OPEN ACCESS JOURNALS

Indiana Journal of Multidisciplinary Research
Abbreviated Tittle- Ind J Multi Res
ISSN *(Online)*- 2583-3820
Journal Homepage Link- https://indianapublications.com/Journals/IJMR
DOI: https://doi.org/10.5281/zenodo.21698385

INDIANA PUBLICATIONS
PRODUCTIVE AND QUALITY RESEARCH

Research Article

Volume-06|Issue-04|2026

Blockchain-Enabled Zero Trust Architecture for Securing Multi-Cloud Environments in Critical Infrastructure Systems

Ramanjinamma G[1], Deepika G[2], Sowmya H N[3], Pavithra B G[4]

[1,2.3.4]Department of Computer Science & Engineering, Sai Vidya Institute of Technology, Bengaluru, India

Article History
Received: 05.05.2026
Accepted: 22.06.2026
Published: 25.07.2026

Citation
Ramanjinamma, G., Deepika, G., Sowmya, H N., Pavithra, B. G. (2026) Blockchain-Enabled Zero Trust Architecture for Securing Multi-Cloud Environments in Critical Infrastructure Systems. *Indiana Journal of Multidisciplinary Research, 6*(4), 528-531.

Abstract: Critical infrastructure sectors such as healthcare, finance, transportation, and energy are rapidly adopting multi-cloud environments to improve scalability, flexibility, and operational efficiency. However, the increasing dependence on distributed cloud infrastructures has significantly expanded the cyber threat landscape. Traditional perimeter-based security mechanisms are inadequate against modern cyber threats such as insider attacks, privilege escalation, and lateral movement. Zero Trust Architecture (ZTA) has emerged as a promising cybersecurity framework that follows the principle of "never trust, always verify." Nevertheless, implementing Zero Trust across heterogeneous and distributed cloud environments remains a major challenge due to issues in identity verification, policy enforcement, and real-time auditability.

This paper proposes a Blockchain-Enabled Zero Trust Architecture for securing multi-cloud critical infrastructure systems. The proposed framework integrates blockchain technology with Zero Trust principles to provide decentralized identity management, immutable audit logging, and smart contract-based policy enforcement. Hyperledger Fabric is employed as the underlying permissioned blockchain platform to ensure secure, transparent, and tamper-proof access control across multiple cloud providers. The framework enables fine-grained, context-aware authorization while eliminating dependence on centralized trust authorities.

The proposed system is evaluated in a simulated multi-cloud environment using AWS and Azure services. Experimental analysis demonstrates improvements in audit integrity, threat detection, and resistance to insider attacks while maintaining acceptable latency overhead. Comparative analysis with traditional Identity and Access Management (IAM) systems and conventional Zero Trust frameworks validates the effectiveness of the proposed approach. The findings indicate that blockchain-enabled Zero Trust models provide scalable and secure solutions for protecting future cloud-native critical infrastructure systems.

Keywords: Blockchain, Zero Trust Architecture, Multi-Cloud Security, Hyperledger Fabric, Cybersecurity, Access Control, Critical Infrastructure.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (**CC BY-NC 4.0**).

INTRODUCTION

The rapid growth of cloud computing technologies has transformed the digital infrastructure of modern organizations. Critical sectors such as healthcare, transportation, banking, energy, and government services increasingly depend on cloud-based systems for scalability, flexibility, and cost efficiency. Multi-cloud environments, where organizations utilize services from multiple cloud providers such as AWS, Microsoft Azure, and Google Cloud Platform, have become popular due to their operational advantages and reduced vendor dependency.

Despite these advantages, multi-cloud environments introduce several security challenges. Traditional perimeter-based security mechanisms are ineffective against modern cyber threats because they assume that internal users and systems are trustworthy. Such assumptions enable insider attacks, unauthorized privilege escalation, and lateral movement within networks. These limitations have motivated the adoption of Zero Trust Architecture (ZTA), which follows the principle of continuous verification and least-privilege access.

Zero Trust Architecture ensures that every user, device, and application is continuously authenticated and authorized before access is granted. However, implementing Zero Trust in distributed and heterogeneous multi-cloud systems is difficult due to centralized identity management, policy inconsistency, and lack of transparent auditing.

Blockchain technology offers unique advantages for addressing these challenges. The decentralized and immutable nature of blockchain enables secure identity management, transparent policy enforcement, and tamper-proof audit logging. Smart contracts further automate access control decisions without relying on centralized authorities.

This paper proposes a Blockchain-Enabled Zero Trust Architecture using Hyperledger Fabric to provide secure and decentralized access management across multi-cloud infrastructures. The proposed framework integrates smart contracts, blockchain-based identity verification, and context-aware policy enforcement to enhance security, transparency, and accountability.

The remainder of the paper is organized as follows. Section II presents the literature review. Section III explains the proposed system architecture and workflow. Section IV discusses the experimental results and comparative analysis. Finally, Section V concludes the paper and highlights future directions.

LITERATURE REVIEW

Cloud security and Zero Trust Architecture have gained significant attention in recent years due to the rapid adoption of distributed cloud systems. Researchers and organizations have explored several approaches for improving identity management, access control, and cybersecurity in cloud environments.

Forrester Research first introduced the concept of Zero Trust, which was later standardized by the National Institute of Standards and Technology (NIST SP 800-207). Zero Trust eliminates implicit trust and enforces continuous verification of every user and device. Several studies proposed Zero Trust models for enterprise environments; however, many existing implementations still rely on centralized architectures that create single points of failure.

Blockchain technology has also emerged as an important solution for distributed security management. Dorri et al. demonstrated the application of blockchain in Internet of Things (IoT) security to provide decentralized trust and secure communication. Zyskind et al. proposed blockchain-based identity management frameworks to improve privacy and authentication.

Traditional identity and access management systems such as AWS IAM and Azure Active Directory provide centralized authentication and authorization mechanisms. Although these systems are effective in single-cloud environments, they face interoperability and trust management challenges in multi-cloud infrastructures.

Recent studies have attempted to combine blockchain and cloud security. Liu et al. proposed a blockchain-based federated access control framework for multi-cloud systems. Singh and Chatterjee implemented Ethereum-based smart contracts for cross-cloud access control. However, these approaches suffer from scalability issues, latency overhead, and limited real-time policy enforcement.

Permissioned blockchain platforms such as Hyperledger Fabric provide improved scalability, low-latency consensus mechanisms, and fine-grained access control suitable for enterprise-grade applications. However, the integration of blockchain with Zero Trust principles in multi-cloud critical infrastructure systems remains underexplored.

The literature review reveals that existing approaches lack a comprehensive decentralized framework capable of enforcing Zero Trust policies dynamically across distributed cloud environments. This research addresses these limitations by integrating blockchain-based identity management, smart contracts, immutable audit logging, and context-aware access control into a unified architecture.

PROPOSED SYSTEM

The proposed Blockchain-Enabled Zero Trust Architecture provides secure and decentralized access control for multi-cloud environments. The framework integrates Zero Trust principles with blockchain technology to ensure secure identity verification, dynamic policy enforcement, and immutable auditing.

System Architecture

The proposed system consists of the following major components:

User

Users may include administrators, employees, automated systems, or third-party entities requesting access to cloud resources.

Authentication and Authorization Module

This module validates user credentials using blockchain-based identity records. Cryptographic techniques such as digital signatures are used for secure authentication.

Policy Engine

The Policy Engine evaluates context-aware policies based on user role, device status, location, and trust score.

Policy Enforcement Point (PEP)

The PEP enforces access control decisions generated by the Policy Engine and communicates with the blockchain network.

Multi-Cloud Infrastructure

The framework supports cloud services such as AWS, Microsoft Azure, and Google Cloud Platform while maintaining consistent policy enforcement.

Blockchain Network

Hyperledger Fabric serves as the decentralized trust layer. The blockchain stores:

- User identity information
- Smart contract-based access policies
- Immutable audit logs
- Trust scores and security events

Formal Trust Model

The trust score of a user is calculated as:

$$T_n = \alpha B_n + \beta C_n + \gamma D_n - \delta R_n$$

***Corresponding Author:** Ramanjinamma G

Where:

- B_n = Behavioral compliance score
- C_n = Credential validity score
- D_n = Device posture score
- R_n = Recorded risk incidents
- $\alpha, \beta, \gamma, \delta$ are weighting parameters

Access is granted only when the trust score exceeds a predefined threshold and all policy conditions are satisfied.

Workflow Overview

1. The user submits an access request to the cloud provider.
2. The Authentication Module verifies user identity using blockchain-backed credentials.
3. The Policy Engine retrieves smart contract policies from the blockchain.
4. The Policy Enforcement Point evaluates context-aware access conditions.
5. Access is granted or denied based on policy evaluation.
6. All access events are permanently recorded on the blockchain.

Smart Contract State Transition Model

The system operates using the following states:
S = {Init, Authenticated, PolicyChecked, Granted, Denied, Logged}
Each transition is securely executed and recorded within Hyperledger Fabric.

RESULTS AND DISCUSSION

The proposed framework was implemented using Hyperledger Fabric and evaluated within a simulated multi-cloud environment consisting of AWS and Microsoft Azure services. The performance of the proposed model was compared with traditional IAM systems and conventional Zero Trust frameworks.

Policy Evaluation Time

The proposed framework recorded an average policy evaluation time of 80 ms. Although slightly higher than traditional IAM systems due to blockchain operations and smart contract execution, the performance remained suitable for real-time applications.

Access Latency

The average access latency of the proposed framework was 55 ms. The additional latency is primarily caused by blockchain-based verification processes. However, the use of Hyperledger Fabric optimized the consensus mechanism and reduced overhead.

Audit Integrity

The blockchain-enabled framework achieved an audit integrity score of 95/100 due to immutable and tamper-proof logging. Traditional IAM systems scored significantly lower because of mutable centralized logs.

Threat Detection Rate

The proposed system achieved a threat detection rate of 90% using context-aware verification and trust-score evaluation mechanisms. This significantly outperformed conventional IAM and non-blockchain Zero Trust systems.

Comparative Analysis

Metric	Traditional IAM	Zero Trust	Proposed Blockchain-Enabled ZTA
Policy Evaluation Time	45 ms	70 ms	80 ms
Access Latency	30 ms	50 ms	55 ms
Audit Integrity Score	60	75	95
Threat Detection Rate	40%	65%	90%
Scalability	Medium	High	High
Insider Threat Resistance	Low	Medium	High

The results demonstrate that the proposed framework significantly improves auditability, trust management, and threat detection while maintaining acceptable system performance.

Challenges And Future Directions

Although the proposed framework demonstrates improved security and auditability, several challenges remain.

- Blockchain operations may introduce latency overhead in large-scale environments.
- Managing trust scores dynamically requires continuous monitoring and optimization.
- Scalability must be improved to support millions of transactions in real-time critical systems.
- Privacy-preserving techniques are required to protect sensitive identity information.

Future research can focus on integrating artificial intelligence and machine learning algorithms for anomaly detection and adaptive policy generation. The incorporation of decentralized oracles and edge computing can further improve real-time security and scalability.

CONCLUSION

This paper presented a Blockchain-Enabled Zero Trust Architecture for securing multi-cloud critical infrastructure systems. The framework integrates blockchain technology with Zero Trust principles to provide decentralized identity management, immutable audit logging, and context-aware access control.

Hyperledger Fabric was used as the blockchain platform to ensure secure and transparent policy enforcement across distributed cloud environments. Experimental evaluation demonstrated improvements in audit integrity, threat detection, and resistance to insider attacks compared to traditional IAM systems and conventional Zero Trust models.

The proposed architecture provides a scalable and secure foundation for future cloud-native cybersecurity systems. The integration of blockchain and Zero Trust principles can significantly strengthen the security of modern multi-cloud infrastructures.

REFERENCES

1. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication No. 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
2. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops (SPW)* (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27
3. Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). Blockchain in Internet of Things: Challenges and solutions. In *Proceedings of the 2016 IEEE/ACM International Symposium on Edge Computing (SEC)* (pp. 1–2). IEEE. https://doi.org/10.1109/SEC.2016.17
4. Liu, Y., Huang, L., & Wu, J. (2022). A federated blockchain-based access control system in multi-cloud environments. *IEEE Access, 10*, 47851–47863.
5. Shin, D., Kim, S., & Lee, J. (2021). Dynamic zero trust model for cloud security. In *2021 IEEE International Conference on Big Data and Smart Computing (BigComp)*. IEEE.
6. Singh, M., & Chatterjee, K. (2021). Smart contract-based cross-cloud access control using Ethereum blockchain. *International Journal of Information Security and Privacy, 15*(3), 20–38.
7. Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In *2017 19th International Conference on Advanced Communication Technology (ICACT)* (pp. 464–467). IEEE. https://doi.org/10.23919/ICACT.2017.7890132
8. Hardjono, T., Smith, N., & Shrier, D. (2019). *Decentralized trusted identity as a service: Blockchain-based identity*. MIT Connection Science.
9. Hyperledger Foundation. (2023). *Hyperledger Fabric documentation* (Version 2.5). https://hyperledger-fabric.readthedocs.io/
10. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2019). Smart contract-based access control for the Internet of Things. *IEEE Internet of Things Journal, 6*(2), 1594–1605. https://doi.org/10.1109/JIOT.2018.2847705.

***Corresponding Author:** Ramanjinamma G