International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 4, Issue 1, January-February 2022 |

DOI:10.15662/IJEETR.2022.0401001

Blockchain-Based Secure Authentication Framework for IoT Networks

Ramdhari Singh Dinkar

CMR Institute of Technology, Bengaluru, India

ABSTRACT: With the rapid expansion of the Internet of Things (IoT), the need for secure, scalable authentication mechanisms has escalated alongside concerns regarding centralized trust, device identity spoofing, and resource constraints. Traditional centralized authentication models are vulnerable single points of failure and often unsustainable for large-scale IoT deployments. Blockchain, with its decentralized ledger, tamper resistance, and trustless trust model, presents a compelling alternative.

This research investigates blockchain-based authentication frameworks tailored for IoT environments before 2021. It examines lightweight consensus algorithms such as Proof-of-Authentication (PoAh), designed for resource-constrained devices, achieving block validation in mere seconds—unlike heavy Proof-of-Work schemes unsuitable for IoT contexts . We also explore hardware-assisted models like **PUFchain**, which integrates Physical Unclonable Functions (PUFs) to generate unique and unclonable device identities. The PUF-Enabled Authentication (PoP) consensus mechanism dramatically enhances security while maintaining high throughput and low latency .

Layered architectures such as **IoTChain** provide three-tier designs comprising authentication, blockchain, and application layers, enabling identity verification, lightweight access control, resilience to node failure, and integrity protection . Other frameworks leverage permissioned blockchains like Hyperledger Fabric to manage identities and authentication flexibly for smart device environments .

Overall, pre-2021 blockchain-enabled IoT authentication frameworks demonstrate promising avenues that reconcile decentralized trust, device constraints, and strong security guarantees, laying a foundation for more robust, scalable authentication infrastructures in the evolving IoT landscape.

KEYWORDS: IoT Authentication, Blockchain-Based Identity, Lightweight Consensus, Proof-of-Authentication (PoAh), PUFchain (Hardware-Assisted Security), Permissioned Blockchain, Hyperledger Fabric, Decentralized Identity, Resource-Constrained Devices, Authentication Architecture

I. INTRODUCTION

As IoT ecosystems proliferate, securing device identity and ensuring robust authentication across heterogeneous, resource-constrained networks have become critical challenges. Traditional centralized authentication systems incur latency, single points of failure, and scalability issues. Blockchain's decentralized, immutable ledger and smart contract capabilities offer a path forward by enabling secure authentication without centralized trust.

However, blockchain implementation in IoT must address constraints around device processing power, energy usage, and limited storage. Conventional consensus mechanisms like Proof-of-Work (PoW) are computationally intensive and unsuitable for IoT. Emerging research addresses this by devising lightweight, tailored blockchain models for IoT contexts.

Pre-2021, researchers developed novel consensus algorithms such as Proof-of-Authentication (PoAh), enabling rapid block validation using simple cryptographic proofs—achieving latency around three seconds—even on devices like Raspberry Pi . Hardware-backed approaches like **PUFchain** further embed Physical Unclonable Functions into authentication workflows, delivering unique, unclonable identities and dramatically reducing resource overheads compared to PoW .

Architectural frameworks like **IoTChain** feature layered designs—authentication, blockchain, application—to enhance resilience, access control, and privacy while remaining lightweight . Parallel approaches using permissioned ledgers like Hyperledger Fabric support device identity, registration, and revocation through flexible smart contract mechanisms without overburdening constrained devices . This converging body of research sets a foundation for designing resilient, efficient, and scalable blockchain-based authentication frameworks enabling IoT devices to maintain security and trust in dynamic, decentralized environments.

II. LITERATURE REVIEW

Proof-of-Authentication (PoAh): PoAh introduces a lightweight alternative to PoW for IoT blockchains, facilitating scalable, decentralized authentication. It replaces computationally heavy mining with cryptographic authentication compatible with constrained devices. Simulation and real deployment on platforms like Raspberry Pi show PoAh achieves block validation latencies around three seconds, demonstrating practicality in IoT contexts .

PUFchain and PoP (Hardware-Assisted Authentication): PUFchain merges blockchain with hardware security by integrating Physical Unclonable Functions (PUFs). These produce unique device identities derived from manufacturing characteristics. The Proof-of-PUF-Enabled Authentication (PoP) consensus is significantly faster—up to 1,000× more efficient than PoW and 5× faster than PoAh—while bolstering security and reducing energy usage .

IoTChain Architecture: This three-tier blockchain framework contains an authentication layer for identity and access control, a lightweight blockchain layer managing device registry and resilience, and an application layer facilitating IoT service integration. It balances identity validation, privacy protection, and resource efficiency, while improving tolerance to denial-of-service attack vectors and node failures .

Permissioned Blockchain for Identity Management (Hyperledger Fabric-based Models): IoT identity solutions leveraging Hyperledger Fabric are explored in smart home use cases. These implementations create consortium networks for flexible identity, authentication, and revocation management via multiple ledgers and channels, offering resiliency and interoperability . Additional works employ Hyperledger for attribute-based IoT access control and optimized processing for latency-sensitive environments .

Collectively, these pre-2021 frameworks illustrate a trend toward balancing IoT constraints with security using blockchain: lightweight or hardware-backed consensus models, multi-layered designs for scalability, and permissioned frameworks for flexible identity management—all forming the basis for a future secure authentication ecosystem in IoT.

III. RESEARCH METHODOLOGY

This study synthesizes pre-2021 research to propose a blockchain-based authentication framework tailored for IoT networks. Our methodology comprises:

1. **Literature Review**
2. We examined blockchain–IoT authentication schemes, including three-tier architectures like IoTChain that separate authentication, blockchain, and application layers to enable identity verification, access control, privacy protection, and resilience against DoS and node faults . We also considered concepts such as A²Chain, which uses edge-based sidechain models for scalable, cross-domain authentication .
3. **Comparative Analysis**
4. We compared consensus mechanisms (PoW, PoS, PBFT) and lightweight alternatives like PoAh, specifically designed for IoT devices . We assessed identity management strategies using RFID, PUFs, and smart contracts for unique device authentication .
5. **Framework Design Principles**
6. The proposed framework integrates:

○ A **permissioned blockchain** approach for efficient validation.
○ **Edge authentication nodes**, following sidechain-edge design patterns to reduce latency and storage burden .
○ **Identity-based signatures** as lightweight alternatives to traditional certificate systems .

7. **Simulation and Evaluation (Theoretical)**
8. Drawing from EdgeChain's performance evaluations, which showed acceptable costs in integrating blockchain into IoT deployments , we outline evaluation strategies to test authentication latency, resource usage, and scalability.

This methodology blends survey analysis with practical design synthesis and evaluation insights, ensuring the resulting framework is informed by key challenges and proven architectural models.

Backend server hosted in cloud
Web API
Multi-lingual text
Google Translate Application Programming Interface (API)
English question
DR-COVID question-answering chatbot model (spaCy + fine-tuned COVID-BERT)
Question
Training Dataset (Q&A Pairs)
Answer
Embedding representation
Similarity calculation (matching)
Top 1/Top3 Question(s)
Query answer
English answer
Google Translate Application Programming Interface (API)
Web API
Multi-lingual text
Telegram Messenger
Telegram Messenger

IV. KEY FINDINGS

1. **Three-Tier Architectures Enhance Resilience and Functionality**
2. IoTChain illustrates a layered model—authentication, blockchain, application—that supports fault tolerance, lightweight performance, and secure logging, reducing single-point vulnerabilities and enabling access control and privacy protection .
3. **Consensus Optimization for IoT Constraints**
4. Traditional PoW is resource-heavy. PoAh offers a streamlined consensus ideal for resource-constrained IoT (e.g., Raspberry Pi), instituting authentication rather than computation-heavy validation, with latency around 3 seconds .
5. **Edge Computing Reduces Latency & Storage Load**
6. A²Chain introduces edge authentication nodes and sidechains to localize authentication requests, reducing latency and blockchain storage burdens, and supporting cross-domain authentication efficiently .
7. **Lightweight Identity Mechanisms Are Practical**
8. Implementations using identity-based signatures, RFID, or physical unclonable functions enable secure authentication without heavy certificate infrastructures—suited for constrained devices .
9. **Unified Frameworks Offer Scalability and Trust**
10. Surveys reveal that combining blockchain with zero-trust models, attribute-based access control, or hierarchical trust systems significantly enhances scalability and cross-domain security in IoT environments.

These findings collectively support an architecture design that balances security, performance, and practicality for IoT authentication.

V. WORKFLOW

1. **IoT Device Registration**
2. Each device registers via an edge authentication node (EAN), providing identification (e.g. RFID tag, PUF-generated ID). The EAN verifies identity and records a minimal credential hash on the IoT-specific blockchain.
3. **Consensus & Authentication Recording**
4. The framework employs a lightweight consensus (e.g. PoAh) to validate registration transactions securely and efficiently, ensuring tamper-resistant ledger entry.
5. **Access Requests & Verification**
6. When a device attempts network or cross-domain access, it contacts the nearest EAN. The EAN verifies credentials via local blockchain or sidechain, using identity-based signature authentication, reducing latency.
7. **Cross-Domain Validation**
8. For access across domains, sidechain mechanisms allow verification via Simplified Payment Verification (SPV) or compact credential transfer, avoiding full blockchain replication and storage burden.
9. **Smart Contract Enforcement**
10. Access policies and authentication rules are enforced via smart contracts residing on the blockchain, ensuring non-repudiation and automatic policy enforcement.
11. **Monitoring & Logging**
12. All authentication events are logged for auditing and traceability. Key metrics—latency, computational overhead, error rates—are recorded to monitor performance.
13. **System Scaling & Maintenance**
14. As network scales, new EANs and sidechains are added, enabling modular expansion. Periodic pruning or archival techniques maintain storage efficiency in edge nodes.

This workflow blends decentralized trust, edge-based efficiency, and blockchain transparency to support secure, scalable IoT authentication.

IV. ADVANTAGES & DISADVANTAGES

Advantages

- **Decentralized Trust**: Removes central authentication bottlenecks and single points of failure.
- **Low Latency via Edge Nodes**: EANs reduce access delay and bandwidth load on the network.
- **Resource-Efficient**: Lightweight consensus (PoAh) and identity-based signatures suit constrained devices.
- **Audit & Integrity**: Blockchain ensures tamper-proof logging and policy enforcement.
- **Cross-Domain Support**: Sidechains allow secure interoperability without redundant storage.

Disadvantages

- **Complexity**: Implementing and maintaining blockchain infrastructure with smart contracts introduces system complexity.
- **Edge Node Trust Assumption**: Requires secure edge nodes—compromise there undermines the system.
- **Consensus Overhead**: Though lightweight, consensus still incurs delay—PoAh's ~3 sec latency may be non-trivial for some use cases.
- **Adoption Barriers**: IoT manufacturers may resist due to cost and integration challenges.

VII. RESULTS AND DISCUSSION

Integrating IoTChain's architecture demonstrates feasible authentication performance with acceptable overhead . PoAh shows lightweight consensus viable on low-resource hardware, with latency in seconds . A²Chain's design reduces latency and cross-domain authentication burden, though implementation complexity remains. Identity-based and PUF-based mechanisms minimize computational load, offering practical authentication without overtaxing IoT devices .
However, trade-offs are inherent: edge node deployment increases system management effort; coordination between sidechains may become complex; in threat models, edge nodes or smart contracts might become new attack surfaces. Still, compared to centralized authentication, this architecture presents marked improvements in resilience, scalability, and decentralization.

VIII. CONCLUSION

Before 2021, blockchain-based authentication frameworks like IoTChain, A²Chain, and PoAh demonstrated that decentralized, edge-supported, and identity-lightweight systems can provide secure, scalable authentication for IoT networks. By combining permissioned blockchains, sidechain architecture, and lightweight consensus, such frameworks address challenges of device resource constraints, latency, trust, and scalability while ensuring secure access control and logging.

IX. FUTURE WORK

- **Prototype & Performance Testing**: Implement full-scale prototype in real-world IoT deployment to evaluate latency, energy consumption, and throughput.
- **Dynamic Consensus Mechanisms**: Explore adaptive consensus that adjusts to network load or device capability.
- **Security Analysis**: Conduct adversarial testing on edge nodes, smart contracts, and sidechain interconnections.
- **Interoperability Standards**: Define cross-domain protocols and standards to harmonize identity and access across IoT ecosystems.
- **Machine Learning Integration**: Add anomaly-based detection at edge nodes to detect compromised devices and revoke credentials dynamically.

REFERENCES

1. Bao et al. (2018). *IoTChain: A Three-Tier Blockchain-Based IoT Security Architecture* .
2. Puthal et al. (2020). *PoAh: A Novel Consensus Algorithm for Fast Scalable Private Blockchain for IoT*.
3. Hammi et al.; A²Chain framework (2020).
4. Studies on lightweight identity authentication using RFID, PUFs, smart contracts.
5. Surveys on blockchain, zero-trust, and trust management in IoT authentication contexts