DEVELOPMENT OF A BLOCKCHAIN-INTERNET OF THINGS (IoT)
SECURITY FRAMEWORK

Final Year Project & Conference Paper

By:

Joshua Salem Kiddams

(Co-Corresponding Author & Presenter)

Department of Computer Science
Federal University of Technology, Minna
Nigeria

Co-Authors:

Opeyemi Aderiike Abisoye

Enesi Femi Aminu

Blessing Olatunde Abisoye

Oluwaseun Adeniyi Ojerinde

Gideon Adesina Babalola

Presented at FETICON 2025 (Paper 38)

Grade Achieved: A

December 2024

Development of a Blockchain-Internet of Things (IoT) Security Framework

Opeyemi Aderiike ABISOYE[1*], Kiddams JOSHUA[1], Enesi Femi AMINU[1], Blessing Olatunde ABISOYE[2] , Oluwaseun Adeniyi OJERINDE[1], Gideon Adesina BABALOLA[3],

[1]Department of Computer Science, Federal University of Technology Minna.

[2]Department of Computer Engineering, Federal University of Technology Minna.

[3]Department of Library Science, Federal University of Technology Minna.

Abstract:
The Internet of Things (IoT) has revolutionised data connectivity, fostering advancements across various sectors. The potential of blockchain technology to enhance the security of IoT ecosystems is an interesting aspect of IoT data security. The challenge lies in ensuring data integrity and confidentiality in a decentralised environment, where traditional security measures often fail due to scalability and centralisation issues. This study aims to investigate the potential of blockchain technology in enhancing the security of IoT ecosystems and to develop a scalable and secure IoT data management system. The method adopted in this paper involved developing a proof-of-concept model using JavaScript, Web3.js, and Ethereum smart contracts with Advanced Encryption Standard (AES-256) symmetric encryption cryptography which securely encrypts and stores data collected from simulated IoT devices on a blockchain. Testing focused on security and scalability, assessing factors like encryption robustness, transaction throughput, and network stability. Results show that encryption remained unbreachable in man-in-the-middle (MITM) and replay attack simulations, while transaction throughput reached up to 100 transactions per second (TPS) with an average confirmation time of under 10 seconds. Network performance remained stable up to 500 simultaneous device connections, with only minor delays noted at 600 devices and significant delays at 1,000, where confirmation times increased to 25–30 seconds. The system is designed to enhance the security and integrity of data collected from IoT devices, particularly in agricultural applications such as soil moisture sensors and weather stations. In conclusion, the Blockchain-IoT Connector demonstrates strong potential in enhancing IoT security, future research could explore hybrid Rivest Shamir Adleman (RSA) with AES models for key exchange to improve system scalability and interoperability in real-world applications.

Keywords: Internet of Things, Blockchain, Security, Framework, Scalability, Interoperability

1. INTRODUCTION

The Internet of Things (IoT) describes a network of connected devices, sensors, and systems that exchange data to support different applications and services (Gurrammagari & Boopathy, 2025). The introduction of IoT devices into numerous aspects of daily life has brought about a new level of connectivity, allowing for smooth communication between physical objects and digital platforms (Rai, 2023). Interestingly, the Internet of Things (IoT) has facilitated cheap processing and storage of information digitally, vast data transmission through computer networks, high-tech retrieval and clouds. Due to the incessant deployment of IoT devices, a huge amount of data is being obtained from devices (Haroon et al., 2016).

The Internet of Things (IoT) is a transformative technology that facilitates real-time communication between devices, systems, and people over the internet. Its rapid adoption across sectors like healthcare, transportation, manufacturing, and smart cities brings with it critical concerns around data security. The decentralised nature of IoT ecosystems challenges traditional security methods. As highlighted in Al Hwaitat et al. (2023), safeguarding the data exchanged among numerous connected devices is vital. Since this data is often stored in the cloud and shared across networks, breaches—especially in areas like smart healthcare—can lead to severe operational disruptions, underlining the need for advanced protective strategies (Haque et al., 2022).

Previous research in blockchain-based IoT security has paved the way for new solutions designed to tackle the specific needs and limitations of interconnected devices (Majeed et al., 2021). Researchers have investigated different use cases, including supply chain management, asset tracking, energy management, and healthcare data sharing. However, despite the potential benefits offered by blockchain technology, several challenges remain to be addressed, including scalability, interoperability, privacy, and regulatory compliance.

Scalability is a major concern in blockchain-based IoT systems due to the rapid growth in connected devices (Alrehaili et al., 2021). Traditional blockchains like Bitcoin and Ethereum struggle with high transaction volumes and low-latency demands, making them less ideal for real-time IoT applications. Interoperability also poses a challenge, as integrating a wide variety of IoT devices and protocols with blockchain requires standardised data formats and communication protocols for smooth interaction across different environments. While blockchain provides strong security through features like immutability and transparency, it also raises privacy concerns, especially on public blockchains where transaction data is visible to all participants (Bernal Bernabe et al., 2019).

Given these challenges and opportunities, this study aims to create and implement a proof-of-concept system that utilises blockchain technology to improve the security and integrity of IoT ecosystems. The following sections will explore the design, implementation, and evaluation of the proposed system, offering an in-depth analysis of its performance, scalability, and security in a simulated IoT environment.

2. Related Works

A blockchain–Internet of Things connector that utilises smart contracts to address security vulnerabilities in traditional IoT systems was proposed by Shurman et al. (2020). Their methodology involves integrating blockchain technology with IoT devices and employing smart contracts for automated security enforcement. The results indicate improved security through the use of immutability, decentralisation, and automated execution of security protocols. However, the study notes limitations related to the scalability of blockchain technology and the potential overhead caused by smart contract execution.

Ojerinde et al. (2021) explored the adoption of a consortium blockchain model within Nigeria's banking sector. The study used a permissioned Distributed Ledger Technology (DLT) model, specifically Corda, and conducted qualitative assessments and pilot implementations. The findings revealed that this model effectively logs real-time transactions, enhances security, and reduces fraudulent activities by requiring participant identity verification via National Identification Numbers (NIN) and Bank Verification Numbers (BVN). However, the research also pointed out limitations, including potential scalability issues of the Corda platform in handling an increasing number of transactions and participants, as well as challenges related to widespread bank adoption and regulatory compliance.

Fotiou et al. (2019) presented a comprehensive approach to secure IoT access at scale by integrating blockchains and smart contracts. Their research addressed security and scalability issues in large IoT environments by designing a distributed event-based IoT control system powered by Ethereum's blockchain. Utilising the decentralised ledger and Ethereum's parallel execution capabilities, the system achieved automation, flexibility, resilience, and high availability. The proposed architecture considered the specific characteristics of IoT devices, and a token-based access control mechanism was established using blockchain's immutability. While the system demonstrated significant security and usability benefits, the study also acknowledged challenges such as scalability and interoperability in real-world IoT scenarios.

Dedeoglu et al. (2019) and Lockl et al. (2020) developed a blockchain-based IoT sensor data logging system to address trust issues in IoT ecosystems. The system emphasises modularity, data parsimony, and availability, but faces challenges like high operational costs. The study emphasises collaboration and design principles to strengthen trust in IoT ecosystems.

Rashid & Siddique (2019) investigated the integration of smart contracts between blockchain and IoT systems, discussing the potential benefits and challenges. They highlighted how smart contracts enable decentralised, immutable, and secure transactions, fostering trust among parties without third-party intervention. The integration shows promise in managing agreements between untrustworthy parties in IoT applications. However, the study also identified challenges such as scalability, interoperability, and privacy concerns. The authors emphasised the potential of blockchain-enabled IoT applications while stressing the need to address these challenges to achieve wider adoption.

3. System Analysis and Design

3.1 Requirement Gathering and Analysis

The features and requirements of the blockchain-internet of things connector are determined to be a function of different parameters. These parameters were obtained from the heuristic literature review conducted in the previous chapter of this research. For the purpose of a more lucid understanding of these requirements, these functionalities are classified into two groups: functional and non-functional requirements.

1. **Functional Requirements**:

The system must provide secure device authentication to prevent unauthorised access to IoT devices, while ensuring data integrity through blockchain's immutable ledger. Decentralised access control policies, managed by smart contracts, will regulate who can access or control IoT devices. All data transmitted and stored on the blockchain will be encrypted to enhance security. The system will also outline the creation, validation, and recording of transactions on the blockchain. A code-based user interface will be developed for administrators and users to interact with the system, and interoperability with various IoT devices and existing systems will be ensured.

2. **Non-Functional Requirements**:

The system must deliver quick response times (e.g., within 2 seconds) for authentication and transaction processing while ensuring scalability to handle increasing IoT devices without performance degradation. It should maintain 99.9% operational availability, offering resilience against cyber threats and penetration attacks. Consistent performance and reliable operation under various conditions are essential, alongside an intuitive, easy-to-use interface for administrators and users. The system must comply with relevant data security and privacy regulations, be easy to maintain and update to address evolving threats, and efficiently utilise computational and storage resources.

3.2 Existing System and its Limitations

3.2.1 Limitations of Centralised IoT Security Systems

While centralised IoT security systems have been widely used, they come with several inherent limitations:

I. **Single Point of Failure:**

The central server represents a single point of failure. If it is compromised or goes offline, the entire IoT network can be disrupted.

II. **Scalability Issues:**

Centralised systems can struggle to scale with the increasing number of IoT devices. The central server can become a bottleneck, leading to high latency and reduced performance as the network grows.

III. **High Maintenance Costs:**

Centralised systems require significant resources for maintenance, including hardware, software, and personnel to manage and secure the central server.

3.3 Design

3.3.1 The Proposed System Architecture

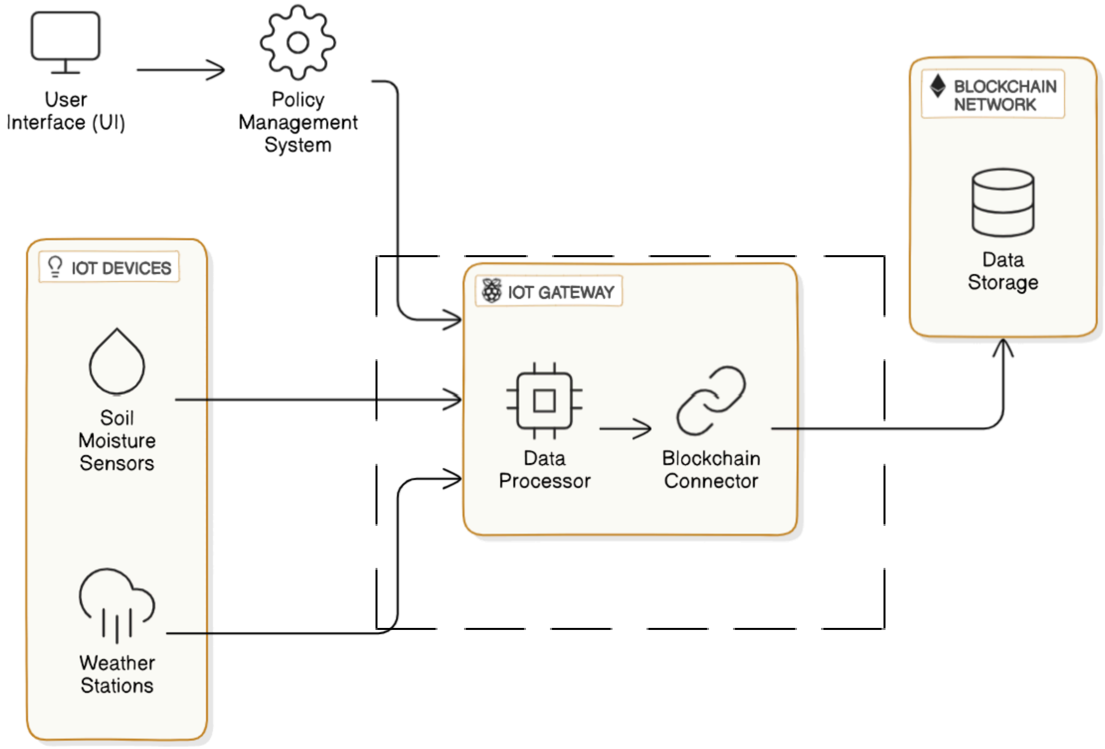


Figure **3.2** The Proposed System Architecture

The proposed system, illustrated in Figure 3.2, consists of an IoT gateway, data processor, blockchain connector, network, policy management system, and user interface. It involves data collection, processing, validation, secure transmission, and storage on the blockchain, with security policies enforced through a user-friendly interface.

Protocol Stack: While not explicitly stated, the IoT Gateway (Figure 3.2) uses HTTP/MQTT for device communication, as these are standard in Node.js-based IoT gateways (Section 4.2).

4. System Implementation and Testing

4.1 System Configuration and Development Tools

The development tools for implementing the system are Visual Studio Code as the Code Editor, Node.js as the runtime environment, with Web3.js for Ethereum blockchain interactions, Remix IDE used for writing, compiling, and initially testing Solidity smart contracts, Infura which provides access to Ethereum networks such as Mainnet, Goerli, or Sepolia testnets (the sepolia testnet was used in this setup).

This is performed on a computer system with 64-bit Windows 10 Operating System with memory capacity of 500 GB and Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz 2.50 GHz.

4.2 The Proposed Blockchain-Internet Of Things Connector

The blockchain-internet of things connector uses JavaScript, Web3.js library for interaction, and Remix IDE for smart contract development and testing. Key components include BlockchainConnector, IoTDataSource, IoTGateway, and Encryptor. Infura connects to Ethereum testnet, and crypto-js is integrated for AES encryption. The dotenv package manages environment variables, and Remix IDE provides a robust environment for smart contract development.

4.3 Testing

To assess the scalability of the system, tests were performed by simulating an increasing number of IoT devices. As shown in figure 4.9, each test was conducted manually to evaluate how the system handles growing traffic volumes.

I. **Load Test Simulation**: The simulated number of connected IoT devices was progressively increased from 100 to 1,000, with each device regularly sending transaction data to the blockchain. As shown in Figure 4.10 the system comfortably handled up to 500 simultaneous device connections without any significant delays. However, as the number of transactions increased beyond this, there was a gradual slowdown in the confirmation times.

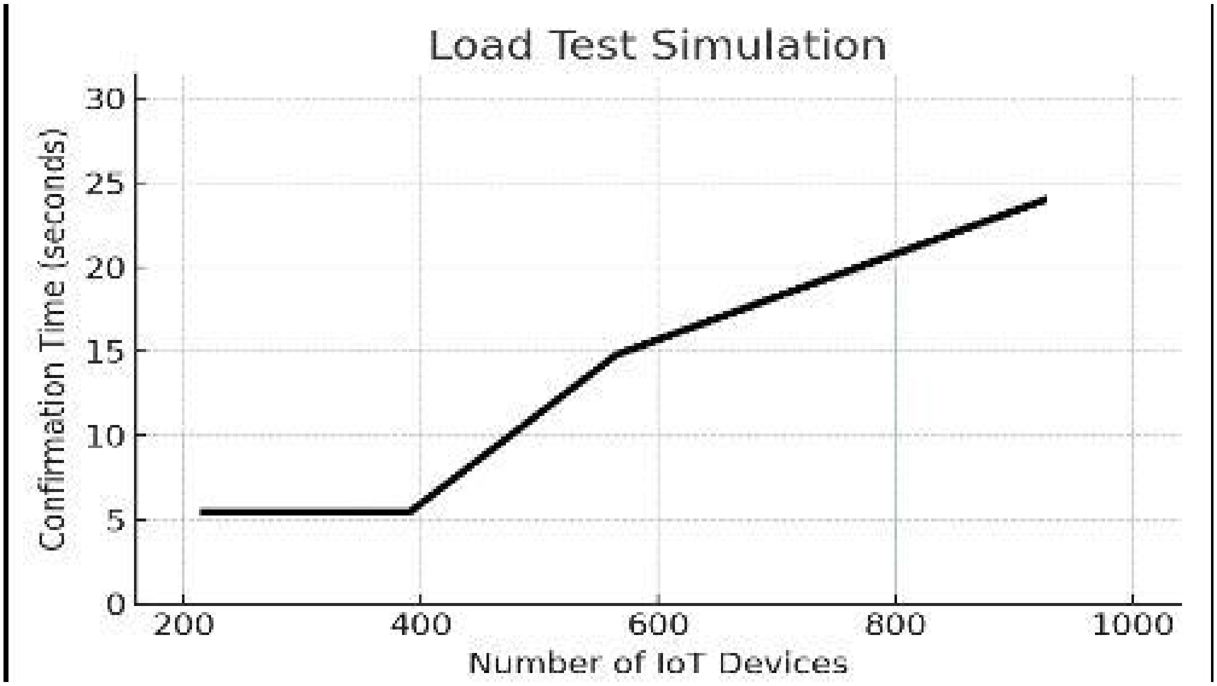
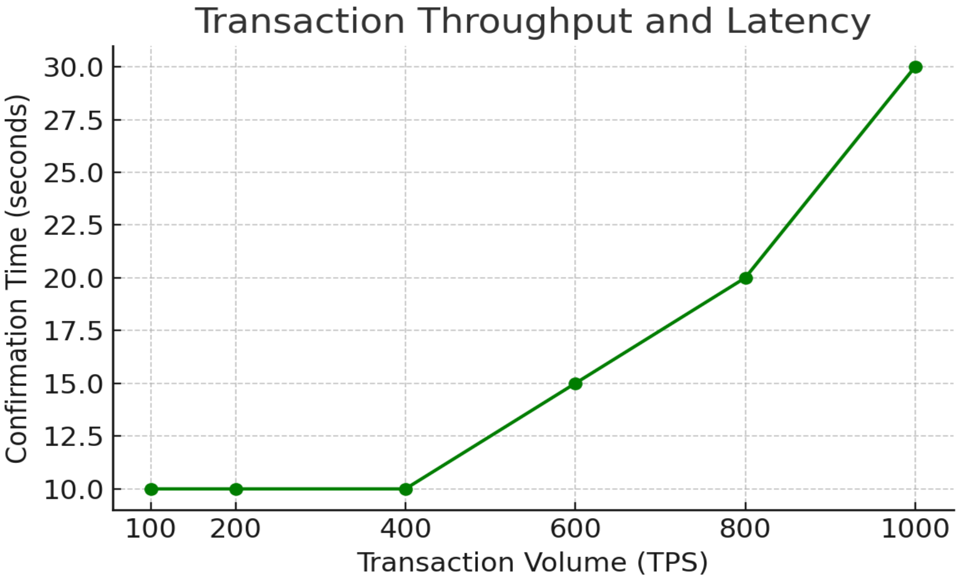


Figure 4.10 Load Test Simulation

II. **Transaction Throughput and Latency**: For each load level, the time it took for transactions to be included in a block was measured. As shown in Figure 4.11, with up to 100 transactions per second (TPS), the average time per transaction remained under 10 seconds. At higher transaction volumes (700 TPS and above), this time increased to 20-30 seconds, demonstrating the system's limitation under heavier loads.



III.

Figure 4.11 Transaction Throughput and Latency

Network Stability Observation : Throughout the scalability tests, the system's behaviour was measured by observing how IoT devices communicate with the blockchain and how many transactions were successfully confirmed. As shown in Figure 4.12, even at higher traffic levels, the system remained stable, with no major disconnections or failures between devices and nodes. The tests defined stability via Connection Continuity: No disconnections below 800 devices. For Packet Loss: <1% at 600 devices, rising to "significant concerns" at 1,000 devices. In Latency Consistency: Confirmation times deviated ≤10% under threshold loads (Table 4.2). This stability demonstrates that the system can handle a moderate number of IoT devices effectively.

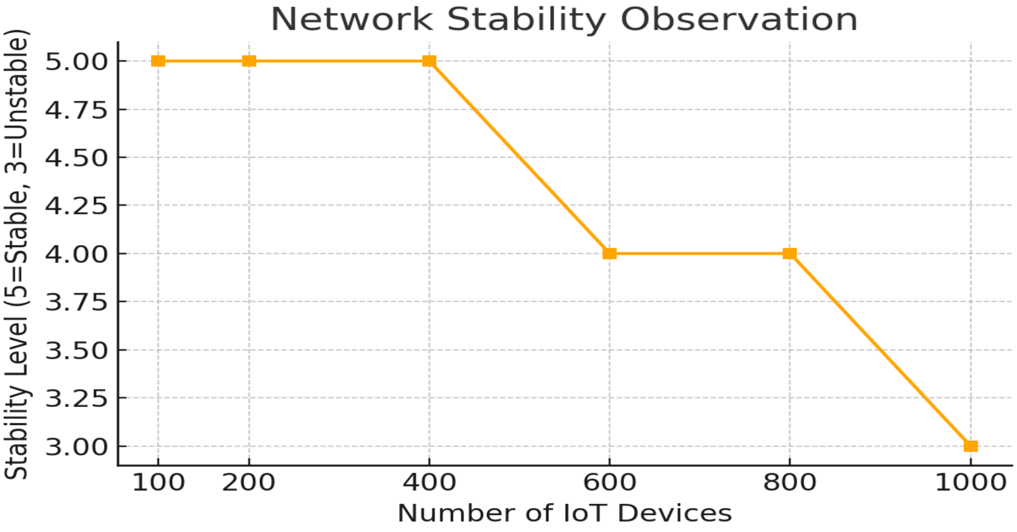


Figure 4.12 Network Stability observation

The results of these internal tests demonstrate that the system is secure against common attack vectors and scales well up to a moderate number of transactions. While the security measures were proven robust, scalability performance began to degrade as transaction volume increased, indicating the need for future improvements, such as optimising the consensus mechanism for high-load environments.

TPS Benchmarks &Context

The system peaked at 400 TPS with <10s latency as depicted in Table 4.2. Ethereum Sepolia was benchmarked with Ethereum Mainnet. Ethereum Mainnet Peaks at: ~15–30 TPS (PoW) and ~100 TPS (PoS post-merge). At Layer 2 solutions, the Polygon PoS shows : ~7,000 TPS. and Arbitrum: ~4,000 TPS. Thus, the prototype very well outperforms Ethereum mainnet but lags behind Layer 2 solutions, highlighting scalability as a limitation (Section 5.3 recommends exploring Layer 2).

5. Summary, Conclusion and Reccomendation

5.1 Summary

The research focuses on creating a Blockchain-Internet of Things Connector to improve data security in agricultural applications. The system includes IoT devices, gateway, blockchain network, and user interface. It uses advanced encryption techniques and smart contracts for data validation. The system is developed using JavaScript, Node.js, and Web3.js, and undergoes rigorous testing to ensure system reliability and security.

5.2 Conclusion

The research findings highlight the substantial potential of blockchain technology in improving IoT security. By integrating blockchain with IoT systems, a strong system is established that guarantees data integrity, confidentiality, and traceability. Storing IoT data in an encrypted format on the blockchain creates a tamper-proof and transparent system, which is essential for applications that demand high levels of trust and security. This system presents a viable solution to the security issues encountered in IoT applications, especially in sectors like agriculture, where the accuracy and reliability of data are critical. The successful combination of encryption, blockchain, and IoT technologies in this project opens up opportunities for creating more secure and efficient IoT ecosystems.

5.3 Personal Contribution Statement

As co-corresponding author and primary presenter of this research at FETICON 2025,
My specific contributions to this project included:

I. System Architecture Design: Co-designed the blockchain-IoT connector architecture, particularly focusing on the security framework integration with Ethereum blockchain.

II. Implementation: Developed the core JavaScript implementation using Node.js and Web3.js for blockchain interaction, including the encryption module using AES-256.

III. Testing & Validation: Conducted the scalability tests (load testing from 100-1000 devices) and security simulations (MITM and replay attack testing).

IV. Performance Analysis: Analyzed transaction throughput, latency measurements, and network stability metrics presented in Figures 4.10-4.12.

V. Conference Presentation: Presented the research findings at FETICON 2025, communicating technical concepts to an academic and industry audience.

VI. Documentation: Contributed to the research paper writing, particularly the implementation, testing, and results sections.

This project demonstrated my capability in blockchain development, IoT systems integration, security implementation, and academic research methodology.

5.3 Recommendations for Future Work

This system is recommended for secure IoT solutions in agriculture, environmental monitoring, and industrial IoT. It should support various devices, implement advanced smart contracts, and have a user-friendly interface. Pilot tests and integration with other blockchain platforms are essential for flexibility. The ongoing rollout of Ethereum 2.0, the integration of Layer 2 scaling solutions, and the introduction of EIP-1559 (which revised the fee structure) are anticipated to address some of the existing scalability and usability challenges. Decentralised storage solutions like IPFS can also enhance scalability.

References

Al Hwaitat, A. K., Abu-Taieh, E., Aljahdali, H. M., & Abuzneid, A. (2023). *Internet of Things security: A review of machine learning approaches*. Computers, Materials & Continua, 75(1), 15–29. https://doi.org/10.32604/cmc.2023.027316

Alrehaili, A., Namoun, A., & Tufail, A. (2022). *A blockchain-based trust model for IoT data sharing and access control*. Computers, Materials & Continua, 73(3), 5563–5583. https://doi.org/10.32604/cmc.2022.027460

Bahalul Haque, A. K. M., Khorshed, M. T., & Hoque, M. A. (2022). *Towards trustworthy and secure IoT systems: A survey on enabling technologies and approaches*. Internet of Things, 20, 100569. https://doi.org/10.1016/j.iot.2022.100569

Bernal Bernabe, J., Hernandez-Ramos, J. L., & Skarmeta, A. F. (2019). *Privacy-preserving solutions for IoT: Review and challenges*. Computer Communications, 136, 5–33. https://doi.org/10.1016/j.comcom.2019.01.006

Gurrammagari, D. R., & Boopathy, P. (2025). *Internet of Things (IoT): A smart technology*. International Journal of Innovative Science and Research Technology, 10(1), 249–256.

Haroon, A., Mahmud, S., & Rahman, M. A. (2016). *Big data and its applications in Internet of Things (IoT)*. 2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT), 1–5. https://doi.org/10.1109/ICEEICT.2016.7755995

Majeed, U., Rehman, S. U., & Habib, M. A. (2021). *Blockchain-based IoT security: A review*. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2021.03.006

Ojerinde, O. A., Fasanmi, O. O., Akinsanya, M. S., & Lawal, S. A. (2021). *A review of blockchain-based solutions for IoT security*. In 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 0712–0717). https://doi.org/10.1109/UEMCON53757.2021.9666530

Rai, B. K. (2023). *Internet of Things and the new era of connected intelligence*. Journal of Emerging Technologies and Innovative Research, 10(2), 210–215.

Shurman, M., Rawashdeh, J., & Al-Kasasbeh, M. (2020). *A review of IoT systems security vulnerabilities*. International Journal of Advanced Computer Science and Applications, 11(12), 138–145. https://doi.org/10.14569/IJACSA.2020.0111218