International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 03 | Mar 2026 www.irjet.net p-ISSN: 2395-0072

Securing IoT Data Using Block Chain Technology

Dr.M.VINAYA BABU[1], J.Shivraj[2], J.Sudheer[3], K.Mahesh[4]

[1] Associate Professor, Department of Computer Science and Engineering
[2,3,4] B.Tech Students, Department of Computer Science and Engineering
Teegala Krishna Reddy Engineering College , Telangana, India

Abstract - *The rapid growth of the Internet of Things (IoT) has enabled real-time monitoring systems across various industries such as healthcare, logistics, and manufacturing. However, traditional IoT-based monitoring systems often rely on centralized databases, which are vulnerable to data manipulation, security breaches, and system failures. To address these challenges, this project proposes a secure temperature monitoring system that integrates IoT technology with blockchain to ensure data integrity, transparency, and reliability. In the proposed system, IoT devices continuously collect temperature data from the environment and transmit it to the system through a network connection. The collected data is then encrypted and converted into hash form before being stored on the blockchain. Due to the decentralized and immutable nature of blockchain, once the data is recorded it cannot be altered, ensuring tamper-proof storage and trustworthy records. The system also provides user registration and authentication mechanisms, allowing only authorized users to access real-time and historical temperature data. Administrators can monitor transaction logs, manage users, and verify stored data through hash validation. This integration of IoT and blockchain improves security, reliability, and transparency in data monitoring systems. The proposed solution is scalable and can be effectively applied in environments where maintaining accurate and secure environmental data is critical.*

***Key Words*: Internet of Things (IoT), Blockchain Technology, Data Security, Temperature Monitoring System, Hash Encryption, Decentralized Storage, Real-Time Monitoring.**

1.INTRODUCTION

The Internet of Things (IoT) refers to a network of interconnected physical devices that collect and exchange data through the internet. IoT technology enables real-time monitoring and automation in various sectors such as healthcare, logistics, agriculture, and manufacturing. Sensors and smart devices continuously gather environmental information such as temperature, humidity, and pressure to support efficient decision-making. However, as the number of IoT devices increases, ensuring the security and reliability of the collected data becomes a significant challenge. Traditional IoT systems often rely on centralized servers for storing and managing data, which creates risks related to data tampering, unauthorized access, and system failures [3].

Despite the advantages of IoT systems, they face several security challenges due to their distributed nature and large number of connected devices. Centralized storage systems are vulnerable to cyberattacks, data manipulation, and single points of failure. Attackers may intercept or modify the data transmitted from IoT devices, leading to inaccurate monitoring results and compromised system reliability. In applications such as temperature monitoring in healthcare or logistics, inaccurate data may lead to serious consequences. Therefore, ensuring data integrity, transparency, and secure storage is essential for the effective operation of IoT-based monitoring systems [4].

Blockchain technology is a decentralized and distributed digital ledger that records transactions securely across multiple nodes. Once information is recorded in a blockchain, it becomes extremely difficult to modify or delete, ensuring data immutability and transparency. Each block contains a cryptographic hash of the previous block, which links all blocks together and maintains the integrity of the entire system. Blockchain eliminates the need for centralized authorities and provides secure data sharing among multiple participants in the network. Due to these properties, blockchain has gained significant attention for improving security in IoT systems [1]. Integrating blockchain with IoT provides a reliable solution for addressing security issues in IoT networks. Blockchain ensures that data generated by IoT devices is securely recorded and cannot be altered once stored. By encrypting and storing IoT data in the form of hash values on the blockchain, the system ensures transparency, authenticity, and tamper-proof storage. This integration allows authorized users to verify the stored data and maintain trust in the monitoring system. Many recent studies have highlighted the benefits of combining IoT and blockchain technologies for secure data management and decentralized monitoring systems [6].

2. PROPOSED SYSTEM

The proposed system aims to provide a secure and reliable temperature monitoring platform by integrating Internet of Things (IoT) devices with blockchain technology. The system collects temperature data using IoT sensors and stores it securely in a blockchain network to ensure data integrity, transparency, and protection against tampering. Unlike traditional centralized systems, the proposed approach uses decentralized storage where data cannot be easily modified or deleted. The architecture consists of multiple components

including IoT devices, encryption mechanisms, blockchain storage, and user access modules. Initially, users register and log in to the system to gain authorized access, after which IoT devices continuously collect temperature data from the environment and transmit it to the system. The collected data is processed and encrypted using hashing techniques, converting it into a secure hash value before being stored in the blockchain network. Blockchain acts as a secure storage layer that ensures immutability, where each data record is stored as a block linked with previous blocks using cryptographic hashes, making the data tamper-proof and transparent. The system provides a user-friendly interface that allows authorized users to monitor real-time temperature readings as well as access historical data for analysis. Additionally, a verification mechanism is implemented where stored hash values are compared with newly generated hashes to ensure data integrity and detect any unauthorized modifications. The integration of IoT and blockchain enhances system reliability by enabling continuous monitoring, secure data storage, and transparent data access. Overall, the proposed system offers significant advantages such as improved security, real-time monitoring, data integrity, transparency, and scalability, making it suitable for applications in healthcare, logistics, and industrial environments where accurate and secure environmental monitoring is essential.

3. IMPLEMENTATION DETAILS

The implementation of the proposed system involves the integration of IoT devices, data encryption techniques, blockchain storage, and a web-based interface to ensure secure temperature monitoring and data management. The system is designed to collect temperature data from IoT sensors, process it securely, and store it in a blockchain network where it can be accessed and verified by authorized users. It is developed using a combination of hardware and software technologies, including Python as the programming language, Django as the web framework, and HTML, CSS, and JavaScript for the frontend interface. A temperature sensor connected to a microcontroller is used as the IoT device to continuously measure environmental temperature and transmit the data to the system through an internet connection. Once the data is received, it is processed and converted into a secure format using a hashing algorithm, which generates a unique hash value for each data record, ensuring data integrity and preventing tampering. The processed data, along with its hash value and timestamp, is then stored in a blockchain network where each block is linked to the previous one using cryptographic hashing, ensuring immutability and transparency. The system also includes a user-friendly web interface that allows users to register, log in, and monitor real-time as well as historical temperature data, while administrators can manage users, monitor system activity, and access transaction logs. Additionally, a data verification mechanism is implemented to compare stored hash values with newly generated hashes, enabling the detection of any unauthorized modifications and ensuring the reliability of the stored data. Overall, the implementation ensures secure data collection, efficient processing, and trustworthy storage, making the system robust and suitable for real-time monitoring applications.

4. RESULTS AND PERFORMANCE ANALYSIS

The proposed system was implemented to evaluate the effectiveness of integrating IoT devices with blockchain technology for secure temperature data monitoring and storage. The system provides a web-based interface where users can register, log in, monitor IoT device data, and verify stored data using blockchain-based hash validation. The results demonstrate that the system successfully provides secure data storage, real-time monitoring, and reliable verification mechanisms.

4.1 User Profile Management

The system allows users to securely manage their personal information through the User Profile module. After successful login, users can access their profile details, including their name and email information. This feature ensures that only authenticated users can interact with the system and access IoT monitoring services.

The profile interface provides a simple and user-friendly layout for managing account settings.

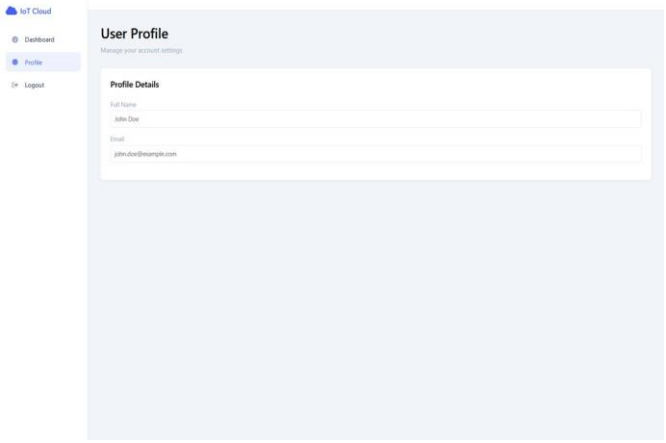

Fig - 4.1: User Profile Interface

4.2 IoT Device Monitoring Dashboard

The dashboard provides an overview of all connected IoT devices in the system. It displays important parameters such as device connections, system load, node ID, device status, type, and value. This information allows users and administrators to monitor device activity in real time. Through this dashboard, users can easily track the operational status of IoT devices and identify whether the devices are active or inactive.

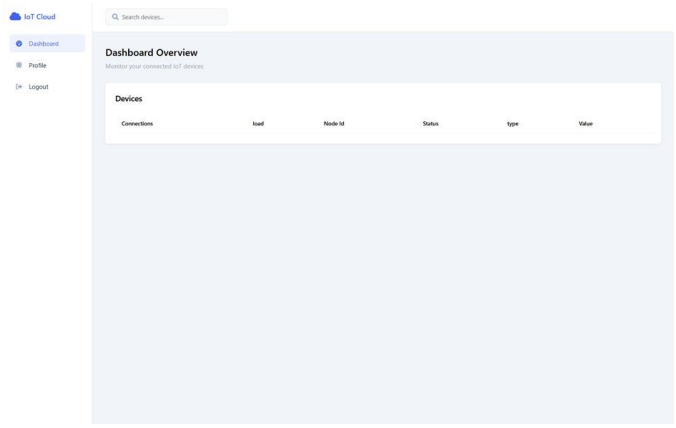

Fig - 4.2: IoT Device Monitoring Dashboard

4.3 IoT Device Data Visualization

The system displays IoT device data in a structured table format that allows users to view device-related information clearly. Each device entry includes metrics such as load value, node identifier, operational status, and device type. The system also shows the generated hash value, which represents the encrypted data stored in the blockchain.

This visualization helps users understand how device data is processed and stored securely.

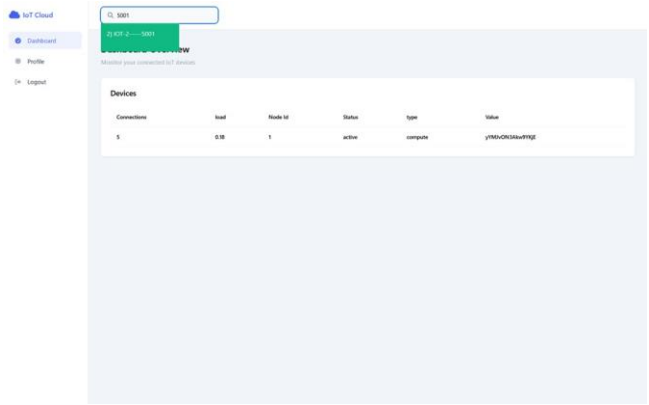

Fig - 4.3: IoT Device Data Table with Hash Value

4.4 Data Security and Integrity Verification

The implemented system successfully demonstrates how hash-based encryption combined with blockchain storage ensures data integrity. Every IoT data record is converted into a hash value before being stored. The blockchain structure ensures that once the data is recorded, it cannot be altered or deleted.

The verification mechanism compares stored hash values with newly generated hashes to confirm that the data has not been tampered with. This improves trust and reliability in the monitoring system.

4.5 System Performance Evaluation

The performance of the proposed system was evaluated based on the following criteria:

Parameter	Result
Data Security	High (Blockchain-based storage)
Data Integrity	Ensured through hash verification
Real-Time Monitoring	Successfully implemented
System Reliability	Improved due to decentralized storage
User Accessibility	Secure login-based access

The evaluation results indicate that the system effectively improves data security, transparency, and reliability compared to traditional centralized monitoring systems.

5. CONCLUSIONS

This project presented a secure temperature monitoring system by integrating Internet of Things (IoT) devices with blockchain technology. The system was designed to address the limitations of traditional centralized monitoring systems, which are vulnerable to data manipulation, security breaches, and system failures. By using IoT sensors, the system continuously collects temperature data and processes it in real time. The collected data is then encrypted using hashing techniques and stored securely in a blockchain network.

The use of blockchain ensures that the stored data is immutable, transparent, and tamper-proof, thereby improving trust and reliability in the monitoring system. The developed web-based interface allows users to register, log in, and access real-time as well as historical temperature data. Administrators can monitor system activities, manage users, and verify stored data through hash validation. The results demonstrate that integrating IoT with blockchain significantly enhances data security, integrity, and accessibility. Therefore, the proposed system can be effectively applied in industries such as healthcare, logistics, and manufacturing where accurate and secure environmental monitoring is essential.

6. FUTURE WORK

Although the proposed system successfully provides secure temperature monitoring using IoT and blockchain technologies, there are several areas where further improvements can be made. In the future, the system can be enhanced by integrating additional environmental sensors such as humidity, pressure, and gas sensors to support broader monitoring applications.

Another possible improvement is the implementation of advanced blockchain frameworks and smart contracts to automate data validation and access control processes. This would further increase system efficiency and security. The system can also be extended to support mobile applications that allow users to monitor IoT device data remotely through smartphones.

Additionally, future research can focus on improving system scalability to handle a large number of IoT devices and high volumes of data. Machine learning techniques can also be integrated to analyze temperature patterns and predict anomalies automatically. These enhancements will make the system more intelligent, scalable, and suitable for real-world industrial applications.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.

[4] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1–10, 2017.

[5] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," IEEE/ACS International Conference on Computer Systems and Applications, pp. 1–6, 2016.

[6] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979–33001, 2018.

[7] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT: Challenges and Opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[8] W. Viriyasitavat, D. Hoonsopon, and M. Niyato, "Blockchain-based Business Process Management (BPM) Framework for Service Composition in Industry 4.0," Journal of Network and Computer Applications, vol. 111, pp. 14–24, 2018.