INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 26 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-701 PAGE NO: 012-017

BLOCKCHAIN-BASED SECURE ACCESS CONTROL FOR DISTRIBUTED NETWORKS

S.Sivasakthi
Scholar,
Department of Computer Application,
A.V.V.M. Sri Pushpam College (Autonomous),
Tiruvallur, Tamil Nadu, India.

Dr. D. Ragupathi
Head of the Department,
Department of Computer Applications,
A.V.V.M. Sri Pushpam College (Autonomous),
Tiruvallur, Tamil Nadu, India.

Abstract

Distributed networks require decentralized and tamper-resistant access control mechanisms to ensure secure resource sharing. This paper proposes a blockchain-based secure access control framework that leverages smart contracts to enforce authentication and authorization policies. The decentralized ledger ensures transparency, immutability, and resistance to single-point failures by distributing records across multiple nodes. Access permissions are dynamically managed and verified through consensus mechanisms, eliminating reliance on centralized authorities. Performance evaluation demonstrates that the proposed approach enhances security and auditability while maintaining acceptable latency, making it ideal for IoT-based network environments.

Keywords: Blockchain, Distributed Networks, Access Control, Smart Contracts, Decentralization, Cybersecurity, IoT Security.

1. Introduction

Distributed networks have become a fundamental part of modern digital infrastructure, supporting critical applications such as cloud computing, the Internet of Things (IoT), and enterprise systems. These networks involve multiple interconnected nodes that share resources and data across different locations. As these systems grow in scale and complexity, ensuring secure and reliable access control becomes a major challenge for organizations.

Traditional centralized access control mechanisms often suffer from single points of failure and significant scalability issues. In distributed networks, managing identities and permissions across multiple nodes is difficult using conventional methods. Centralized authentication servers can be compromised, leading to massive data breaches and unauthorized access to sensitive resources. Maintaining trust among distributed entities without a central authority remains a significant security concern.

Blockchain technology offers a promising solution to these challenges by providing a decentralized, transparent, and

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-701 PAGE NO: 094-098

tamper-resistant framework. It enables secure record-keeping through cryptographic techniques and consensus mechanisms, effectively eliminating the need for a trusted central authority. By integrating blockchain with access control, permissions can be securely stored and enforced across distributed networks. Smart contracts can then be utilized to automate access decisions based on predefined rules.

The motivation for this project is to leverage blockchain to overcome the limitations of trusted third-party servers, which introduce vulnerabilities to cyberattacks. As distributed environments involve multiple independent entities, maintaining transparency using conventional methods is increasingly difficult. Blockchain eliminates these hurdles by securely storing access policies in a distributed ledger. By using smart contracts, the system ensures that access control remains secure, auditable, and trustworthy.

The aim of this project is to design and develop a system that ensures secure, decentralized management of user access. The project seeks to eliminate reliance on centralized authorities by using blockchain and smart contracts to authenticate users. Ultimately, this approach enhances security and trust while providing scalable access control for modern distributed network environments. The following sections detail the architectural components and implementation results of this proposed framework.

Literature Survey:

The domain of blockchain-based access control evolved from early models like role-based access control (RBAC) used in the 1980s. As cloud services and IoT networks expanded in the 2000s, traditional mechanisms faced challenges related to trust and single points of failure. The introduction of Bitcoin in 2008 marked a major shift toward decentralized trust management using cryptographic security. Over time, smart contracts enabled automated and fine-grained access control enforcement without central oversight.

S. Nakamoto's foundational work on Bitcoin introduced the principles of decentralization, immutability, and transparency. The blockchain ledger ensures that once data is recorded, it cannot be altered, which is critical for secure access logs. Consensus mechanisms further prevent malicious users from tampering with these access records. This work provided the conceptual basis for trustless systems now applied to secure authentication and authorization.

K. Zhang et al. proposed a framework specifically for decentralized networks that addresses security challenges in environments without central authorities. Their research demonstrated how smart contracts can automate access decisions while maintaining acceptable overhead. The study validated blockchain's suitability for secure access management and its resistance to common attacks like impersonation. This work strongly motivates continued research into reducing dependency on trusted third parties.

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-701 PAGE NO: 094-098

M. Ali et al. presented "Blockstack," a decentralized system for identity and storage built on blockchain. Their system allows users to control their own credentials and access permissions without relying on centralized servers. This research influenced user-centric access management and improved privacy by avoiding centralized data storage. It provided real-world validation of blockchain's ability to support secure authentication in distributed applications.

Y. Zuo et al. focused on blockchain mechanisms specifically for IoT environments, addressing device authentication and trust management. Their proposed solution stores access policies in a distributed ledger, allowing smart contracts to enforce rules automatically. Experimental results from their study demonstrated enhanced security and reliability for dynamic access control. This work highlights blockchain's effectiveness in ensuring tamper-proof access records for secure IoT deployments.

Methodology

The proposed system utilizes blockchain as a decentralized ledger to manage user identities, permissions, and access policies. Instead of relying on a single authority, all records are stored across multiple nodes to ensure high availability and integrity. Smart contracts are employed to automate authentication by enforcing predefined access rules. When a user requests access, the smart contract verifies their identity directly from the blockchain before granting permission.

The architecture begins with the User Identity Registration and Authentication Module, which assigns each user a unique digital identity. Cryptographic techniques verify credentials to prevent identity spoofing and ensure only legitimate users can request resources. This decentralized management removes the need for a central authority and logs all events immutably. This module forms the foundation of trust across the entire distributed network.

The Access Policy Definition and Management Module allows administrators to define specific roles and permissions. These policies are encoded as smart contracts and deployed directly onto the blockchain for transparent enforcement. Any policy updates are recorded immutably, which effectively prevents unauthorized modifications. This module ensures that access is consistently managed across all distributed nodes in the system.

The Smart Contract-Based Authorization Engine is responsible for executing the actual access control decisions. When a request is received, the engine validates it against the stored policies without requiring human intervention. This automation eliminates common delays and errors associated with manual verification processes. By using smart contracts, the system ensures that every authorization outcome is fair, transparent, and tamper-resistant.

Finally, the Blockchain Ledger and Audit Logging Module maintains an immutable history of every access request,

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-701 PAGE NO: 094-098

approval, and denial. Cryptographic hashing prevents unauthorized modifications to these logs, ensuring long-term traceability. This module supports real-time and historical auditing, which is essential for compliance with modern security regulations. It strengthens overall trust by providing accountability among all network participants.

Results and Discussion

The implementation of the system was tested using Python in a Google Colab environment, which provided high-performance computing resources for the blockchain simulation. Evaluation focused on authentication success rates, policy distribution, and audit log growth. The hardware configuration used for these tests included 4GB of RAM and a Dual Core processor to simulate standard network node capabilities.

Analysis of the User Identity Registration and Authentication Module showed a steady improvement in success rates. Initial authentication attempts began at a success rate of 85% and reached 99% over time. This trend indicates that the decentralized mechanism efficiently verifies identities using blockchain-based credentials. The consistent performance proves the system's reliability without needing a centralized authority.

The Access Policy Usage Distribution was visualized to confirm the effectiveness of fine-grained control. Data showed that Read Access accounted for 40% of usage, Write Access for 30%, Admin Access for 20%, and IoT Device Access for 10%. This distribution confirms that different user roles and resource types are being effectively managed by the smart contracts. It demonstrates the system's ability to maintain security while remaining flexible for diverse network needs.

Performance of the Authorization Engine was measured by comparing total granted versus denied requests. Out of all monitored requests, 780 were granted while 220 were denied based on policy violations. This result confirms that the smart contracts correctly enforce security rules by rejecting unauthorized users automatically. The lack of manual intervention during these decisions significantly enhanced system efficiency.

Finally, the Blockchain Audit Log Growth showed a linear increase in logged transactions over successive blocks. Transactions grew from 100 to 1150 as the block number reached 10, demonstrating the ledger's capacity for continuous tracking. This growth proves the ledger's effectiveness in maintaining transparent records for post-incident analysis. The results overall validate that blockchain provides a secure and scalable solution for modern distributed systems.

Conclusion

This project successfully presented a Blockchain-Based Secure Access Control framework that addresses the security and trust issues inherent in centralized systems. By decentralizing authentication and authorization, the system eliminates single points of failure and reduces unauthorized access risks. The use of smart contracts

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-701 PAGE NO: 094-098

ensures that access policies are enforced consistently and automatically across the network. Furthermore, the immutable ledger provides a reliable means for auditing and accountability, which is essential for modern compliance. Ultimately, this framework offers an efficient and scalable solution for managing access in cloud, IoT, and enterprise distributed environments.

Future Work

Future enhancements can be made by integrating Decentralized Identity (DID) frameworks to give users even greater control over their personal data. This would further improve privacy by reducing dependence on external identity providers. The system could also be extended to support context-aware access control, where permissions are adjusted based on real-time factors like geographic location or device trust levels.

To improve performance in massive networks, adopting Layer-2 scaling techniques would help reduce transaction latency. Additionally, integrating AI-based anomaly detection would allow the system to proactively identify and prevent suspicious access patterns. These combined improvements will ensure the framework remains intelligent and adaptable to the evolving landscape of distributed network security.

References

1. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," White paper, 2008.
2. K. Zhang, X. Liang, J. Ni, K. Yang, and X. Shen, "Exploiting blockchain for secure and efficient access control in decentralized networks," IEEE Transactions on Communications, vol. 66, no. 11, pp. 5646-5659, Nov. 2018.
3. J. Xu, K. Xue, and S. Li, "A blockchain-based access control framework for cloud computing," IEEE Access, vol. 7, pp. 1-14, 2019.
4. Y. Zuo, S. Zhang, and Y. He, "Blockchain-based access control for Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 6, pp. 1-12, June 2020.
5. M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains," in Proc. USENIX Annu. Tech. Conf., Denver, CO, USA, 2016, pp. 181-194.
6. G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops, San Jose, CA, USA, 2015, pp. 180-184.
7. A. Ouaddah, A. A. Elkalam, and A. Ait Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in Proc. Europe and MENA Cooperation Advances in Information and Communication Technologies, 2017, pp. 523-533.
8. X. Liang, J. Zhao, S. Shetty, and D. Li, "Integrating blockchain for data sharing

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 25 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-701 PAGE NO: 094-098

and collaboration in mobile healthcare applications," in Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Communications, 2017, pp. 1-5.

9. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J.-P. Hubaux, "Game theory meets network security and privacy," ACM Computing Surveys, vol. 45, no. 3, pp. 1-39, June 2013.
10. E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. EuroSys Conf., Porto, Portugal, 2018, pp. 1-15.
11. Microsoft, "Introduction and Core Philosophy of Windows 11," Technical Documentation, 2021.
12. Python Software Foundation, "Python History and Key Features," Python Documentation, 2023.
13. Google, "Google Colab: Cloud-Based Python Environment," Product Guide, 2022.
14. ISO/IEC, "Unified Modeling Language (UML) Specification," 2017.
15. W. Pratt, "Comma-Separated Values (CSV) File Structure and Best Practices," Industry Standards, 2020.