JOURNAL ON COMMUNICATIONS

ISSN:1000-436X

Scopus®

REGISTERED

www.jocs.review

SECURE IOT DATA MONITORING USING BLOCKCHAIN

M.Raja[1],M.Ishaaq[2],M S.Padmasharan[3],S.Sasithar[4]

[1,2] Assistant Professor, Department of Electrical and Electronics Engineering, Paavai Engineering College, Namakkal, Tamilnadu, India.

[3,4,5]UG Students Department of Electrical and Electronics Engineering, Paavai Engineering College, Namakkal, Tamilnadu, India.

ABSTRACT:

The rapid advancement of Internet of Things (IoT) technology has enabled intelligent monitoring systems capable of collecting and transmitting real-time data from physical environments. IoT-based monitoring systems are widely used in renewable energy applications, industrial automation, environmental monitoring, and smart city infrastructure. However, conventional IoT systems rely heavily on centralized cloud storage, which introduces several challenges including data tampering, privacy risks, cyberattacks, and single-point system failures. This paper proposes a Secure IoT Data Monitoring System using Blockchain Technology to overcome these limitations. The proposed system monitors electrical parameters generated from a solar panel using a current sensor connected to a NodeMCU ESP8266 microcontroller. The collected data is processed locally and transmitted through Wi-Fi communication to a cloud platform. A ESP-WROOM-32device acts as an interface between IoT devices and blockchain services, enabling decentralized verification and secure storage of monitoring data.

Blockchain technology stores monitoring records as cryptographically linked blocks, ensuring immutability and transparency. A 16×2 LCD display provides real-time visualization of system parameters. The proposed system enhances security, reliability, and trust compared to traditional monitoring systems. Experimental results demonstrate that blockchain integration effectively prevents data modification and ensures secure monitoring. The system can be extended for smart grid applications, industrial monitoring, and large-scale renewable energy management systems.

Keywords— Internet of Things, Blockchain Technology, NodeMCU ESP8266, Solar Monitoring, Data Integrity, Cloud Computing, Secure Monitoring.

1. INTRODUCTION:

The Internet of Things (IoT) represents a technological paradigm where physical devices equipped with sensors and communication modules interact through the internet to exchange data. IoT technology has significantly transformed monitoring and automation systems by enabling real-time data acquisition and remote control capabilities.

Renewable energy systems, particularly solar power generation, require continuous monitoring of electrical parameters such as current, voltage, and power output to ensure efficient operation. Traditional monitoring approaches involve centralized servers where sensor data is collected and stored. Although centralized systems provide ease of management, they introduce several security concerns. Unauthorized access, data manipulation, and server failures can compromise system reliability.

Blockchain technology has emerged as a promising solution for secure data management. Blockchain is a decentralized distributed ledger that records transactions across multiple nodes. Each record is stored as a block connected using cryptographic hash functions. Once data is stored, it becomes nearly impossible to alter, ensuring data integrity and transparency.

By integrating blockchain technology with IoT monitoring systems, secure and trustworthy monitoring platforms can be developed. This work focuses on designing a blockchain-enabled IoT monitoring system for solar energy applications that ensures secure transmission, verification, and storage of monitoring data.

2. METHODOLOGY:

The proposed Secure IoT Data Monitoring System using Blockchain is developed by integrating renewable energy monitoring, IoT communication, and blockchain-based security mechanisms to ensure reliable and tamper-proof data storage. The system begins with a solar panel that converts solar energy into electrical energy through the photovoltaic effect. The generated DC power is supplied to a load, and the electrical parameters are continuously monitored for performance analysis. A current sensor is used to measure the electrical current flowing through the circuit in real time. The sensor converts physical electrical quantities into electrical signals that can be processed by the controller.

The sensed data is transmitted to the NodeMCU ESP8266 microcontroller, which acts as the central processing unit of the system. The controller reads sensor values, performs basic data processing, and prepares the information for transmission. Since different electronic modules operate at different voltage levels, a logic level converter is used to ensure safe communication and voltage compatibility between the connected devices. The processed data is displayed locally using a 16×2 LCD display, allowing users to monitor system parameters directly in real time.

Using its built-in Wi-Fi capability, the NodeMCU transmits monitoring data to a cloud server for remote access and storage. The IoT communication stage enables continuous monitoring and data availability from any location through internet connectivity. A ESP-WROOM-32device functions as a gateway between the IoT system and the blockchain network. It receives monitoring data and performs blockchain interaction for secure verification. Each dataset is converted into a blockchain transaction and validated using cryptographic techniques before being added to the distributed ledger.

Once verified, the monitoring information is stored as blocks within the blockchain network, where each block is linked with the previous block using hash values. This structure ensures data immutability and prevents unauthorized modification or deletion. Any attempt to alter stored data changes the cryptographic hash and immediately indicates tampering. Through this methodology, the proposed system achieves secure real-time monitoring, decentralized verification, and reliable storage of solar energy data, thereby improving transparency and cybersecurity in IoT-based monitoring applications.

3. RESEARCH AIM:

The main aim of this research is to design and develop a secure Internet of Things (IoT) based monitoring system integrated with blockchain technology for reliable and tamper-proof data management. The project focuses on monitoring electrical parameters generated from a solar energy system in real time while ensuring secure transmission and storage of collected data. By combining IoT communication with blockchain's decentralized architecture, the system aims to eliminate issues related to centralized data storage such as unauthorized access, data manipulation, and single-point system failure. The research also intends to enhance transparency, data integrity, and trustworthiness in monitoring applications by implementing cryptographic verification mechanisms. Furthermore, the proposed work aims to provide a low-cost, scalable, and energy-efficient solution suitable for renewable energy monitoring, smart grid systems, and future secure IoT applications.

4. SYSTEM ARCHITECTURE:

The system architecture consists of hardware and software components that work together to monitor electrical data and store it securely using blockchain technology. The main components

of the system include sensors, microcontroller, display unit, gateway device, cloud server, and blockchain network.

The system uses a universal power sensor to measure electrical parameters such as voltage, current, and power from different power sources. The sensor continuously collects real-time data and sends it to the microcontroller. The microcontroller used in this system is the NodeMCU, which acts as the central controller. It processes the sensor data and displays the values on a 16×2 LCD display for local monitoring.it is shown in figure 1.

The NodeMCU also sends the processed data to a gateway device such as the ESP-WROOM-32 using Wi-Fi or serial communication. The ESP-WROOM-32 acts as an interface between the IoT device and the cloud server. It receives the data from the microcontroller and transmits it to the cloud server through the internet.

The cloud server is used to store the IoT data and provide remote access to users. Users can monitor the data from anywhere using mobile phones or computers. After storing the data in the cloud, the data is recorded in a blockchain network to ensure secure and tamper-proof storage. Blockchain technology maintains an immutable ledger where once data is recorded, it cannot be modified or deleted.

Thus, the system architecture integrates IoT devices, cloud computing, and blockchain technology to provide secure, reliable, and real-time data monitoring and storage.

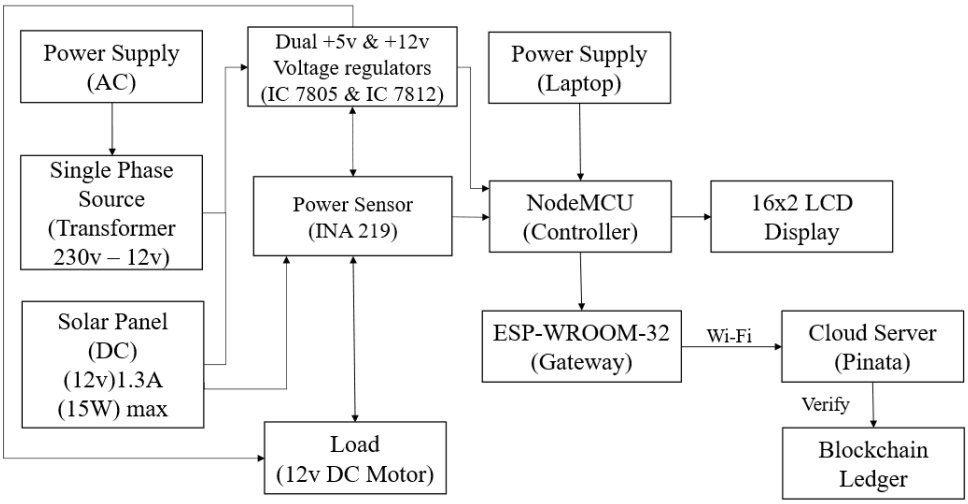

Fig1: Block diagram of Secure IoT Data Monitoring Using Blockchain

Power Monitoring and Data Acquisition

The system continuously monitors electrical parameters such as voltage, current, and power using a universal power sensor. The sensor is connected to different power sources such as AC supply, DC supply, and laptop power supply. The sensor measures the electrical parameters in real time and sends the measured data to the microcontroller for processing. This continuous monitoring helps in analyzing power usage and system performance.

Data Processing and Controller Operation

The microcontroller used in the system is the NodeMCU, which acts as the central controller of the system. The NodeMCU receives the sensor data and processes it in real time. The controller converts the sensor readings into voltage, current, and power values. It also compares the measured values with predefined threshold values to identify abnormal conditions such as over voltage, over current, or unusual power consumption. If any abnormal condition is detected, the system identifies it as a fault event.

Fault Detection Mechanism

The system continuously monitors the electrical parameters and checks whether the measured values are within the safe operating range. Under normal conditions, the voltage and current remain within the predefined limits. When abnormal conditions such as overload or short circuit occur, the current or voltage value increases beyond the safe limit. The NodeMCU detects this condition and identifies it as a fault. This fault detection mechanism helps in early detection of electrical problems and improves system safety.

Circuit Protection Operation

Once a fault condition is detected, the NodeMCU sends a control signal to the driver circuit. The driver circuit activates a relay unit that disconnects the electrical circuit from the power supply. The relay acts as a protection device similar to a circuit breaker. This disconnection prevents excessive current flow and protects the connected devices from damage. The circuit remains disconnected until the fault is cleared and the system is reset.

Cloud Communication and Data Transmission

After monitoring the electrical parameters and detecting fault events, the system sends the data to a gateway device such as the ESP-WROOM-32. The gateway device transmits the data to the

cloud server through the internet. The cloud server stores the electrical data and fault event information for remote monitoring and analysis. Users can monitor system data, power usage, and fault history through the cloud platform from anywhere.

Blockchain-Based Data Storage

To ensure data security and integrity, the data stored in the cloud is recorded in a blockchain network. Blockchain technology stores data in blocks that are cryptographically linked to each other. Once data is stored in the blockchain, it cannot be modified or deleted. This ensures secure and tamper-proof data storage. The blockchain system maintains a permanent record of electrical data and fault events, which improves transparency and reliability of the monitoring system.

Local Monitoring and Display

In addition to cloud monitoring, the system also provides local monitoring using a 16×2 LCD display. The display shows real-time electrical parameters such as voltage, current, power, and system status. During normal operation, the display shows the real-time electrical values. When a fault occurs, the display shows fault messages and indicates that the circuit has been disconnected. This helps the user to easily identify system status without accessing the cloud platform.

5. WORKING PRINCIPLE:

The working principle of the proposed Secure IoT Data Monitoring using Blockchain system is based on real-time data acquisition, wireless communication, and decentralized secure storage. The system operates by continuously monitoring electrical parameters generated from a solar energy source and securely storing the collected data using blockchain technology. Initially, when sunlight falls on the solar panel, it converts solar energy into direct current (DC) electrical energy through the photovoltaic effect. This generated energy is supplied to a connected load while the system simultaneously measures electrical parameters for monitoring purposes.

A current sensor placed in the circuit continuously measures the current flowing through the load. The sensor converts the measured electrical quantity into electrical signals that are transmitted to the NodeMCU ESP8266 microcontroller. The NodeMCU acts as the main controller of the system, where sensor readings are processed, calibrated, and converted into digital data suitable for transmission. A logic level converter is used to maintain proper voltage compatibility between interconnected devices, ensuring safe and reliable communication.

The processed monitoring data is displayed locally on a 16×2 LCD display, allowing users to observe real-time system performance directly. Using its built-in Wi-Fi module, the NodeMCU establishes an internet connection and periodically transmits sensor data to a cloud server for remote monitoring. The cloud platform enables users to access monitoring information from any location.

A ESP-WROOM-32device functions as a gateway between the IoT system and the blockchain network. The received monitoring data is verified using blockchain protocols and converted into secure transactions. Each dataset is stored as a block containing encrypted information along with a timestamp and hash value linked to previous records. This chaining mechanism ensures that once data is stored, it cannot be modified or deleted without detection.

Through this process, blockchain technology guarantees data integrity, transparency, and protection against unauthorized access or tampering. The overall working principle ensures secure real-time monitoring of solar energy parameters while maintaining decentralized and trustworthy data storage for IoT applications.

6. CONCLUSION:

This paper presented a Secure IoT Data Monitoring System using Blockchain technology for monitoring electrical parameters and ensuring secure data storage. The system was designed to monitor voltage, current, and power in real time using sensors and a microcontroller such as the NodeMCU. The system is capable of detecting abnormal conditions such as overload and short circuit, and it automatically disconnects the circuit using a relay for protection. This improves the safety and reliability of the electrical system.

The monitored data and fault information are transmitted to the cloud through a gateway device such as the ESP-WROOM-32, which enables remote monitoring and data storage. Users can monitor the electrical parameters, system status, and fault history from anywhere using the internet. This makes the system suitable for smart monitoring applications and industrial monitoring systems.

To enhance data security, blockchain technology is used for storing the monitoring data and fault records. Blockchain provides a secure, decentralized, and tamper-proof data storage system where once data is recorded, it cannot be modified or deleted. This ensures data integrity,

transparency, and reliability of the stored data. The blockchain-based storage system also creates a permanent record of system events and fault history.

Overall, the proposed system improves electrical monitoring, fault detection, circuit protection, remote monitoring, and data security. The integration of IoT, cloud computing, and blockchain technology makes the system more secure, reliable, and efficient compared to traditional monitoring systems. This system can be used in smart homes, industries, energy monitoring systems, and IoT-based automation applications for secure and efficient data monitoring.

7. REFERENCE:

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

[2] M. A. Khan and K. Salah, “IoT Security: Review, Blockchain Solutions, and Open Challenges,” IEEE Access, vol. 6, pp. 57751–57772, 2018.

[3] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, 2018.

[4] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards Blockchain-Based Auditable Storage and Sharing of IoT Data,” IEEE Conference, 2017.

[5] S. Seshadri et al., “IOTCOP: A Blockchain-Based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems,” IEEE Internet of Things Journal, vol. 8, pp. 3346–3359, 2020.

[6] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, “A Survey of IoT and Blockchain Integration: Security Perspective,” IEEE Access, vol. 9, pp. 156114–156150, 2021.

[7] J. Granjal, E. Monteiro, and J. Sá Silva, “Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

[8] M. Conoscenti, A. Vetrò, and J. C. De Martin, “Blockchain for the Internet of Things: A Systematic Literature Review,” IEEE Conference, 2016.

[9] V. Buterin, “Ethereum: A Secure Decentralized Transaction Ledger,” Ethereum White Paper, 2014.

[10] H. Ning and H. Liu, “Cyber-Physical-Social Systems in Internet of Things,” IEEE Internet of Things Journal, 2015.

[11] L. Da Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” IEEE Transactions on Industrial Informatics, 2014.

[12] M. Swan, Blockchain: Blueprint for a New Economy, O’Reilly Media, 2015.

[13] T. M. Fernández-Caramés and P. Fraga-Lamas, “A Review on Blockchain for Internet of Things,” IEEE Access, 2018.

[14] S. Pal, A. Dorri, and R. Jurdak, “Blockchain for IoT Access Control: Recent Trends and Future Research Directions,” IEEE Conference, 2021.

[15] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Conference, 2016.