforms such as a spread spectrum-based secret modulation, and Deniable Authentication deals with empowering the sender with the ability to reject the authentication process to any third party. Multi-factor authentication is considered a core element of a foolproof Identity and Access Management (IAM) policy scheme. MFA is used for enhanced security through multitude expansion in the key spectrum against brute force attacks and stolen third-party parameters, etc.

3.1.5. Zero-Trust Architecture

Zero trust architecture is defined as a security framework that assumes no user or device can be trusted by default, requiring continuous verification and authentication to grant access to network resources. Zero Trust Architecture (ZTA) can be designed for 6G networks by implementing a framework that verifies user identity, device security, and access rights in real-time, continuously authenticating and authorizing every transaction. Zero Trust Architecture, or ZTA, assumes no inherent trust and relies more on continuous authentication and authorization for access. In the case of 6G, ZTA offers solutions to answer high device density, heterogeneous technologies, ultra-low latency, and security needs that must be mission critical. It minimizes attack surfaces while mitigating unauthorized access and data breaches with validation of all interactions within the network. Zero Trust Architecture is the strongest pillar to counter 6G security threats, which are triggered by new communication technologies (Saranath and Sreeji 2025).

3.1.6. Secure Multi-Party Computation

Secure multi-party computation is defined as a cryptographic technique that enables multiple parties to jointly perform computations on private data without revealing individual inputs. Secure multi-party computation for 6G networks can be designed by using secure collaborative computations among multiple parties without revealing individual inputs. This helps to protect sensitive data and ensure privacy while facilitating secure data sharing and analysis in 6G applications, surpassing the security capabilities of 5G networks. This is a cryptographic technique that enables multiple parties to collaboratively compute a function over their private inputs without revealing those inputs to one another. This ensures data confidentiality while allowing secure data analysis and decision-making, making it essential for privacy-preserving applications in 6G networks (Zhou, 2024).

According to Collins (2025), this method is particularly useful for secure federated learning, encrypted data analytics, and confidential transactions, where sensitive information, such as medical records or financial data, must be processed without exposing individual details. By enabling distributed trust and privacy-preserving computations, secure multi-party computation strengthens security in decentralized 6G applications, including IoT, AI, and cloud-edge environments.

3.1.7. Blockchain Integration

Blockchain integration is defined as a decentralized security approach that utilizes immutable ledgers to provide transparent and secure management of network transactions, identity verification, and data sharing. Blockchain integration for 6G networks can be designed through the use of decentralized, authentic, immutable ledgers to secure data transactions and provide transparent audit trails. This helps to enhance security, trust, and integrity in 6G applications and services, which is beyond what is possible in 5G networks. The emergence of blockchain technology and 6G networks has revolutionized service migration. Service migration is an important aspect of digital transformation. This involves the movement of services from one carrier/platform to another or from one system to another. As reported by Moubayed (2022) and Ahmed et al. (2024), blockchain technology and 6G networks will bring many benefits, such as improved scalability, enhanced security, increased flexibility, lower latency, greater energy efficiency, and more economic opportunities. Within the realm of 6G networks, users can acquire network access privileges through identity authentication mechanisms, while smart contracts within the blockchain ensure compliance with established rules. In the context of applications combining blockchain and 6G networks, identity authentication mechanisms further guarantee that only authorized users can access shared data (Liu *et al.* 2024).

3.1.8. Enhanced Visibility and Control

Enhanced visibility and control is defined as a security approach that provides real-time monitoring and management of security threats, network traffic, and system performance. Enhanced visibility and control for 6G networks can be designed by using the advanced monitoring, analytics, and AI-driven insights in order to provide real-time threat detection, granular control over network traffic, and dynamic policy enforcement. This helps in enabling more effective security management, enabling swift detection and faster incident response in 6G compared to what is obtainable in 5G networks.

3.2 Advantages of sixth generation (6G) Network

The following are some advantages of 6G

3.2.1. Faster Speeds: 6G is expected to be 100 times faster than 5G, with speeds reaching up to 1 terabit per second (Tbps), enabling instantaneous downloads and supporting data-heavy technologies like holographic calls and real-time virtual environments.

3.2.2. Ultra-Low Latency: 6G aims to achieve latency as low as 1 microsecond, significantly lower than 5G's 1 millisecond, which is crucial for applications like remote surgery, autonomous vehicles, and immersive virtual reality experiences.

3.2.3. Enhanced Network Capacity: 6G can support over 10 million connected devices per square kilometer, a significant increase from 5G's 1 million, making it ideal for the Internet of Everything (IoE).

3.2.4. Advanced AI Integration: 6G networks will leverage artificial intelligence for self-optimizing and self-healing capabilities, improving network efficiency, reliability, and user experience.

3.2.5. Improved Security: 6G is anticipated to incorporate advanced security features for data transmission and network infrastructure, critical for robust cybersecurity.

3.2.6. Enhanced Mobile Broadband: 6G will deliver high-speed, high-capacity mobile broadband, enabling seamless streaming, online gaming, and real-time applications.

3.2.7. Real-Time Applications: With 6G's ultra-low latency, real-time applications like remote surgery, autonomous vehicles, and virtual reality experiences will become more precise and reliable.

4.0 Conclusion

The research on the study of the enhanced security features of 6g network over 5G network has been carried out with the aim of determining the ways 6G network is more secure than 5G network. The research made use of secondary data such as online materials and library sources, as well as the descriptive and review research methods. The result shows that some of the techniques adopted in 6G, which make it highly secured compared to 5G, are zero-trust architecture, AI-driven security, quantum-secure communication, network slicing security, enhanced visibility and control, improved authentication, secure multi-party computation, and blockchain integration. It was also observed from the results that 6G has some advantages over 5G, such as advanced AI integration, ultra-low latency, faster speeds, enhanced network capacity, improved security, and real-time applications. It concluded, based on the results, that 6G networks will have enhanced security compared to 5G networks when 6G is being deployed.

References

1. Arti Prasad and Pooja Singh (2023): 6G Wireless Communications: Introduction of New Technologies and Their Challenges. International Journal of Creative Research Thoughts. Volume 11, Issue 3. Pp c684 – c687
2. Ajeng Wulandari, Aurelius Elvin, Jonathan Albert Purnawan, Reynaldi Ishaka (2021): Challenges in the Migration to 6G Mobile Systems. International Joint Conference on Science and Engineering. Advances in Engineering Research, volume 209. Pp 660 – 664
3. AlHajri M., Ali N., and Shubair R. (2018): "A Machine Learning Approach for the Classification of Indoor Environments Using RF Signatures" 10.1109, GlobalSIP.8646600.
4. AlHajri M., Ali N., and Shubair R. (2019): Indoor Localization for IoT Using Adaptive Feature Selection: A Cascaded Machine Learning Approach," arXiv: 1905.01000,
5. Huang, T., Yang, W., Wu, J., Ma, J., Zhang, X., & Zhang, D. (2019). A survey on green 6G network: Architecture and technologies. IEEE Access, 7, 175758-175768
6. Allaw, Z.; Zein, O.; Ahmad, A.-M. (2025): Cross-Layer Security for 5G/6G Network Slices: AnSDN, NFV, and AI-Based Hybrid Framework. Sensors, 25, 3335. https://doi.org/10.3390/s2511333
7. Ahmed Al-Ansi, Abdullah M. Al-Ansi, Ammar Muthanna, Andrey Koucheryavy (2024): Blockchain technology integration in service migration to 6G communication networks: a comprehensive review. Indonesian Journal of Electrical Engineering and Computer Science. Vol. 34, No. 3, June 2024, pp. 1654~1664
8. Dylan A. Sherman and Simon Brawey (2024): 6G mobile technology. Parliament.uk/post. DOI: https://doi.org/10.58248/PN734
9. Collins Omondi Ogolla (2025): Security in the sixth-generation cellular networks: A review, World Journal of Advanced Research and Reviews, 2025, 25(03), 2305-2334
10. Helena Rif˙a-Pous, Victor Garcia-Font, Carlos N´u˜nez-G´omez, and Julian Salas (2024): Security, Trust and Privacy challenges in AI-driven 6G Networks. International Conference on Network and Communications, pp 1 – 19.
11. Kazmi, S.H.A.; Hassan, R.; Qamar, F.; Nisar, K.; Ibrahim, A.A.A. Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions. Symmetry 2023, 15, 1147. https:// doi.org/10.3390/sym15061147
12. Letaief, K.B., Chen, W., Shi, Y., Zhang, J., Zhang, Y.J.A. (2019): The roadmap to 6G: AI empowered wireless networks. IEEE communications magazine 57(8), 84–90.

13. Letaief, K.B., Shi, Y., Lu, J., Lu, J. (2021): Edge artificial intelligence for 6g: Vision, enabling tech nologies, and applications. IEEE Journal on Selected Areas in Communications 40(1), 5–36.

14. Li, Q.; Wu, G. (2017); Papathanassiou, A.; Mukherjee, U. An end-to-end network slicing framework for 5G wireless communication systems. arXiv, arXiv:1608.00572.

15. Liu Y, Peng S, Zhang M, Shi S, Fu J (2024) Towards secure and efficient integration of blockchain and 6G networks. PLoS ONE 19(4): e0302052. https://doi.org/10.1371/journal. pone.0302052

16. Moubayed A, A. Shami, and A. Ibrahim (2022): "Intelligent transportation systems' orchestration: lessons learned and potential opportunities," arXiv preprint arXiv:2205.14040.

17. Mengxu Zheng and Yubo Xuan (2025): *Quantum-Encrypted 6G Fronthaul Network:* EnhancingSecurity and Efficiency in Next-Generation Wireless Communication. Proceedings of the 3rd International Conference on Mechatronics and Smart Systems. DOI: 10.54254/2755-2721/141/2025.21689.

18. Muhammad Azeem Akbar, · Arif Ali Khan, Sami Hyrynsalmi, Javed Ali Khan (2024): 6G secure quantum communication: a success probability prediction model. Automated Software Engineering (2024) 31:31 https://doi.org/10.1007/s10515-024-00427-y.

19. Oztoprak, K., Tuncel, Y.K., Butun, I. (2023): Technological transformation of telco operators towards seamless IoT edge-cloud continuum. Sensors 23(2), 1004.

20. Ordonez-Lucena, J.; Ameigerias, P.; Lopez, D.; Ramos-Munoz, J.J.; Lorca, J.; Folgueira, J. (2017): Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges. IEEE Commun. 55, 80–87.

21. Pavan Kumar Gade, Narayana Reddy Bommu Sridharlakshmi, Abhishekar Reddy Allam, Samuel Koehler (2021): Machine Learning-Enhanced Beamforming with Smart Antennas in Wireless Networks. ABC Journal of Advanced Research, Volume 10, No 2, 207 – 220

22. Saranath U, and Sreeji K B (2025): Zero Trust And 6g: Enhancing Security In Next Generation Networks, International Journal of Current Science. Volume 15, Issue 2. Pp 175 – 175.

23. Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang (2021): "Low-Latency Federated Learning and Blockchain for Edge Association in Digital Twin Empowered 6G Networks," in IEEE Transactions on Industrial Informatics, vol. 17, no. 7, pp. 5098-5107.

24. Zhou I, Tofigh F, Piccardi M, Abolhasan M, Franklin D, Lipman J. Secure multi-party computation for machine learning: A survey. IEEE Access. 2024 Apr 15.