Bulletin of Business and Economics, 13(2), 1090-1095
https://bbejournal.com
https://doi.org/10.61506/01.00434

Revolutionizing Access Control in IoT Systems through Blockchain Technology

Muhammad Awais[1], Dr. Muhammad Waseem Iqbal[2], Prof. Saleem Zubair Ahmad[3], Sabah Arif[4]

Abstract
The widespread adoption of the Internet of Things (IoT) has raised significant concerns regarding security and privacy. Among these concerns, access control stands out as a matter of paramount importance, generating substantial interest and discourse. Centralized systems, due to their reliance on external sources, often face challenges related to scalability and availability, which can lead to performance issues. This paper introduces an efficient, decentralized, and innovative approach to implementing secure access control systems within IoT frameworks. The proposed solution leverages a multi-agent system integrated with blockchain technology. The central focus of this methodology revolves around the deployment of Blockchain Managers to ensure the security of IoT access control and facilitate secure communication between neighboring IoT devices. An added advantage of this system lies in its establishment of a secure linkage among fog nodes, cloud servers, and IoT devices.
Keywords: security, privacy, access control, blockchain managers, multi-agent system

1. Introduction

The term "Internet of Things" (IoT) refers to a network of interconnected electronic devices that enable seamless communication and data exchange among them. This interconnectedness empowers collaboration and enables businesses to develop robust strategies. While IoT holds the potential to transform our daily lives, it also presents significant challenges, particularly in the domains of security, privacy, data management, and infrastructure development (Alkhateeb et al., 2022). Ensuring security and privacy within the IoT landscape is a complex endeavor, primarily due to the proliferation of diverse connected devices. Robust authentication and authorization systems are crucial, especially for resource-constrained IoT devices. This study introduces an innovative architectural framework built around a multi-agent system integrated with a distributed private blockchain (Krichen et al., 2022). The overarching goal is to provide secure, efficient, and decentralized access control for IoT devices, thus ensuring comprehensive security for the entire IoT infrastructure, including cloud computing, fog nodes, and IoT device connectivity.
The contributions of our research are as follows:

- Development of a pioneering architectural design rooted in blockchain technology, featuring a multi-agent system and a decentralized access control mechanism.
- Implementation of mobile agent software to optimize traffic management, enhance mobility, and boost intelligence.
- Creation of a versatile and adaptable system capable of effectively managing a wide array of IoT applications.

What sets our approach apart is the utilization of a private hierarchical blockchain system, which not only addresses the aforementioned challenges but also alleviates network congestion through a lightweight consensus mechanism tailored to the unique requirements of IoT and mobile agent software (Liang and Ji, 2022). Furthermore, the integration of Mandatory Access Control further strengthens security measures.
In the realm of security, the authentication of individuals before granting access to confidential information and systems is of paramount importance (Tanwar et al., 2022). Access control (AC) principles and mechanisms play a pivotal role in governing authorization and resource access. Authentication and authorization, particularly within the context of IoT, have been extensively discussed, especially concerning scalability and efficiency (Abdelmaboud et al., 2022). While common authorization methods include Access Control Lists (ACLs), Role-Based Access Controls (RBACs), and Attribute-Based Access Controls (ABACs), they may not always align seamlessly with the intricacies of IoT requirements.

- ACLs, owing to their centralized nature, often suffer from limited granularity and scalability (Pal et al., 2022).
- RBAC and ABAC, while conceptually straightforward, may not always facilitate direct device-to-device communication effectively (Pennino et al., 2022).
- Capability-Based Access Control (CapAC) emerges as a more tailored approach for IoT, thanks to its reduced vulnerability to inherent complexities (Rahman et al., 2022).
- The ABAC paradigm, though comprehensive, introduces management complexities as IoT device numbers grow.

Our proposed solution harnesses a private blockchain to address these multifaceted challenges, providing a decentralized, robust, and efficient approach to secure IoT access control.
The rest of this article is structured as follows: Section 2 discusses the literature review. Section 3 explains the proposed architecture in depth. Section 4 includes the results and discussion session. Finally, Section 5 concludes the paper and discusses future work.

2. Literature Review

This paper explores data access management in IoT devices, focusing on their user-like behavior and persistent settings. It introduces conditional data access control within the IoT context, offering a detailed implementation process and a real-world case study. The system relies on a confidential key for broadcast encryption. Conditional data access keys are encrypted before storage on the blockchain, while data is encrypted and stored in a non-blockchain streaming source. Empirical findings indicate that key management's performance impact is minor compared to decoding keys. The study's approach is practical and evaluated using Ethereum blockchain technology (Mihaljević et al., 2023).
In the IoT ecosystem, securing access to devices and data is crucial due to the decentralized, energy-efficient, and diverse nature of IoT networks. This study explores a novel approach to access control, combining Software-Defined Networking (SDN) and blockchain technology. The integration enhances security, leveraging smart contracts for verifiable, immutable access policies. These policies are designed to be stringent, adaptable, and self-executing. A proof of concept demonstrates the system's potential

[1] Department of Computer Science & Information Technology, Superior University, Lahore-54000, Pakistan, ibneajmal77@gmail.com
[2] PhD. Associate Professor, Department of Computer Science & Information Technology, Superior University, Lahore-54000, Pakistan, waseem.iqbal@superior.edu.pk
[3] Department of Computer Science & Information Technology, Superior University, Lahore-54000, Pakistan, saleem.zubair@superior.edu.pk
[4] Department of Computer Science & Information Technology, Superior University, Lahore-54000, Pakistan, sabah.arif@superior.edu.pk

applicability on a broader scale. Evaluation metrics include throughput and resource access latency. Interestingly, as the number of IoT nodes and access requests increase, no linear or exponential relationship between throughput and response time is observed. The proposed approach exhibits consistent performance even with growing node and query volumes (Khalid et al., 2023).

The widespread adoption of IoT devices has heightened the importance of data security and privacy. This study introduces the CcBAC model, a blockchain-based cryptographic access control system, to address IoT security concerns. The model aims to provide precise access control and comprehensive auditing. The paper outlines the model's concepts, features, and current research status. It also details the model's structure and its compatibility with various access control systems. Theoretical and experimental assessments reveal that the approach enhances resource management, enforces strict access restrictions, and can be successfully validated (Jiang et al., 2023).

The Internet of Things (IoT) comprises interconnected electronic devices that observe and control their surroundings, collecting data sent to a centralized database for processing. To ensure secure and uninterrupted operations, advanced security technologies are essential. One solution is ZAIB (Zero-Trust and ABAC for IoT using Blockchain), which dynamically regulates access control based on device behavior. ZAIB employs attribute-based access control (ABAC) and blockchain for transaction recording and user/device registration. The InterPlanetary File System (IPFS) safeguards IoT device attributes and data. Rigorous assessments confirm ZAIB's effectiveness in safeguarding smart grid networks, ensuring robust end-to-end security for users, data, and services (Awan et al., 2023).

IoT device nodes' dynamic, massive, and lightweight nature presents security challenges. Traditional access control falls short, and attribute encryption, while offering finer access granularity, can compromise user anonymity. This study introduces a blockchain-based access management system for IoT, offering robust internal security. It employs blockchain technology for decentralized access control. The system records encrypted text hash values on the blockchain, ensuring tamper-proof protection and third-party storage reliability. Smart contracts are used to monitor and regulate access control for IoT data, mitigating unauthorized access. Inner product encryption on attribute vector representations grants precise access control for small IoT devices while safeguarding user information. Experimental results affirm the system's effectiveness in addressing IoT access control needs securely and efficiently (Han et al., 2023).

Most decentralized IoT research has been limited in scope, offering few solutions to address privacy and trust concerns. Implementing blockchain technology is crucial for enhancing IoT network security. A blockchain-based authentication system can serve as device ID verification and decentralized storage, enabling secure communication without relying on trust. However, current IoT systems face challenges due to high data storage costs. To tackle these issues, we developed a novel approach based on permissioned blockchain architecture. This approach enhances user identity verification and data storage capabilities while addressing scalability concerns. Homomorphic encryption protects IoT data before transmission to the cloud. Simulation data undergoes thorough evaluation and comparison to demonstrate the approach's effectiveness. This research introduces an innovative methodology to enhance IoT security, emphasizing trust-awareness for improved network security and IoT service provision (Al Hwaitat et al., 2023).

Table 1: Comparative Analysis

Ref	Security Mechanisms	Scalability	Efficiency	Interoperability	Privacy Preservation
Mihaljević et al. (2023)	Key management, encryption, blockchain storage	No	medium	No	Emphasizes encryption
Khalid et al. (2023)	Smart contracts, blockchain, immutability	No	medium	No	Focuses on security
Jiang et al. (2023)	Blockchain-based cryptographic access control	No	Medium	No	Comprehensive auditing
Awan et al. (2023)	ABAC, blockchain for transaction recording	No	medium	No	Safeguarding IoT device attributes and data
Han et al. (2023)	Blockchain-based decentralized access control	No	Low	No	Emphasizes decentralized access control
Al Hwaitat et al. (2023)	Blockchain for network security	Yes	High	No	Utilizes homomorphic encryption

3. Proposed Solution

The proposed approach leverages a private blockchain within a multi-agent infrastructure for enhanced security. In this IoT system, we implement a lightweight and autonomous access control mechanism. Figure 1 depicts the structural arrangement of the system under consideration. The architecture features a multi-tier blockchain setup, consisting of three primary components:

- Fog Blockchain Manager (FBCM): Comprising fog/edge nodes.
- Core Fog Blockchain Manager (CFBCM): Comprising core fog nodes.
- Local Blockchain Manager (LBCM): Comprising IoT devices.

Additionally, a Cloud Blockchain Manager (CBCM) is responsible for overseeing and managing any blockchain systems hosted in a cloud environment. The Blockchain Configuration Manager (BCM) encompasses three essential elements: block headers, MAC policy headers, and a set of transactions. Our solution adheres to the stringent criteria set forth by the Central Intelligence Agency (CIA), ensuring confidentiality, integrity, and availability. This feasibility is made possible by its adaptable nature, decentralized structure, and minimal device dependency. Moreover, our architecture addresses potential security concerns, such as the vulnerability associated with a single point of failure. It also caters to the requirements of Internet of Things (IoT) applications. Consequently, our architectural framework can be seamlessly customized to integrate with a wide range of IoT software applications.

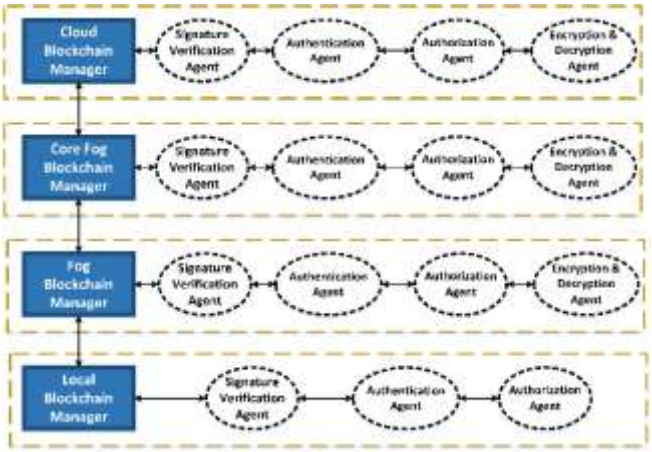

Figure 1: Blockchain-Based Framework For Access Control

The incorporation of blockchain technology in Internet of Things (IoT) systems presents various challenges. These stem from the constrained resources of IoT devices and the computational complexities related to addressing cryptographic issues, such as Proof of Stake (PoS). Our proposed approach involves integrating a miner into the Blockchain Manager (BCM), a pivotal component within the system. This miner assumes the crucial role of overseeing all communication activities among different BCMs. Additionally, the responsibility for monitoring any changes or additions to IoT devices falls under the purview of the Business Continuity Manager (BCM). The BCM also possesses the capability to efficiently supervise and regulate communications among multiple BCMs through the implementation of a media access control (MAC) policy.

Handling identity, authorization, encryption, and decryption functions of each Blockchain Manager (BCM) is delegated to mobile agents. Despite the growing complexity of encryption and decryption algorithms, IoT devices continue to grapple with processing limitations. The absence of an encryption/decryption function in the Local Blockchain Manager (LBCM) is attributed to this limitation. Devices connected to the IoT typically have limited computational capabilities. The suitability of Proof of Work (PoW) and other public blockchain consensus methods for IoT networks is questioned for several reasons. Public blockchains expose the consensus process and all transactions to every network participant. This aspect poses a challenge in implementing commercial blockchain solutions, as it heightens the risk of exposing critical information. A potential outcome of a 51% attack on publicly distributed ledgers could have significant and far-reaching consequences. To address these IoT challenges, lightweight consensus mechanisms and the adoption of private or permissioned blockchains have emerged as viable solutions. Permissioned blockchains restrict mining activities to verified enterprises. In the following sections, we will delve into the key components of our proposed framework.

3.1. Transaction

A transaction in the context of the Internet of Things (IoT) refers to the exchange of data or information among various entities. These entities encompass IoT devices, a central fog node, and a cloud computing system. Transactions can take various forms, including access, update, addition, monitoring, and removal. Within a Business Continuity Management (BCM) framework, the observation of data triggers the creation of an access transaction. This activity is closely intertwined with the implementation of access control. Update transactions, on the other hand, come into play when devices or nodes need to modify previously stored information. This process requires proper authorization for both reading and writing. Business process management systems (BPMs) offer a wide range of functionalities, including data reading and writing, event generation, deletion, and monitoring. The introduction of a new IoT device or node can lead to the generation of fresh transactions while removing an operation results in its deletion. Transaction monitoring becomes a crucial aspect when examining and analyzing data sourced from IoT devices and nodes.

3.2. Mandatory Access Control Policy

Access to this platform will be exclusively granted to individuals authorized as Blockchain Content Managers (BCMs). This strict authorization process significantly reduces the likelihood of security errors. Our Mandatory Access Control (MAC) system operates based on a security classification for subjects (secret, top secret, or confidential) and resource classification for objects (secret, top secret, or confidential). Security stickers contain information regarding clearance and classification, which in turn determine access permissions for authorized individuals. The Bell-LaPadula model is a widely recognized framework for constructing access control systems that adhere to various security principles. The primary role of this entity is to ensure compliance with MAC regulations by comparing the clearance level of the subject with that of the object they are trying to access (Satheesh & Sree, 2022). As depicted in Figure 2, this system effectively prevents individuals from accessing confidential information beyond their authorized security level.

3.3. Blockchain Managers

Multiple entities, including the Local Blockchain Manager (LBCM), Fog Blockchain Manager (FBCM), Core Fog Blockchain Manager (CFBCM), and Cloud Blockchain Manager (CBCM), play crucial roles in managing interactions. Business Continuity Managers (BCMs) are tasked with developing and enforcing access privilege policies across all organizational levels. The blockchain consists of blocks, each containing two headers: a block header and a policy header. Within the foundational block structure, every transaction in the blockchain system adheres to the Mandatory Access Control (MAC) rule. Each activity is accompanied by a policy header, aiding BCMs in identifying authorized individuals for specific resources. The initiation of each blockchain block is marked by a policy header. BCMs continually rely on the latest policy, typically located at the top of the block header, for policy authentication and updates. In our proposed system, the miner associated with each node assumes the role of the Blockchain Central Miner (BCM). This BCM is responsible for essential tasks such as transaction validation, township inspection, and user authentication. Furthermore, the policy stated in the previous section extends into the subsequent

section, establishing a connection between the two sections. Consequently, the blockchain expands by incorporating an additional block, facilitated by the utilization of Blockchain Consensus Mechanisms (BCMs).

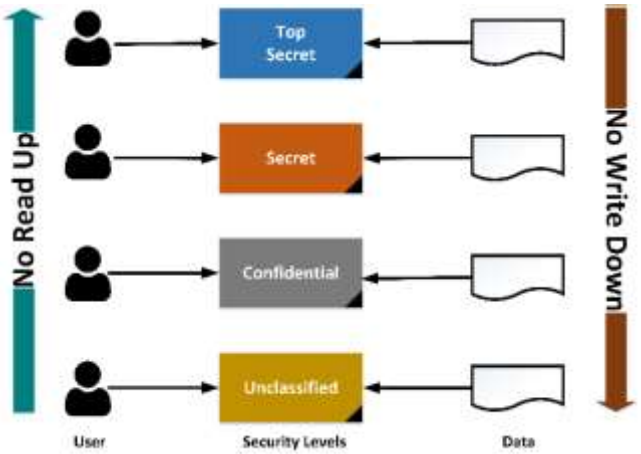

Figure 2: Bell-LaPadula Model

3.4. Software Agent

The architecture presented here features a highly capable software agent with autonomous initiation and termination capabilities, complemented by mobility, adaptability, transparency, and robustness. Furthermore, Internet of Things (IoT) devices, which often have limited resources, can potentially enhance their resource allocation and cost-efficiency by utilizing software bots. To achieve this objective, these devices possess the capability to collaborate with other units, thereby optimizing the utilization of available resources. In the following sections, we will provide a detailed overview of each software agent that constitutes our proposed architecture.

3.5. Signature Verification Agent

The mobile agent is integrated within the border control modules (BCMs). Instead of relying on encryption techniques, the agent's primary function is to authenticate the sender's identity and ensure the integrity of the transmitted message. The Limited Connectivity Base Model (LBCM) is primarily designed to mitigate the risk of unauthorized data manipulation. This is achieved through the use of symmetric key techniques and shared secret keys. These procedures aim to establish a level of trustworthiness in IoT products.

To assist low-powered Internet of Things (IoT) devices, verification bots, and a lightweight hashing approach are employed. Each sender computes the hash value of the LBCM layer using the original message. Subsequently, the messages are encrypted with a mutually agreed-upon secret key. To authenticate data from the Layered Broadcast Cryptographic Module (LBCM), the encrypted message is decrypted using the shared secret key, and the generated hash value is compared to the original hash value for verification purposes. Both CFBCM and CBCM versions utilize digital signatures, as illustrated in Figure 3, to provide additional computational capacity. Creating a signature involves combining a hash of the transmitted message with the sender's private key. To establish the authenticity of the contents, the message must be decrypted using the sender's public key. The hash value obtained at the outset can then be compared to the received one. When these two values match, it confirms both the sender's identity and the message's integrity.

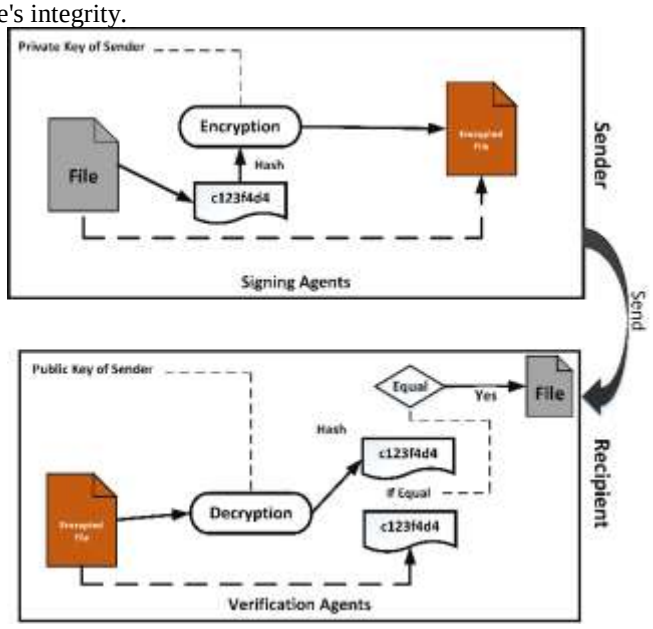

Figure 3: Signing & Verification Agents For Fog, Core Fog, & Cloud Blockchain Manager

3.5.1.1. Authentication Agent

The designated agent is responsible for verifying user identities and granting them appropriate access. To ensure secure communication within the network, it's essential for all devices and nodes to use a consistent secret key. Each BCM miner is

equipped with an authentication agent tasked with verifying user identities, and ensuring the authenticity of Internet of Things (IoT) devices and nodes. Within each tier, the BCM miner generates a confidential key used for communication by the respective agent. The Diffie-Hellman key exchange protocol facilitates the creation of a shared secret key between two entities without prior knowledge of each other. This ensures the privacy of individuals, even when they communicate over an insecure link.
Before initiating the convergence process, the agent verifies the presence of the correct shared key among IoT devices or nodes at the same organizational level. Public key cryptography is employed to enable communication between Base Communication Modules (BCMs) deployed across various tiers of an IoT system. If the agent has concerns about the individuals involved, the interaction is disregarded. Once both agents' identities are validated by the Authorization Agent, they can synchronize their operations. The Authorization Agent's role involves evaluating the MAC policy and determining appropriate access levels for the agents, considering the now accessible resources.

3.5.1.2. Authorization Agent

An "Authorization Agent" is an entity, whether a device or an individual, responsible for conveying positive affirmations or comments. The agent described above has the key role of enforcing permission restrictions and allocating privileges to requesters based on their digital identification and subsequent authentication. Using the Mandatory Access Control (MAC) policy, the BCM miner can accurately determine the operational characteristics of Internet of Things (IoT) devices and nodes. The authentication agent not only authorizes the contact but also verifies the identity of the requester. Subsequently, the user's security level and access privileges to resources are determined by referencing the MAC policy of the Boundary Control Mechanism (BCM). By examining the latest block header, the BCM miner can identify the active MAC policy file. This agent efficiently identifies the appropriate authorizations, particularly in terms of read or write permissions, by employing the MAC policy framework, which incorporates the security classification level. The Authentication Agent is responsible for assigning a confidence rating to each Internet of Things (IoT) device or node. This rating is determined by evaluating the activities performed by the device or node. The utilization of the Bell-LaPadula model played a critical role in formulating the user access policy for the system. This policy governs the allocation of user privileges for resource access.

3.5.1.3. Encryption and Decryption Agent

The implementation of this mobile agent effectively safeguards sensitive data from unauthorized access, and it operates within three distinct areas: FBCM, CFBCM, and CBCM. While ensuring privacy for IoT devices in the context of LBCM is not considered essential, maintaining confidentiality remains paramount in all business continuity management (BCM) practices. This agent can perform encryption and decryption operations on both information and ACL rules transferred between BCMs. In the realm of public cryptography, an asymmetric technique involves encrypting the agent's message using the intended recipient's public key. The encrypted message is then decrypted using the recipient's private key. The process diagram illustrates the interaction among the Authentication Agent, the Authorization Agent, the resource, and the BCM in response to a user's request to modify data within the resource, as depicted in Figure 4. This section showcases the user's ability to modify existing information within the specified framework. Verifying the identity of a user seeking to modify pre-existing data involves the Authentication Agent sending a formal request to the user's chosen authentication provider. Both parties share a common concealed key. The authentication agent performs identity verification by generating a secure identification (ID) using the designated key. Subsequently, the user submits a formal request to the Authorization Agent, who utilizes the provided ID to enable the use of MAC. This paper delves into the Mandatory Access Control (MAC) requirements that users and resources must adhere to. User access is granted based on their membership in the appropriate cohort and their proficiency in reading and writing within a specific range. To engage in MAC-permitted actions involving data alteration, users must formally request authorization from an authorized entity. When a modification is made to a resource, a new transaction is added to the blockchain, and a fresh hash value is submitted to the Ledger-Based Consensus Mechanism (LBCM). The Local Byzantine Consensus Mechanism (LBCM) then updates the blockchain's hash value to incorporate the newly acquired resource. Subsequently, it disseminates a new transaction to the Authorized Agents (AA).

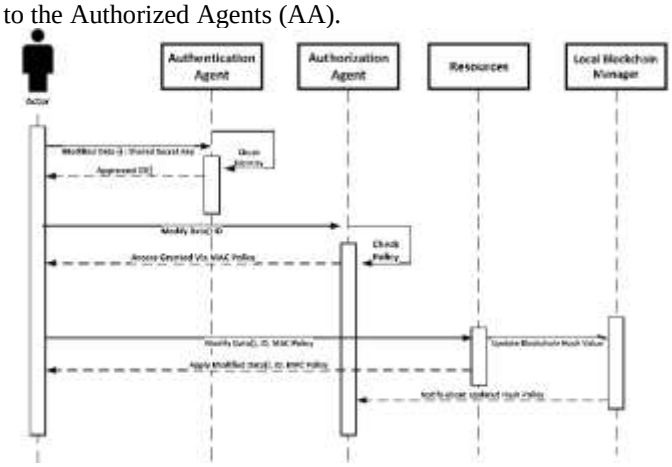

Figure 4: Event Diagram for Authorization and Authentication Agents

4. Result and Discussion

The inadequacy of current IoT security solutions is attributed to the fragmented structure of IoT networks and the limited capabilities of IoT devices. Traditional access control systems are costly due to their dependence on electricity and processing expenses. Public blockchains are incompatible with low-powered IoT devices that lack the necessary processing resources for mining. To address these issues, we propose an innovative IoT security solution based on a hierarchical blockchain structure and multi-agent systems. Our primary goal is to enhance operational efficiency and decentralized access control. The

architecture includes components like Cloud Blockchain Manager (CBCM), Core Fog Blockchain Manager (CFBCM), Local Blockchain Manager (LBCM), Fog Blockchain Manager (FBCM), and Fog/Edge Node Manager (FBCM).

We adhere to the "security trinity" of the Central Intelligence Agency (CIA), focusing on confidentiality, integrity, and availability. Our solution also offers scalability, decentralization, limited device interoperability, and resilience against single points of failure, making it suitable for IoT security needs. However, we acknowledge potential performance and usability issues that may arise during implementation and subsequent analysis. Smart homes face various security risks, including data breaches, privacy vulnerabilities, and complexity issues.

In October 2016, the Mirai botnet disrupted IoT systems, impacting the global DNS administration and rendering many devices and websites non-functional. To mitigate these risks, our hierarchical framework employs various levels of blockchain managers, including the Local Blockchain Manager (LBCM) to oversee smart home devices. The Local Broker Communication Mechanism (LBCM) facilitates device coordination, while the Fog Blockchain Manager (FBCM) can oversee multiple clusters of FBCMs for security and scalability. Cloud-based federated blockchain consensus mechanisms (CFBCMs) aid data storage and retrieval. Authentication and authorization are crucial. The Mandatory Access Control (MAC) policy enforces access restrictions and verifies security labels.

Signature verification ensures data integrity. We also address Distributed Denial of Service (DDoS) attacks, which pose a significant threat to the IoT ecosystem. Our hierarchical security paradigm, combined with device authentication, helps mitigate DDoS impacts. We employ a multi-layer security (MLS) strategy grounded in the Bell-LaPadula model to control access to IoT devices within a residential setting (Kumar & Tripathi, 2021). An Authorization Agent assigns security levels to devices, and trust values are maintained. Compromised devices may be banned if they engage in fraudulent activities. In summary, our proposed solution aims to address IoT security challenges, enhance smart home security, and protect against various threats, including DDoS attacks and unauthorized access.

5. Conclusion

In conclusion, the IoT's rapid expansion has heightened security and privacy concerns. This study presents an innovative approach to enhancing IoT access control security through a multi-agent system overseen by Blockchain Community Managers. It integrates various technologies, including cloud infrastructure, on-premises IoT devices, and fog nodes. While past research focused on specialized IoT applications, this study emphasizes the need for further research and development. The study's core objectives include data integrity, authentication, authorization, and privacy protection. Future work will involve refining the proposed architecture for IoT security and exploring case studies while deploying private blockchain platforms and Raspberry Pi-based IoT devices.

References

Abdelmaboud, A., Gherbi, A., Raggad, B., Yagoub, M., Yousfi, A., & Mezrag, A. (2022). Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges, and future research directions. *Electronics*, 11(4), 630.

Al Hwaitat, A. K., Alhwaitat, M. S. K., Aqel, M. J., & Ghrir, A. M. (2023). A new blockchain-based authentication framework for secure IoT networks. *Electronics*, 12(17), 3618.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors*, 22(4), 1304.

Awan, S. M., Azad, M. A., Arshad, J., Waheed, U., & Sharif, T. (2023). A blockchain-inspired attribute-based zero-trust access control model for IoT. *Information*, 14(2), 129.

Han, P., Zhang, Z., Ji, S., Wang, X., Liu, L., & Ren, Y. (2023). Access control mechanism for the Internet of Things based on blockchain and inner product encryption. *Journal of Information Security and Applications*, 74, 103446.

Jiang, W., Li, E., Zhou, W., Yang, Y., & Luo, T. (2023). IoT access control model based on blockchain and trusted execution environment. *Processes*, 11(3), 723.

Khalid, M., Hameed, S., Qadir, A., Shah, S. A., & Draheim, D. (2023). Towards SDN-based smart contract solution for IoT access control. *Computer Communications*, 198, 1–31.

Krichen, M., Ammi, M., Mihoub, A., & Almutiq, M. (2022). Blockchain for modern applications: A survey. *Sensors*, 22(14), 5274.

Kumar, R., & Tripathi, R. (2021). Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model. *Journal of Ambient Intelligence and Humanized Computing*, 12(2), 2321–2338.

Liang, W., & Ji, N. (2022). Privacy challenges of IoT-based blockchain: A systematic review. *Cluster Computing*, 25(3), 2203–2221.

Mihaljević, M. J., Knežević, M., Urošević, D., Wang, L., & Xu, S. (2023). An approach for blockchain and symmetric keys broadcast encryption-based access control in IoT. *Symmetry*, 15(2), 299.

Pal, S., Dorri, A., & Jurdak, R. (2022). Blockchain for IoT access control: Recent trends and future research directions. *Journal of Network and Computer Applications*, 203, 103371.

Pennino, D., Pizzonia, M., Vitaletti, A., & Zecchini, M. (2022). Blockchain as IoT economy enabler: A review of architectural aspects. *Journal of Sensor and Actuator Networks*, 11(2), 20.

Rahman, M. S., Islam, M. A., Uddin, M. A., & Stea, G. (2022). A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges. *Internet of Things*, 19, 100551.

Satheesh, K. K., & Sree, T. K. (2022). AB-DAM: Attribute-based data access model in blockchain for healthcare applications. *Multimedia Tools and Applications*, 81(17), 23567–23588.

Tanwar, S., Gupta, N., Iwendi, C., Kumar, K., & Alenezi, M. (2022). Next generation IoT and blockchain integration. *Journal of Sensors*, 2022.