International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1(s) (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A New Scalable and Secure Access Control Scheme Using Blockchain Technology for IoT

Pankaj Sathe
Sarola Baddi, Jamkhed Road, 1, MH MSH 2, Maharashtra 414201

Abstract— **The Internet of Things (IoT) involves many devices that share data, which creates chances but also problems with security and growth. Usual access control systems often don't work well as the network gets bigger because they can fail easily, have delays, and aren't clear.**

This paper suggests a blockchain access control system made for IoT. By using blockchain's decentralized and secure record, the system does not need a central authority and makes sure every access request is checked and noted safely. Smart contracts handle the authentication and authorization automatically, giving rule-based access management that is clear and dependable in real-time.

This method improves trust, growth, and data accuracy in IoT systems while cutting down on delays and unapproved access tries. Tests show faster access times and better energy use than older models. In general, this system gives a safe, expandable, and open way to handle IoT access, opening doors for connection with AI security and simple blockchain rules for IoT devices with limited resources.

Keywords: Internet of Things (IoT), Blockchain Technology, Smart Contracts, Access Control, Security, Scalability, Decentralization, Data Integrity, Authentication, Authorization

I. INTRODUCTION

The Internet of Things (IoT) has grown to be a very important technology. It links many devices that can sense things, talk to each other, and do things by themselves. IoT has changed how devices work together and share info in areas such as smart homes, healthcare, factories, and cities. As this network gets bigger, problems arise, mainly with security, privacy, and who gets to use the system.

Right now, many IoT systems use central access control, where one server checks and controls who gets access. This works okay for smaller networks, but it can become slow and unsafe as the system grows. If the main server fails, the whole network could shut down. It also gets hard to keep trust and openness across many devices. Central systems might not be the best choice for large IoT setups.

Blockchain tech gives another option to fix these problems. Blockchain is like a digital record book that is spread across many computers and can't be easily changed. It does not need a central controller. Its main traits, like being spread out, open, unchangeable, and reliable, make it good for keeping IoT communications safe. By using blockchain with IoT, devices can verify each other, get permission, and share data securely and clearly.

This paper looks at creating a system for controlling access to IoT setups safely and on a large scale using blockchain tech. The idea is to use smart contracts to automatically decide who gets access and keep a permanent record of everything in the blockchain. This method not only stops unwanted access but also makes sure that rules are applied quicker and the system can grow easier than with older methods.

In summary, this work aims to build an IoT system that uses blockchain to get rid of single points of failure, build trust between devices, and make access control work well in a decentralized way. The system is designed to be a base for future IoT networks, where security, openness, and the ability to grow go together.

II. RELATED WORK

Over the last several years, considerable work has aimed to improve security and access management in Internet of Things (IoT) settings. Initial systems often used centralized designs like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC). These methods worked acceptably for smaller setups but had problems with growing size, delays, and security issues when used for extensive IoT networks.

To address these problems, researchers started looking at blockchain tech as a way to spread control across many points. Blockchain's shared record-keeping and agreement methods are great for keeping data reliable and open without needing a central authority.

Nakamoto (2008) shared the basic plan for blockchain through Bitcoin, which showed how a spread-out network can keep trust between untrusted parts. Later, Christidis

and Devetsikiotis (2016) showed how smart agreements could make access choices automatic and cut down on needing to approve things by hand in IoT systems. In a related way, Ouaddah et al. (2016) suggested FairAccess, an early blockchain-based setup for IoT access control. Their plan used smart agreements to set and apply access rules openly, but it had limits when used for large networks because of size and speed.

Dorri et al. (2020) shared a simple blockchain plan made for IoT devices, aiming to lower communication needs and make answers quicker. Tian et al. (2020) put forward a way to control access using blockchain tokens, which made security and tracking better while staying adaptable. Kumar and Goyal (2020) gave a broad review of joining blockchain with IoT and noted that being able to grow and work with different systems are still the biggest problems to figure out.

Newer papers have also mixed attribute-based encryption and spread-out identity control with blockchain to make access control more detailed and safeguard privacy. For instance, Christidis et al. (2021) mixed blockchain and encryption to handle IoT access rules safely. Liang et al. (2018) suggested a spread-out identity plan that lets IoT devices manage their data and actions on their own.

Even though these studies give good signs, most current plans have either high calculation costs, delays, or trouble changing to fit real IoT situations. There is still a need for a system that is simple, can grow, and is safe, while giving clear and automatic access management.

The work in this writing builds on these ideas and shares a new access control setup using blockchain that can grow and is safe, focusing on making trust, spreading control, and applying rules right away better. It uses smart agreements to make choices automatically and makes sure all actions are noted in a way that cannot be changed, reaching both openness and dependability in big IoT areas..

III. BACKGROUND

The Internet of Things (IoT) has changed global communication. Many devices, such as sensors in homes and industrial machines, now form an interconnected network. This network gathers, processes, and shares info instantly, opening doors in health care, agriculture, delivery, smart cities, and home systems

As more devices join this network, security worries grow. IoT networks manage private info and vital tasks, but many depend on central systems for managing logins and data use. Since these setups keep user info and permissions on a main server, they can fail if that server is hacked or overloaded, putting the entire network at risk.

Typical access controls like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) can't handle the size and complicated nature of IoT. They might be okay for smaller systems but not for today's changing, spread out, and limited IoT networks. Delays, bottlenecks, unclear processes, and limited growth are typical issues that hurt how well these systems work.

Blockchain tech is a possible answer. Originally made for digital money, blockchain is good at building systems that are spread out, open, and safe from tampering. Instead of a main server, blockchain keeps data on many spots. This means nobody has total power. Data, once saved, can't be changed or removed. Its trust system builds trust among users.

Using blockchain with IoT can really help devices confirm identity, share info, and check access. Smart contracts can apply rules on their own, cutting out human mistakes. This mix allows for safe, expandable, and verifiable access control that fits the spread-out form of IoT.

This work hopes to close the space between IoT's need for safe, massive message sharing and blockchain's skill at offering trust and automation that is spread out. By putting these two things together, this project plans to create a system that makes sure it is reliable, safe, open, and able to grow – things that are key for the next IoT networks.

IV. CHALLENGES IN THE FOUNDER JOURNEY

Creating a tech company, particularly one that combines fields such as IoT, Blockchain, and Security, presents significant difficulties. The experience of a founder is often a mix of excitement and confusion as they try to solve problems. It involves more than just tech since they must also maintain their vision while adapting to unexpected events.Initially, founders must clarify their goals by determining exactly what to build and why. Founders are often overwhelmed with ideas, opinions, and suggestions, which distracts them. It takes work, validation, and focus to narrow the scope to a practical problem, such as using blockchain to secure IoT access, and to ignore distractions.The technical work is another source of trouble. Dealing with IoT devices and blockchain needs experience. The tech is still developing, the instructions are spread out, and combining them needs knowledge of hardware rules and decentralized design. Keeping performance, scalability, and cost in line with security standards needs constant learning.

Resource management is also difficult. Founders often start with little money, few people, and too many ideas. It can be hard to manage time spent on development, testing, paperwork, and presentations while teaching themselves new tools or systems. Making even a simple model takes more work than one might guess. The emotional aspects, like the worry to keep going when results are slow, are rarely mentioned. It is normal to feel unsure, face criticism, and have technical problems. When something

goes wrong, as it does, one has to find a solution without losing sight of the goal Finally, being a founder constantly checks one's power to adjust and guide. As a project grows, one learns that doing well involves more than just writing good code or making a smart model. It also means creating a way of thinking that can handle mess, learn quickly, and make wise choices with limited data. In conclusion, being a founder involves more than designing a product; it requires being able to recover from setbacks. Every problem, whether technical, mental, or strategic, drives one to improve to the point where they can not only construct systems but also lead in unsure situations. That is the real reward of any successful tech project.

V. FRAMEWORK AND DESIGN PRINCIPLES

The system, a scalable and secure access control scheme using blockchain for IoT, aims to create a security setup that is trustless, decentralized, and scalable. The main idea is to let IoT devices interact safely without needing a central authority. It brings together IoT architecture, blockchain, and smart contracts into a working model that handles access control in real time.

1. Overall Framework

The system is structured in three layers:

IoT Device Layer:

This layer has all the IoT devices, sensors, and gateways that gather data or take actions. Each device gets a unique digital identity on the blockchain when it is registered. Whenever a device wants to access a resource or another device, it signs the request digitally and sends it to the blockchain for checking.

Blockchain Layer:

This is the main part of the system. It works as a decentralized access control and verification system. Smart contracts are put on the blockchain to set and apply access control rules. These contracts manage authentication, authorization, and record-keeping. Every transaction that is either allowed or denied is kept forever on the blockchain, making sure things are clear and unchangeable.

Cloud/Storage Layer:

To make things more scalable and perform better, big or less critical data is kept off-chain using distributed storage options like IPFS or cloud servers. Only the key access logs and authentication proofs are stored on the blockchain. This mixed approach lowers load and response times while keeping trust and the ability to audit high.

2. Design Principles

The system is based on some key ideas that guide how it works:

Decentralization:

It does not rely on central servers or other authorities. Every node in the blockchain helps to check transactions, which gets rid of single points of failure.

Transparency and Auditability:

All access events and decisions are recorded permanently on the blockchain. This makes the system fully auditable, guaranteeing accountability and tracking for every action a device takes.

Scalability:

It is made to handle an increasing number of IoT devices without slowing down. The use of off-chain storage and simple agreement methods makes sure access verification is quick and efficient.

Security and Trust:

Each device and user has digital credentials for identification and authentication. Smart contracts make sure access rules are followed automatically and fairly.

Automation through Smart Contracts:

Smart contracts automatically manage access control decisions, like allowing, denying, or changing permissions. This cuts down on mistakes and administrative work.

Interoperability:

The system can work with different IoT platforms, blockchain systems (like Ethereum or Hyperledger), and outside systems through APIs.

Low Latency and Efficiency:

The system keeps communication overhead low by using blockchain verification with off-chain data handling. This provides quick response times that are good for real-world IoT uses.

3. Working Flow

Device registers with a unique blockchain identity.

Administrator sets access control rules using smart contracts.

Device asks for access → Smart contract checks identity and rules.

If valid, access is allowed, and the event is noted on the blockchain.

If invalid, access is denied, and an audit log is still recorded.

VI. REFERENCE SYSTEM ARCHITECTURE

The Reference System Architecture defines the overall structure and workflow of the proposed blockchain-based access control framework for IoT. It acts as a blueprint that connects all major system components — IoT devices, blockchain network, smart contracts, and cloud infrastructure — into a single, secure ecosystem. This architecture is designed to achieve the key goals of decentralization, transparency, scalability, and security. It ensures that every IoT device can authenticate and communicate safely without relying on a centralized authority.

1. Architectural Overview

The proposed architecture is structured into three main layers:

IoT Device Layer

This is the foundation of the system, containing all IoT nodes, sensors, actuators, and gateways.

Each device generates a unique cryptographic identity and registers itself on the blockchain.

When a device requests access to data or another device, the request is digitally signed and sent to the blockchain for validation.

Blockchain Layer

This layer serves as the trust backbone of the architecture.

It includes smart contracts that automate access control policies — verifying identities, validating permissions, and logging every transaction.

Once a transaction is confirmed, it is stored on the immutable distributed ledger, ensuring auditability and tamper resistance.

The consensus mechanism (e.g., Proof of Authority or Proof of Stake) ensures secure and efficient validation across nodes.

Cloud / Off-Chain Layer

Since IoT devices generate massive amounts of data, storing everything directly on the blockchain would be impractical.

To handle this, large or non-critical data is stored off-chain using cloud storage or distributed file systems like IPFS.

The blockchain only stores metadata and access proofs, linking them to the off-chain data through secure hash references.

This hybrid design keeps the system scalable while maintaining integrity and verifiability.

2. System Components

Device Registration Module: Handles identity generation and registration of IoT devices onto the blockchain.

Access Request Module: Allows devices or users to request access to resources through digitally signed messages.

Smart Contract Module: Contains access control logic that automatically approves, denies, or revokes access based on defined policies.

Blockchain Ledger: Stores all transactions, access decisions, and event logs in a tamper-proof manner.

Monitoring and Audit Module: Enables administrators to view, track, and analyze all access activities for security and compliance.

Off-Chain Storage: Manages scalable storage for IoT data while keeping blockchain usage optimized and lightweight.

3. Workflow of the Architecture

Device Registration:

Every IoT device is assigned a unique digital ID and public-private key pair. The registration details are stored on the blockchain.

Access Policy Definition:

The system administrator defines policies (who can access what, under which conditions) using smart contracts.

Access Request:

When a device requests access, it sends a signed transaction to the blockchain network.

Authentication & Authorization:

Smart contracts verify the request based on digital signatures and predefined policies.

Decision Logging:

The outcome — access granted or denied — is recorded immutably on the blockchain ledger.

Data Retrieval / Action Execution:

Once verified, the device can securely access the requested data or service from the IoT or cloud layer.

4. Advantages of the Reference Architecture

No Single Point of Failure: Decentralization ensures that no single server controls the system.

Enhanced Security: All communications and transactions are cryptographically protected.

Transparency: Every access decision is visible and traceable through blockchain records.

Scalability: Off-chain integration allows efficient handling of high data volume from IoT devices.

Automation: Smart contracts eliminate manual verification and reduce latency.

5. Summary

The reference system architecture provides a modular and distributed foundation for managing IoT access control using blockchain. Each layer has a specific role — IoT devices for data generation, blockchain for trust and policy

enforcement, and cloud for large-scale data storage. Together, they form a secure, transparent, and efficient ecosystem capable of supporting the next generation of IoT networks.Would you like me to create a diagram explanation for this section too (like a labeled figure "Proposed Blockchain-IoT Reference Architecture") with a short caption paragraph describing each component visually? It's standard for dissertation formatting and makes this section much stronger.

IX. REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1666–1689, 2016.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1654–1682, 2020.

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

[5] H. F. Atlam, A. Alenezi, and G. B. Wills, "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions," International Journal of Intelligent Systems and Applications, vol. 10, no. 6, pp. 40–48, 2018.

[6] X. Liang, S. Shetty, D. Bowden, J. Liu, and D. Li, "Towards Decentralized Accountability and Self-Sovereignty in IoT Systems," IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3016–3025, 2018.

[7] H. Tian, M. Dong, J. Wu, and J. Li, "Secure and Scalable IoT Data Access Control Using Blockchain-Based Capability Tokens," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8754–8767, 2020.

[8] R. Kumar and P. Goyal, "Blockchain-Based IoT Security: A Comprehensive Survey," IEEE Access, vol. 8, pp. 117134–117153, 2020.

[9] Y. Zhang, J. Wen, and X. Xu, "Smart Contract-Based Access Control for IoT Systems Using Blockchain," IEEE Access, vol. 8, pp. 155779–155791, 2020.

[10] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things," Security and Communication Networks, vol. 9, no. 18, pp. 5943–5964, 2016.

[11] M. Banerjee, J. Lee, and K. Choo, "Blockchain-Based Secure Device Management Framework in IoT," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2179–2190, 2021.

[12] P. K. Sharma and S. Y. Moon, "Message Authentication and Route Security in IoT Using Blockchain Technology," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3163–3170, 2019.

[13] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Proc. IEEE Security and Privacy Workshops, pp. 180–184, 2015.

[14] A. Sharma, M. Tiwari, and S. Kumar, "Decentralized Access Control and Data Security in IoT Using Blockchain and Smart Contracts," Journal of Network and Computer Applications, vol. 180, 2021.

[15] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979–33001, 2018.

[16] S. Malik, P. Dutta, and S. K. Singh, "Blockchain-Based Authentication and Trust Management in IoT: A Systematic Review," Computer Networks, vol. 190, 2021.

[17] S. Cha, J. Park, and S. Kim, "IoT Security Enhancement Using Blockchain Technology," Sensors, vol. 21, no. 10, p. 3491, 2021.

[18] M. Samaniego and R. Deters, "Hosting Virtual IoT Resources on Edge-Hosts with Blockchain," in Proc. IEEE Int. Conf. Edge Computing, pp. 43–50, 2016.

[19] S. Singh and N. Singh, "Blockchain: Future of Financial and Cyber Security," in Proc. IEEE Symposium on Cloud Computing, 2016.

[20] J. Kang, R. Yu, X. Huang, M. Wu, and S. Maharjan, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4660–4670, 2019.