www.ijarp.com ISSN 2456-9992 Page: 01-11

International Journal Advanced Research Publications

Review Article
Volume: 02
Issue: 06

ZERO-TRUST SECURITY TECHNIQUES FOR 6G WIRELESS COMMUNICATION SYSTEMS: A COMPREHENSIVE REVIEW

[*1]Sreejith. P. P., [2]Dr. P. Nirmaladevi

[1]Research scholar, Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode.

[2]Assistant Professor, Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode.

Article Received: 8 May 2026, Article Revised: 28 May 2026, Published on: 18 June 2026

***Corresponding Author: Sreejith. P. P.**

Research scholar, Department of Computer Science, Nandha Arts and Science College (Autonomous), Erode.

Doi: https://doi-doi.org/101555/ijarp.5829

ABSTRACT

The continuous advancement of wireless network technologies has accelerated the development of sixth-generation (6G) networks, which are expected to significantly enhance the capabilities of future digital infrastructures. These networks aim to distribute extremely high data transmission rates, ultra-low latency communication, intelligent network automation, and seamless connectivity among billions of interconnected devices. Such capabilities will enable emerging applications including immersive virtual environments, autonomous transportation, smart healthcare systems, and large-scale Internet of Things (IoT) ecosystems. However, the increasing complexity and distributed architecture of 6G networks introduce serious security concerns. The integration of heterogeneous devices, edge computing, and cloud-based infrastructures increases the attack environment and itmakesthe state-of-the-art perimeter-based security techniquesunsatisfactory for protecting modern communication environments.To resolve these drawbacks, the Zero-Trust Security Architecture (ZTSA) has gained significant attention as a robust security paradigm for next-generation networks. Unlike conventional security approaches that rely on predefined trust boundaries, ZTSA operate under the principle that no entity should be trusted by default, regardless of its location within the network. Instead, it continuouslyauthenticates every access request before access to network resources is granted. In this context, the present review paper provides a comprehensive examination of ZTSA for 6G wireless communication systems. The study discusses the fundamental principles of ZTSA, its

incorporation with advanced technologies i.e. artificial intelligence, block-chain, and edge computing, and the key security challenges associated with large-scale deployment. Furthermore, the paper analyzes existing research contributions and identifies potential directions for future investigation aimed at developing scalable, intelligent frameworks for next-generation wireless networks.

KEYWORDS: 6G Networks, Zero-Trust Security, Wireless Communication, Network Security, Block-Chain, Artificial Intelligence.

I. INTRODUCTION

Wireless communication technologies have experienced rapid development during the last few decades, evolving from early analog systems to highly sophisticated digital networks. The future6G wireless communication systems are expected to provide unprecedented capabilities such as extremely high data transmission rates, ultra-reliable low-latency communication, and seamless connectivity among billions of intelligent devices. As highlighted by Mohsan and Li (2023), 6G networks will integrate advanced technologies including artificial intelligence, edge computing, and large-scale Internet of Things (IoT) infrastructures to support emerging applications such as immersive virtual environments, smart cities, and autonomous systems. Despite these technological advances, ensuring secure communication in such highly distributed environments remains a major challenge.

Conventional network security approaches generally rely on perimeter-based protection, assuming that devices operating inside the network boundary can be trusted. However, this assumption becomes unrealistic in modern networks where devices frequently connect from multiple locations and environments.To overcome these limitations, researchers have proposed the ZTSA. According to Syed et al., (2022), the ZTSAis based on the theory of "never trust, always verify." In this paradigm, all user devices must be constantlyverified and authorized before accessing network resources. This review paper aims to examine how ZTSAprinciples can be applied to safeguard 6G wireless communication systems, while also identifying current research challenges and potential future directions.

II. OVERVIEW OF 6G WIRELESS NETWORKS

The development of 6G communication systems represents the next milestone in wireless networking. Compared with existing 5G infrastructures, 6G networks are expected to providedrasticallyenhanced performance in terms of speed, reliability, and intelligence. These

networks will likely support data transmission speeds approaching terabit-per-second levels, enabling advanced digital services that require extremely high bandwidth.

Tripi et al., (2024)emphasize that 6G networks will also incorporate emerging technologies including terahertz communication, intelligent spectrum management, and integrated satellite-terrestrial networking. However, the increased complexity of 6G architectures also introduces several security vulnerabilities. The massive number of connected devices and distributed computing environments significantly expand the potential attack surface. As discussed by Scalise et al., (2024), future wireless networks must adopt advanced security mechanisms capable of addressing both traditional cyber threats and newly emerging attack strategies.

III. ZERO-TRUST SECURITY ARCHITECTURE

ZTSArepresents a fundamental shift from traditional network security models. Instead of assuming that internal network components are inherently trustworthy, ZTSArequire continuous verification of every access request. According to the framework proposed by Syed et al., (2022), ZTSArelies on several key principles:

- **Continuous identity verification**: all users devices are must authorize before accessing resources.
- **Least-privilege access control**: entities are granted only the minimum permissions to carry out their tasks.
- **Micro-segmentation**: the network is partitioned into smaller pieces to reduce the spread of attacks.
- **Real-time monitoring**: system activity is continuously analyzed to detect abnormal behavior.

These principles help reduce the risk of illegitimate access and safeguards attackers from moving across within the network.Furthermore, Ramezanpour and Jagannath (2022)designed an intelligent ZTSAthat integrates machine learning techniques to dynamically evaluate trust levels and adapt security policies accordingly.

IV. ZTSA FOR 6G NETWORKS

Applying ZTSAto 6G networks requires modifications to several components of the communication architecture. The Figure 1 shows a simple architecture representationofZTSA in 6G wireless communication networks.

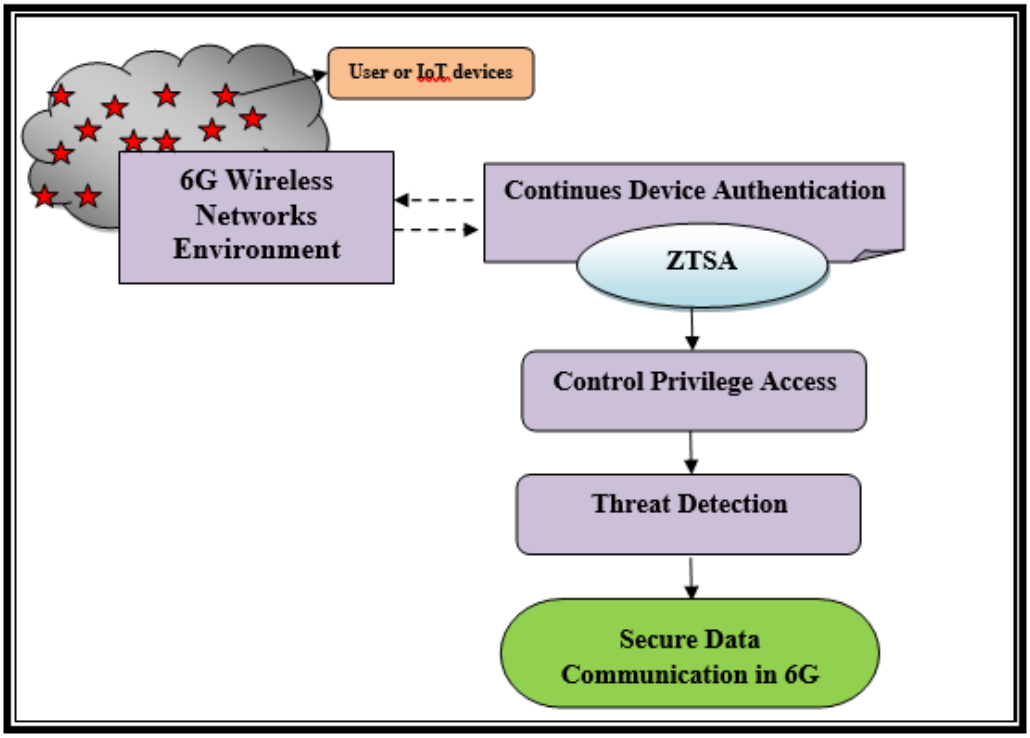

Figure 1 ZTSA For 6G network.

As presented in above Figure 1,one of important aspect in ZTSA is device authentication. Because future networks will connect billions of user devices, ensuring that each device can be securely identified becomes critical. Research by Li et al., (2022) demonstrates that ZTSAcan significantly improve the security of industrial IoT environments.

Another key mechanism is network micro-segmentation, which partitions the network into isolated zones. This approach limits the ability of attackers to move across different parts of the system once an initial compromise occurs. In addition, artificial intelligence techniques can enhance ZTSAby enabling real-time threat detection. For example, Celik and Eltawil (2024)highlight the potential of AI-driven analytics for identifying suspicious network behavior and automatically enforcing security policies.

Blockchain technology has also been proposed as a complementary solution for decentralized trust management. Al-Matari et al., 2024 demonstrates that blockchain-based frameworks can provide secure and tamper-resistant mechanisms for managing authentication and spectrum access in wireless networks.

V. LITERATURE STUDY

Several studies have explored ZTSAand 6G network security solutions.Alnaim and Alwakeel (2025) implemented ZTSAfor cyber-physical systems in 6G environments. This framework

improves system resilience by minimizing implicit trust between network entities. However, computational complexity was higher when deployed in large cyber-physical infrastructures. Jeysuriya et al., (2026) developed a quantum-resilient cross-trust evaluation mechanism to strengthen ZTSAin next-generation wireless networks. But, the mechanism remains largely theoretical and requires further practical validation in real-world 6G systems.

Syed et al., (2022) presented a comprehensive survey of ZTSA, discussing its core principles, implementation models, and potential applications in modern network environments. However, the study primarily focuses on general networking systems and offers limited discussion on the specific requirements of 6G communication networks. Chen et al., (2022) introduced a ZTSAdesigned to address emerging security threats in future 6G wireless systems. Their framework integrates advanced authentication mechanisms and dynamic access control policies to strengthen network security. This model enhances protection against unauthorized access and insider attacks in distributed network environments. Despite its advantages, the architecture may face scalability challenges when applied to extremely large networks with billions of connected devices.

Ramezanpour and Jagannath (2022) intended an intelligent ZTSAfor securing 5G and emerging 6G networks by integrating artificial intelligence techniques into security decision processes. This intelligent approach improves adaptive threat detection and network monitoring capabilities. However, computational overhead was more which may affect real-time network performance. Enright et al., (2022) developed a learning-based ZTSAaimed at securing future network infrastructures. This approach improves attack detection accuracy by leveraging machine learning models. Though, the efficiency was not adequate as itbased on availability of large training datasets and reliable network monitoring data.

Mohsan and Li (2023) conducted a comprehensive survey of 6G wireless communication technologies, discussing key architectural components, enabling technologies, and security challenges. However, the survey does not propose a specific security framework for addressing these challenges.Sedjelmaci et al., (2024)planned a ZTSA for improving the resilience of 6G radio access networks. This framework improves the reliability and robustness of distributed communication infrastructures. However, the performance evaluation of the system is limited and requires further experimental validation.

Nahar et al., (2024) investigated the applications of ZTSAwithin 6G communication networks and analyzed its potential benefits for securing distributed infrastructures. Nevertheless, the work mainly presents conceptual discussions without detailed implementation strategies.Tripi et al., (2024) examined the evolving role of protection and

trust management in 6G. Their research highlights emerging cyber threats associated with advanced wireless communication technologies. However, it does not present a concrete ZTSAspecifically tailored for 6G communication systems.

Scalise et al., (2024) analyzed the major security challenges affecting both 5G and emerging 6G communication networks. Their study identifies vulnerabilities associated with large-scale IoT connectivity, network virtualization, and edge computing infrastructures. However, the work primarily focuses on identifying challenges rather than proposing detailed mitigation strategies.Li et al., (2022) presented a ZTSAfor industrial Internet of Things environments. This framework improves data protection and reduces the risk of unauthorized access within industrial networks. However, the architecture may result in higher energy consumption.

Trinh-Nguyen et al., (2024)intended a trust management framework designed to support secure communication in 6G networks. Thisframework improves trust assessment accuracy in highly dynamic communication environments. But, the framework requires complex trust computation mechanisms that may increase system latency.Al-Matari et al., 2024 presented a block-chain-enabled security mechanism for 6G communication networks. The use of block-chain enhances data integrity and trust management across decentralized networks. However, block-chain implementation may introduce latency and scalability challenges in large-scale network environments.

Celik and Eltawil (2024) explored the use of artificial intelligence to enhance intelligent communication and security in 6G wireless systems. Their research highlights the potential of AI-driven automation for improving network management and threat detection. However, the integration of generative AI raises concerns related to data privacy and model reliability.Siniarski et al., (2025)present an automated security service platform designed for future 6G communication networks. This framework enhances network resilience through intelligent security orchestration. However, the implementation complexity of the proposed platform may limit its deployment in resource-constrained environments.

Sedjelmaci and Ansari (2023) developed a ZTSA-enabled attack detection framework for securing 6G edge computing environments. This approach improves the ability to detect sophisticated cyber threats targeting edge networks. However, the framework may require significant computational resources for continuous monitoring and analysis.El-Hajj (2025) proposed a ZTSAand federated learning framework for optimizing security in 6G systems. The framework enhances trust management while enabling collaborative learning across distributed network nodes. But, federated learning processes may introduce communication overhead and increased system complexity.

Enright et al., (2022) also presented learning-based ZTSAat the IEEE Future Networks World Forum. The architecture improves adaptive threat detection capabilities in evolving network environments. However, the framework requires continuous data collection, which may raise privacy concerns.Bhagyalakshmi et al., (2026)introduced an artificial intelligence-enabled ZTSAdesigned to mitigate cyberattacks in decentralized 6G networks. This model enhances security resilience in distributed network infrastructures. However, the integration of AI-based mechanisms increases system complexity and computational requirements.

Table 1 Literature Review Comparison.

No	Author / Year	Method / Technology	Application Area	Key Contribution	Limitations
1	Syed et al., (2022)	Zero-Trust Architecture Survey	Network Security	Comprehensive analysis of ZTA principles and frameworks	Limited discussion on 6G integration
2	Chen et al., (2022)	Zero-Trust Security Model	6G Networks	Proposed security architecture for future wireless networks	Implementation complexity
3	Ramezanpour and Jagannath, (2022)	AI-based Zero-Trust Framework	5G/6G Security	Introduced intelligent security model for network access control	High computational overhead
4	Enright et al., (2022)	Machine Learning based ZTA	Future Networks	Adaptive security monitoring using learning models	Scalability issues
5	Mohsan and Li, 2023	6G Network Security Survey	Wireless Networks	Overview of security challenges and emerging technologies	Lack of detailed ZTA solutions
6	Sedjelmaci et al., (2024)	Secure RAN with ZTA	Radio Access Networks	Improved security in distributed network environments	Performance evaluation limited
7	Nahar et al., (2024)	ZTA for 6G Survey	6G Communication	Comprehensive study of ZTA applications in 6G	Practical implementation challenges
8	Tripi et al., (2024)	Risk Mitigation Framework	6G Security	Identified security threats and mitigation	No detailed authentication mechanism

				strategies	
9	Scalise et al., 2024	Security Framework	5G/6G Networks	Survey of network security techniques	Limited focus on trust models
10	Li et al., (2022)	Zero-Trust IoT Framework	Industrial IoT	Secure device authentication and communication	High energy consumption
11	Trinh-Nguyen et al., (2024)	Trust Management Model	6G Networks	Global trust evaluation framework	Lack of decentralized trust management
12	Al-Matari et al., (2024)	Blockchain Security Model	Cognitive Radio IoT	Secure spectrum access using blockchain	High latency in blockchain transactions
13	Celik and Eltawil (2024)	Generative AI Security Model	6G Communication	AI-driven security management	Data privacy concerns
14	Siniarski et al., (2025)	Automated Security Platform	6G Networks	Self-adaptive security service framework	Implementation complexity
15	Jeysuriya et al., (2026)	Quantum-Resilient Trust Model	Future Wireless Security	Proposed quantum-resistant trust evaluation	Early stage research

These studies demonstrate the growing importance of ZTSAin future wireless communication systems.

VI. RESEARCH CHALLENGES

Although ZTSAoffers significant advantages for securing next-generation networks, several practical challenges must still be addressed before large-scale deployment becomes feasible.One major concern is scalability. Future 6G networks may include billions of connected devices, making continuous authentication and policy enforcement extremely complex. Efficient identity management systems are therefore required to handle large-scale deployments. Another challenge is computational overhead. Continuous monitoring and verification processes may increase processing requirements, which could affect network performance, particularly in latency-sensitive applications.

Privacy protection is also a critical issue. Identity-based authentication mechanisms must ensure that user data and personal information are not exposed during the verification process. Finally, integrating ZTSAwith existing network infrastructures presents significant

implementation challenges, particularly in hybrid environments where legacy systems coexist with new technologies.

VII. FUTURE RESEARCH DIRECTIONS

Future research in ZTSAfor 6G networks may focus on the following areas:

- AI-based autonomous security management
- Quantum-resistant cryptographic algorithms
- Lightweight authentication protocols for IoT devices
- Blockchain-based decentralized trust management
- Privacy-preserving security frameworks

According to Jeysuriya et al., (2026), quantum-resistant trust evaluation models may play a significant role in securing future wireless networks.

VIII. CONCLUSION

The emergence of 6G wireless communication systemsformulates significant security problems owing to their distributed and heterogeneous nature. Traditional security approaches based on implicit trust are insufficient for protecting future networks. ZTSA has emerged as a robust and forward-looking approach that fundamentally redefines trust management in communication systems. By enforcing strict identity verification, continuous authentication, ZTSA minimize the risk of unlawful access within the network. The incorporation of complementary technologies such as artificial intelligence, block-chain, and edge computing further strengthens the ability of ZTSA to detect threats and respond proactively to emerging cyber risks in future 6G environments.

Despite its significant advantages, the large-scale deployment of ZTSA within 6G networks remains an evolving research domain that presents several technical and operational challenges. Issues related to scalability, computational overhead, interoperability across heterogeneous platforms, and privacy protection must be carefully addressed to ensure practical implementation. In particular, managing authentication and access control for billions of interconnected devices requires highly efficient identity management frameworks and lightweight security mechanisms. Additionally, the integration of intelligent automation and decentralized trust models will play a vitalpart in improving the adaptability and resilience of future network security infrastructures. Therefore, continued research efforts are essential to design scalable, privacy-preserving, and performance-efficient zero-trust solutions that can effectively safeguard next-generation wireless communication systems.

Such advancements will be critical for establishing secure, trustworthy, and reliable 6G networks capable of supporting digital ecosystems of the future.

REFERENCES

1. Alnaim, A. K., & Alwakeel, A. M. (2025). Zero trust strategies for cyber-physical systems in 6G networks. Mathematics, 13(7), 1108.
2. Jeysuriya, K., Renjith, P. N., & Sudhakaran, G. (2026). Quantum-resilient cross-trust evaluation for zero trust 5G security. Scientific Reports.
3. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture: A comprehensive survey. IEEE Access.
4. Chen, X., Feng, W., Ge, N., & Zhang, Y. (2022). Zero trust architecture for 6G security. IEEE Communications.
5. Ramezanpour, K., & Jagannath, J. (2022). Intelligent zero trust architecture for 5G and 6G networks. Computer Networks.
6. Enright, M., Hammad, E., & Dutta, A. (2022). Learning-based zero trust architecture for future networks. IEEE Future Networks.
7. Mohsan, S. A. H., & Li, Y. (2023). A contemporary survey on 6G wireless networks. IEEE Communications Surveys.
8. Sedjelmaci, H., Kaaniche, N., & Tourki, K. (2024). Secure and resilient 6G radio access networks with zero-trust architecture. Journal of Network Systems.
9. Nahar, N., Andersson, K., Schelén, O., & Saguna, S. (2024). Zero trust architecture applications in 6G networks. IEEE Access.
10. Tripi, G., Iacobelli, A., Rinieri, L., & Prandini, M. (2024). Security and trust in the 6G era. Electronics.
11. Scalise, P., Boeding, M., Hempel, M., Sharif, H., & Reed, J. (2024). Security challenges in 5G and 6G networks. Future Internet.
12. Li, S., Iqbal, M., & Saxena, N. (2022). Zero-trust security framework for industrial IoT. Information Systems Frontiers.
13. Trinh-Nguyen, B., et al. (2024). Trust management in 6G networks. Journal of Network and Computer Applications.
14. Al-Matari, N. Y., et al. (2024). Blockchain-enabled security for 6G networks. Scientific Reports.
15. Celik, A., & Eltawil, A. M. (2024). Generative AI for 6G wireless intelligence. IEEE Communications.

16. Siniarski, B., et al. (2025). Automated security service platform for 6G networks. Future Generation Computer Systems.
17. Sedjelmaci, H., & Ansari, N. (2023). Zero trust architecture empowered attack detection framework to secure 6G edge computing. IEEE Network, 38(1), 196-202.
18. El-Hajj, M. (2025). Secure and trustworthy open radio access network (O-RAN) optimization: A zero-trust and federated learning framework for 6G networks. *Future Internet*, *17*(6), 233.
19. Enright, M. A., Hammad, E., & Dutta, A. (2022, October). A learning-based zero-trust architecture for 6g and future networks. In *2022 IEEE Future Networks World Forum (FNWF)* (pp. 64-71). IEEE.
20. Bhagyalakshmi, L., Suman, S. K., Singh, S., & Assaf, M. H. (2026). AI-Enabled Zero Trust Model for Cyberattack Mitigation in Decentralized 6G Network. *International Journal of Communication Systems*, *39*(7), e70465.