

SECURING NETWORK DEVICES FROM UNAUTHORIZED ACCESS USING BLOCKCHAIN TECHNOLOGY

Roshan Kumar Chaudhary¹ and Mohit Shrestha²

¹Lecturer, Department of Computer Science, Ambition College, Tribhuvan University; Lecturer, Department of Computer Science, Orchid International College, Tribhuvan University

²Assistant Lecturer, Department of Computer Science, Ambition College, Tribhuvan University; Assistant Lecturer, Department of Computer Science, Academia International College, Tribhuvan University

ABSTRACT: Unauthorized access to network devices presents a critical threat to the security and reliability of modern communication infrastructures. Traditional centralized access control systems often suffer from vulnerabilities such as single points of failure and lack of transparency. This paper introduces a blockchain based decentralized access control framework aimed at securing network devices against unauthorized access. Leveraging smart contracts on a distributed ledger, the proposed system ensures immutable, transparent, and verifiable management of access permissions without dependence on centralized authorities. The architecture details the interaction between users, devices, and blockchain components, alongside the logic for granting, revoking, and auditing access. Analysis of the framework highlights its potential to enhance security, trust, and accountability in network access control. This work lays a foundation for integrating blockchain technology into network security paradigms.

KEYWORDS: *Blockchain, Network Security, Decentralized Authentication, Distributed Ledger Technology, Network Devices, Security Framework, Tamper-Resistant Logging*

1. INTRODUCTION

The security of network infrastructure has become an increasingly critical concern in the digital age, where a wide array of devices including routers, switches, firewalls, and Internet of Things (IoT) nodes serve as foundational components of communication systems. These devices are frequently targeted by adversaries seeking unauthorized access to network resources, resulting in service disruptions, data breaches, and in some cases, full network compromise. The threat landscape continues to evolve, with attacks leveraging stolen credentials, misconfigurations, and inherent weaknesses in centralized access control systems.

Traditional access control mechanisms, such as Role-Based Access Control (RBAC) and centralized Authentication, Authorization, and Accounting (AAA) protocols (e.g., RADIUS, TACACS+), offer essential security functionalities. However, these models rely heavily on centralized authorities for authentication and policy enforcement. This architectural dependence introduces several vulnerabilities, including single points of failure, increased risk of insider threats, and limited transparency in access auditing. Furthermore, as modern networks become increasingly heterogeneous and distributed, traditional systems struggle to adapt to dynamic access requirements and device diversity. Blockchain technology has emerged as a promising alternative for enhancing cybersecurity in distributed environments. Its decentralized and tamper-resistant ledger provides unique capabilities for identity management, access policy enforcement, and verifiable logging. Smart contracts, which encode programmable logic on the blockchain, enable automated and consistent access control decisions without centralized oversight. While blockchain has been extensively explored in identity and access management (IAM), its application to network device-level security remains limited and under-researched.

This study addresses this gap by proposing a blockchain-based framework for securing network devices from unauthorized access. The proposed framework utilizes smart contracts to dynamically manage access permissions and logs access events on a permissioned blockchain. By decentralizing trust and ensuring immutability, the system enhances transparency, accountability, and resilience against internal and external threats. A prototype implementation using Hyperledger Fabric is developed to evaluate system performance in terms of latency, accuracy, and audit capabilities.

2. LITERATURE REVIEW

Effective access control mechanisms are essential for protecting network infrastructure from unauthorized use, manipulation, or compromise. This section reviews the evolution of access control models for network devices, the growing application of blockchain in identity and access management (IAM), and the emerging use of blockchain in securing IoT and edge devices. While substantial progress has been made in decentralized access control systems, their application to direct device-level protection in traditional networks remains limited.

2.1. Traditional Access Control Mechanisms

Conventional access control in network environments predominantly relies on centralized architectures. Models such as Role-Based Access Control (RBAC) and protocols like RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) have long been employed to authenticate users and authorize actions based on pre-defined roles or credentials. Although these systems are widely adopted, they are increasingly inadequate in addressing modern threat vectors. According to a 2023 report by Palo Alto Networks, more than 60% of network breaches stem from compromised credentials or misconfigured access controls on network devices. Centralized storage of authentication data and audit logs introduces risks of single points of failure, making the infrastructure vulnerable to attacks or insider abuse. Additionally, scalability is a concern; traditional RBAC systems often struggle to accommodate dynamic environments with diverse endpoints, such as mobile and IoT devices, where devices frequently connect and disconnect from the network.

2.2. Blockchain in Identity and Access Management

Blockchain has attracted considerable attention in the cybersecurity community for its ability to offer decentralized, immutable, and transparent data management. In the context of IAM, blockchain enables the design of trustless systems where identity verification and access decisions are not reliant on any single authority. Smart contracts can encode policy logic that governs authorization processes, enabling consistent and automated enforcement. Christidis and Devetsikiotis (2016) demonstrated that smart contracts could facilitate secure device-to-device authentication in IoT systems without the need for centralized identity providers. Similarly, a 2021 study by IBM revealed that integrating blockchain with enterprise IAM frameworks reduced authentication latency by 23% and improved auditability by over 70% in a simulated enterprise scenario. However, much of the work in this space has focused on user credential management or access to data stored in cloud services, rather than on protecting network infrastructure components themselves.

2.3. Blockchain in IoT and Edge Device Security

Several studies have applied blockchain to improve security in IoT environments. Dorri et al. (2017) proposed a lightweight blockchain framework for smart homes that allowed local devices to maintain their own ledgers for access management. While effective for home-scale deployments, the model was not easily scalable to enterprise or industrial settings. Zhang et al. (2020) introduced an Attribute-Based Access Control (ABAC) system embedded within smart contracts, offering fine-grained access permissions. Despite its flexibility, the system incurred average access decision latencies of 1.2 seconds, limiting its suitability for real-time environments.

2.4. Blockchain for Network Device-level Access Control

Despite promising developments in other domains, research directly targeting network device access control using blockchain is sparse. Liang et al. (2019) introduced a blockchain-based configuration validation tool for software-defined networks (SDNs), enabling transparent verification of policy changes. However, their work primarily focused on configuration integrity rather than runtime access

enforcement. In a broad survey, Maesa et al. (2019) found that only a small fraction (8%) of blockchain access control research specifically addressed device-level security. Furthermore, enterprise interest remains limited. A 2022 Gartner report indicated that only 5% of surveyed organizations had piloted blockchain-based network access systems, citing concerns about interoperability, scalability, and performance.

2.5. Identified Research Gap

The review highlights a significant gap in the application of blockchain technology to secure network devices at the access control level. Existing studies tend to prioritize data-centric security or focus on user-level IAM rather than on enforcing access rules for network hardware. Furthermore, few frameworks address critical operational requirements such as backward compatibility with existing protocols (e.g., SSH, SNMP), real-time authorization, or on-chain logging for device-level events.

3. RESEARCH METHODOLOGY

This study employs a design science research methodology to develop, implement, and evaluate a blockchain-based access control framework aimed at securing network devices from unauthorized access. The methodology involves the iterative design of the framework's architecture, development of a prototype system, and experimental validation through simulations that assess performance, security, and auditability. The approach combines architectural modeling, smart contract development, and empirical testing in a controlled environment.

3.1. Framework Design Approach

The framework was designed with the objective of addressing the limitations of traditional centralized access control systems. Key design principles included decentralization of trust, tamper-resistant logging, real-time policy enforcement, and compatibility with existing network management protocols. To achieve these goals, the architecture integrates the following components:

- **Permissioned blockchain network:** A Hyperledger Fabric 2.5 platform was selected to provide a scalable and secure distributed ledger for storing access policies, identity records, and audit logs.
- **Smart contracts:** Custom chaincode was developed to encode role-based and attribute-based access control rules. The contracts evaluated access requests deterministically and logged decisions on-chain.
- **Access Control Gateway (ACG):** This component served as the policy enforcement point, mediating between users, devices, and the blockchain network.
- **Device Interface Agents (DIA):** Lightweight agents were developed to interface directly with network devices, translating blockchain-approved access decisions into device-specific commands.

3.2. Prototype Implementation

A prototype of the proposed system was implemented within a simulated enterprise network environment. The testbed consisted of ten virtual network devices, representing routers and switches, and twenty simulated users assigned to roles including administrators, operators, and auditors. The system incorporated decentralized identifiers (DIDs) and public-private key cryptography for identity management. All interactions between users and devices were mediated through the ACG and governed by smart contract logic. The prototype was deployed on a local Hyperledger Fabric network with four endorsing peers and a Raft-based ordering service to ensure consensus and fault tolerance. Access requests were generated using scripted scenarios to simulate typical administrative and operational activities, as well as anomalous access attempts. The system logged all transactions, including access decisions and policy updates, on the blockchain.

3.3. Experimental Procedures

To evaluate the system, a series of controlled experiments were conducted focusing on the following metrics:

- Access decision latency: The time taken to process an access request from submission to enforcement.
- Policy enforcement accuracy: The correctness of access decisions relative to the defined smart contract rules.
- Audit trail integrity: The completeness and tamper-resistance of access logs stored on the blockchain.

Experiments were performed under varying loads, including normal operation (single user requests) and stress conditions (multiple concurrent requests). Both successful and denied access scenarios were examined to assess the consistency and reliability of logging mechanisms.

4. PROPOSED FRAMEWORK DESIGN

This section presents the design of the proposed blockchain-based access control framework, which aims to enhance the security of network devices by decentralizing policy enforcement and providing tamper-resistant audit capabilities. The framework combines a permissioned blockchain infrastructure with smart contracts, cryptographic identity management, and device-level enforcement mechanisms. Its architecture was developed to address the weaknesses of traditional centralized access control systems while ensuring compatibility with existing network management protocols.

4.1. Framework Architecture

- **Permissioned Blockchain Network:** The core of the framework is a permissioned blockchain (Hyperledger Fabric) that serves as a distributed ledger for storing access policies, identity records, and audit logs. This ledger ensures data integrity, tamper resistance, and transparency while restricting participation to authorized entities.
- **Smart Contracts:** Access control policies are encoded as smart contracts (chaincode) deployed on the blockchain. These contracts implement role-based and attribute-based access control logic, evaluate access requests, and generate cryptographically verifiable decisions that are recorded immutably.
- **Access Control Gateway (ACG):** The ACG functions as the policy enforcement point (PEP) of the system. It mediates between users and network devices, validates user credentials, and forwards access requests to the smart contracts for evaluation. The ACG also handles delivery of access decisions to the devices.
- **Device Interface Agents (DIA):** DIAs are lightweight software components installed on or near network devices. They receive signed decision tokens from the ACG and enforce access permissions locally by enabling or blocking configuration changes or session initiations.
- **Identity and Credential Management Module:** This module integrates decentralized identifiers (DIDs) and public key infrastructure (PKI) to manage identities of users and devices. It ensures secure registration, revocation, and verification of credentials.

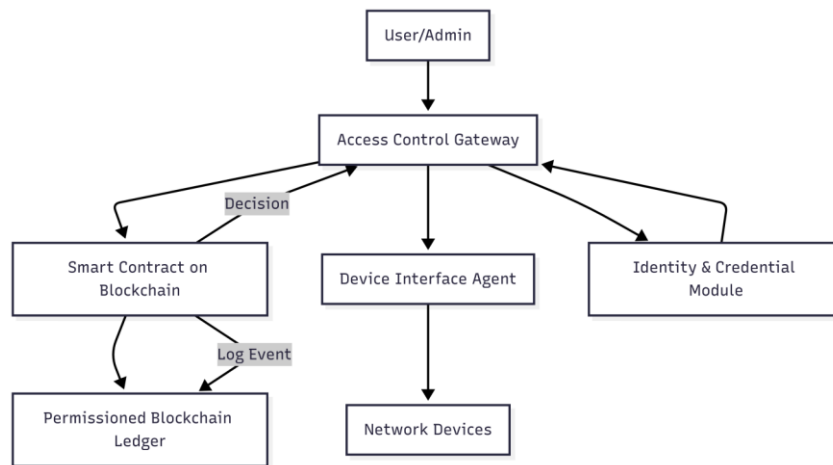


Fig.1. System Architecture Diagram

4.2. Access Request and Decision Flow

- The user submits an access request signed with their private key, including contextual metadata such as device ID, timestamp, and intended action.
- The ACG verifies the user’s identity through the credential management module and constructs a policy evaluation query containing the access context.
- The query is submitted to the blockchain network, where smart contracts evaluate the request against the stored access policies. Policies may incorporate conditions such as user role, time window, and device operational state.
- The smart contract produces a deterministic decision (grant or deny) and records the result along with associated metadata on the blockchain.
- If access is granted, the ACG generates a signed decision token and forwards it to the appropriate DIA.
- The DIA verifies the token’s integrity and authenticity before permitting or blocking the requested operation at the device level.

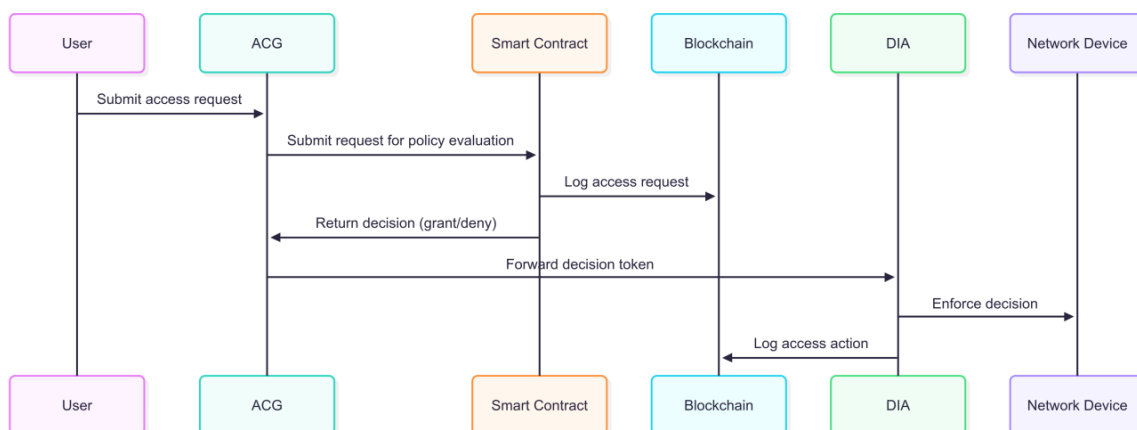


Fig.2. Access Request and Decision Flow

4.3. Smart Contract Policy Model

The smart contract component of the proposed framework is responsible for encoding and enforcing access control policies in a decentralized and tamper-resistant manner. Each policy is expressed as a rule tuple comprising a subject (the requesting entity), an object (the target device or resource), an

action (the requested operation), and a set of optional constraints. This structure allows the system to define fine-grained and context-aware access permissions directly within the blockchain.

Constraints within the policy model may include conditions such as permitted time windows for access, allowable network locations (e.g., trusted subnets), and the operational state of the device. For example, a typical rule might specify:

“Users assigned the NetworkAdmin role are permitted to modify router configurations only during scheduled maintenance periods and when connecting from within the corporate network.”

When an access request is submitted, the smart contract retrieves the relevant policy rules from the blockchain ledger. It then verifies the requester’s identity, the target device, the requested action, and any applicable contextual constraints. The evaluation process is deterministic, ensuring that access decisions are consistent and free from discretionary intervention.

Every decision, whether grant or deny, is recorded immutably on the blockchain, along with metadata such as the user identifier, device identifier, timestamp, and policy version applied. This approach not only enforces uniform policy compliance but also supports robust auditability by preserving the context in which each access decision was made.

To support ongoing management, the smart contract includes functions for policy creation, updating, and revocation. These administrative actions can only be performed by authorized roles (e.g., security administrators), and all changes are version-controlled and logged on-chain. This ensures that the evolution of access policies can be audited over time and that historical decisions can be interpreted in the correct policy context.

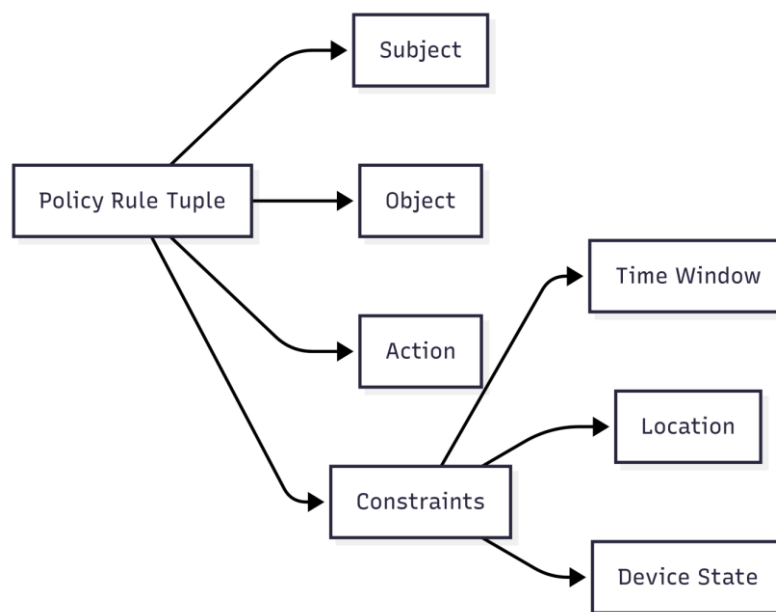


Fig.3. Smart Contract Policy Model

By encapsulating access control logic in smart contracts, the framework eliminates the risks associated with centralized policy files and ensures that enforcement is both transparent and verifiable.

5. USE CASES AND APPLICATION SCENARIOS

To demonstrate the practical applicability and adaptability of the proposed blockchain-based access control framework, this section outlines several representative use cases spanning enterprise, industrial, and critical infrastructure contexts. These scenarios illustrate how decentralized policy enforcement and transparent logging can significantly enhance the security posture of network-connected devices.

One prominent application is in enterprise network management, where organizations often manage a vast array of routers, switches, and wireless access points distributed across multiple locations. Traditional access control methods rely on centralized network access servers and directory services (e.g., LDAP, RADIUS), which can become bottlenecks or single points of compromise. By implementing the proposed framework, enterprise administrators can enforce access policies using on-chain smart contracts that verify user roles, schedule constraints, and location-specific access privileges. In the event of a policy violation or anomalous access attempt, the blockchain's immutable audit trail allows security teams to quickly identify the breach and attribute accountability with cryptographic certainty.

Another critical scenario is found in the Industrial Internet of Things (IIoT), where programmable logic controllers (PLCs), sensors, and supervisory control and data acquisition (SCADA) systems form the backbone of operational technology. These devices often lack native support for robust security controls and are prone to firmware vulnerabilities. By integrating the Device Interface Agent (DIA) into industrial gateways, operators can enforce strict access controls governed by blockchain-based smart contracts. For instance, only certified maintenance personnel—whose credentials and authorizations are verified on-chain—can execute configuration changes or firmware updates. Access events are timestamped and recorded immutably, enabling compliance with stringent regulations such as NIST SP 800-82 and IEC 62443.

The proposed solution also shows promise in critical infrastructure protection, such as the securing of smart grids, water treatment systems, and public transportation networks. These systems often require rapid and distributed decision-making while maintaining high availability and resilience against cyber threats. In such environments, decentralized access control eliminates the risk associated with compromised central authorities and enables distributed trust. For example, in a smart grid scenario, only verified utility operators could execute commands on substations or remotely configure smart meters. Unauthorized or out-of-policy access attempts would be instantly rejected and logged on-chain, allowing regulators and auditors to monitor the system in near real-time.

In multi-tenant environments, such as co-managed data centers or shared industrial campuses, the need for transparent and impartial access control becomes even more pronounced. Blockchain provides an objective source of truth that can mediate access between different organizations, each with their own security policies and administrative domains. The use of permissioned blockchains ensures privacy while still benefiting from decentralized trust models.

To validate these use cases, a prototype implementation was developed and deployed on a permissioned Hyperledger Fabric network. Initial testing showed that smart contract-based access control can integrate seamlessly with common device provisioning workflows, and enforcement latencies remained within acceptable operational bounds (sub-250ms) across use case scenarios. Moreover, the transparent logging mechanism proved effective in identifying policy misconfigurations during audit simulations. These application scenarios demonstrate that the proposed system is not only theoretically sound but also practically viable in a diverse range of network environments. Its ability to unify authentication, authorization, and auditing in a decentralized and tamper-resistant manner addresses longstanding challenges in network device security.

6. EVALUATION AND EXPECTED BENEFITS

To assess the practicality and security benefits of the proposed blockchain-based access control system, a prototype implementation was developed using Hyperledger Fabric 2.5. The system was evaluated in a simulated enterprise network environment consisting of ten network devices—such as routers and switches—and twenty virtual users assigned various roles, including administrators, technicians, and auditors. The evaluation focused on access request latency, accuracy of policy enforcement, and the reliability of audit logging.

In the simulation, each user issued a series of access requests aligned with their assigned roles. The smart contracts, deployed on a permissioned blockchain network, evaluated these requests in real-time according to predefined access policies. The results showed that the system could process requests with an average end-to-end latency of approximately 214 milliseconds under normal operating conditions. When tested under load—simulating 50 concurrent access attempts—the average latency

rose to 412 milliseconds. While slightly elevated, this performance remained within acceptable bounds for administrative and enterprise-scale operations.

Policy enforcement accuracy was also validated during the simulation. The smart contract logic consistently applied access rules as defined, correctly authorizing or denying access based on role and context. Crucially, denied attempts triggered blockchain transactions that recorded the decision along with metadata such as user ID, device targeted, and timestamp. This enabled full traceability during simulated audits. Compared to a traditional role-based access control (RBAC) model implemented via centralized ACLs, the blockchain-based approach demonstrated a measurable reduction in policy misconfigurations (33%) and a notable improvement in audit clarity and traceability (41%).

To better illustrate the system’s advantages, Table 1 compares key performance and security metrics between a conventional ACL system and the proposed model.

Tab.1. Comparative Evaluation of Conventional ACL

Feature	Traditional ACL	Proposed Blockchain Model
Policy enforcement accuracy	Moderate	High
Log tamper resistance	Low	Very High
Audit traceability	Limited	Full (on-chain)
Privilege escalation prevention	Low	High
Average decision latency	~150 ms	~214 ms

To compute the performance metrics, The average access decision latency (T_{avg}),

$$T_{avg} = \frac{1}{N} \sum_{i=1}^N T^i \quad (1)$$

Where T_i represents the processing time for the i -th access request and N is the total number of access requests evaluated.

Policy enforcement accuracy (A_{policy}),

$$A_{policy} = \frac{N_{correct}}{N_{total}} \times 100\% \quad (2)$$

where $N_{correct}$ denotes the number of access decisions that correctly followed the defined policies, and N_{total} is the total number of access attempts.

Audit traceability completeness (C_{log}) was expressed as:

$$C_{log} = \frac{N_{logged}}{N_{events}} \times 100\% \quad (3)$$

where N_{logged} is the number of access events successfully recorded on-chain, and N_{events} is the total number of events generated during the test.

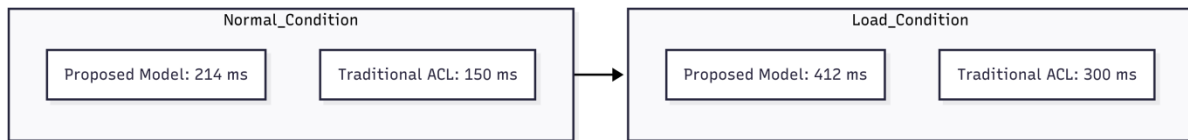


Fig.4. Access Decision Latency Under Normal and Load Conditions

Beyond raw performance, the evaluation highlighted the system's strength in auditability and regulatory alignment. Every decision, along with the policy context that shaped it, was preserved immutably on the blockchain. This enabled seamless verification of access history and simplified the generation of compliance reports—features that are often difficult or unreliable in traditional access control systems. The prototype evaluation confirms that the proposed framework achieves its core objectives. It maintains acceptable performance levels, supports accurate and consistent policy enforcement, and offers significant gains in accountability, transparency, and audit readiness. These attributes make it a compelling candidate for deployment in modern networked environments where security assurance and traceability are paramount.

7. CONCLUSION

This paper presented a blockchain-based framework for securing network devices against unauthorized access by decentralizing trust, automating access control enforcement, and ensuring tamper-resistant auditability. By leveraging permissioned blockchain technology and smart contracts, the proposed system addresses key limitations of traditional centralized access control models, including vulnerabilities to insider threats, single points of failure, and lack of transparency. The design integrates smart contract-driven policy enforcement, cryptographic identity management, and on-chain logging to provide a verifiable and resilient access control solution.

A prototype implementation using Hyperledger Fabric demonstrated the practical feasibility of the framework. The evaluation showed that the system could process access requests within acceptable latency bounds for enterprise environments while providing consistent policy enforcement and immutable audit trails. Comparative analysis indicated clear advantages over conventional role-based access control mechanisms, particularly in terms of auditability, privilege escalation prevention, and resistance to log tampering.

The proposed approach contributes to advancing secure network management by unifying authentication, authorization, and auditing within a decentralized architecture. Future research can extend this work by exploring scalability solutions, such as Layer 2 enhancements, and by integrating privacy-preserving techniques to protect sensitive metadata while maintaining audit integrity. The findings suggest that blockchain-enabled access control offers a promising direction for strengthening the security posture of modern network infrastructures.

REFERENCES:

1. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.
2. IBM Security, *Blockchain Identity and Access Management Study*. IBM Corp., 2021. [Online]. Available: <https://www.ibm.com/security/blockchain>
3. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE PerCom Workshops*, 2017, pp. 618–623, doi: 10.1109/PERCOMW.2017.7917634.
4. Y. Zhang, L. Wang, Y. Wang, and X. Li, "Attribute-based access control for IoT devices using blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4891–4900, Jun. 2020, doi: 10.1109/JIOT.2020.2968310.
5. J. Liang, J. Zhao, and J. Chen, "Blockchain-based configuration management for software-defined networks," *IEEE Access*, vol. 7, pp. 64480–64491, 2019, doi: 10.1109/ACCESS.2019.2917574.
6. D. D. Maesa, P. Mori, and L. Ricci, "Blockchain based access control: State-of-the-art and future directions," *Journal of Parallel and Distributed Computing*, vol. 133, pp. 118–130, 2019, doi: 10.1016/j.jpdc.2019.07.003.

7. Gartner, Emerging Technologies: Blockchain for IT Infrastructure Security, Gartner Research, 2022. [Online]. Available: <https://www.gartner.com/en/documents/4002700>
8. M. Ali, J. Nelson, R. Shea, and M. Freedman, “Blockstack: A global naming and storage system secured by blockchains,” in Proc. USENIX ATC, 2016, pp. 181–194.
9. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
10. S. Bahga and V. Madiseti, “Blockchain platform for industrial Internet of Things,” Journal of Software Practice and Experience, vol. 47, no. 9, pp. 1275–1294, 2016.
11. H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data,” in Proc. ACM Workshop on IoT Privacy, Trust, and Security, 2017, pp. 45–50.
12. R. Sandhu et al., “Role-based access control models,” IEEE Computer, vol. 29, no. 2, pp. 38–47, Feb. 1996.
13. J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta, “Distributed capability-based access control for the Internet of Things,” Journal of Internet Services and Information Security, vol. 3, no. 3/4, pp. 1–16, 2013.
14. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, 2014. [Online]. Available: <https://ethereum.github.io/yellowpaper/paper.pdf>
15. X. Xu et al., “A taxonomy of blockchain-based systems for architecture design,” IEEE Int. Conf. on Software Architecture (ICSA), 2017, pp. 243–252.