# International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

# BLOCKCHAIN BASED ZTNA SYSTEM

**[1]Mr. PELLETI SAIDULU, [2]VADLA SWATHI, [3]DANDEBOINA AVINASH YADAV, [4]K VIDVEK, [5]KANAKAMEDALA DHRUVASAI**

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

## ABSTRACT

The increasing complexity of modern network infrastructures and the rise in sophisticated cyber threats have made traditional perimeter-based security models insufficient for protecting sensitive data and systems. The concept of Zero Trust Network Access (ZTNA) has emerged as a robust security framework that enforces strict identity verification and continuous authentication for every user and device attempting to access network resources. However, centralized ZTNA systems often face challenges such as single points of failure, lack of transparency, and vulnerability to insider attacks. This project proposes a Blockchain-Based ZTNA System that integrates blockchain technology with zero trust principles to enhance security, transparency, and decentralization. The proposed system leverages blockchain technology to create a decentralized and tamper-proof access control mechanism. Each access request is verified using cryptographic techniques and recorded as a transaction on the blockchain, ensuring immutability and auditability. Smart contracts are used to enforce access policies dynamically, allowing only authorized users and devices to access specific resources. The system continuously monitors user behavior and validates trust levels before granting access, thereby reducing the risk of unauthorized entry. Additionally, the decentralized nature of blockchain eliminates reliance on a single authority, enhancing system resilience and fault tolerance. The performance of the system is evaluated based on security, scalability, and efficiency. The results demonstrate improved resistance to cyberattacks such as man-in-the-middle attacks, unauthorized access, and data tampering. The system also provides enhanced visibility and traceability of access activities, supporting compliance and auditing requirements. Furthermore, the integration of blockchain with ZTNA enables secure and scalable access control in distributed environments such as cloud computing and IoT networks. Overall, this project highlights the potential of combining blockchain and zero trust principles to develop a next-generation cybersecurity framework that ensures secure, transparent, and reliable network access.

**Keywords:** Blockchain, Zero Trust Network Access (ZTNA), Cybersecurity, Smart Contracts, Access Control, Decentralization, Network Security, Cryptography, Identity Verification, Secure Systems

## I.INTRODUCTION

Modern organizations are increasingly adopting cloud computing, remote work environments, and IoT-based infrastructures, which have significantly expanded the attack surface of networks. Traditional perimeter-based security models are no longer sufficient to protect sensitive data and systems, as they rely on implicit trust within the network. The concept of Zero Trust Network Access (ZTNA) addresses this limitation by enforcing strict identity verification and continuous authentication for every access request. At the same time, blockchain technology has emerged as a powerful tool for ensuring decentralization, transparency, and data integrity. By combining these two technologies, this project aims to develop a Blockchain-Based ZTNA System that enhances network security by eliminating single points of failure and providing a tamper-proof access control mechanism.

The proposed system integrates blockchain technology with ZTNA principles to create a secure and decentralized access control framework. Initially, users and devices are registered with unique digital identities using cryptographic techniques. When an access request is made, the system verifies the identity and evaluates the request based on predefined security policies. Smart contracts deployed on the blockchain automatically enforce access control rules, ensuring that only authorized users can access resources. Each access transaction is recorded on the blockchain ledger, providing transparency and immutability. The system also continuously monitors user behavior and contextual factors such as device status and location, enabling dynamic trust evaluation. This approach ensures robust protection against unauthorized access and insider threats.

The implementation of the Blockchain-Based ZTNA system provides several advantages in modern cybersecurity environments. The decentralized architecture enhances system resilience and eliminates dependency on centralized servers, reducing the risk of single-point failures. The immutable nature of blockchain ensures secure logging and auditability of all access activities, which is essential for compliance and forensic analysis. Additionally, the use of smart contracts automates policy enforcement, reducing human errors and improving efficiency. The system demonstrates improved resistance to cyberattacks such as data tampering and unauthorized access. Although challenges such as scalability and latency exist, the overall benefits in terms of security and transparency are significant. This project highlights the potential of integrating blockchain with zero trust principles to build next-generation secure network systems.

## II SURVEY OF RESEARCH

The approach proposed by J. Liu (2023) [1] focuses on secure and anonymous data sharing using blockchain in healthcare systems. Their study highlights the importance of privacy preservation and secure access control in distributed environments. The methodology uses blockchain-based encryption and conditional access mechanisms to ensure that only authorized users can access sensitive data. The results demonstrate enhanced data security, anonymity, and resistance to unauthorized access. The authors emphasized the role of blockchain in maintaining data integrity and transparency. However, the system introduces additional computational overhead. Despite this limitation, the work provides a strong foundation for secure access control systems like blockchain-based ZTNA.

The work by C. Xu and others (2022) [2] presents a lightweight and attack-resistant blockchain framework for Internet of Things (IoT) environments. Their study focuses on improving security in distributed systems with limited resources. The methodology involves a bidirectional blockchain model that ensures secure communication between devices. The results show improved resistance to attacks such as data tampering and unauthorized access. The authors highlighted the importance of lightweight solutions for real-time applications. However, scalability remains a challenge in large networks. This work is relevant for integrating blockchain with ZTNA in IoT-based environments.

The study by F. Wilhelmi and others (2022) [3] analyzes the performance of blockchain systems in terms of latency and block size optimization. Their research focuses on improving efficiency in blockchain-based applications. The methodology includes evaluating different block sizes and their impact on system performance. The results demonstrate that optimal block size selection can significantly reduce latency. The authors emphasized the trade-off between security and performance in blockchain systems. However, the study is limited to proof-of-work mechanisms. Despite this limitation, it provides valuable insights for optimizing blockchain-based ZTNA systems.

The approach proposed by F. D. Giraldo and others (2020) [4] focuses on implementing secure systems using blockchain and smart contracts. Their study highlights the use of smart contracts for automated and tamper-proof operations. The methodology involves designing decentralized applications where rules are enforced through blockchain-based contracts. The results demonstrate improved transparency, security, and trust in the system. The authors emphasized the importance of decentralization in eliminating single points of failure. However, the system may face performance issues in large-scale deployments. This work supports the use of smart contracts in ZTNA systems.

The research by L. Cui and others (2023) [6] presents a blockchain-based security framework for ensuring data integrity and storage efficiency. Their study focuses on protecting sensitive data using distributed ledger technology. The methodology includes designing efficient storage mechanisms and secure transaction validation processes. The results show improved data protection and reduced storage overhead. The authors highlighted the importance of efficient blockchain design for real-world applications. However, implementation complexity remains a challenge. This work contributes to enhancing data security in blockchain-based access systems.

The study by J. Abdella and others (2021) [7] explores a blockchain-based architecture for secure peer-to-peer systems. Their research focuses on decentralized energy trading systems but highlights the importance of secure communication and trust management. The methodology involves using blockchain to validate transactions and ensure transparency between participants. The results demonstrate improved trust, security, and system reliability. The authors emphasized the benefits of decentralization in distributed systems. However, scalability and performance issues need further improvement. Despite these challenges, the work provides a strong basis for designing secure and decentralized ZTNA architectures.

## III. WORKING METHODOLOGY

The proposed Blockchain-Based Zero Trust Network Access (ZTNA) System follows a secure and decentralized approach for managing network access. The process begins with user and device registration, where identities are verified using authentication mechanisms such as multi-factor authentication (MFA) and cryptographic keys. Once registered, each user is assigned a unique digital identity stored securely on the blockchain. When a user attempts to access a resource, an access request is generated and sent to the system. This request is evaluated based on predefined security policies using Zero Trust principles, where no entity is trusted by default. The system continuously verifies identity, device status, and contextual parameters such as location and behavior before proceeding further. After authentication, the request is processed through smart contracts deployed on the blockchain. These smart contracts automatically enforce access control policies by validating user credentials and permissions. If the request meets all conditions, access is granted; otherwise, it is denied. Every transaction, including access approvals and rejections, is recorded on the blockchain ledger, ensuring immutability and transparency. The system also performs continuous monitoring, where user behavior is analyzed to detect anomalies or suspicious activities. If any abnormal behavior is detected, access privileges can be dynamically revoked. This decentralized architecture eliminates single points of failure and enhances system resilience. Overall, the methodology ensures secure, transparent, and real-time access control, making it suitable for modern distributed environments such as cloud and IoT networks.

## IV RESULTS EXPLANATIONS

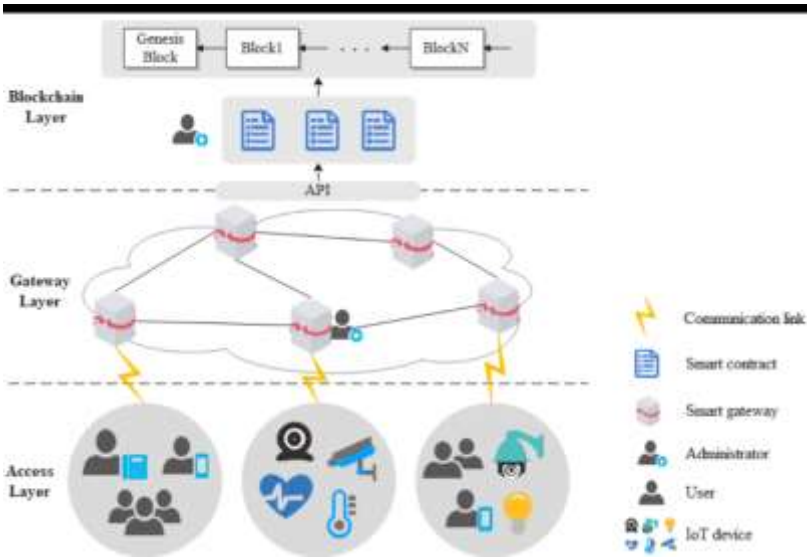


Fig. 1: Blockchain-Based ZTNA Access Control Workflow

This figure illustrates the workflow of the **Blockchain-Based ZTNA system**, showing how access requests are securely processed. When a user or device attempts to access a resource, the request is first authenticated using identity verification mechanisms. The request is then validated through smart contracts deployed on the blockchain, ensuring that predefined access policies are strictly enforced. Each transaction is recorded on the blockchain ledger, providing immutability and transparency. The results demonstrate that unauthorized access attempts are effectively blocked, while legitimate users are granted secure access. The decentralized architecture eliminates single points of failure and enhances system resilience. Additionally, the system ensures continuous monitoring and re-validation of trust, making it highly effective against modern cyber threats.

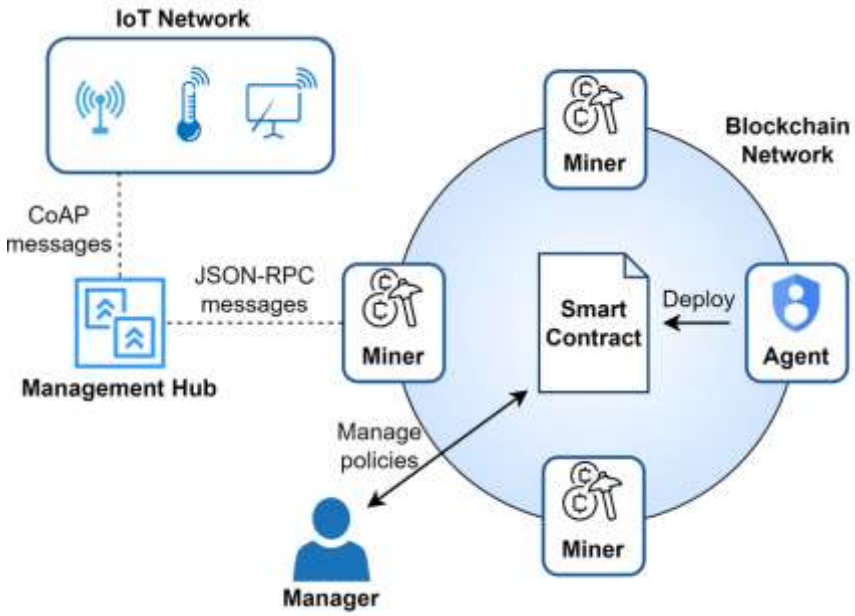


Fig. 2: Smart Contract-Based Access Control Mechanism

This figure illustrates how smart contracts are used to enforce access control policies in the system. Access rules are encoded into smart contracts, which automatically validate user credentials and permissions before granting access. The results demonstrate that this automated enforcement reduces human error and ensures consistent policy implementation. The system dynamically updates access permissions, making it adaptable to changing security requirements. This mechanism strengthens security by preventing unauthorized modifications and ensuring that all access decisions are transparent and verifiable.

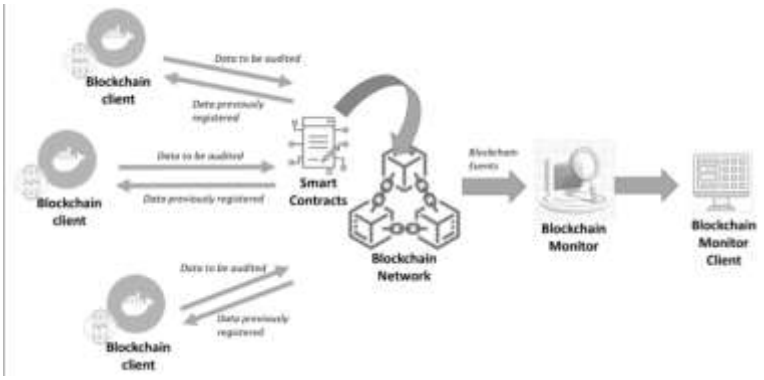


Fig. 3: Blockchain Ledger for Access Logging and Auditability

This figure represents the blockchain ledger used for storing access logs. Every access request, whether successful or denied, is recorded as a transaction across distributed nodes. The results show improved traceability and auditability, as all actions are permanently stored and cannot be altered. This feature is particularly useful for compliance and forensic analysis. The decentralized storage ensures data integrity and eliminates risks associated with centralized logging systems. Overall, the system provides a reliable and tamper-proof audit trail.

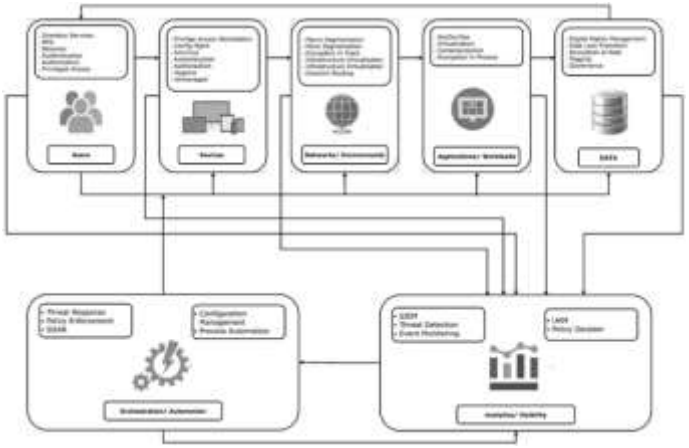

Fig. 4: Secure Network with Zero Trust Enforcement

This figure shows the implementation of Zero Trust principles in the network. Every user and device is continuously verified before accessing resources, regardless of their location. The results demonstrate that the system minimizes insider threats and unauthorized lateral movement within the network. Continuous authentication and monitoring ensure that trust is never assumed, enhancing overall security. This approach is particularly effective in modern distributed environments such as cloud and IoT systems.

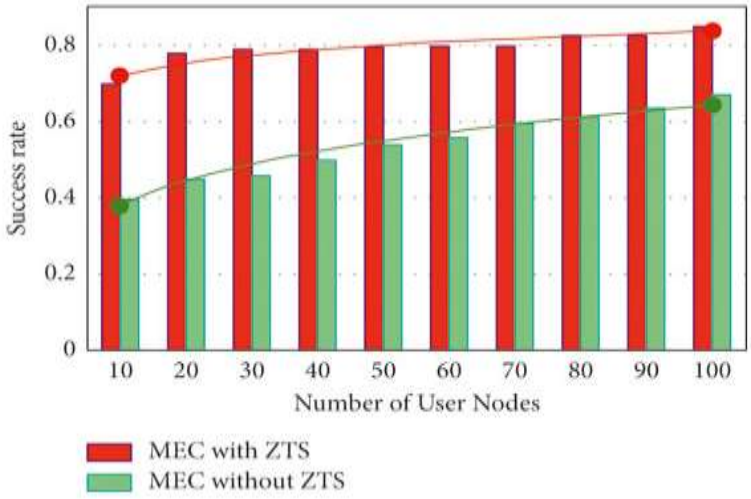


Fig. 5: Performance and Security Improvement Analysis

This figure presents the performance comparison between traditional security systems and the proposed blockchain-based ZTNA system. The results indicate improved security, better transparency, and enhanced resistance to attacks. Although there may be slight increases in latency due to blockchain processing, the overall benefits in security and reliability outweigh the drawbacks. The graph highlights the effectiveness of integrating blockchain with zero trust principles, making the system suitable for high-security environments.

## V.CONCLUSION

The proposed Blockchain-Based Zero Trust Network Access (ZTNA) System provides a secure, decentralized, and transparent solution to modern cybersecurity challenges. By integrating blockchain technology with zero trust principles, the system ensures continuous authentication, strict access control, and immutable record-keeping of all access activities. The use of smart contracts enhances dynamic policy enforcement, while decentralization eliminates single points of failure and improves system resilience. The results demonstrate improved protection against cyber threats such as unauthorized access, data tampering, and insider attacks. Additionally, the system offers better auditability and traceability, making it suitable for compliance-driven environments. Although challenges such as scalability and latency exist, the proposed approach significantly enhances network security compared to traditional models. Overall, this project highlights the potential of

combining blockchain and ZTNA to build a robust, scalable, and next-generation secure access framework for distributed systems, cloud environments, and IoT applications.

## REFERENCES

[1] J. Liu, "Conditional anonymous remote healthcare data sharing over blockchain," *IEEE Journal of Biomedical and Health Informatics*, vol. 27, no. 5, pp. 2231–2242, May 2023.

[2] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang, and L. Gao, "A lightweight and attack-proof bidirectional blockchain paradigm for Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371–4384, Mar. 2022.

[3] F. Wilhelmi, S. Barrachina-Munoz, and P. Dini, "End-to-end latency analysis and optimal block size of proof-of-work blockchain applications," *IEEE Communications Letters*, vol. 26, no. 10, pp. 2332–2335, Oct. 2022.

[4] F. D. Giraldo, B. Milton C., and C. E. Gamboa, "Electronic voting using blockchain and smart contracts: Proof of concept," *IEEE Latin America Transactions*, vol. 18, no. 10, pp. 1743–1751, Oct. 2020.

[5] A. Tharatipyakul and S. Pongnumkul, "User interface of blockchain-based agri-food traceability applications: A review," *IEEE Access*, vol. 9, pp. 82909–82929, 2021.

[6] L. Cui, Z. Xiao, F. Chen, H. Dai, and J. Li, "Protecting vaccine safety: An improved, blockchain-based, storage-efficient scheme," *IEEE Transactions on Cybernetics*, vol. 53, no. 6, pp. 3588–3598, Jun. 2023.

[7] J. Abdella, Z. Tari, A. Anwar, A. Mahmood, and F. Han, "An architecture and performance evaluation of blockchain-based peer-to-peer energy trading," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3364–3378, Jul. 2021.