International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

Securing IoT Devices with Blockchain at the Edge: A Decentralized Framework for Trust and Integrity

Dr. Amit Saxena
Department of CSE
Moradabad Institute of Technology, Moradabad
er.amitsaxena79@gmail.com

Abstract

The Internet of Things (IoT) is undergoing explosive growth, connecting billions of resource-constrained devices to the internet. This hyper-connectivity, however, has introduced significant security and privacy challenges, primarily stemming from centralized architectures, weak device security, and a lack of data integrity. Traditional cloud-centric security models suffer from single points of failure, latency issues, and high operational costs. This paper proposes a novel framework that synergistically combines blockchain technology and edge computing to create a decentralized, secure, and resilient ecosystem for IoT. By deploying a lightweight, distributed ledger on edge nodes, our architecture establishes a tamper-proof system for device identity management, secure data transactions, and autonomous access control via smart contracts. Edge computing mitigates the latency and scalability issues inherent in blockchain by processing data locally, while blockchain provides the trust, immutability, and auditability that IoT networks critically lack. We analyze the proposed architecture, detailing its key components for device authentication, data integrity, and firmware updates. Finally, we discuss the significant security benefits, performance considerations, and outstanding challenges, concluding that the convergence of blockchain and edge computing represents a paradigm shift in securing the future of the Internet of Things.

Keywords: Internet of Things (IoT), Blockchain, Edge Computing, Cybersecurity, Decentralization, Smart Contracts, Data Integrity.

1. Introduction

The Internet of Things (IoT) is rapidly evolving from a niche concept into a pervasive reality, with projections of over 75 billion connected devices by 2025 [1]. These devices, ranging from smart home sensors to industrial control systems, generate vast amounts of data and enable unprecedented levels of automation and efficiency. However, the foundational architecture of most IoT deployments remains highly centralized, relying on cloud servers for data processing, storage, and device management.

This centralized model presents severe security vulnerabilities:

- **Single Point of Failure:** A successful attack on a central cloud server can compromise the entire network, leading to massive data breaches or service outages.
- **Data Integrity and Trust:** Data transmitted from IoT devices can be intercepted and manipulated en route to the cloud, making it difficult to trust the authenticity of the information.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

- **Privacy Concerns:** Centralized entities control vast troves of sensitive user data, creating privacy risks and potential for misuse.
- **Scalability and Latency:** As the number of devices grows, routing all traffic through a central cloud introduces significant latency and bandwidth bottlenecks, which is unacceptable for time-critical applications like autonomous vehicles or remote surgery.

The inherent resource constraints of most IoT devices (limited processing power, memory, and battery life) further exacerbate these issues, making it impractical to implement robust, conventional security protocols on the devices themselves. The Mirai botnet attack, which hijacked hundreds of thousands of insecure IoT devices to launch a massive Distributed Denial of Service (DDoS) attack, serves as a stark reminder of these vulnerabilities [2].

To address these fundamental challenges, this paper proposes a decentralized security framework that leverages the complementary strengths of **blockchain technology** and **edge computing**. Blockchain offers a distributed, immutable, and transparent ledger, providing a trustless environment for transactions and interactions [3]. Edge computing shifts computation and data storage closer to the sources of data, reducing latency and reliance on the cloud [4].

Our proposed framework integrates these two transformative technologies to create a secure, resilient, and efficient architecture for IoT. By moving the blockchain's trust and verification mechanisms to the edge layer, we can secure IoT devices and their data without overburdening the end devices or the central cloud. This paper makes the following contributions:

1. It presents a multi-layered architecture that integrates IoT devices, edge nodes, and a blockchain network.
2. It details specific mechanisms for decentralized identity management, smart contract-based access control, and secure data and firmware management.
3. It provides a comprehensive analysis of the security benefits and performance trade-offs of this approach.
4. It identifies key challenges and outlines future research directions for this promising field.

The remainder of this paper is organized as follows: Section 2 provides background on IoT security challenges, blockchain, edge computing, and related work. Section 3 details the proposed architectural framework. Section 4 analyzes the framework's security benefits and performance. Section 5 discusses challenges and future research directions. Finally, Section 6 concludes the paper.

2. Background and Related Work

2.1 IoT Security Challenges

Traditional IoT security is often an afterthought. Key challenges include weak or hardcoded passwords, lack of secure update mechanisms, insecure data transfer and storage, and heterogeneous device standards. The centralized client-server model is a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

primary culprit, creating a lucrative target for attackers and a single point of failure that can cripple entire ecosystems.

2.2 Blockchain Technology

Blockchain is a decentralized, distributed ledger technology. Its core properties—immutability, transparency, and decentralization—are secured through cryptographic hashing and consensus algorithms (e.g., Proof of Work, Proof of Stake, or Proof of Authority). **Smart contracts**, which are self-executing contracts with the terms of the agreement directly written into code, can automate and enforce rules within the network without a central intermediary [5]. These features make blockchain a powerful tool for establishing trust in a trustless environment.

2.3 Edge Computing

Edge computing is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed. Instead of sending raw data to a distant cloud, edge nodes (such as gateways, routers, or on-premises micro-servers) perform initial processing, filtering, and analysis. This reduces latency, conserves network bandwidth, and enables real-time responsiveness for critical IoT applications.

2.4 Related Work

Several researchers have explored using blockchain for IoT security. Huh et al. [6] proposed a system for managing IoT devices using a blockchain, but it relied on a centralized authority for key management. Ali et al. [7] introduced a blockchain-based framework for secure smart home data sharing, highlighting smart contracts for access control. However, many early proposals overlooked the significant latency and computational overhead of running blockchain protocols in an IoT context, often assuming direct interaction between resource-constrained devices and the blockchain, which is impractical.

The integration of edge computing is a more recent and promising development. Sharma et al. [8] proposed a distributed blockchain-based architecture for IoT using software-defined networking and edge computing, focusing on anomaly detection. Puthal et al. [9] explored the security of edge-of-things (EoT) data, using a flexible blockchain model to manage data provenance. Our work builds upon these foundations by proposing a holistic framework that explicitly leverages the edge layer to run lightweight blockchain clients and smart contracts, thereby creating a scalable and practical solution for device identity, access control, and data integrity.

3. Proposed Architecture: A Blockchain-Edge Framework for IoT Security

We propose a three-layer architecture designed to address the core security challenges of IoT. This architecture distributes trust and computation across the network, minimizing reliance on a central authority.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

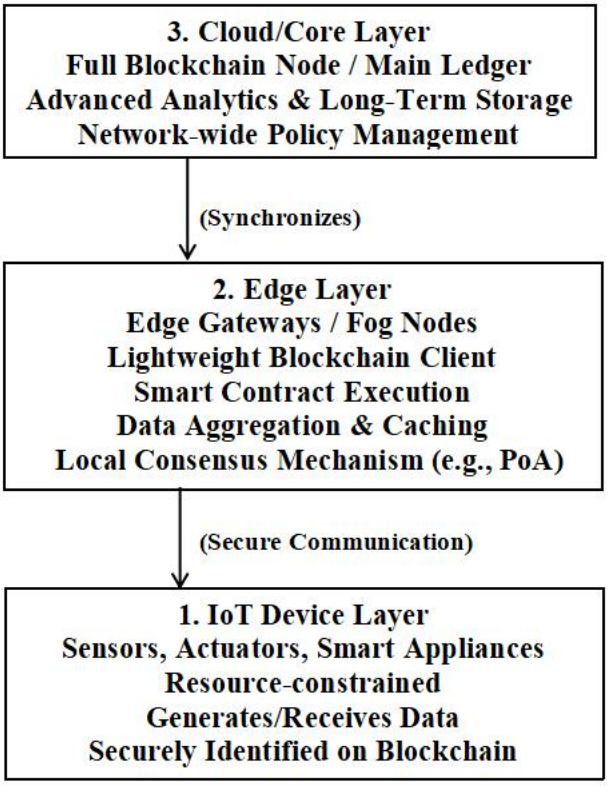

Figure 1: Proposed Three-Layer Architecture

3.1 Layer 1: IoT Device Layer

This layer consists of the end devices (sensors, actuators). These devices are typically resource-constrained and are not expected to run a blockchain client. Their primary roles are to generate data, receive commands, and possess a unique cryptographic identity registered on the blockchain.

3.2 Layer 2: Edge Layer

This is the core of our framework. It comprises edge nodes (e.g., IoT gateways, routers, or micro-servers) located physically close to the IoT devices. These nodes have sufficient computational power to:

- Run a **lightweight blockchain client**.
- **Execute smart contracts** for access control and other automated tasks.
- **Aggregate and pre-process** data from IoT devices.
- Participate in a **local, efficient consensus mechanism**, such as Proof of Authority (PoA), which is more suitable for private or consortium networks than energy-intensive Proof of Work.

3.3 Layer 3: Cloud/Core Layer

The cloud layer manages the overarching network. It may host a full node of the blockchain, storing the complete historical ledger. Its primary functions are long-term data storage, running complex, resource-intensive analytics on aggregated data, and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

setting network-wide policies that can be pushed down to the edge layer via smart contracts.

3.4 Key Security Mechanisms

1. Decentralized Device Registration and Identity Management: When a new IoT device is to be added to the network, its manufacturer generates a public-private key pair for it. The public key, along with device metadata (e.g., device type, serial number), is registered as a unique identity in a transaction on the blockchain. This creates an immutable and auditable record of all legitimate devices in the network, effectively creating a decentralized Public Key Infrastructure (PKI). Any communication from the device must be cryptographically signed with its private key, and the signature can be verified by the edge node against the public key on the ledger.

2. Smart Contract-Based Access Control: Access control policies are encoded into smart contracts and deployed on the blockchain. For example, a smart contract could define a policy such as: *"Allow User A's smartphone (identified by its public key) to access the video feed from Camera C (identified by its public key) only between 9:00 AM and 5:00 PM on weekdays."* When User A requests access, the request is routed to the local edge node. The edge node queries the relevant smart contract on its local ledger copy. The smart contract automatically verifies the requester's identity, the target device, and the policy conditions (e.g., time of day). If all conditions are met, access is granted; otherwise, it is denied. This process is autonomous, transparent, and tamper-proof.

3. Data Integrity and Transaction Management: To ensure data integrity without bloating the blockchain with raw IoT data, we adopt a hash-based approach.

1. An IoT device sends its data (e.g., a temperature reading) to its local edge node.
2. The edge node validates the device's signature, processes the data, and computes a cryptographic hash of the data packet (or a batch of data packets).
3. The edge node then creates a transaction containing this hash, along with relevant metadata (timestamp, device ID), and commits it to the blockchain.
4. The raw data can be stored off-chain, either on the edge node for short-term access or in a distributed storage system (like IPFS) or the cloud for long-term retention. Anyone wishing to verify the data's integrity can re-compute its hash and compare it with the immutable hash stored on the blockchain.

4. Secure Over-the-Air (OTA) Firmware Updates: Unauthorized firmware updates are a major attack vector. Our framework secures this process by:

1. The device manufacturer publishes the cryptographic hash of a new, legitimate firmware update to a smart contract on the blockchain.
2. The update file itself is hosted on a distribution server (e.g., CDN or IPFS).
3. Edge nodes notify their connected IoT devices of the available update.
4. The IoT device downloads the firmware and, before installation, requests the official hash from its edge node (which reads it from the blockchain).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

5. The device calculates the hash of the downloaded file and proceeds with installation only if it matches the hash on the ledger. This prevents the installation of malicious or corrupted firmware.

4. Analysis and Discussion

4.1 Security Benefits

- **Decentralization and Resilience:** By removing the central server as a single point of failure, the framework is more resilient to DDoS attacks and server outages. The network can continue to operate locally even if connectivity to the cloud is lost.
- **Immutability and Auditability:** All transactions—device registrations, access requests, data hashes, and firmware updates—are recorded on an immutable ledger. This creates a transparent and tamper-proof audit trail for forensic analysis and compliance.
- **Enhanced Data Integrity:** Cryptographic hashing ensures that data cannot be altered after it has been recorded on the blockchain, providing a strong guarantee of its authenticity.
- **Autonomous and Secure Access Control:** Smart contracts automate policy enforcement without human intervention, reducing the risk of error or malicious administrative action.
- **Improved Privacy:** While the blockchain provides transparency for transactions, user and device identities are pseudonymous (represented by cryptographic addresses). Advanced cryptographic techniques like zero-knowledge proofs could be integrated for further privacy enhancement.

4.2 Performance Considerations

- **Latency:** By handling most transactions at the edge layer, the framework significantly reduces the round-trip time compared to a cloud-only blockchain implementation. This makes it viable for latency-sensitive applications.
- **Throughput and Scalability:** The scalability of the blockchain itself remains a challenge. A public blockchain like Bitcoin or Ethereum has very low transaction throughput. Our model mitigates this by:
    - Using a **private or consortium blockchain**, which allows for more efficient, non-competitive consensus algorithms (e.g., PoA).
    - Processing **transactions locally** within an edge cluster.
    - **Storing only hashes** on-chain, keeping the ledger lightweight.
- **Computational Overhead:** Edge nodes must have sufficient resources to run a blockchain client and execute smart contracts. This necessitates more powerful hardware than typical IoT gateways but is far more feasible than deploying such capabilities on end devices.

5. Challenges and Future Research Directions

Despite its promise, the proposed framework is not without challenges:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

- **Scalability:** While the edge layer helps, scaling a single blockchain to billions of devices and trillions of transactions remains a major research problem. Solutions like sharding or hierarchical blockchain structures need further investigation.
- **Smart Contract Security:** A bug in a smart contract is immutable and can be exploited. Rigorous testing, formal verification, and standardized, audited contract templates are essential.
- **Interoperability:** The IoT and blockchain ecosystems are fragmented. Standardizing communication protocols between devices, edge nodes, and various blockchain platforms is crucial for widespread adoption.
- **Key Management:** Securely managing the private keys for billions of IoT devices throughout their lifecycle is a complex logistical and security challenge.
- **Data Privacy:** While pseudonymous, transaction patterns on a blockchain can be analyzed to de-anonymize users. Further research into privacy-preserving technologies like zk-SNARKs and confidential transactions is needed.

6. Conclusion

The centralized security paradigms of the past are ill-suited for the dynamic, distributed, and massive-scale nature of the Internet of Things. The convergence of blockchain and edge computing offers a powerful and compelling solution to a new class of security threats. The framework proposed in this paper leverages the edge to overcome the performance limitations of blockchain while using blockchain's decentralized trust model to secure IoT devices at their core. By providing immutable identity, autonomous access control, and verifiable data integrity, this synergistic approach lays a robust foundation for a more secure, resilient, and trustworthy IoT ecosystem. While significant challenges remain, particularly around scalability and standardization, the blockchain-at-the-edge model represents a crucial step towards realizing the full, secure potential of the connected world.

References

[1] Statista. "Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030." Statista Research Department, 2021.

[2] Antonakakis, M., et al. "Understanding the Mirai Botnet." *26th USENIX Security Symposium (USENIX Security 17)*, 2017.

[3] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[4] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. "Edge Computing: Vision and Challenges." *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, Oct. 2016.

[5] Buterin, V. "A Next-Generation Smart Contract and Decentralized Application Platform." *Ethereum White Paper*, 2014.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 05, IIRA 5.0 (2026)

[6] Huh, S., Cho, S., & Kim, S. "Managing IoT devices using blockchain platform." *19th International Conference on Advanced Communication Technology (ICACT)*, 2017.

[7] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. "Applications of blockchains in the Internet of Things: A comprehensive survey." *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676-1717, 2019.

[8] Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT." *IEEE Communications Magazine*, vol. 55, no. 10, pp. 78-85, 2017.

[9] Puthal, D., Mohanty, S. P., Nanda, P., & Choppali, U. "Proof-of-Authentication for Scalable and Lightweight Blockchain in Edge-of-Things (EoT) Devices." *IEEE Transactions on Big Data*, 2021.