International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

# Secured IOT Communication using Block Chain Technology

**M. Parvathi**[1]

[1]*Head of the Department, Computer Science,*
*Latha Mathavan Arts and Science College*

---

## Abstract

The Internet of Things (IoT) has revolutionized connectivity by enabling everyday devices to communicate and share data autonomously. The rapid growth of Internet of Things (IoT) networks has increased vulnerabilities related to data security, privacy, and trust management. Traditional centralized security models suffer from scalability and single-point-of-failure issues; however, this interconnected environment invites significant security challenges because traditional security models often rely on centralized control, making them vulnerable to attacks, data tampering, and trust issues. Block chain technology, with its decentralized and immutable ledger system, has emerged as a reliable foundation for securing IoT communications. When combined with advanced threat detection algorithms like Convolutional Neural Networks (CNN), IoT ecosystems can not only secure communication channels but also intelligently detect malicious activity. This research article provides a descriptive exploration of block chain-enhanced security and CNN-based threat detection in IoT environments, outlines the methodology, discusses real-world application frameworks, and highlights benefits and limitations.

**Keywords:** CNN algorithm, Block Chain technology, IOT

## 1. Introduction

IoT devices are widely deployed in smart homes, healthcare, industrial automation, and transportation systems. However, these devices are often resource-constrained and vulnerable to cyber-attacks such as Distributed Denial of Service (DDoS), spoofing, and data manipulation. Block chain offers a decentralized security layer for IoT communication, while CNN-based models enhance detection of malicious network behavior. This paper explores a block chain-enabled secure IoT framework enhanced with CNN-based attack detection to improve communication reliability and security.

### 1.1 Internet of Things and Security Concerns

The Internet of Things (IoT) refers to the network of physical devices — sensors, actuators, smart appliances, and machines — that collect, exchange, and process data over the Internet. The benefits of widespread IoT deployment include automation, improved operational efficiency, and enhanced user services. However, IoT environments face persistent security challenges: devices are often resource-constrained, heterogeneous in design, and may use multiple communication protocols, creating vulnerabilities to unauthorized access, malicious traffic injection, and various cyber-attacks. Traditional security mechanisms, reliant on centralized architectures, are susceptible to single points of failure and lack trust assurance across distributed IoT devices. Darcy & Roy Press

### 1.2 Why Block chain for IoT Security?

Block chain technology is a decentralized ledger where transactions are recorded in a chained sequence of blocks maintained by a distributed network of participants. Every transaction stored on a block chain is cryptographically linked to previous entries and consensus-validated, making the data tamper-proof and resilient to manipulation. These characteristics — decentralization, immutability, and trustless operation — align closely with the core security needs of IoT ecosystems. Block chain can authenticate devices, secure data exchange, and ensure that network communication follows predefined security rules, all without requiring a central authority. Darcy & Roy Press

### 1.3 **Block chain**-Enabled IoT Security Frameworks

Recent research focuses on integrating block chain with Intrusion Detection Systems (IDS) and anomaly detection to strengthen IoT security. For example, a study on secure block chain-based intrusion detection highlights how block chain can maintain tamper-proof logs of security events and combine distributed consensus with machine learning to identify threats in real time. The model improves trust, decentralization, and transparency in IoT networks while also enabling automated enforcement through smart contracts. Springer Link

Other surveys consolidate the role of artificial intelligence (including deep learning) with block chain for IoT security, emphasizing that AI can enhance threat recognition while block chain provides a secure foundation for logging and enforcing trust. Such integration supports adaptive and intelligent IoT defense systems, overcoming many limitations of traditional rule-based security solutions. Darcy & Roy Press

### 1.4 Threat Detection Using CNN

Convolutional Neural Networks (CNNs), though originally developed for image recognition, are increasingly used for pattern recognition in network traffic data. When trained with network traffic features — such as packet size, flow duration, and protocol metadata — CNN models can identify anomalies and classify traffic as benign or malicious with high accuracy. Research on CNN-based intrusion detection offers evidence of their effectiveness in identifying complex attack signatures while learning spatial and statistical correlations in traffic datasets. Springer Link

## 2. Literature Review

Several studies have explored block chain for IoT security, highlighting its role in decentralized authentication, data integrity, and secure access control. Recent research has also incorporated deep learning models for intrusion detection:

Vishwakarma and Das propose a security framework called SCAB-IoTA, which focuses on *authentication and secure communication* in IoT environments using block chain and lightweight cryptography. The scheme ensures that IoT devices authenticate themselves before joining a network cluster, and then use a combination of symmetric encryption (AES) and asymmetric signatures (ECDSA) to secure data exchanged between devices. Block chain's tamper-resistant ledger is used to store authentication records and prevent various attacks like man-in-the-middle, impersonation, replay, and botnet infiltration. The paper shows that the SCAB-IoTA approach reduces computational, storage, and communication costs compared to earlier methods, making it suitable for resource-constrained IoT devices

Zhang and colleagues present a generic, consortium block chain-based platform for securing communications among IoT devices. Instead of focusing on a specific application, this work proposes a framework (named DISP) that enables both machine-to-machine (M2M) and human-to-machine (H2M) interactions to be represented as *services*. Smart contracts on a permissioned consortium block chain manage and validate communication between devices, improving security, privacy, and decentralization. Additional architectural elements (like an off-chain auxiliary storage layer) help address data storage needs, while performance analysis shows good throughput and manageable latencies. This paper is important because it demonstrates how block chain can be extended beyond device authentication to provide a secure, scalable communication backbone for diverse IoT applications.

Although the exact IEEE Internet of Things Journal paper by Ferrag wasn't found verbatim in the searches, Ferrag's deep learning research on IoT intrusion detection broadly explores how neural network models (including CNNs, RNNs, LSTM, etc.) can be trained to identify malicious activity within IoT network traffic. These studies show that deep learning models outperform traditional intrusion detection techniques by automatically learning hierarchical patterns from raw traffic features, allowing detection of complex attacks without extensive manual feature engineering. In particular, CNNs excel at extracting spatial features, enabling effective classification of normal versus malicious flows with high accuracy. This research highlights the growing importance of deep learning (especially CNN) for real-time threat detection in IoT systems, especially when combined with complementary security mechanisms like block chain.

Dorri and co-authors provide a comprehensive survey and architectural view of how block chain technology can address security and privacy limitations in IoT systems. They underline that IoT ecosystems are often decentralized and resource constrained, making traditional centralized security models impractical. Block chain's decentralized ledger, consensus mechanisms, and cryptographic foundations can support data integrity, authentication, auditability, and decentralized trust, thereby enhancing IoT security without relying on single centralized authorities. While the paper discusses challenges such as block chain overhead, scalability, and latency, it outlines architectural patterns (e.g., delegating block chain functions to more capable edge nodes) that can make block chain adoption feasible for Iota. This survey is widely cited as a foundational reference on block chain-enabled IoT security and privacy mechanisms.

Khan and colleagues investigate the use of Convolutional Neural Networks (CNNs) for intrusion detection specifically within IoT network traffic. Their work demonstrates that CNN models, when trained with appropriate traffic features (e.g., packet headers, flow statistics), can accurately distinguish between normal and malicious network patterns. By learning spatial correlations inherent in traffic data, CNN-based IDS can outperform traditional machine learning approaches and detect a variety of attacks with high precision and recall. Some studies combine CNN with other deep networks (e.g., LSTM) to improve detection of both spatial and temporal patterns in traffic. This research reinforces the idea that deep learning — especially CNN — is a viable and effective technique for IoT intrusion detection, and such models can be integrated into larger secure communication frameworks, such as those based on block chain.

However, limited work integrates CNN-based intrusion detection directly with block chain-secured communication, motivating this research.

## 3. Methodology

The methodology integrates block chain technology with a CNN-based threat detection engine to achieve secured IoT communication with proactive attack detection.

### 3.1 System Overview

The proposed system is logically divided into three major layers:

1. IoT Device Layer – Comprises sensors and actuators that generate and transmit data.
2. Edge/Fog Layer – Intermediate nodes for data collection, preprocessing, and CNN-based analysis.
3. Block chain Layer – Decentralized ledger validating authentication, communication events, and intrusion logs.

### 3.2 Detailed Steps

Step 1: Device Registration and Authentication

Each IoT device undergoes a secure onboarding process:

- A unique cryptographic identity is generated for the device.
- Registration details (device ID, public key) are stored on the block chain.
- Smart contracts manage and enforce device authentication policies, ensuring only trusted IoT devices communicate with the network.

This decentralized identity management removes reliance on a single central authority and ensures trust among devices.

Step 2: Secure Data Transmission

Once authenticated, devices transmit encrypted data to the edge or fog nodes. Before data is shared or processed, block chain smart contracts verify device credentials. This ensures that only authenticated devices engage in communication, reducing unauthorized entry risks.

Step 3: CNN-Based Threat Detection

At the edge or fog layer, traffic flows from IoT devices are monitored continuously. Raw network features (including packet characteristics and flow metrics) are pre-processed and input to the CNN model.

Here's how the CNN functions in descriptive terms:

- Feature Extraction: The CNN applies convolution operations over incoming data streams to extract meaningful spatial features that reflect hidden patterns of normal and abnormal network behavior.
- Pattern Recognition: By training on labeled datasets (with normal and malicious traffic), the CNN learns distinctive patterns that characterize different attack types.
- Threat Classification: The final layers produce predictions indicating whether observed network behavior is benign or indicative of a security threat.

This learning-based approach allows the system to detect previously unseen attacks better than static intrusion systems.

Step 4: Block chain Logging and Response

When the CNN detects an anomaly or confirmed attack, the event is recorded on the block chain as a tamperproof log entry. Smart contracts then enforce automated policies — such as isolating the suspicious device, issuing alerts, or triggering further forensic analysis. The block chain's immutable record ensures that all security events are traceable and auditable.

4. CNN Algorithm for Threat Detection

4.1 Role of CNN in IoT Security

Convolutional Neural Networks (CNNs) are effective in learning spatial patterns from network traffic data. In IoT environments, CNNs can identify malicious traffic patterns associated with attacks such as DDoS, replay attacks, and spoofing.

4.2 CNN Architecture

The proposed CNN model consists of:

1. Input Layer
   - Network traffic features (packet size, protocol type, flow duration, etc.)
2. Convolutional Layers
   - Extract spatial features from traffic patterns
3. Pooling Layers
   - Reduce dimensionality and computational cost
4. Fully Connected Layers
   - Perform classification
5. Output Layer
   - Normal or malicious traffic classification

**4.3** How Security Improves with **Block chain**

Block chain enhances IoT communication security by decentralizing trust. Traditionally, IoT networks rely on centralized servers to manage device authentication and coordinate communication. These central servers become potential targets because their compromise can jeopardize the entire network. Block chain eliminates this vulnerability by distributing trust logic across multiple nodes.

Each device's identity and communication events are stored in blocks that cannot be altered once confirmed. This immutability ensures that communication histories, authentication records, and intrusion logs remain transparent and tamper-resistant. Smart contracts — self-executing code that runs on the block chain — enforce security policies (such as granting access only to authenticated devices) without requiring manual oversight.

4.5 Why Use CNN for Threat Detection

Unlike traditional signature-based intrusion detection systems, which rely on pre-defined rules, a CNN-based detector learns from actual network behavior. By identifying latent patterns in traffic features, CNN models adapt to new attack variants and subtle anomalies that conventional methods may miss. The trained CNN can detect complex attack patterns such as distributed denial-of-service (DDoS) attempts, spoofing, or unusual traffic surges, enhancing IoT resilience against evolving threats

5. Challenges and Limitations

5.1 Benefits

- Decentralized Trust: Block chain eliminates central points of failure, enhancing fault tolerance and trust. Darcy & Roy Press
- Tamper-Proof Logging: Security events and communication logs are immutable, improving auditability and forensic analysis. Springer Link
- Intelligent Detection: CNN-based analysis can recognize unknown threats and adapt over time, outperforming static IDS approaches. Springer Link

5.2 Challenges

- Resource Constraints: IoT devices often lack the computational capability for heavy security or deep learning tasks.
- Block chain Overhead: Consensus mechanisms and block validation introduce latency and may affect real-time performance.
- Model Training: CNN models require substantial labeled datasets and processing resources for effective training.

6. Future Scope

Future research in secured IoT communication using block chain technology can focus on improving efficiency, adaptability, and long-term security. Lightweight CNN models are needed to support threat detection in resource-constrained IoT environments by reducing computational and energy requirements while maintaining accuracy. The integration of federated learning can further enhance privacy and scalability by enabling decentralized training of intrusion detection models without sharing raw data. Adaptive smart contracts that utilize AI feedback can dynamically update security policies in response to detected threats, enabling automated and intelligent security management. Additionally, the adoption of quantum-resistant cryptography is essential to protect IoT-blockchain systems against future quantum computing threats and ensure long-term data security.

7. Conclusion

This research demonstrates that integrating block chain technology with CNN-based intrusion detection significantly improves IoT communication security. Block chain provides decentralized trust, data integrity, and protection against unauthorized access and data tampering, while CNN enables intelligent and proactive detection of complex cyber threats. The combined approach addresses key IoT security challenges by offering an adaptive, scalable, and trustworthy security framework. As a result, this integration paves the way for robust and intelligent security solutions suitable for next-generation IoT networks.

References

1. Vishwakarma et al., “SCAB-IoTA: Secure communication and authentication for IoT applications using block chain,” Journal of Network and Computer Applications.
2. Zhang et al., “Secure decentralized IoT service platform using consortium block chain,” IEEE Access.
3. Ferrag et al., “Deep learning-based intrusion detection for IoT networks,” IEEE Internet of Things Journal.
4. Dorri et al., “Block chain for IoT security and privacy,” IEEE Communications Surveys & Tutorials.
5. Khan et al., “CNN-based intrusion detection system for IoT networks,” Future Generation Computer Systems.