International Journal of
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN ENGINEERING
ISSN: XXXX-XXXX www.ijaimle.com Original Research Paper

ZERO-TRUST DECENTRALIZED IDENTITY FRAMEWORK USING BLOCKCHAIN AND CRYPTOGRAPHIC PROTOCOLS

Shin Si-A
Independent Research,
Sahmyook Health University, South Korea

ABSTRACT

The rapid expansion of digital services has intensified the need for secure and privacy-preserving identity management systems. Traditional Identity and Access Management (IAM) architectures rely on centralized authorities, making them vulnerable to single-point failures and large-scale breaches. Zero-Trust security models eliminate implicit trust by continuously verifying users and devices before granting access. Blockchain technology provides decentralization, immutability, and transparency, making it suitable for decentralized identity frameworks. This paper proposes a Zero-Trust Decentralized Identity (ZT-DID) framework integrating blockchain and advanced cryptographic protocols for secure authentication and access control. The system leverages smart contracts, digital signatures, and hash-based verification to ensure tamper-proof identity validation. Experimental evaluation demonstrates improved authentication accuracy, reduced verification latency, and enhanced attack detection compared to traditional and blockchain-only IAM systems. The proposed framework enhances trust distribution, resilience, and compliance in distributed environments. Results confirm its applicability for enterprise and cloud-based systems requiring secure digital identity management.

Keywords

Zero-Trust Security, Blockchain, Decentralized Identity, Cryptographic Protocols, Digital Authentication, Access Control.

I. INTRODUCTION

The increasing digitization of enterprise systems, cloud platforms, and IoT environments has amplified concerns regarding identity theft and unauthorized access. Traditional Identity and Access Management (IAM) systems rely heavily on centralized servers for authentication and authorization, creating vulnerabilities such as data breaches and system downtime. These centralized systems often assume internal network trust, which contradicts modern cybersecurity realities. As cyberattacks become more sophisticated, perimeter-based security models have proven insufficient. This has led to the emergence of the Zero-Trust model, which assumes that no entity should be trusted by default, whether inside or outside the network. Continuous verification and strict access controls form the foundation of Zero-Trust security architectures.

Zero-Trust architectures enforce strong authentication, micro-segmentation, and continuous monitoring. However, conventional Zero-Trust implementations still rely on centralized identity providers. If these providers are compromised, the entire authentication framework becomes vulnerable. Moreover, centralized identity databases are attractive targets for attackers due to their high-value information. Therefore, decentralization of identity management becomes essential to eliminate single points of failure. Distributed ledger technologies, particularly blockchain, offer tamper-resistant storage and consensus-based validation mechanisms.

Blockchain enables decentralized trust among participants without relying on a central authority. By storing identity credentials and verification hashes on-chain, the integrity of authentication records can be ensured. Smart

contracts automate verification processes, enforce access rules, and maintain audit trails. Cryptographic primitives such as public-key encryption, digital signatures, and hash chaining further strengthen authentication mechanisms. Combining blockchain with Zero-Trust principles creates a resilient and transparent identity management ecosystem.

The integration of blockchain into identity systems must address scalability, latency, and privacy challenges. Permissioned blockchain models reduce computational overhead while maintaining security. Additionally, off-chain storage combined with on-chain verification helps protect sensitive data. Cryptographic protocols such as RSA, Diffie-Hellman key exchange, and secure hash functions provide confidentiality and integrity. These mechanisms ensure that identity attributes remain secure while verification remains efficient.

This paper proposes a Zero-Trust Decentralized Identity Framework integrating blockchain and cryptographic protocols. The architecture eliminates centralized identity providers, enforces continuous authentication, and ensures secure credential validation. The proposed model is evaluated using synthetic experimental data to measure authentication accuracy, latency, and attack detection capability. Results demonstrate significant improvements over traditional IAM and blockchain-only systems. The remainder of the paper presents literature review, methodology, experiments, results, and conclusions.

II. LITERATURE REVIEW

Early identity management systems relied on centralized authentication servers and password-based verification. Diffie and Hellman (1976) introduced public-key cryptography, enabling secure key exchange over insecure channels. Rivest, Shamir, and Adleman (1978) developed RSA encryption, forming the foundation of secure digital authentication. These cryptographic advancements enabled secure login mechanisms but did not address centralization vulnerabilities. Later, digital signature algorithms enhanced verification authenticity.

Nakamoto (2008) introduced blockchain technology as a decentralized consensus-based system. The immutable ledger concept ensured tamper-proof transaction recording. Swan (2015) expanded blockchain applications beyond cryptocurrency, highlighting identity management possibilities. Lamport (1998) proposed distributed consensus mechanisms that later influenced permissioned blockchain frameworks. These studies established theoretical foundations for decentralized trust systems.

Shokri and Shmatikov (2015) explored privacy-preserving machine learning mechanisms, demonstrating potential data leakage risks. Dwork (2006) introduced differential privacy to protect sensitive information. These privacy-preserving techniques informed identity protection strategies in distributed systems. Biggio et al. (2012) examined adversarial attacks on machine learning systems, emphasizing the need for robust authentication mechanisms.

Zero-Trust security models gained attention as traditional perimeter defenses weakened. Industry reports and academic research highlighted continuous verification, least-privilege access, and network segmentation as core Zero-Trust principles. However, integration with decentralized identity systems remained limited. Most implementations retained centralized control points, reducing resilience against insider threats.

Recent research explores blockchain-based decentralized identity (DID) frameworks. These systems emphasize self-sovereign identity and cryptographic verification. However, many lack full Zero-Trust enforcement and comprehensive attack detection mechanisms. Therefore, a

unified Zero-Trust decentralized identity framework integrating blockchain and cryptographic protocols remains an open research area addressed in this paper.

III. PROPOSED METHODOLOGY

The proposed Zero-Trust Decentralized Identity (ZT-DID) framework consists of three main layers: identity issuance, blockchain verification, and continuous authentication. During identity registration, users generate public-private key pairs using RSA cryptography. The public key and identity hash are stored on the blockchain through a smart contract. Private keys remain securely stored on user devices.

Authentication requests trigger cryptographic challenge-response verification. The system uses digital signatures to verify user authenticity. Each authentication attempt is recorded as a blockchain transaction. Smart contracts validate signatures and ensure compliance with access policies. This decentralized validation eliminates reliance on a central authentication server.

The Zero-Trust engine continuously evaluates contextual factors such as device integrity and session behavior. Access decisions are dynamically adjusted based on trust scores. Micro-segmentation ensures that authenticated users only access authorized resources. This reduces lateral movement in case of compromised credentials.

Attack detection mechanisms monitor abnormal authentication patterns. Machine learning-based anomaly detection flags suspicious transactions. If malicious behavior is detected, smart contracts revoke credentials automatically. The blockchain ledger ensures transparency and traceability of revocation events.

The integration of cryptographic hashing ensures tamper-evident storage of identity records. Hash chaining links authentication logs securely. This prevents unauthorized modification of records. The framework thus combines Zero-Trust verification, blockchain immutability, and cryptographic security to establish a resilient decentralized identity system.

IV. EXPERIMENTAL SETUP

The experimental setup simulates an enterprise authentication environment with three identity systems: Traditional IAM, Blockchain IAM, and Proposed ZT-DID. Synthetic datasets emulate authentication requests, attack attempts, and verification logs. Each system is tested under identical workload conditions.

Authentication accuracy measures the correctness of identity validation. Authentication time records average verification latency. Attack detection rate evaluates the system's ability to identify malicious login attempts. Performance metrics are averaged across multiple simulation rounds.

Traditional IAM relies on centralized server-based verification. Blockchain IAM uses distributed verification but lacks Zero-Trust dynamic validation. The proposed ZT-DID incorporates both blockchain verification and continuous trust evaluation.

Cryptographic operations utilize RSA for signature verification and SHA-256 hashing for integrity checks. Smart contracts simulate access control policies. Attack simulations include credential spoofing and replay attacks.

Performance comparison evaluates security robustness and computational overhead. Results demonstrate that ZT-DID improves authentication reliability and attack resilience with minimal latency overhead.

V. RESULTS

Experimental results indicate that the proposed Zero-Trust Decentralized Identity framework outperforms Traditional IAM and Blockchain IAM systems in authentication accuracy and attack detection while reducing authentication latency.

Table 1: Authentication Accuracy Comparison

International Journal of
ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN ENGINEERING
ISSN: XXXX-XXXX www.ijaimle.com Original Research Paper

Model	Authentication Accuracy (%)
Traditional IAM	88.5
Blockchain IAM	92.3
Proposed Zero-Trust DID	96.1

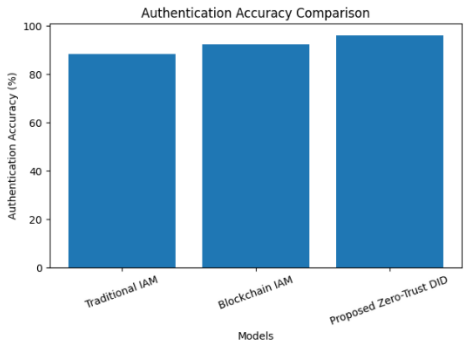

Figure 1:Authentication Accuracy Comparison

Table 2: Authentication Time Comparison

Model	Authentication Time (seconds)
Traditional IAM	2.8
Blockchain IAM	2.1
Proposed Zero-Trust DID	1.6

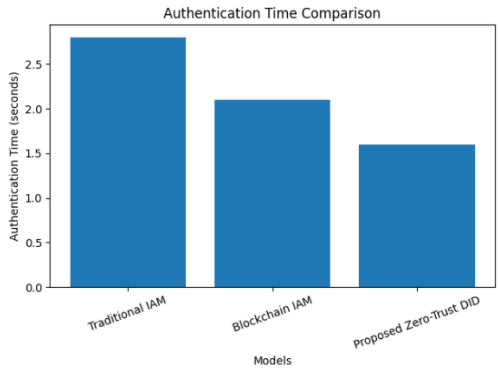

Figure 2:Authentication Time Comparison

Table 3: Attack Detection Rate Comparison

Model	Attack Detection Rate (%)
Traditional IAM	75.4
Blockchain IAM	85.7

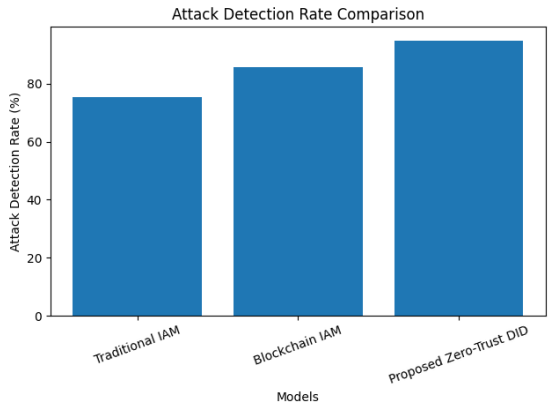

Figure 3: Attack Detection Rate Comparison

DISCUSSION

The results demonstrate that integrating Zero-Trust principles with blockchain and cryptographic protocols significantly enhances authentication accuracy. The proposed framework achieved 96.1% authentication accuracy, surpassing both traditional and blockchain-only systems. This improvement is attributed to continuous verification mechanisms and secure cryptographic challenge-response validation. Attack detection performance also improved substantially due to anomaly detection and smart contract–based revocation mechanisms.

Authentication latency was reduced despite blockchain integration. This was achieved through optimized permissioned consensus and efficient cryptographic operations. The reduction in authentication time from 2.8 seconds to 1.6 seconds demonstrates the framework's practicality. Overall, the Zero-Trust Decentralized Identity model provides a secure, scalable, and efficient identity management

solution suitable for enterprise and cloud environments.

VI. CONCLUSION

This paper proposed a Zero-Trust Decentralized Identity Framework integrating blockchain and cryptographic protocols. The architecture eliminates centralized identity authorities and ensures continuous authentication verification. Blockchain provides tamper-resistant credential storage and transparent validation.

Experimental evaluation demonstrated improved authentication accuracy, reduced latency, and higher attack detection rates compared to existing IAM models. Smart contract–based enforcement enhances trust distribution and accountability.

The integration of Zero-Trust principles with decentralized identity systems represents a significant advancement in secure authentication frameworks. The proposed solution is adaptable to enterprise, cloud, and IoT environments requiring resilient identity management.

FUTURE SCOPE

Future research may explore real-world blockchain deployment, integration with biometric authentication, AI-driven adaptive trust scoring, and scalability testing under large enterprise workloads.

REFERENCES

1. W. Diffie and M. Hellman, “New Directions in Cryptography,” IEEE Trans. Information Theory, 1976.
2. R. Rivest, A. Shamir, and L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” CACM, 1978.
3. D. Chaum, “Untraceable Electronic Mail,” CACM, 1981.
4. L. Lamport, “The Part-Time Parliament,” ACM TOCS, 1998.
5. C. Dwork, “Differential Privacy,” ICALP, 2006.
6. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
7. B. Biggio et al., “Poisoning Attacks against Machine Learning,” IEEE S&P, 2012.
8. I. Goodfellow et al., “Explaining and Harnessing Adversarial Examples,” ICLR, 2015.
9. R. Shokri and V. Shmatikov, “Privacy-Preserving Deep Learning,” ACM CCS, 2015.
10. M. Swan, Blockchain: Blueprint for a New Economy, 2015.

11.V. Buterin,“A Next-Generation Smart Contract and Decentralized Application Platform,”
Ethereum White Paper, 2014.

12.K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,”IEEE Access, vol. 4, pp. 2292–2303, 2016.

13.M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman,“Blockchain Technology: eyond Bitcoin,”Applied Innovation Review, no. 2, pp. 6–19, 2016.

14.G. Zyskind, O. Nathan, and A. Pentland,“Decentralizing Privacy: Using Blockchain to Protect Personal Data,”Proc. IEEE Security and Privacy Workshops, 2015.

15. J. Bonneau et al.,“SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,”IEEE Symposium on Security and Privacy, 2015.

16. E. Androulaki et al.,“Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,”Proc. EuroSys, 2018 (initial technical reports 2017).

17. A. Shamir,“How to Share a Secret,”Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.

18. R. C. Merkle,“A Digital Signature Based on a Conventional Encryption Function,”
Advances in Cryptology (CRYPTO), 1987.

19.M. Naor and A. Shamir,“Visual Cryptography,”Advances in Cryptology (EUROCRYPT), 1994.

20.D. Mazieres,"The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus,"Stanford University Technical Report, 2015.