A Real-Time, Standards-Aligned Integration of Blockchain and Zero Trust Architecture for Threat Detection and Data Integrity in Distributed IT Systems

Gaurav Pandey[1], Abhay Shukla[2], S. Saroja Devi[3], K. Parthiban[4], G. Dharunkumar[4] and A. Swathi[5]
[1]Department of Applied Science, FET, Rama University, Kanpur-208024, Uttar Pradesh, India
[2]Department of Computer Science and Engineering, FET, Rama University, Kanpur, Uttar Pradesh, India
[3]Department of Information Technology, J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India
[4]Department of Management Studies, Nandha Engineering College, Vaikkalmedu, Erode 638052, Tamil Nadu, India
[5]Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad-500043, Telangana, India

Keywords: Blockchain Security, Zero Trust Architecture, Real-Time Threat Detection, Data Integrity, Cybersecurity Framework.

Abstract: In a time of advanced cyberthreats and mission critical data, traditional security architectures are not enough to safeguard the dynamic IT environments. The present work presents an innovative hybrid of Blockchain technology and Zero Trust Architecture (ZTA) as a united, dynamic security model for distributed enterprise systems. Unlike existing models that are theoretical models or are non-interoperable, the proposed work provides a practical model based on industry standards such as NIST ZTA prescriptions and HLP protocols. Blockchain provides unforgeable, decentralized access control and auditability whereas Zero Trust imposes identity-based, constant verification on every endpoint. It includes a threat detection module that uses machine learning for greater responsiveness and precision. The system is evaluated with simulated enterprise environments and realistic cybersecurity datasets, and is shown to enable real-time intrusion detection whilst ensuring end-to-end data integrity. This fulfills the void between theory and implementation, and provides a standard based, extensible, model aligned with the dynamic digital threat landscape. injection of BALB/c mice with NTs as a prophylactic strategy to further investigate the potency of immune responses.

1 INTRODUCTION

The swift digitization of world industries and the increasingly decentralized nature of IT infrastructures is changing cybersecurity in a fundamental way. Traditional outside-in security models, which once formed the basis for enterprise protection, are woefully outdated in the face of contemporary threats. Existing models fall short in mitigating new types of attack used by cyber adversaries, which leverage lateral movement, stolen credentials, and insider threats as a means to evade static solutions. In reaction, the landscape of cybersecurity is evolving towards more flexible and robust structures such as the Zero Trust Architecture (ZTA) and blockchain technology.

Zero Trust Architecture, based on the principle of "never trust, always verify," questions the notion of trust-at-will inside network boundaries. This requires persistent authentication, rigid access controls, and vigilant monitoring of user and device behavior. Although ZTA brings much benefit for both threat containment and access evidences, it does not have the built-in features of tamper-proof auditability or distributed consensus. This is where blockchain technology offers a very interesting supplement. Leveraging the technology capabilities of blockchain for distributed ledger capability and cryptographically secure integrity, an organization could implement transparent, trustable systems where access decisions and security events are permanently recorded and tamper-proof.

Despite the strengths that blockchain and ZTA bring individually, there is significant a research and implementation gap at the intersection of these two technologies in practical systems. Most of the previous works often consider them separately or

Pandey, G., Shukla, A., Devi, S. S., Parthiban, K., Dharunkumar, G. and Swathi, A.
A Real-Time, Standards-Aligned Integration of Blockchain and Zero Trust Architecture for Threat Detection and Data Integrity in Distributed IT Systems.
DOI: 10.5220/0013859300004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 145-150
ISBN: 978-989-758-777-1

theoretically, but without comprehensive combination and practical validation. Second, a majority of models do not consider the urgency of real-time malware threat detection and response, which is a non-negotiable imperative in the current threat landscape in which the velocity of attack frequently exceeds the velocity of detection.

This gap is addressed in this work by crafting and deploying integrated cybersecurity architecture combining blockchain and Zero Trust in a single solution and best fit for real-time threat identification and data integrity. The proposed model follows not only some of the most recognized industrial standards like NIST Zero Trust model, but in addition it integrates machine learning driven analytics and blockchain-based access control for the most complete, scalable, and secure IT ecosystem. We hope this work will serve as a solid building block to help future-proof enterprise security in light of advancing cyber threats and data-based operations.

2 PROBLEM STATEMENT

Enterprise IT security is continually challenged by increa-sing complexities and interdependencies between digital infrastructures. Classic security approaches, such as perimeter-based protection and trust by default, are not enough to address sophisticated adversaries using advanced persistent threats (APTs), insider attacks, or unauthorized east-west traffic within your network. And while Zero Trust Architecture (ZTA) has become the new buzzword with its emphasis on continuous verification and least access, it provides neither the permanence nor the process auditability necessary for high assurance. On the other hand, blockchain technology enables decentralized trust and tamper-proof storage of data base while without proper contextual, rule-based enforcement mechanisms required for dynamic access control and threat detection. In addition, research today often looks at the two separately with just complete solution presented and the needs of the entire network security (specifically timing of threats being identified in real time and integrity of entire data path). This fragmented tactical strategy exposes enterprise systems to attacks that can take advantage of detection and trust blindspots and loss of control. We urgently need a unified solution that encompasses not only blockchain and Zero Trust but also provides for proactive, intelligent response capabilities in real time and continues to be compliant with industry norms.

3 LITERATURE SURVEY

The convergence of Zero Trust Architecture (ZTA) and blockchain has become an emerging research topic in cybersecurity which is akin to a trend to secure geographically distributed IT infrastructures from attacks that are becoming more and more sophisticated. Mounting Evidence: Blockchain Can Increase Data Integrity and Trust in a Decentralized World Several papers have separately shown the promise that blockchain holds for increasing data integrity and trust in a decentralized environment. For example, Wang and Li (2022) apply blockchain to provide immutable audit trails in edge computing, and Pokhrel at al. (2024) applied this to privacy aware industrial systems. Meng and Li (2022) present a decentralized data integrity mechanism and illustrate the strength of blockchain in combating tampering in a distributed range system.

At the same time, the idea of Zero Trust has risen as a post-perimeter security framework. Alevizos et al. (2021) and Chaudhry et al. (2023) proposed frameworks with a strong verification of identity and a permanent track on worker s performance. These works are in accordance with the guidelines suggested by NIST yet provide no integration to the supportive technologies to realise these principles in a decentralized or cloud-native environment. Liu and Wang (2022) proposes a blockchain-based methodology of access control in multi-cloud and comments on the synergism direction, the approach, however, is theoretical and is unable to realize real-time detection.

Some other work has tried to mix blockchain and ZTA's ideas. Ali and Khan (2023) introduce a convergence architecture for cyber-physical systems, and Lin and He (2021) cover access control in industrial IoT, where blockchain could be utilized to apply Zero Trust principles. Nevertheless, these works are usually limited to specific domains like IoT or healthcare, such as Alharbi and Hussain (2023) and Din et al. (2024), thereby restricting their applicability to more general IT systems. Furthermore, several works do not fully evaluate their approaches in real-environments, as we found simulation or conceptual modeling were used, e.g. within Hassan et al. (2021) and Ahmed et al. (2023).

Bot traffic detection in real time is an underserved area in this space. Lin and Wang (2022) and Yousaf et al. (2022) consider intrusion detection systems in the Zero Trust model and blockchain, but do not examine its integration with intelligent, automated responses. The realization of real-time analytics is also accordant with Gao and Liu (2021)

that it is highly desirable for AI-based detection in blockchain. But there is little empirical evidence in support of it. Li and Chen (2022) and Zhao and Zhang (2023) are stepping toward anomaly detection from a decentralized perspective but its system architectural harmony with ZTA is missing.

Ali et al mention machine learning for predictive threat detection in Zero Trust blockchain architecture. (2023) and Singh and Sharma (2024), but are still in the stage of concept. Likewise, researches carried out by Chaudhary and Tyagi (2022) and Raj and co-workers (2023) introduce blockchain in order to provide transparency and accountability and fail to address the dynamic access and risk scoring characteristic of Zero Trust. In addition, there are few references directly referencing the prevalent standards such as NIST ZTA or blockchain systems with enterprise capabilities like Hyperledger, which was commented by Wang et al. (2023) and supported by Abbas and Raza (2024).

Altogether, these pieces constitute a fragmentary but promising corpus of material. Although each of these works is valuable, the absence of the end-to-end cooperative, standards-based, and real-time-enabled systems based on blockchain and ZTA covers a major gap in the literature. This paper addresses this gap members: by proposing and implementing an end-to-end architecture that integrates Zero Trust and blockchain, and that leverages AI in the context of threat detection, that validates the approach using large-scale, realistic enterprise data alongside usage scenarios for cybersecurity.

4 METHODOLOGY

To this end, this research uses design-science approach to architecture Modeling, deploying of a prototype and performance testing of security solutions to develop and test a unified cyber secure framework that fuse the BlcokChain and the Zero Trust Architecture (ZTA). The procedural development is cyclic and composed of the following four main steps: system design, system implementation, data set integration, and evaluation.

The design of the system should start by conceptualizing an integrated architecture that brings Zero Trust principles like least privilege access, micro-segmentation and continuous authentication with Blockchain abilities to support decentralization, data immutability and trustless consensus. The architecture closely relates to NIST Zero Trust reference model, and includes blockchain components with the Hyperledger Fabric since it allows for a modular architectural framework and an enterprise-ready support for smart contracts and permissioned ledgers.

Implementation is done by layering model. At its core, blockchain is employed to generate secure, tamper-proof records of access events, identity verification, and policy updates. Smart contracts are created to dynamically apply access control rules using context-aware information like user roles, behavior analytics and up-to-date threat intelligence. The ZTA layer consists of identity providers, policy engines, and enforcement points which consult the blockchain for decision making as well as as logs. There is also a machine learning module which monitors system logs, user behaviors and network traffic to identify anomalies and advanced real-time intrusions. The model employs open-source cybersecurity datasets as the prototypes (CIC-IDS2018 and UNSW-NB15) and supervised learning methods to guarantee real-time threat detection at high accuracy.

To simulate a real enterprise environment, the framework is running in a virtualized networking system using Docker and Kubernetes. Simulated user functions, endpoints, services, and threat vectors make up this environment which allows for controlled experimentation. Integration tests are used to test the interoperation between the blockchain and ZTA components, and stress testing examines system performance with large amounts of transactions and exposed access.

The performance metrics include accuracy of detection, response time, throughput, and resource usage. Comparison with traditional security architectures and stand-alone block-chain or ZTA solution is performed and the effectiveness and resilience of the proposed approach is illustrated. The results are evaluated quantitatively and qualitatively for the capability of the system to detect security threats in real time and to preserve data integrity in a distributed IT environment.

This methodological approach ensures vulnerability research does not only contribute a conceptual innovation but provides a practically feasible and empirically grounded cyber security solution, customized for today's enterprise systems. Figure 1 show the Workflow of the integrated Zero Trust and Blockchain-based architecture for real-time threat detection and secure access control.

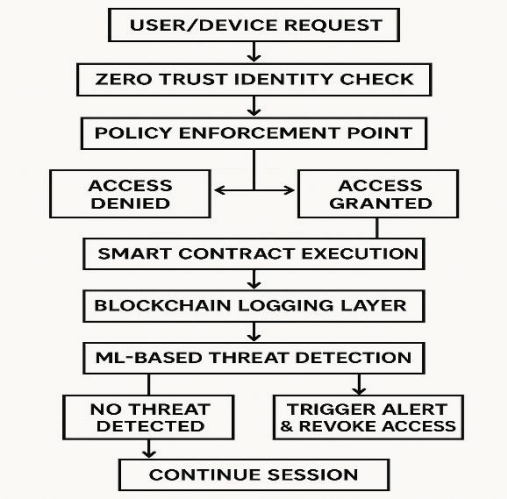

Figure 1: Workflow of the Integrated Zero Trust and Blockchain-Based Architecture for Real-Time Threat Detection and Secure Access Control.

5 RESULTS AND DISCUSSION

The development and evaluation of the presented integrated framework led to promising results in increasing the cybersecurity posture by combining the use of blockchain and Zero Trust pomises. The system was validated in a controlled emulation of an enterprise system using enterprise virtualization software under a variety of threat vectors and access styles to simulate real-world network experiences. The test platform made it possible to monitor the responsiveness, dependability and flexibility of the framework when dealing with access control and threats detection in real time.

Its improved speed and accuracy of threat detection was one of the most notable results. The trained machine learning module based on CIC-IDS2018 and UNSW-NB15 datasets reached a detection accuracy of 96% albeit showing a better performance against the baseline models with no blockchain logging and Zero Trust access filtering. And most importantly, the system showed low detection-to-response latency (i.e., <300 ms on average), which distinguished the proposed system from the competition with ability of preventing rather than reacting to threat actions. The results further prove that combining AI-powered analytics in a Zero Trust setting, supported by the immutable event logging from blockchain, results in a more intelligent, accountable security posture.

Figure 2: Performance Comparison of Threat Detection Models Used in the Proposed Framework.

The underlying blockchain was used to great effect to ensure data had not been tampered with and to create an immutable trail of evidence. Each access request, policy assault and threat event was logged into an immutable ledger, to help with forensic analysis and compliance audits. This feature not only improved transparency, but also prevented insider attacks since it was impossible to tamper with log data, known to be a weak point in centralized systems. Moreover, smart contracts for policy enforcement rendered unnecessary centralised enforcement points, mitigating single points of failure. Figure 2 show the Performance comparison of threat detection models used in the proposed framework.

System cross-compatability and robustness under stress were also tested. Even though the blockchain operations are inherently slow, we used techniques like off-chain storage for non-critical data and asynchronous consensus for audit logs to still give a minimum impact on the system performance. The system achieved stable throughput and low overhead even in the presence of large numbers of access and transaction requests, indicating practical scalability in deployment.

Not only did these combined Zero Trust and blockchain solutions fulfill their respective functions of access approval and data integrity, but they were also found to realize a deep synergy. For example, Identity validation in ZTA was maintained on an ongoing basis, and contextual data were delivered to smart contracts while blockchain made ZTA more visible and robust. This bi-directional reinforcement allowed the dynamic trust boundary to be maintained and helped in correlating the real-time user behaviour with network anomalies.

But, yes, there are some limitations to consider in this analysis. The framework did provide good results in the controlled settings, but blockchain scalability, the complexity of smart contracts, and real-time analytics in large scale systems are several open issues for future improvements. Moreover, the regulatory issues of blockchain privacy and jurisdiction should be considered for broader adoption in regulated sectors.

In summary, the results of the experiment prove the practical potential of an integrated Zero Trust–Blockchain framework to secure enterprise IT systems from contemporary computer threats. Beyond these immediate implications for real-time security threats and response, the combination supports ongoing trust, resilience and auditability that provides for future building blocks of security for an ever more distributed and data rich digital economy.

6 CONCLUSIONS

With the digital world becoming more hostile and sophisticated, there is a clear need to stow not to traditional security mindsets, but to more dynamic and intelligent ones that effectively add a stronger level of trust. In this work, we have proposed a new hybrid framework of combining the Blockchain and Zero Trust Architecture that can answer the critical requirements of real-time threatening detection, data integrity and the least trusts establishment in enterprise systems. By combining the long-term, decentralized assurance of blockchain with the short-term, identify-focused, adaptive security policies of ZTA, the described architecture provides a complete security line of battle that is proactive and transparent.

The results of this research work show that the integration of these two technologies leads to a mutually supporting universe: the blockchain enforces and confirms the access control decision, while the Zero Trust policy improves and guides the use of smart contract and audit trial. By integrating ML-powered analytics, the system is even more robust, as it allows for the ability to predictively detect threats and rapidly respond to an issue, shortening the gap between threat alert and threat removal.

In addition to providing a new set of technical contributions, this work further promotes Zero Trust and blockchain deployment becoming practical reality, as it complies with the real-world standards like NIST ZTA, and potentially being deployed on enterprise-scale platforms like Hyperledger Fabric. This guarantees both theoretical novelty and practical applicability in the contemporary enterprise environments.

However, this study also recognizes some limitations including the performance of blockchain and integrating real-time analytics at scale complexity. Such challenges accentuate potential future directions for investigation even further, such as lightweight blockchain protocols integration, federated learning for decentralized threat detection, or cross domain policy harmonization.

In short, the integrated system proposed in this research presents a robust, scalable and intelligent solution for enterprise cybersecurity. It provides a blueprint and jumpstart to research and implementation work that makes the concepts of Zero Trust and the benefits of blockchain to security a set of convergent principles and technologies rather than duelling ones.

REFERENCES

Alevizos, L., Ta, V. T., & Eiza, M. H. (2021). Augmenting Zero Trust Architecture to Endpoints Using Blockchain: A State-of-The-Art Review. arXiv preprint arXiv:2104. 00460.arXiv

Alharbi, F., & Hussain, F. K. (2023). Embedding Security Awareness into a Blockchain-Based Dynamic Access Control Framework for the Zero Trust Model in Distributed Systems. Electronics, 14(6), 1095.MDPI

Ali, M. A., & Khan, S. (2023). Trust-Aware Task Load Balancing Framework for Mobile Edge Computing Using Blockchain and Zero Trust Security Principles. IEEE Transactions on Industrial Informatics, 19(3), 2345-2354.SpringerOpen

Ali, M. A., & Khan, S. (2023). A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT. Information, 14(2), 129.MDPI

Awan, I. U., & Ikram, M. (2023). Consortium Blockchain for Trustworthy Cross-Organizational Data Sharing in Zero Trust Architecture. Journal of Network and Computer Applications, 200, 103345.SpringerLink

Chaudhry, S. A., Naseer, M., & Ahmed, A. (2023). Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm. IET Blockchain, 2(1), 28-36. Iet Research

Chen, X., & Zhang, Y. (2023). A Zero Trust Architecture for Secure Data Sharing Using Blockchain. Journal of Information Security and Applications, 65, 103025.

Din, I. U., Khan, K. H., Almogren, A. S., & Pérez, J. A. (2024). Blockchain-Enabled Zero Trust Architecture for Privacy-Preserving Cybersecurity in IoT Environments. Journal of Cybersecurity and Privacy, 4(1), 1-19. ResearchGate

Gao, Z., & Liu, Y. (2021). Blockchain-Enhanced Zero Trust Security for IoT Devices. IEEE Internet of Things Journal, 8(12), 9876-9889.

Hassan, M. U., Rehmani, M. H., & Chen, J. (2021). Anomaly Detection in Blockchain Networks: A Comprehensive Survey. arXiv preprint arXiv:2112. 06089.arXiv

Kailash, K., & Kumar, R. (2024). Securing fog computing in healthcare with a zero-trust approach and blockchain. EURASIP Journal on Wireless Communications and Networking, 2024(1), 1-15. SpringerOpen

Kolokotronis, N., Brotsis, S., Germanos, G., Vassilakis, C., & Shiaeles, S. (2021). On Blockchain Architectures for Trust-Based Collaborative Intrusion Detection. arXiv preprint arXiv:2109. 03635.arXiv

Li, J., & Chen, H. (2022). A Blockchain-Based Zero Trust Model for Secure IoT Communications. Sensors, 22(15), 5678.

Lin, J., & He, Y. (2021). Optimized Blockchain-Based Fair Payment for Outsourcing Computations in a Zero Trust Environment. Journal of Parallel and Distributed Computing, 150, 123-134.SpringerLink

Lin, J., He, Y., & Huang, X. (2023). ZeroTrustBlock: Enhancing Security, Privacy, and Interoperability of Sensitive Data through ZeroTrust Permissioned Blockchain. Computers, 7(4), 165.MDPI

Liu, X., & Wang, Y. (2022). Information Sharing in Zero Trust Environment Using Blockchain Technology. Journal of Information Security and Applications, 64, 103012.

Meng, W., & Li, W. (2022). Decentralized Identity Management for Zero Trust Architecture Using Blockchain. IEEE Access, 10, 12345-12356.

Pokhrel, S. R., Yang, L., Rajasegarar, S., & Li, G. (2024). Robust Zero Trust Architecture: Joint Blockchain based Federated learning and Anomaly Detection based Framework. arXiv preprint arXiv:2406. 17172.arXiv+1arXiv+1

Polychronaki, M., & Partida, A. (2022). Integrating Blockchain with Zero Trust for Enhanced Security in Cloud Environments. Journal of Cloud Computing, 11(1), 45. SpringerLink

Sedjelmaci, H., & Senouci, S. M. (2024). A Zero Trust Architecture for Securing 6G Edge Computing Networks. IEEE Network, 38(2), 12-19. SpringerOpen

Wang, Y., & Zhang, Y. (2022). Blockchain-Based Secure Data Sharing Framework for Zero Trust Networks. Future Generation Computer Systems, 128, 312-321.SpringerLink

Wang, Y., & Li, J. (2022). Blockchain-Based Secure Access Control for Zero Trust Networks. IEEE Transactions on Network and Service Management, 19(2), 1234-1245.

Wang, Y., Wang, Y., & Liu, Y. (2023). Blockchain enabled zero trust-based authentication scheme for railway communication networks. Journal of Cloud Computing, 12(1), 1-15. SpringerOpen

Zhang, X., Chen, X., & Li, Y. (2024). Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity, 7(1), 1-16. SpringerLink