e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

ENHANCING SECURITY AND PRIVACY IN 6G NETWORKS: CHALLENGES, INNOVATIONS, AND FUTURE DIRECTION

Dr. Thara L*1, Pitchiah Parameshwaran S*2, Sowmiya R*3

*1Associate Professor, Department Of Computer Applications (MCA) PSG College Of Arts & Science, Coimbatore, Tamil Nadu, India.

*2,3MCA, Department Of Computer Applications (MCA) PSG College Of Arts & Science, Coimbatore, Tamil Nadu, India.

ABSTRACT

The rising implementation of sixth generations (6G) technology allows systems to achieve ultra-state data rates, ultra-low latency, massive connectivity and intelligent communication capabilities. The same technological advances generate substantial privacy and security issues which include risks from cyber threats and breaches of privacy together with risks from artificial intelligence technologies. This research examines how geopolitics addresses security and privacy main topics in 6G while outlining solutions for dealing with threats and potential future work areas. The discussion will focus on sound solutions which secure the most protected waves for communication while preserving privacy because these solutions will fuel 6G network evolution through quantum-key cryptography and blockchain with AI-based security and zero-trust architecture components.

Keywords: 6G Networks, Security And Privacy, Cyber Threats, AI-Based Security.

I. INTRODUCTION

6G network technology now starts implementation because wireless communications enter an era of rapid enhancement. 6G-one technology will deliver better performance than 5G because it promises performance attributes including speed, resilience, capacity and intelligence. Ultra-low latency and increased spectral efficiency together with massive connectivity and integration with AI as well also Edge Computing. IoT and Blockchain represent the main goals that drive the development of 6G technology [1]. Multiple security breaches in 6G networks will occur because of AI and decentralized system and ultra-dense network implementation which expands the network's vulnerability to enhanced cyber attacks. The 6G will diverge from its parent technologies by establishing distributed computing as its primary user service platform through a combination of cloud-edge systems and edge computing technologies [2]. Several security threats generated by 6G network implementation across such sectors involve maintaining data integrity and performing client authentication along with securely sharing data between domains[3].

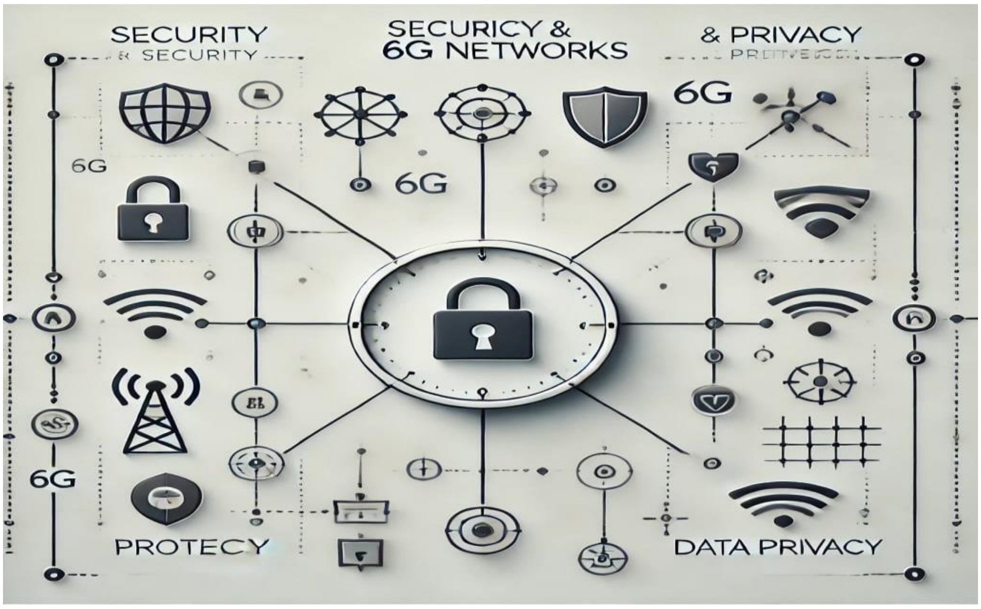

Fig 1. 6G Network Technologies

II. SECURITY AND PRIVACY CHALLENGES IN 6G NETWORKS

Security threats alongside privacy concerns in 6G networks will multiply because the systems will become more interconnected and perceptive.

2.1. AI-Driven Cyber Threats

AI functions will automate the control functions of 6G networks while simultaneously enabling unknown malicious access points to appear. AI-based attackers will seek out manipulation points within networks through methods never possible for traditional cyber threat control [4].

2.1.1. Adversarial Machine Learning (ML) Attacks

Attackers achieve undesirable effects on the network by corrupting data which results in unpredictable AI behavior through traffic misidentification and false security warnings [4].

2.1.2. Phishing and AI-generated Kindfaking

Artificial Intelligence helps cybercriminals create fraudulent authentication details for security system penetration or develop deceiving messages that impersonate genuine communication [4].

2.2. Quantum Computing Threats

The threat posed by quantum computing ranks as the most severe because it breaks all classical encryption methods [5].

2.2.1. Breaking Public-Key Cryptography

RSA and ECC encryption methods rely on the belief that large prime number factorization remains an extremely difficult mathematical operation. These problems will eventually be solved thus rendering current encryption insufficient because of Shor's algorithm on quantum computers [6].

2.3. Privacy Concerns in Massive IoT and Edge Computing

Online information from Internet of Things (IoT) devices processes directly on network edges instead of cloud servers thus creating new privacy exposure points among its vast number of connected devices [7]. Significant data collection occurs on a massive scale.

Multiple types of personal data accumulate each second from IoT devices which results in potential security risks. The unauthorized access to this data can trigger identity theft while enabling surveillance operations that result in infrastructure manipulation attempts.

2.3.1. Vulnerabilities in edge computing

Security in edge-computed systems spreads across multiple locations because decentralized acceptance makes it hard to implement a single unified security control system. the way cloud computing does with its centralized policies. Attacks on edge nodes could occur when these weak security measures allow the attackers to access processes of data delivery and gain unauthorized control.

2.4. Zero-Day Exploits of Software defined networking and Network Function Virtualization

The future 6G networks will require complete adoption of SDN and NFV to achieve a flexible programmable and dynamic network control system [8]. The expanded attackable areas become more accessible through these emerging technologies.

2.4.1. Zero-day exploits

SDN controllers together with NFV infrastructure run through software-based functions that expose possible unknown vulnerabilities during their operation. The exploitation of known vulnerabilities with established weaknesses occurs before these weaknesses receive their fixes [8].

2.4.2. Malicious SDN Controllers

The control plane processes known as decision-makers rest separately from the data plane which carries out traffic forwarding under the SDN framework. An SDN controller under malicious control enables hackers to take over network traffic by performing traffic redirection attacks or by initiating distributed denial-of-service attacks [8].

2.4.3. NFV Service Chain Attacks

Through NFV technology network functions can deliver firewalls together with intrusion detection systems as virtualized features. Hacker exploitation of single network functions would render the service chain able to disable security features thus allowing unauthorized traffic to bypass inspection. For 6G networks to achieve balance in their security risks there needs to be continuous monitoring and AI-driven threat detection alongside regular software updates [8].

Table 1. Challenges and Threats in 6G Networks

Challenge	Description
Adversarial Machine Learning Attacks	Through corrupting data attackers create misidentification errors combined with false security alerts within AI systems.
Phishing & AI-generated Kindfaking	By using AI technology cybercriminals can develop false authentication credentials together with deceptive communications.
Breaking Public-Key Cryptography	The encryption protocols RSA together with ECC can be breached by quantum computing leading to the obsolescence of existing security techniques.
Post-Quantum Cryptography Solutions	The encryption protocols RSA together with ECC can be breached by quantum computing leading to the obsolescence of existing security techniques.
IoT Data Privacy Risks	Huge volumes of collected data regarding IoT devices enhance the possibility of identity theft as well as surveillance risks.

III. INNOVATION FOR PRIVACY AND SECURITY IN 6G

3.1 Quantum cryptography

The encryption system in Quantum Key Distribution (QKD) uses quantum mechanics principles for creating keys that attackers cannot decipher [9]. The Post-Quantum Cryptography (PQC) family of algorithms functions to protect data from quantum decryption methods [6].

3.2Blockchain based security frameworks

The protection of data through federated blockchains becomes stronger because of advanced access control measures [7]. Smart contracts provide effi-cient authentication processes which are managed through these contracts to ensure reliability. Security systems that utilize Artificial Intelligence serve as the third major element in this list. Artificial Intelligence based abnormal behavior and intrusion detection systems function as a protective layer for securing the network infrastructure. The utilization of federated learning elevates privacy levels because distributed data enables training of artificial intelligence algorithms.

3.3 ZTA: Zero trust architecture

Under ZTA users experience total system restrictions because they need to present identification at all times. Through micro-segmentation organizations decrease the chances of targeted attacks by isolating different network parts [8].

3.4 S2 MEC: Secure S2 Multi-Access Edge Computing

Together with a homomorphic encryption technology users can execute calculations on their network data near the edge while keeping it encrypted. Devices maintain enhanced security because trusted execution environments (TEE) protect them [7].

IV. FUTURE RESEARCH DIRECTIONS

6G security has progressed significantly. Corresponding investigations is require completion in multiple research fields.

4.1. Development of Standardized Security Frameworks

Standardization at a global level should focus on achieving security and privacy compliance requirements with operability [1].

4.2. AI-Powered Adaptive Security Solutions

The capacity of adaptive security systems to create dynamic responses toward potential cyber threats increases because emerging threats keep evolving [4].

4.3. Privacy-Preserving Techniques for Data Sharing

Secure federated learning and differential privacy represent two strategic approaches which should be investigated for preserving user data protection [7].

Secure data sharing methods should achieve a proper middle ground between protecting privacy and operational effectiveness.

4.4. Quantum-Resistant Security Mechanisms

You should dedicate resources to speed up existing research on post-quantum public key algorithms. Security experts should establish new hybrid cryptography which combines classical and quantum protection methods [6].

4.5. Ethical and Legal Considerations

Through policies and regulations we must investigate ethical problems which appear during AI surveillance and data collection systems. The 6G network security responsibilities must be described through lawful guidelines established to ensure safe operations [10].

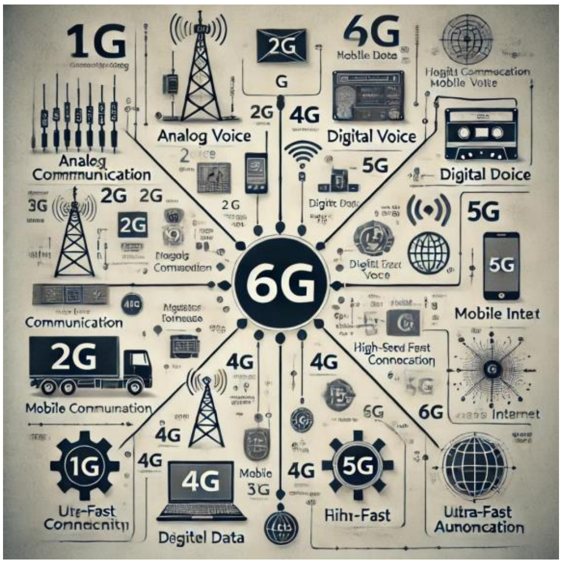

Fig 2. Evolution of Wireless Networks: From 1G to 6G

V. CONCLUSION

The upcoming 6G networks will advance wireless communication while creating advanced security and privacy issues for resolution. The main security threats through analysis of new solutions and established future research opportunities. Four primary security measures exist to protect 6G networks which include quantum cryptography along with blockchain implementation and AI-based security models and zero trust architectural frameworks. To establish a robust 6G ecosystem which stands resistant to attacks researchers must connect with all necessary stakeholders through additional study initiatives.

VI. REFERENCE

[1] W. Jiang, B. Han, M. A. Habibi and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 334-366, 2021.

[2] Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "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, July 2021.

[3] K. B. Letaief, W. Chen, Y. Shi, J. Zhang and Y. -J. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," in IEEE Communications Magazine, vol. 57, no. 8, pp. 84-90, August 2019.

[4] Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2017). "Practical black-box attacks against machine learning."

[5] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in IEEE Security & Privacy, vol. 16, no. 5, pp. 38-41, September/October 2018.

[6] Roman, R., Lopez, J., & Mambo, M. (2018). "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges.

[7] D. Kreutz, F. M. V. Ramos, P. E. Veríssimo, C. E. Rothenberg, S. Azodolmolky and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, Jan. 2015.

[8] Bennett, C. H., & Brassard, G. (1984). "Quantum cryptography: Public key distribution and coin tossing.

[9] Hoi-Kwong Lo, H. F. Chau ,Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. Science283,2050-2056(1999).

[10] Shor, P. W. (1997). "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer."