Blockchain-Powered Authentication Protocol for Next-Generation IoT Systems

Abarajitha M[1], Rajadhurai S[2]
[1]*M.sc cyber forensic and information security (CFIS) student,*
Dr. M.G.R Educational and Research Institute
[2]*Assistant Professor, Dr. M.G.R Educational and Research Institute*
doi.org/10.64643/IJIRTV13I1-204541-459

***Abstract*— Growing interconnectivity among IoT devices has exposed deep-rooted weaknesses in conventional, server-centric authentication approaches. To tackle these vulnerabilities, this paper presents a decentralized file-sharing and authentication architecture grounded in blockchain principles. Unlike centralized systems that are prone to single-point failures, unauthorized intrusions, and data manipulation, the proposed framework distributes trust across a network of blockchain nodes, cloud servers, data owners, and data consumers. A multi-role governance model is enforced through cloud-level administrative controls, ensuring that access rights are granted deliberately and transparently. File contents are shielded using Advanced Encryption Standard (AES) encryption, with each file receiving a distinct encryption key. To prevent in-app exposure, decryption keys are dispatched securely via email only after administrative clearance. File integrity is continuously verified through hash-based mechanisms distributed across independent storage nodes, making covert tampering detectable and reversible. The outcome is a cohesive security ecosystem that pairs decentralized storage with rigorous access governance**

***Index Terms*—Access control, AES Encryption, Blockchain, Decentralized Authentication, Decentralized identifiers Edge Computing, Internet of Things (IoT), Smart Contracts.**

I. INTRODUCTION

The rapid proliferation of IoT devices has fundamentally altered how data is generated, processed, and exchanged across networked environments. As computation migrates toward the periphery of networks closer to sensors and actuators the question of how to reliably verify device identities becomes both urgent and complex. Edge computing accelerates data handling by reducing reliance on distant cloud infrastructure, but it simultaneously introduces a wider attack surface that traditional authentication mechanisms are ill-equipped to address. This paper presents a blockchain-anchored authentication protocol designed specifically for edge-IoT deployments. By harnessing the distributed trust model inherent to blockchain networks, the proposed system enables IoT devices to mutually verify identities without delegating that responsibility to a central authority. The combination of blockchain's cryptographic guarantees with the low-latency advantages of edge computing yields a security architecture that is both operationally responsive and structurally resilient.

The protocol's significance extends beyond technical performance. As IoT ecosystems scale into the billions of devices spanning healthcare, transportation, smart infrastructure, and industrial automation the inadequacy of centralized authentication becomes a systemic risk. The proposed framework offers a forward-compatible solution, one capable of evolving alongside the expanding IoT landscape.

A. Scope of the Project

The scope of this project encompasses the end-to-end design, implementation, and evaluation of a decentralized authentication system tailored for edge-connected IoT devices. The system eliminates the structural vulnerabilities of centralized identity verification by relocating trust to a permissioned blockchain network governed by smart contracts.

Key implementation activities include deploying blockchain infrastructure, integrating edge gateway nodes with local authentication engines, configuring smart contract logic for identity verification and access control, and validating system behavior under realistic IoT network conditions. The resulting system is

intended to serve as a replicable blueprint for secure, scalable IoT deployments.

II. LITERATURE REVIEW

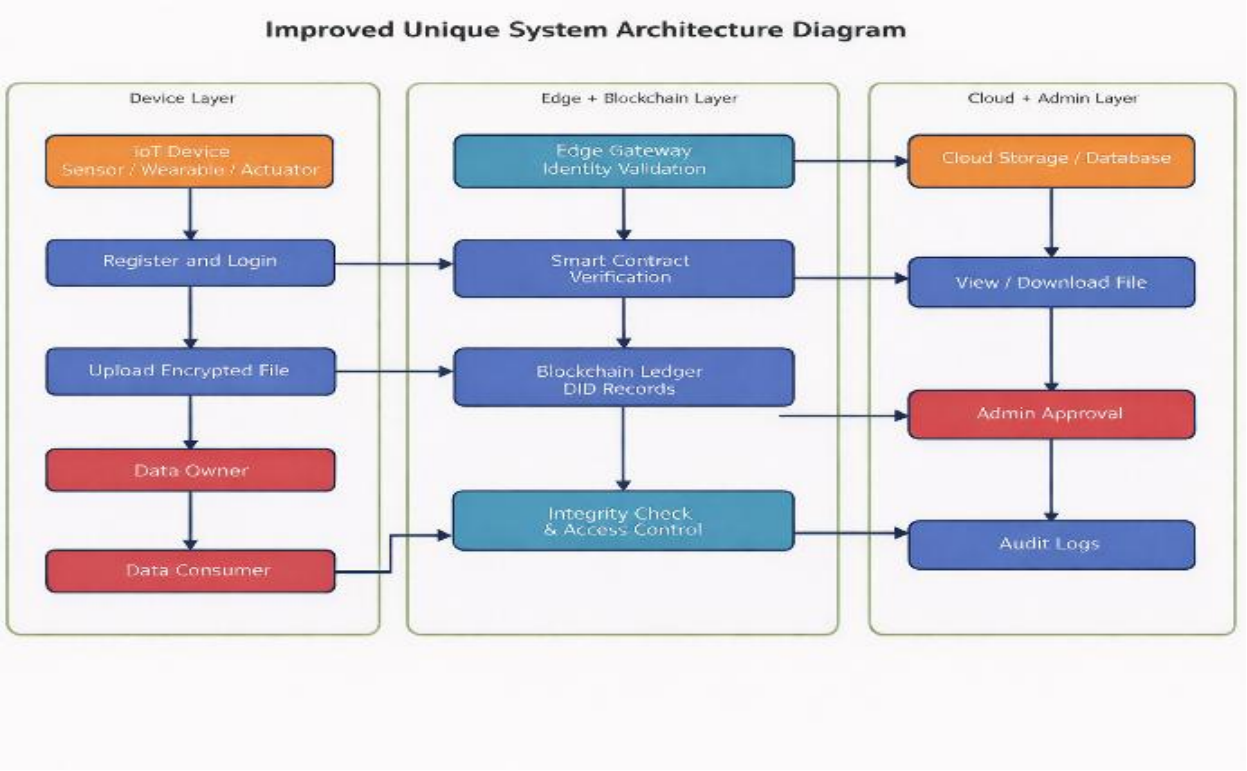
[1] Zhao, Q., Zhang, W., & He, J. (2020): Introduced a Physically Unclonable Function (PUF)-based key agreement mechanism tailored for maritime IoT systems, demonstrating that hardware-rooted identity primitives can effectively underpin blockchain-secured data acquisition in large-scale environments.

[2] Zhang, Y., Deng, R. H., & Chen, J. (2021): Constructed a formal tripartite authentication model covering entity, action, and claim verification using Communicating Sequential Processes (CSP). The study validated this framework in smart home scenarios, emphasizing lightweight operations compatible with constrained devices.

[3] Liu, X., Zhang, X., & Xu, Z. (2020): Surveyed the convergence of blockchain and edge computing for IoT, exploring consensus variants such as Proof-of-Work and Proof-of-Stake. The authors highlighted unresolved tensions between computational overhead, latency targets, and network scalability.

[4] Fang, L., & Xie, W. (2020): Investigated lightweight blockchain architectures including Hyperledger Fabric, IOTA, and DAG-based chains for IoT suitability. A hierarchical model was proposed wherein edge nodes assume validation duties, easing the computational burden on end devices.

III. SYSTEM OVERVIEW



A. IoT Devices (End Nodes)

At the perimeter of the network sit IoT endpoints sensors, actuators, wearables, and embedded systems that continuously produce and consume data. Before these devices can interact with edge infrastructure or peer nodes, their identities must be cryptographically confirmed. Given the memory and processing constraints typical of such hardware, authentication relies on computationally light primitives, particularly Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKP).

B. Edge Nodes (Authentication and Processing Layer)
Edge gateways bridge the gap between raw device activity and the blockchain ledger. They locally handle authentication requests, sparing devices from the overhead of direct blockchain interaction. Their responsibilities span three domains:

- Acting as identity validators that cross-check device credentials against blockchain-stored records.
- Preprocessing data streams through filtering, aggregation, and encryption before ledger submission.
- Executing smart contract logic that governs decentralized access control policies in real time. selected.

C. Blockchain Network (Distributed Ledger Layer)
The blockchain layer serves as the immutable backbone of the authentication architecture. Device identities, authentication events, and access control rules are recorded in a tamper-evident ledger that no single party controls. This layer relies on:

- Consensus protocols Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), or Practical Byzantine Fault Tolerance (PBFT) to validate authentication transactions across nodes.
- Smart contracts that autonomously execute registration workflows, identity checks, and permission changes without human mediation.
- Decentralized Identifiers (DIDs) that grant each device a self-sovereign identity, removing dependence on conventional certificate authorities.

D. Cloud/Off-Chain Storage (Optional Layer for Scalability)
To prevent the blockchain from becoming a bottleneck for voluminous IoT data, off-chain systems such as IPFS, sidechains, or distributed relational databases handle bulk storage. Authentication logs and identity records, however, remain anchored to the blockchain, preserving their auditability and integrity.

IV. EXISTING SYSTEM

Current IoT authentication schemes predominantly follow a hub-and-spoke model, routing device verification through centralized cloud platforms using established protocols such as Public Key Infrastructure (PKI) and OAuth. While familiar and relatively straightforward to deploy, these approaches carry inherent structural weaknesses that become increasingly problematic as IoT deployments grow:

- Single Point of Failure: A compromised or unavailable central server can render an entire authentication network inoperable.
- Elevated Latency: The round-trip to remote cloud servers introduces delays that are incompatible with time-sensitive applications like autonomous vehicles and industrial control systems.
- Scalability Ceiling: Centralized infrastructure struggles to process exponentially growing volumes of concurrent authentication requests.
- Interoperability Gaps: Vendor-specific authentication protocols fragment ecosystems, complicating cross-platform device interaction.
- Attack Surface: Centralized trust models are prime targets for identity spoofing, replay attacks, and man-in-the-middle interception.

V. PROPOSED SYSTEM

The framework proposed in this paper supersedes centralized authentication by distributing trust across a blockchain network augmented by edge computing. The system grants IoT devices autonomous control over their credentials through Self-Sovereign Identity (SSI) principles and Decentralized Identifiers (DIDs), eliminating the need for third-party identity custodians. Smart contracts manage the verification lifecycle automatically, enforcing rules coded into the blockchain itself rather than maintained by an external service.
Authentication happens at the network edge rather than in the cloud, cutting round-trip latency and reducing bandwidth consumption. This architectural shift is essential for applications that demand near-real-time responses, such as industrial automation, connected healthcare, and smart city management.
A. IoT Device Layer (End Nodes)

- Diverse device classes sensors, smart meters, wearables, industrial controllers are onboarded with unique DIDs anchored to the blockchain, enabling trust less peer verification.
- Lightweight cryptographic operations (ECC, SHA-256) are prioritized to accommodate devices with limited computational resources.

B. Edge Computing Layer

- Edge nodes intercept and locally resolve authentication requests, acting as proximity-based gatekeepers for IoT services.
- By handling verification locally, these nodes eliminate cloud round-trips, directly reducing authentication latency.
- Smart contract-driven verification ensures that authentication decisions are deterministic, tamper-proof, and auditable.
- Frequently authenticated devices are cached at the edge layer to further accelerate repeat interactions.

C. Blockchain Network Layer

- A shared, permissioned ledger maintains verified device profiles and a complete, time-stamped record of authentication events.
- Smart contracts enforce access policies autonomously, removing the need for centralized policy administrators.
- Consensus mechanisms PoS, PBFT, or DPoS validate incoming authentication transactions, ensuring agreement across nodes.
- Blockchain immutability and cryptographic signing collectively neutralize identity spoofing, replay, and MITM threats.

D. Decentralized Identity Management (DID-Based Authentication)

Rather than relying on identity providers that represent single points of failure, the system adopts a model in which devices generate and manage their own DIDs on the blockchain. This eliminates certificate authorities from the trust chain entirely, simplifying the identity lifecycle while strengthening security guarantees.

E. Blockchain Smart Contract Authentication

- Authentication workflows are fully encoded in smart contracts, removing manual intervention from the verification process.
- Devices submit signed authentication requests; contracts validate signatures against ledger-stored credentials automatically.
- Adaptive security logic within contracts can blacklist devices exhibiting anomalous behaviour, such as repeated failed authentication.

F. Edge Computing for Low-Latency Authentication

By relocating authentication computation from distant cloud servers to nearby edge nodes, the framework achieves response times suitable for real-time IoT applications. Each completed authentication event is recorded on-chain via smart contract, producing an auditable trail while ensuring that only verified devices gain access to protected resources.

VI. SYSTEM ANALYSIS

The proposed framework weaves together blockchain's foundational properties decentralization, immutability, and transparency with the performance benefits of edge computing to deliver a comprehensive security solution for IoT environments,

A. Objectives

- Remove Centralized Vulnerabilities: Distribute authentication across the network to eliminate structural dependencies on single-authority servers.
- Strengthen Security via Blockchain: Use an immutable ledger to preserve tamper-evident authentication histories.
- Minimize Latency through Edge Processing: Bring authentication logic to the network edge for real-time performance.
- Support Resource-Constrained Devices: Implement lightweight cryptographic protocols compatible with low-power IoT hardware.

B. Feasibility Study

The feasibility of the project is analyzed across three dimensions to ensure the proposed system is both practical and beneficial:

Economic Feasibility: The majority of enabling technologies blockchain frameworks, cryptographic libraries, and database systems are open-source and freely accessible. Investment is required only for bespoke components, keeping total development costs within reach for institutional and enterprise adopters.

Technical Feasibility: The system is built on widely supported technologies including Java, MySQL, and established blockchain SDKs. Standard hardware configurations meet all operational requirements, removing the need for specialized infrastructure.

Social Feasibility: Role-specific dashboards and intuitive navigation reduce the learning curve for Cloud Administrators, Data Owners, and Data Users.

Accompanying training materials further facilitate smooth organizational adoption.

VII. SYSTEM DESIGN AND ARCHITECTURE

The design and architecture of the Blockchain-Powered Authentication Protocol for Next-Generation IoT Systems system aim to provide a scalable, secure, and decentralized framework for authenticating IoT devices in an Edge-IoT environment. By leveraging blockchain technology, the system ensures robust device identity management, tamper-proof authentication logs, and efficient distributed access control mechanisms.

A. System Architecture

The architecture is organized into four cooperating layers, each with well-defined responsibilities:

- Endpoint sensors and smart devices equipped with embedded DIDs and lightweight cryptographic modules for low
- Proximity authentication engines that evaluate identity verification requests in real time using pre-deployed smart contract logic.
- An immutable distributed ledger that records device identities, authentication events, and access control policies with full auditability.
- A supplementary storage tier using IPFS or distributed databases to archive large IoT data volumes without burdening the blockchain.

B. Software Description

The software stack is composed of tightly integrated modules. The blockchain core acts as a distributed identity registry and authentication log, running smart contracts under energy-efficient consensus protocols such as PoS or PBFT.

The Edge Authentication Engine, deployed on gateway nodes, handles verification locally. It incorporates ECC, Zero-Knowledge Proofs, and hash-based encryption to authenticate resource-constrained endpoints without performance penalties.

The Decentralized Identity Management System (DIMS) operationalizes Self-Sovereign Identity, assigning each device a blockchain-anchored DID that any authorized edge node can independently verify. No central certificate authority is involved.

Complementing these modules is an AI-driven anomaly detection layer that continuously analysis authentication logs for behavioral irregularities such as unusual access patterns or repeated credential failures and triggers automated countermeasures when threats are identified.measures.

C. Hardware and Software Requirements

Hardware Requirements: Intel i3 processor or above, 64-bit quad-core at 2.5 GHz minimum per core, 4 GB RAM minimum, 40 GB Hard Disk storage.

Software Requirements: Front-end: HTML, CSS, JavaScript, JSP, Servlets; Back-end: MySQL Database; Operating System: Windows 10 or Windows 11; IDE: Java Development Kit (JDK).

VIII. CONCLUSION

The blockchain-driven authentication framework presented in this paper directly addresses the security deficiencies that have long accompanied centralized IoT authentication. As device counts scale and edge deployments grow more complex, the structural fragility of hub-and-spoke trust models becomes untenable. The proposed system counters this by distributing authentication authority across an immutable blockchain, pushing verification computation to the network edge, and granting devices sovereign control over their own identities.

The practical outcomes are significant: reduced latency, resistance to single-point compromise, automatic enforcement of access policies, and a transparent audit trail of every authentication event. While challenges related to consensus performance on constrained hardware, cross-chain compatibility, and energy efficiency remain open areas of inquiry, the framework provides a structurally sound foundation for addressing them. Future research will prioritize consensus optimization for low-resource environments, expanded interoperability across heterogeneous blockchain networks, and more sophisticated anomaly detection capabilities.

ACKNOWLEDGMENT

I would like to express our sincere gratitude to all those who contributed to the successful completion of this research work. First and foremost, we extend our heartfelt thanks to Dr. M.G.R. Educational and Research Institute, Chennai, for providing us with the necessary infrastructure and academic environment to carry out this project. I deeply thankful to Mr.

RAJADHURAI S, Assistant Professor, Dr. M.G.R. Educational and Research Institute, Chennai, India, for his invaluable guidance, continuous support, and insightful feedback throughout the research. His expertise and mentorship were instrumental in shaping the direction and quality of this work. I also extend our appreciation to our colleagues and peers who provided constructive suggestions and moral support throughout this journey. Special thanks to the faculty of the Department of Computer Science Engineering for their encouragement and academic assistance.

REFERENCES

[1] Q. Zhao, W. Zhang, and J. He, "Blockchain-Based Secure and Decentralized Authentication for Internet of Things," *IEEE Access*, vol. 8, pp. 95343–95355, 2020.

[2] Y. Zhang, R. H. Deng, and J. Chen, "Edge Computing and Blockchain Integration: A Survey on Technologies, Applications, and Challenges," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3313–3321, 2021.

[3] H. Huang and Y. Liu, "Secure and Efficient Blockchain-Based Authentication for IoT in Edge Computing Environments," *Future Generation Computer Systems*, vol. 108, pp. 788–799, 2020.

[4] X. Liu, X. Zhang, and Z. Xu, "Blockchain for Edge Computing: A Survey on Applications, Architectures, and Open Challenges," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5630–5639, 2020.

[5] D. Patel and P. Patel, "Blockchain-Enabled Authentication for IoT and Edge Networks: Challenges and Opportunities," *IEEE Transactions on Industrial Informatics*, 2021.

[6] S. Ghosh and S. Saha, "A Secure Blockchain-Based Authentication Model for IoT Devices in Edge Networks," *Journal of Information Security and Applications*, vol. 53, Art. no. 102456, 2020.

[7] L. Fang and W. Xie, "Decentralized Authentication Scheme Based on Blockchain for IoT Devices in Edge Networks," *Journal of Cloud Computing*, 2020.

[8] H. Bhang and Y. Liu, "Secure and Efficient Blockchain-Based Authentication for IoT in Edge Computing Environments," *Future Generation Computer Systems*, vol. 108, pp. 788–799, 2020.