IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202002 |

Trust and Security Frameworks for Next-Generation 6G Networks: A Review

Thushara A

Department of Computer Science and Engineering, TKM College of Engineering, Kollam, India

ABSTRACT: As 6G technology evolves, strong security and trust will be the only ways to go. Widespread adoption of 6G in industries and society will bring numerous benefits, but it also introduces new challenges. This paper focuses on the security aspect of 6G, with an emphasis on issues like complex network structures, cloud-based environments, and multi-stakeholder ecosystems. It discusses how artificial intelligence, machine learning, quantum-safe encryption, and privacy preservation contribute to better cybersecurity and build trust in the network. Other key innovations that have been discussed include automated security systems, protection against signal interference, physical layer security, and blockchain-based security solutions. With rapid technological advancements and increasing threats in the cyber world, a flexible and transparent security framework is required for better resilience. Such a review emphasizes recent developments and further suggests lines of future work, delivering a roadmap for securing and trusting the 6G era.

KEYWORDS: 6G, security, cyber resilience, privacy, trustworthiness, wireless networks.

I. INTRODUCTION

The development of 6G technology will transform communication systems by connecting the physical, digital, and biological worlds. This new technology will provide people with enhanced experiences, improve human intelligence, and allow better control of automated systems. By the 2030s, 6G is expected to significantly change the way we live[1]. However, to fully benefit from 6G, strong measures for cyber-resilience, privacy, and trust will be essential.

With 6G, people will interact with machines in new ways, and networks will act as sensors providing continuous information. This will greatly benefit healthcare by allowing in-body monitoring and analysis. It will be necessary to ensure that patients' data remains private and secure, even when processed on untrusted platforms. During the pandemic, video conferencing became widespread. This may evolve into holographic experiences in the future. New privacy solutions will be needed to prevent the accidental sharing of sensitive information in video streams. High-resolution mapping for remote driving and transportation will also benefit from 6G and push industries to new levels. Thus protecting sensitive information and maintaining operational security will be critical. In industries, operations will involve collaborations between mobile robots, drone swarms, and systems that require precise positioning and sensing. Protecting the identity and privacy of these autonomous machines will safeguard companies' intellectual property. As networks grow larger, advanced information security solutions will be needed to protect data shared by billions of devices.

Although many studies focus on 6G technologies, research on its security and privacy aspects is still limited. The 6G network will aim to simplify and converge radio access and core networks, building on the foundations of 5G. Open-source methods will help develop solutions that prioritize safety and privacy. To enhance security, measures like redundancy, multi-path routing, and reliable paths for data transfer will be important. The use of open interfaces and collaborative development models will create new security requirements. The growth of edge cloud systems and virtual radio access networks will improve access on a large scale. Hardware solutions will also help optimize 6G performance and strengthen system integrity.

AI and machine learning will play key roles in detecting new security threats, though they could also be used to create more advanced attacks. These technologies will be crucial for keeping networks secure throughout their development and operation. Automated software creation and closed-loop security operations will be essential for building trust in 6G systems. Privacy-preserving technologies such as homomorphic encryption and federated learning will work alongside hardware and cloud-based trust solutions. Quantum-safe security methods will redefine cyber-resilience. Extra measures, such as protection against jamming, physical layer security, and distributed ledger technologies, will further increase the requirements of secure communication.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202002 |

This paper provides an in-depth examination of security and trust issues in emerging 6G technologies, underlining the critical need for strong cybersecurity frameworks. As 6G networks aim to integrate AI, machine learning, and quantum-safe cryptographic methods, the paper explores how these advancements can enhance cyber resilience and privacy protection. It highlights key security enablers, including automated security operations, distributed ledger technologies, and physical layer security, which are essential in mitigating evolving threats. The introduction of the Secure Telecom Operations Map (SecTOM) offers a structured approach to ensuring comprehensive security across the network lifecycle. By addressing the interplay between innovative technologies and security risks, this paper lays the foundation for future research and practical implementations in securing next-generation wireless networks.

II. EVOLUTION OF THE 5G SECURITY PARADIGM

5G security has experienced vast developments to build a solid ground for 6G in the future. Flexibility enhancement, with particular solutions to very difficult security challenges faced by mobile networks, was primarily emphasized in these improvements. It has improved 5G network security mainly to ensure access on different networks that is safe, as supported by organizations like 3GPP and ETSI NFV. Major release 15 was an update that included user authentication that works across different network types. This way, it verifies without compromising security. It enhanced privacy by protecting location data of users. It also added security measures such as encrypting user data and ensuring the integrity of that data. It also included new authentication methods to ensure security in different network slices.

With 5G, service-based architectures were introduced, which included mutual authentication and secure communication between network components. Virtual firewalls and separating traffic into different virtual networks (VLANs and VPNs) helped improve perimeter security. The move to cloud-based networks raised concerns about the security of virtual systems and cloud software, but these were addressed through new standards and focus on secure software deployment.

5G thus adopted advanced cryptographic tools, like 256-bit encryption keys for radio communication, and energy-efficient encryption for low-power devices, to handle dynamic threats. Some privacy features such as secure data processing across networks were also designed. Hardware security was also enhanced with the advancement towards specialized and flexible security features, especially with non-public networks. 5G networks also launched automated security systems, including SOAR (Security Orchestration, Automation, and Response), to protect, detect, and respond to security issues. With a "shift-left" approach to security, in which part of the process of identifying security risks happens early in development, the number of vulnerabilities has decreased, such as those in supply chain attacks. Cloud-native networks posed new challenges, so their component pieces needed to be monitored and updated constantly for security. These improvements in 5G security are laying the groundwork for 6G, which will build on these lessons and provide even stronger protection against emerging threats while ensuring privacy, security, and trust remain at the core of communication technologies.

The table summarizes key features and security enhancements in 5G evolution, highlighting various improvements across multiple areas. These are: Radio communication using 256-bit encryption and energy-efficient algorithms, such as secure data processing and single-use identifiers, which are privacy-preserving technologies. Even subscriber and device identifiers have improved security. 5G brings more robust security in the control plane along with secure network slicing and automated monitoring of microservices in cloud-native networks. Intelligent, self-adaptive security systems (SOAR) were adopted for proactive threat management, while security orchestration and automation were integrated into the overall network management solutions.

Feature	5G Evolution
Crypto algorithms for the radio interface	256-bit keys for encryption, energy-efficient encryption algorithms
Privacy preservation	Secure data processing methods, temporary identifiers used only once
Subscriber and device identifiers	Secure hardware options for end devices
Enhanced control plane robustness	Securing communication between devices and networks
Network slicing and subnetwork security	Secure management and automation of different network sections (network slicing)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202002 |

NFV, SDN, and cloud-native security	Monitoring of software services; protecting platform and workload security during startup and operation
Self-adaptive, intelligent security controls	Automated security response systems (SOAR) that protect, detect, and respond to security threats
Security management and orchestration	Security management and automation integrated with overall network operations solutions

TABLE1 : Key Security Features and Enhancements in 5G Evolution

III. METHODOLOGICAL TRENDS AND DEVELOPMENTS

The research follows a structured approach, with a comprehensive literature survey to identify security challenges and proposed solutions in next-generation wireless networks. Primary sources include peer-reviewed journals, conference proceedings, and whitepapers from industry leaders. The methodology also incorporates comparative analysis by benchmarking 6G security frameworks against 5G security models to identify advancements and gaps.

To assess the role of AI/ML in securing 6G networks[4], the study evaluates AI-based anomaly detection models, automated threat mitigation systems, and adversarial learning techniques. The methodology involves testing existing AI-driven security models on simulated 6G network environments to analyze their effectiveness in detecting and mitigating cyber threats. The research also investigates the vulnerabilities of AI models to adversarial attacks and proposes reinforcement learning-based security enhancements.

This study places significant emphasis on the integration of quantum-safe cryptographic methods into 6G security frameworks. The methodology includes the evaluation of post-quantum cryptographic algorithms, including lattice-based and hash-based encryption techniques, in terms of their resistance to attacks by quantum computing. The effectiveness of these cryptographic methods is evaluated through computational simulations and security robustness tests.

Privacy continues to be a key issue in 6G owing to the sheer volumes of data that the IoT [5], smart cities, and autonomous vehicles generate. The methods involve examining privacy-preserving techniques such as homomorphic encryption, differential privacy, and federated learning. Experimental case studies are conducted to measure the performance of these methods in real-time data-sharing scenarios while ensuring user anonymity and data confidentiality.

Case studies on decentralized identity management, secure data transactions, and trust establishment among network entities will be analyzed in terms of the potential of blockchain for securing multi-stakeholder 6G ecosystems. The methodology will involve prototyping a blockchain-based access control system and testing its scalability and security efficiency in distributed network environments.

Research explores the use of physical layer security mechanisms, which include jamming detection, beamforming for secure communication, and physical unclonable functions (PUFs). The research methodology includes testbed simulation designs to evaluate the resilience of such security techniques to eavesdropping and interference attacks. Another area of focus is the combination of physical layer security with higher-layer encryption protocols to provide additional end-to-end security.

A new idea, Secure Telecom Operations Map (SecTOM), is a comprehensive security management framework in 6G networks. The approach for developing SecTOM involves consultation with experts, security modeling, and iterative testing. It merges AI-driven security orchestration, automated response mechanisms, and real-time network monitoring in order to build cyber resilience.

Table 2 shows a comparative summary of key research papers on 6G security and trust focusing on their research areas, concerns, enablers, and challenges. This review identifies further research areas which include the infusion of quantum communications, AI-driven zero-trust architectures, and standardization of security protocols in 6G. The work also outlines a possible research cooperation between academia, industry, and regulatory bodies towards developing comprehensive security frameworks.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202002 |

Paper	Key Focus	Security Aspects Discussed	Key Technologies	Challenges Addressed
Nawaz et al.[4]	Quantum Machine Learning in 6G	AI/ML for intelligent network orchestration	Quantum computing, machine learning	Security of AI-driven 6G, adversarial attacks
Klaus David et al.[5]	Evolution of mobile communication (1G-6G)	Trust and security from 1G to 6G	Zero-trust architectures, quantum-resistant encryption	Securing AI, wireless energy transmission
Tim O'Shea et.al [6]	Deep learning in physical layer security	AI-based optimization of communication systems	Autoencoders, CNNs, RTNs	Adversarial attacks on ML-based networks
Zhang et al.[7]	6G security and blockchain integration	Trust in heterogeneous networks	Blockchain, quantum-safe encryption, secure AI frameworks	Privacy and security of AI in 6G
Tarik Taleb et al. [8]	Network slicing and security in 6G	Isolating and securing network segments	AI-driven security, blockchain, quantum-safe cryptography	Securing service-tailored mobile networking
Wade Trappe et al. [9]	Physical layer security for 6G	Enhancing authentication and confidentiality	Low-energy IoT security, radio signal encryption	Secure lightweight IoT device communication
Letaief et al. [11]	AI's role in 6G networks	AI-driven security automation	AI-optimized architecture, federated learning	AI security vulnerabilities and adaptive defenses
Rappaport et al.[13]	Wireless communications beyond 100 GHz	High-frequency security concerns	THz communication, beam steering	Ensuring secure ultra-wideband networks
Ping Yang et al.[14]	6G spectrum and security	Trust in ultra-fast networks	THz bands, forward error correction	Data integrity in high-frequency communications
Ying Ju et al.[15]	Physical layer security in mmWave systems	Beamforming techniques for secure transmission	Maximum ratio transmitting, artificial noise	Protecting against eavesdropping in mmWave networks

TABLE 2 : A Comparative Summary of Research Papers On 6G Security And Trust

IV. CHALLENGES AND FUTURE SCOPE OF SECURITY IN 6G NETWORKS

With advancing 6G networks, security is one of the biggest issues. Creation of automated software is also a challenge. These days, most common problems in networks have their roots in software faults; with the growth of 6G technology, software complexity will grow, that is, raise the security threats. AI and ML will still be useful to find and resolve bugs, but full automation in secure software development is not that easy. The research in this area is very new, and there is much to be covered in order for security automation to become reliable.

Another significant challenge is automated security operations. Network misconfigurations often cause security vulnerabilities, and AI/ML-based automation can improve security management. However, developing intelligent and self-adapting security systems is complex. AI-based security solutions must be protected from attacks, and AI itself can be misused to launch cyber threats. This creates a need for ongoing research to develop robust security strategies that can defend against AI-driven threats while ensuring transparency and reliability in AI decision-making.

Privacy-preserving technologies also pose a big challenge in 6G networks. AI/ML models need large amounts of data to ensure accuracy, which raises concerns over data privacy and security. High-precision location tracking and network sensing will generate sensitive information that needs to be protected. A strong privacy framework is needed to regulate data flows and enforce security policies. Technologies such as secure multi-party computation, homomorphic encryption, and distributed cloud processing need to be improved in terms of privacy without sacrificing performance. Theoretical models for privacy and federated learning also need to be developed further to improve security.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202002 |

The hardware and cloud-embedded trust anchors are another challenge. The extension of these network trust anchors to hybrid cloud, based on virtualization technologies, proves difficult. Although server-based security attestation has been successful thus far, it is a challenge to extend that to cloud dynamic networks. Further research will be required in the development of positive security measures, ensuring continuity of trust.

Another security concern is quantum-safe security. Quantum computing poses a threat to current encryption methods, and though researchers have developed quantum-safe cryptographic algorithms, these solutions are still in their infancy. Implementing new security protocols will require great effort and collaboration among global organizations. Standardizing and implementing quantum-safe cryptographic methods across networks will take a lot of time and involve complexity.

The challenges include jamming protection and physical layer security. 6G networks should be low latency, high throughput, and highly secure. Physical layer security methods may protect against eavesdropping and attacks but should be implemented in ways that do not reduce network performance. Another issue is protecting against jamming attacks where malicious actors disrupt network signals. Balancing high spectral efficiency with strong jamming protection is a difficult problem that requires further research.

Finally, the idea of DLT like blockchain will help construct trust in 6G networks based on the verification of device behavior across different network domains. However, DLT does face issues related to its scalability, energy consumption, and speed in processing. These technologies must be made to be much more efficient and integrated into 6G networks without diminishing their performance.

Security in 6G networks will look promising as they are to become the future for global communication and technological development. As 6G develops further, it is going to encompass AI, machine learning, quantum computing, and cloud infrastructure. This means there will be newer security issues and challenges in these areas. Innovations in solution will be necessary to ensure that connected devices, applications, and services are secured. AI-driven security automation, advanced privacy-preserving methods, and secure data processing frameworks will be the key areas required to maintain integrity of data and prevent cyber threats.

Protection against AI-based attacks will be the most prominent aspect of the security mechanism in 6G. Since AI grows in power, and so do its usage to find vulnerabilities within the networks they can steal and use, building an AI security system that cannot be easily manipulated and highlights transparency in decision-making will be quite necessary. Another important aspect will be the adoption of quantum-safe cryptography-the additional protection from future quantum threats against sensitive data.

Physical layer security and jamming protection will be one of the prime concerns to ensure secure communication. As wireless networks become advanced, attackers will evolve sophisticated ways of disrupting signals. Research has to focus on the improvement of security mechanisms that can counter such threats while keeping network performance at high levels.

Privacy issues will also need constant consideration. As 6G networks collect and process large amounts of data, regulations and technologies will be required to protect user privacy. Secure multi-party computation, encryption methods, and decentralized data processing will be necessary to ensure security and prevent unauthorized access to sensitive information.

In the long term, 6G security will be based on global collaboration among researchers, industries, and governments. They will focus on scalability, energy efficiency, and flexibility of solutions adapted to the changing demands of users and industries. Incorporating advanced security technologies and starting from a strong foundation of trust, 6G networks are likely to emerge as the safer, more resilient, and capable infrastructure for critical applications worldwide.

V. CONCLUSION

The successful development and deployment of 6G networks will have to be covered under a robust, continuously evolving research agenda about security, trust, and cyber-resilience. As the progress of AI, machine learning, quantum computing, and cloud technologies advances, these must then be integrated throughout all phases of 6G development, deployment, and management in order to guarantee a safe and trustworthy environment. This is to be done through global collaboration and standardization of security and operational standards by governments and policymakers.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202002 |

Proof-of-concept experiments and case studies will be the backbone in fine-tuning security frameworks, thus ensuring that 6G networks are secure, reliable, and fully integrated into global communications by the 2030s. Overall, 6G success will also rely on how this trusted environment allows society, business, and community to make full use of the next generation network.

REFERENCES

1. ZIEGLER, P. SCHNEIDER, H. VISWANATHAN, M. MONTAG, S. KANUGOVI, AND A. REZAKI, "SECURITY AND TRUST IN THE 6G ERA," IEEE ACCESS, VOL. 9, PP. 86512–86530, 2021. DOI: 10.1109/ACCESS.2021.3088887. AVAILABLE: HTTPS://IEEEXPLORE.IEEE.ORG/DOCUMENT/9570274.
2. H. Viswanathan and P. E. Mogensen, "Communications in the 6G era," IEEE Access, vol. 8, pp. 57063–57074, 2020. DOI: 10.1109/AC- CESS.2020.2996001.
3. M. N. Patwary, S. J. Nawaz, M. A. Rahman, S. K. Sharma, M. M. Rashid, and S. J. Barnes, "The Potential Short- and Long-Term Disruptions and Transformative Impacts of 5G and Beyond Wireless Networks: Lessons Learnt From the Development of a 5G Testbed Environment," IEEE Access, vol. 8, pp. 34163–34183, Jan. 2020. DOI: 10.1109/ACCESS.2020.2964673.
4. S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduz- zaman, "Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future," IEEE Access, vol. 7, pp. 135437-135450, Apr. 2019, doi: 10.1109/ACCESS.2019.2909490.
5. K. David and H. Berndt, "6G Vision and Requirements: Is There Any Need for Beyond 5G?" IEEE Vehicular Technology Magazine, vol. 13, no. 3, pp. 72–80, Sept. 2018, doi: 10.1109/MVT.2018.2848498.
6. T. O'Shea and J. Hoydis, "An Introduction to Deep Learning for the Physical Layer," IEEE Transactions on Cognitive Communica- tions and Networking, vol. 3, no. 4, pp. 563–575, Dec. 2017, doi: 10.1109/TCCN.2017.2758370.
7. Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," IEEE Vehicular Technology Magazine, vol. 14, no. 3, pp. 28–41, Sept. 2019, doi: 10.1109/MVT.2019.2921208.
8. T. Taleb, B. Mada, M. I. Corici, A. Nakao, and H. Flinck, "PERMIT: Network Slicing for Personalized 5G Mobile Telecommunications," IEEE Communications Magazine, vol. 55, no. 5, pp. 88–93, May 2017, doi: 10.1109/MCOM.2017.1600947.
9. W. Trappe, "The Challenges Facing Physical Layer Security," IEEE Communications Magazine, vol. 53, no. 6, pp. 16–20, June 2015, doi: 10.1109/MCOM.2015.7120024.
10. C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 240-254, June 2010, doi: 10.1109/TIFS.2010.2040170.
11. K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, "The Roadmap to 6G: AI Empowered Wireless Networks," IEEE Commu- nications Magazine, vol. 57, no. 8, pp. 84-90, August 2019, doi: 10.1109/MCOM.2019.1900271.
12. K.-C. Chen, T. Zhang, R. D. Gitlin, and G. Fettweis, "Ultra-Low Latency Mobile Networking," IEEE Communications Magazine, vol. 55, no. 7, pp. 84–90, 2017. DOI: 10.1109/MCOM.2017.1601158.
13. T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," IEEE Access, vol. 7, pp. 78729–78757, June 2019. DOI: 10.1109/ACCESS.2019.2921522.
14. P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G Wireless Communications: Vision and Potential Techniques," IEEE Network, vol. 33, no. 4, pp. 70–75, Jul.–Aug. 2019. DOI: 10.1109/MNET.2019.1800418.
15. Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdrop- pers," IEEE Wireless Communications Letters, vol. 17, no. 4, pp. 2675– 2689, Apr. 2018. DOI: 10.1109/TWC.2018.2800747.
16. T. Nakamura, "5G evolution and 6G," in Proc. IEEE Symp. VLSI Technol., Honolulu, HI, USA, Jun. 2020, pp. 1–5. DOI: 10.1109/VL- SITechnology18217.2020.9265094.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details