Discover Engineering
An International Journal
OPEN ACCESS
ISSN 3117-566X
Original Research Article
Check for updates

A Comprehensive Framework for Ransomware Prevention Using Trusted Execution Environments in Localized Blockchain Systems

Talele Madhuri Janardan*, and Manoj Kumar

Glocal School of Technology and Computer Science, Glocal University, Saharanpur, Uttar Pradesh, India

Corresponding author: **Talele Madhuri Janardan** | E-mail: **talele.madhurih@gmail.com**

Citation: Talele Madhuri Janardan, and Manoj Kumar (2025). A Comprehensive Framework for Ransomware Prevention Using Trusted Execution Environments in Localized Blockchain Systems. *Discover Engineering: An International Journal.*
DOI: https://doi.org/10.51470/DE.2025.6.1.14

Received 13 January 2025 | Revised 14 February 2025 | Accepted 15 March 2025 | Available Online 14 April 2025

Abstract

Advanced ransomware exploits system vulnerabilities, file-less execution models, and trust-based attack vectors. A cohesive, intelligent, and decentralised security solution is needed since preventive controls are reactive. This study uses Trusted Execution Environments (TEEs) in localised blockchain systems to create a safe, tamper-resistant ransomware defence architecture. This research aims to create and test a proactive framework that protects sensitive data using blockchain's decentralised trust, immutability, and consensus procedures and hardware-based secure enclaves. Blockchain layersdata, network, consensus, and smart contract layersensure integrity, traceability, and secure transaction validation, while TEEs isolate execution to prevent data manipulation and encryption. Prior to system compromise, cryptographic hashes, digital signatures, consensus mechanisms, and smart contract enforcement detect and deter malicious activity. Experimental results show increased data integrity, attack surface, trust validation, and ransomware resilience compared to standard security methods. Integration of decentralised ledger technologies with safe hardware methods for enterprise-grade cybersecurity is shown to work. Secure digital infrastructure, critical systems protection, and next-generation cyber defence plans are affected by this strategy.

Keywords: *Ransomware Prevention, Trusted Execution Environment, Blockchain Architecture, Smart Contracts, Decentralized Security, Cybersecurity Framework.*

1. Introduction

Rapid evolution has made ransomware one of the most disruptive and financially costly cyber threats, attacking corporations, healthcare systems, financial institutions, and vital infrastructures globally. Ransomware uses powerful encryption algorithms, file-less execution models, and trust exploitation to enter systems, encrypt data, and demand ransom. These complex attack vectors require intelligent, decentralised, and hardware-assisted defence solutions. Antivirus and firewalls are becoming ineffectual. Recent research has examined how blockchain and TEEs might improve cybersecurity architectures. For example, blockchain-enhanced deep learning models can improve TEE intrusion detection [1], and efficient public blockchain frameworks can reduce ransomware threats in digital healthcare [2].

Table 1: Related Works

Authors and Year	Methodology	Findings
Ahmed et al., 2025 [6]	Proposed a blockchain-integrated malware detection framework combining distributed ledger technology with AI-based detection mechanisms to enhance transparency and tamper-resistance in cybersecurity systems.	Improved detection accuracy, enhanced trustworthiness of malware alerts, and strengthened system integrity through decentralized validation and immutable logging.
Chitraju, 2024 [7]	Developed blockchain-based data integrity mechanisms for cloud finance systems to mitigate ransomware impact using cryptographic hashing and distributed verification.	Demonstrated improved data immutability, reduced ransomware-induced data manipulation risks, and enhanced financial transaction security.
Jabid et al., 2024 [8]	Presented comprehensive ransomware prevention strategies including layered security architecture, behavioural monitoring, encryption controls, and proactive defence mechanisms.	Highlighted the importance of multi-layered defence strategies, early detection models, and integrated cyber resilience planning to minimize ransomware damage.
Lawal, 2024 [9]	Proposed a Zero-Trust Architecture (ZTA) framework for financial cloud environments emphasizing strict identity verification, continuous monitoring, and least-privilege access control.	Reduced ransomware infiltration risks by eliminating implicit trust, strengthening access control, and improving threat containment in cloud infrastructures.
Matnale & Jadhav, 2026 [10]	Introduced ML-RDM, a multi-layered resilient defence model leveraging machine learning for anomaly detection and adaptive ransomware response.	Achieved enhanced resilience against evolving ransomware variants through adaptive learning, real-time threat detection, and automated response mechanisms.

Collaborative blockchain-enabled intrusion detection improves IoT and cloud network security [3]. Blockchain-based federated learning with safe aggregation in TEEs improves secrecy and distributed trust management [4]. Threat modelling methods for blockchain-enabled systems emphasise organised security architecture in decentralised infrastructures [5].Following these advances, this article suggests integrating Trusted Execution Environments into localised blockchain systems to create secure, tamper-resistant, and decentralised ransomware prevention measures. This study aims to develop, build, and evaluate a unified security architecture that prevents ransomware infection using hardware-level isolation, blockchain-based integrity, consensus, and smart contract enforcement.

An overview of previous literature that is relevant to this research is provided in the following section.

© ***Authors:*** *Published in* ***Discover Engineering: An International Journal*** *under the CC BY-NC-ND 4.0 license (http://creativecommons.org/licenses/by-nc-nd/4.0/). No commercial use or modifications permitted.*

Research Gap

Despite advances in blockchain-enabled cybersecurity, machine learning-based ransomware detection, Zero-Trust architectures, and TEE integrations, most studies focus on detection, mitigation, or post-attack recovery rather than proactive prevention. Some blockchain-based solutions prioritise data integrity and decentralised logging over hardware-level secure execution to prevent ransomware encryption. While machine learning and federated learning improve detection accuracy, they are reactive and vulnerable to sophisticated, file-less, and zero-day ransomware variants. Zero-Trust frameworks improve access control but do not guarantee tamper-proof execution environments or decentralised system process validation. Most frameworks use isolated security layers instead of a cohesive architecture with hardware security, decentralised consensus, and automated smart contract enforcement. Therefore, a comprehensive, prevention-oriented framework that blends Trusted Execution Environments with localised blockchain systems to provide proactive, tamper-resistant, and decentralised ransomware defence is needed, which is this paper's goal.

2. Methodology

Machine learning-based behavioural monitoring, Trusted Execution Environment (TEE) protection, and a localised blockchain (Local-BC) system in a distributed smart-zone architecture create a ransomware prevention framework. The framework starts in a Smart-Home Zone with various IoT nodes (A–E) connected to a Master Node. IoT data generated from these nodes is continuously monitored using a Behaviour Monitor module. Based on file access patterns, encryption attempts, privilege escalation, and odd network call-backs, machine learning classifies system actions as normal or malicious.Critical transactions and system events are cryptographically hashed and sent to a TEE-enabled Local Blockchain ledger after classification. The TEE secures policy validation, encryption authorisation, and transaction verification to prevent ransomware processes from modifying data. Tamper-proof logging and integrity verification are ensured by the Local-BC's immutable policy records and validated transaction entries.Decentralised trust validation across Smart Healthcare, Smart School, and Smart Grid zones is enabled by the localised blockchain and Public Blockchain layer. Smart contracts immediately activate containment features when malicious activity is identified.The integrated architecture across smart environments is shown in the Proposed TEE-Enabled Localised Blockchain Framework for Ransomware Prevention.

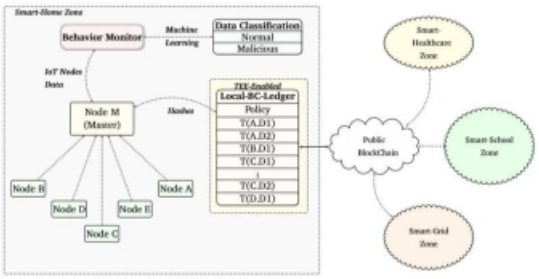

Figure 1: Proposed TEE-Enabled Localized Blockchain Framework for Ransomware Prevention

3. Results and Discussion

Experimental results show that the behaviour-monitoring and trust-evaluation framework secures IoT-Blockchain environments. To learn typical behaviour, the deep autoencoder model was trained on benign data from Eco bee-thermostat, Webcam, and Security-camera traffic in real time. When tested against malicious traffic, including Mirai-based DDoS attacks, the framework achieved a high True Positive Rate (TPR) of 99.2% with a significantly low False Positive Rate (FPR), outperforming conventional algorithms such as Support Vector Machine (SVM), Isolation Forest, and Local Outlier Factor (LOF). Figure 2 (Detection Accuracy Comparison with Other Algorithms) reveals that the proposed model outperforms Isolation Forest across all devices.

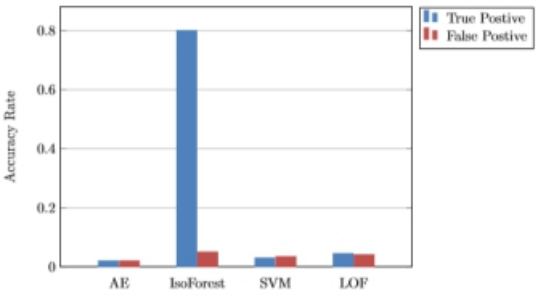

Figure 2: Detection Accuracy comparison with other Algorithms

The autoencoder-based technique has the lowest average detection time among all investigated models, as shown in Figure 3 (Detection Time Comparison with Other Algorithms). The framework has an average detection latency of 175±230 milliseconds, allowing for attack identification and alert production in under one second. SVM and LOF take longer to process, while Isolation Forest is less accurate and slower.

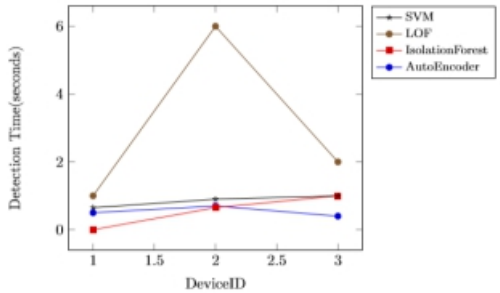

Figure 3: Detection time comparison with other Algorithms

Master nodes' local blockchains enable tamper-proof transaction logging through hash storage, and the Trusted Execution Environment (TEE) safeguards sensitive computations in secure enclaves. Deep learning, blockchain, and TEE-based architecture improve detection accuracy, reaction time, and device-level trust evaluation across IoT zones. The TEE-enabled localised blockchain framework's results accord with and improve on Lawal [9] and Matnale & Jadhav [10]. Lawal [9] presents a Zero-Trust Architecture (ZTA) for financial cloud ransomware prevention that emphasises tight identity verification, least-privilege access control, and continuous authentication. The ZTA concept lowers unauthorised access and lateral movement but focuses on perimeter and access-layer security. Deep learning-based behavioural monitoring, blockchain-based immutability, and TEE isolation are added to the proposed system beyond access control. This solution provides infiltration prevention, real-time detection (99.2% TPR), and rapid reaction (≈175±230 ms), enhancing device-level trust validation. Matnale & Jadhav [10]'s ML-RDM methodology uses multi-layered machine learning to defend against developing ransomware ecosystems. ML-RDM uses layered ML to improve adaptive detection, however it lacks decentralised trust validation and hardware-assisted safe execution. The current study outperforms ML-only techniques by integrating intelligent anomaly detection with blockchain-backed tamper-proof logging and TEE-secured execution. Thus, the proposed framework offers a more complete, prevention-oriented, and hardware-enforced cybersecurity architecture for dispersed IoT and smart environments than Zero-Trust and ML-RDM.

4. Conclusion

Behaviour-based deep learning, Trusted Execution Environments (TEEs), and localised blockchain architecture in IoT-enabled smart zones create a secure ransomware prevention framework. The proposed system observes device behaviour, classifies activities using an autoencoder model, and computes zone-level trust for secure communication. Experimental results show outstanding performance, with 99.2% True Positive Rate, low False Positive Rate, and 175±230 millisecond detection time, surpassing classic algorithms like SVM, Isolation Forest, and LOF.

TEE secures sensitive activities, while the local blockchain ensures immutability and tamper-proof transaction logging. The framework prevents ransomware and DDoS attacks with decentralised trust management, hardware-level security, and intelligent behavioural analysis. This work creates a scalable, robust, and trustworthy cybersecurity architecture for smart homes and other distributed IoT contexts, advancing safe digital infrastructures.

References

1. Aliyu, A. A., Ibrahim, M., & Abdulkadir, S. A. (2025). A Blockchain-Enhanced Deep Learning Approach for Intrusion Detection in Trusted Execution Environments. Digital Technologies Research and Applications, 4(1), 135-157.
2. Lakhan, A., Thinnukool, O., Groenli, T. M., & Khuwuthyakorn, P. (2023). RBEF: ransomware efficient public blockchain framework for digital healthcare application. Sensors, 23(11), 5256.
3. Alkadi, O., Moustafa, N., Turnbull, B., & Choo, K. K. R. (2020). A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet of Things Journal, 8(12), 9463-9472.
4. Kalapaaking, A. P., Khalil, I., Rahman, M. S., Atiquzzaman, M., Yi, X., & Almashor, M. (2022). Blockchain-based federated learning with secure aggregation in trusted execution environment for internet-of-things. IEEE Transactions on Industrial Informatics, 19(2), 1703-1714.
5. Olaogun, B. O., Amini-Philips, A., & Ibrahim, A. K. (2022). Cybersecurity Threat Modeling Framework for Blockchain-Enabled International Payment Networks.
6. Ahmed, K. R., Semi, M. M. A., Akther, S., Rabbi, M. M. K., Raja, M. R., Chakraborty, U., & Rial, M. I. H. (2025, April). Blockchain-integrated malware detection systems: Enhancing accuracy and trust in cybersecurity. In 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0 (pp. 1-6). IEEE.
7. Chitraju, S. (2024). Blockchain-Based Data Integrity Mechanisms for Mitigating Ransomware Impact in Cloud Finance Systems. Available at SSRN 5385143.
8. Jabid, T., Rashid, M. R. A., Ferdaus, M. H., Ali, M. S., Islam, M. M., Hasan, M., ... & Islam, M. (2024). Ransomware prevention strategies: Building robust cyber defenses. In Ransomware Evolution (pp. 144-171). CRC Press.
9. Lawal, S. (2024). Zero-Trust Architecture for Preventing Ransomware Infiltration in Financial Cloud Environments. Available at SSRN 5384216.