Blockchain Enhanced IOT Based Smart Home Automation System

V.P.Patil, Shridevi Hiremath, Prajkta Gudde, Bhagyashri Tingare
(Guide) (Team Leader) (Member) (Member)
Electronics & Telecommunication, Jayawantrao sawant college of engineering, Maharashtra, India.

Abstract - *The Internet of Things (IoT) connects devices that communicate and share data over the internet, and with the vast amount of sensitive information they handle, such as personal and banking data, security is crucial. Key security aspects include protecting privacy through encryption, ensuring only authorized users and devices can access the system through strong authentication, and maintaining data integrity to prevent tampering. Additionally, it's important to ensure the system's availability by keeping it operational, regularly updating devices to address security vulnerabilities, and securing devices even after they are no longer in use. Addressing these concerns helps ensure that IoT systems remain safe and reliable.*

Keywords – *Authentication, Availability, Confidentiality, Physical Unclonable Function,*

Introduction

The Internet of Things (IoT) is a concept of refers to the interconnection of everyday objects through the internet, allow them to communicate with each other and share data without requiring human intervention. This interconnected network of devices is transforming the way we design and manage services and applications, simplifying various aspects of daily life.

IoT (Internet of Things) affects many industries like healthcare, renewable energy, cars, and supply chains. By connecting devices and systems, IoT makes things work more automatically, efficiently, and based on data. For example, in healthcare, IoT helps doctors monitor patients from a distance. In renewable energy, it helps manage energy use with smart grids. Because of this, IoT is seen as an important part of the digital world, helping businesses grow and create new opportunities.The concept of IoT was first introduced in 1999 by Kevin Ashton, the founder of the MIT Auto Identification Center. Ashton believed that IoT had the potential to revolutionize the world, possibly even more than the internet itself. In 2005, the International Telecommunication Union formally recognized the Internet of Things. Since then, various organizations and experts have offered different definitions of IoT, but the most widely accepted definition is the one provided by the ITU in 2012. The ITU defines IoT as "a global infrastructure for the information society, enabling advanced services by connecting physical and virtual things based on existing and developing interoperable information and communication technologies."

One of the key aspects of IoT is its ability to enable devices to communicate directly with one another, without the need for human intervention. This direct communication between devices is expected to become a standard feature of IoT networks in the future. As the IoT ecosystem grows, the number of connected devices is projected to reach 35 billion by 2025, further expanding the impact of IoT on various sectors and industries.

The architecture of IoT has evolved over time, with advancements in technology and communication protocols enabling devices to become more interconnected and intelligent. In the future, IoT systems are expected to operate with greater efficiency, enabling seamless communication between devices and enhancing the overall functionality of the network.

Block Diagram

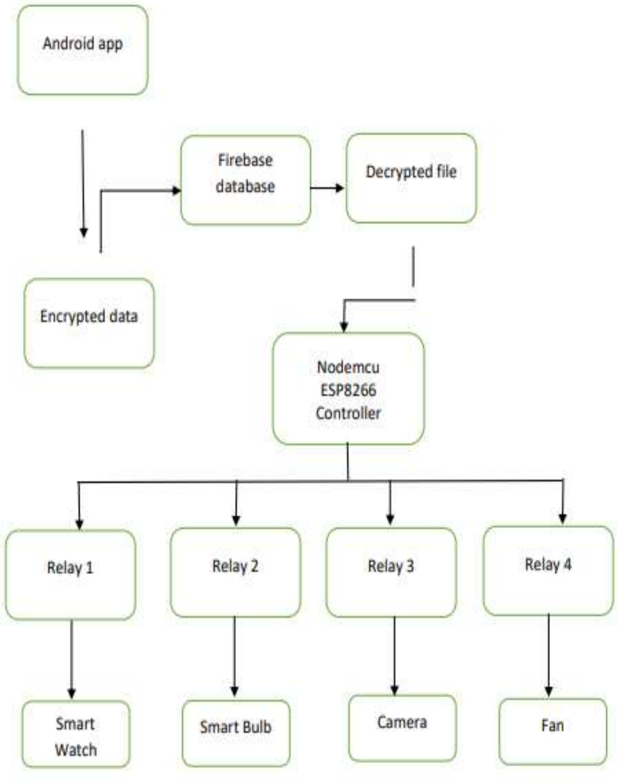


Fig1: Block Diagram Of Proposed system

The project "IoT-based Home Automation with Blockchain Security in Firebase" aims to build a smart home system that is both easy to use and secure. The system uses a NodeMCU ESP8266 microcontroller to control home appliances like lights and fans through a 4-channel relay module.

To keep things secure, the project uses blockchain encryption. This ensures that all the commands you send to the system are safe, unchangeable, and stored in a secure, decentralized ledger. Firebase helps with real-time data updates and user authentication, making sure the system is always up-to-date and that only authorized users can control the devices.You can control the appliances remotely using a mobile app or a web interface, and every action is recorded on the blockchain, offering transparency. This setup boosts security by ensuring only authorized users can access the system.The project combines IoT, blockchain, and cloud technologies to provide a smart home solution that is scalable, efficient, and secure. In the future, features like voice control and energy monitoring could be added. The system is designed to grow, allowing you to add more devices as needed, making it convenient, secure, and energy-efficient.

DETAIL OF INDIVIDUAL BLOCK

Android App: This serves as the user interface for the home automation system, allowing users to control and monitor appliances. The app communicates with Firebase to store or retrieve data about the status of various home appliances.

Encrypted Data: The Android app encrypts control data (such as turning appliances on or off) before sending it. This encryption ensures that the data remains secure as it travels over the network, adding a layer of privacy and security, which aligns with the principles of blockchain for tamper-proof data transfer.

Firebase Database: Firebase acts as the cloud storage for this system, holding the encrypted data. The use of Firebase enables real-time synchronization between the app and the IoT devices (like the ESP8266) connected to the appliances.

Decrypted File: Once the encrypted data reaches the ESP8266 controller, it is decrypted to obtain the original control commands. This decryption is necessary to allow the controller to interpret and execute commands for each appliance accurately.

NodeMCU ESP8266 Controller: The ESP8266 microcontroller is the central component that controls each appliance based on the decrypted commands from the app. The controller receives data from Firebase, decrypts it, and sends corresponding signals to specific relays.

Relays (Relay 1, 2, 3, and 4): Each relay acts as a switch, controlled by the ESP8266 to turn appliances on or off. Relays isolate high-voltage appliances from the low voltage control circuit, ensuring safe operation.

Appliances (Smart Watch , Smart Bulb , Camera, and Fan): These represent the household appliances controlled by the relays. Each relay is connected to an appliance, allowing the user to control them remotely from the Android app.

SH 256 Algorithm

SHA-256 is a member of the SHA-2 family of cryptographic algorithms, where SHA stands for Secure Hash Algorithm. It was developed in 2001 by the NSA and NIST to enhance security compared to the older SHA-1 algorithm, which was becoming vulnerable to specific types of attacks.

The "256" in SHA-256 represents the size of the resulting hash value. Regardless of the length of the original data, the output (or hash) will always be 256 bits long.

Other algorithms in the SHA family operate in a similar way to SHA-256, but they generate different hash sizes. For example, SHA-512 produces a hash that is 512 bits long.

Here are some key points about the SHA algorithm:

- Message Length: The original data (or "plaintext") should be less than 2^64 bits to ensure the output remains as random as possible.
- Digest Length: The result of the hash function will always have a set size—256 bits for SHA-256, 512 bits for SHA-512, and so on. Larger hash outputs need more processing, which can impact speed and storage.
- Irreversible: Hash functions like SHA-256 are designed to be one-way. This means you cannot get the original data back from the hash, and you won't get the same hash if you try the function with the same data again.

Applications of SHA-256

Blockchain technology: SHA-256 is used to maintain data integrity. Each block in the blockchain includes a SHA-256 hash of the previous block. This forms a secure chain of blocks, where modifying one block would change all the following blocks, making any tampering easy to detect.

Digital Signatures: SHA-256 is often used in creating digital signatures. For example, when you sign a message or document, the hash of that document is signed, ensuring both integrity and authenticity of the document.

Password Hashing: When storing passwords in a database, it's common to hash the password with SHA-256. The database only stores the hash, not the original password, making it more secure if the database is breached.

Feature Of Blockchain

- Decentralization: In traditional systems, like banks or governments, a central authority is responsible for verifying transactions. This can create problems, such as bottlenecks or a single point of failure. Blockchain removes the need for a central authority by allowing transactions to be verified directly between users (nodes) on the network. This reduces the risk of failure, cuts service costs, and avoids performance delays.
- Traceability: Every block in a blockchain has a "Timestamp" that records when the transaction happened. This makes it easy to trace where a transaction originated, so users can track the history of their transactions.
- If someone tries to change a block, all following blocks will be invalid. This makes the data very hard to alter. The Merkle tree structure keeps a hash of all transactions, so even small changes create a completely new hash, making tampering easily detectable.

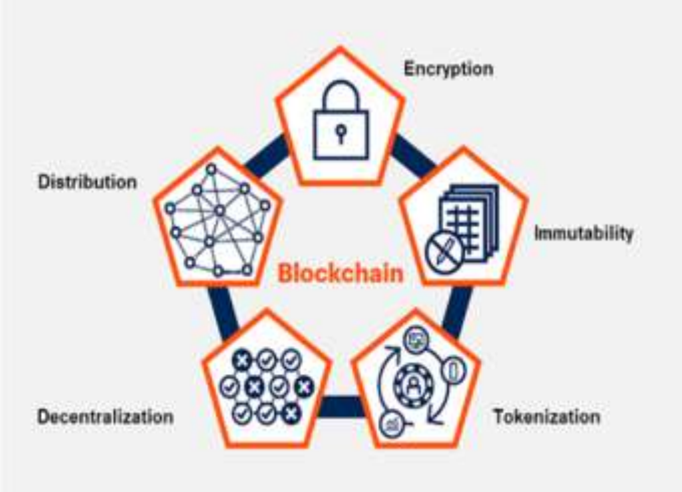


Fig 2: Features of blockchain

- Non-repudiation: Blockchain transactions are secured with cryptographic signatures. The person who initiates the transaction signs it with a private key, and others can verify the transaction with the public key. This ensures the initiator can't deny (repudiate) the transaction later.
- Pseudonymity: Blockchain addresses can be anonymous, meaning users' identities are hidden. This provides a certain level of

privacy while still allowing for secure transactions.

- Transparency: Everyone on the blockchain network has equal access to the data. When a new transaction happens, all nodes (users) in the network verify it. This ensures the system is transparent and fair.
- Fault Tolerance: Since the blockchain is stored on multiple nodes across the network, it's easy to detect if data is tampered with. If someone tries to change the data, the network can detect it and prevent the changes from being accepted.
- Exchange Automa**tion: Blockchain can also automate transactions using smart contracts. These are self-executing contracts with the terms written into** code, allowing for automatic and secure exchanges between parties (like vehicles exchanging information without human intervention).

Integration of Blockchain and IoT for Security:

Blockchain and IoT (Internet of Things) are two advanced technologies that, when used together, can provide stronger security for devices and data within an IoT network. Let's explore how combining these technologies works, with a focus on how blockchain enhances the security of IoT systems.

1. PUF Layer (Physical Unclonable Function)

A PUF (Physical Unclonable Function) is a technology that provides a unique identity to each device, similar to how a fingerprint uniquely identifies a person. This helps ensure that each device in the IoT network can be verified as genuine, reducing the risk of unauthorized or counterfeit devices joining the network.

- Device Authentication: Each device has a unique identifier based on its physical properties. PUF makes it nearly impossible to clone or forge these identifiers, providing a secure method for authenticating devices.
- Integration with Blockchain: PUFs are added before the physical layer in the system, ensuring that every IoT device is authenticated and securely connected to the network. When a device communicates, its identity can be verified using its unique PUF signature, and this can be stored and confirmed on the blockchain for tamper-proof security.

2. Blockchain Layer (Between Application and Network Layers)

Blockchain technology is introduced between the application layer (where the software interfaces with the user or system) and the network layer (where communication between devices occurs). This integration ensures that data exchanges between devices are secure and auditable.

- Secure Data Exchange: Blockchain records every transaction or interaction between devices, providing a transparent, tamper-resistant record. This means that data sent between IoT devices is securely logged in a decentralized ledger, making it immune to tampering or unauthorized access.
- Enhanced Security: By using blockchain, each transaction or message between IoT devices is validated by multiple participants (nodes) on the network, ensuring that no malicious party can alter or corrupt the data.
- Smart Contracts: Blockchain can use smart contracts, which are self-executing contracts written in code, to automate interactions between devices. For example, IoT devices can autonomously exchange data or trigger actions without human intervention, all while ensuring the integrity and security of the transaction.

Conclusion and Feature

Internet of Things (IoT), its structure, and the challenges it faces, especially when it comes to security. It also introduces Blockchain technology and discusses how it can help improve the security of IoT systems. The paper suggests a new approach that combines both Blockchain and Physical Unclonable Function (PUF) technologies to enhance security from the ground up, from the physical devices to the software layer.

The PUF acts like a unique fingerprint for each IoT device, ensuring that each device is properly identified and authenticated before it can participate in the network. This helps secure the communication

between devices, making sure data exchange happens safely.
In the future, the paper plans to explore how combining PUFs and Blockchain can further
improve security in IoT systems. The goal is to create a solution that guarantees secure data

In the future, the paper plans to explore how combining PUFs and Blockchain can further improve security in IoT systems. The goal is to create a solution that guarantees secure data exchange, quickly identifies devices, and keeps things cost-effective and energy-efficient.
In short, the proposed solution aims to fix security problems in IoT by ensuring device identity and secure data transfer using Blockchain and PUF technologies. The IoT-based Home Automation System with Blockchain Encryption and Decryption Security in Firebase provides a secure and efficient solution for managing home appliances remotely. By integrating IoT technology with blockchain, the system ensures secure communication between devices, preventing unauthorized access. Firebase enables real-time data storage, user authentication, and seamless synchronization of device statuses. The system allows users to control appliances like lights and fans from anywhere, promoting convenience and energy efficiency. Blockchain adds transparency and accountability by logging every transaction. The scalability of the system makes it adaptable for future IoT device integrations. Additionally, it contributes to energy conservation by enabling remote control of appliances. This project combines modern technologies to create a safer, more efficient smart home. It offers not only a practical solution for everyday living but also a secure platform for smart homes in the future. The system represents a significant step toward the development of secure, user-friendly, and sustainable home automation solutions.

Flowchart

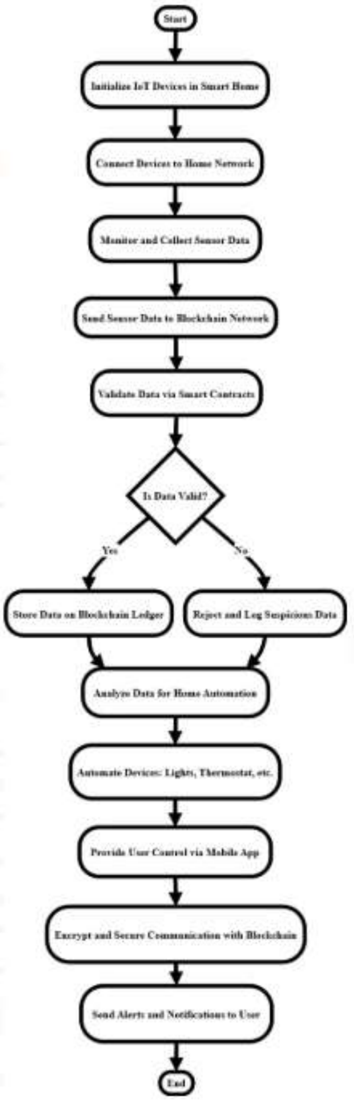
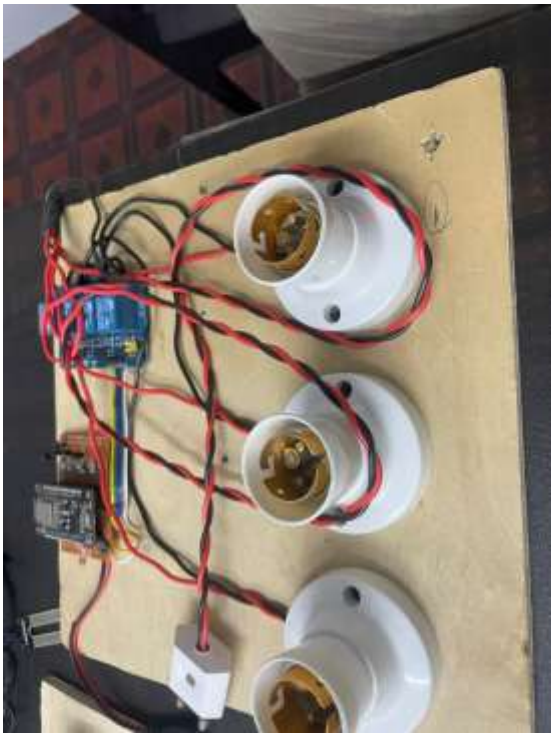
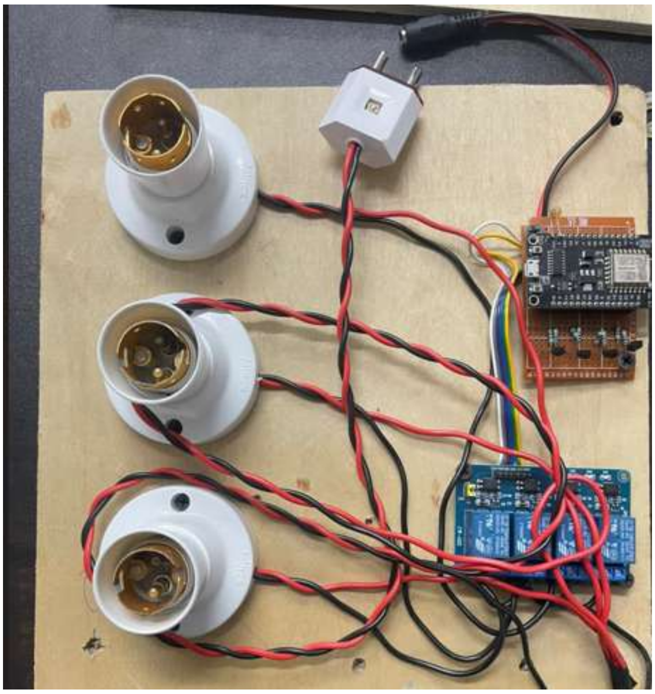

Start
Initialize IoT Devices in Smart Home
Connect Devices to Home Network
Monitor and Collect Sensor Data
Send Sensor Data to Blockchain Network
Validate Data via Smart Contracts
Is Data Valid?
Yes
No
Store Data on Blockchain Ledger
Reject and Log Suspicious Data
Analyze Data for Home Automation
Automate Devices: Lights, Thermostat, etc.
Provide User Control via Mobile App
Encrypt and Secure Communication with Blockchain
Send Alerts and Notifications to User
End

Fig 3:Flowchart of proposed system

Hardware





Specification of proposed System

The proposed IoT-based Home Automation system with Blockchain Encryption and Decryption Security in Firebase has the following specifications:

1. Microcontroller
- NodeMCU ESP8266
- Features: Wi-Fi enabled, low-cost microcontroller for controlling home appliances.
- Operating Voltage: 3.3V (regulated 5V for peripherals).
- Communication: Wi-Fi-based communication for remote access and control.

2. Relay Module
- 4-Channel 5V Relay Module - Allows control of up to 4 devices simultaneously (e.g., AC bulbs, fans). - Relay Type: Mechanical relay for switching AC appliances.

3. Home Appliances –
3 AC Bulbs (230V) - 1 Small 230V AC Fan
- These devices are controlled via the relay module connected to the NodeMCU.

4. Power Supply: -
5V, 1A DC Adapter - Provides stable power to the NodeMCU and connected devices.

5. Blockchain Security
- Blockchain-based Encryption and Decryption
- Ensures secure communication between the IoT devices and the user interface.
- Each command is encrypted, logged, and verified on the blockchain to ensure data integrity and transparency.
- Provides protection against unauthorized access or tampering. 31

6. Cloud Platform
- Firebase Cloud Platform
- Real-time data storage for user authentication, device status updates, and logs.
- Firebase Authentication: Secure login and access control for users.

7. User Interface
- Mobile Application / Web Interface - Provides a user-friendly interface to control appliances remotely.
- Features: On/off control, real-time status updates, appliance usage tracking, and alerts.

8. Security Features
- End-to-End Encryption
- All communication between the user and the system is encrypted using blockchain, ensuring data security and privacy.
- Data integrity: Blockchain ensures that only verified commands and responses are executed.

9. Scalability

- The system can be extended to control additional IoT devices like lights, security cameras, thermostats, etc.

- Future-proof design: Additional IoT devices can be integrated with minimal changes to the existing setup.

10. Connectivity

- Wi-Fi Communication: The system uses the ESP8266's Wi-Fi capabilities for remote access via mobile applications or web interfaces.

- Internet Access Users can access and control the system from anywhere in the world, as long as there is an internet connection.

11. Real-time Alerts

- Users will receive real-time alerts regarding appliance status changes, such as turning on or off, through the Firebase notification system. 32

12. Reliability

- The system is designed for high reliability, with fail-safe mechanisms to ensure uninterrupted operation of appliances even in the case of network issues.

13. Operating Environment - The system is designed to work in typical home environments, supporting 230V AC appliances like bulbs and fans. This specification outlines the key components and features that make the system both secure and user-friendly, with the integration of IoT, blockchain, and cloud technologies providing a reliable and scalable home automation solution.

Conclusion

In conclusion, this paper discusses the Internet of Things (IoT), its structure, and the security challenges it faces. It introduces a solution that combines Blockchain technology with Physical Unclonable Function (PUF) to improve security. PUF works like a unique fingerprint for each device, helping to secure data exchange between devices in the IoT system. The proposed solution strengthens security from the physical layer to the application layer. In the future, we plan to explore how combining PUFs with Blockchain can address IoT security issues. This approach is expected to provide a fast, low-cost, and energy-efficient way to ensure device identification, authentication, and secure data exchange, improving overall IoT security.

Reference

1. Sallam, F. al Qahtani, and A. S. A. Gaid, “Blockchain in Internet of Things: A Systematic Literature Review,” 2021 International Conference of Technology, Science and Administration,ICTSA2021, Mar. 2021, doi: 10.1109/ICTSA52017.2021.9406545.

2.M. J. Baucas, S. A. Gadsden, and P. Spachos, “IoT-Based Smart Home Device Monitor Using Private Blockchain Technology and Localization,” IEEE Networking Letters, vol. 3, no. 2, pp. 52–55, Mar. 2021, doi: 10.1109/LNET.2021.3070270.

3.T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, “Blockchain Applications for Industry 4.0 and Industrial IoT: A Review,” IEEE Access, vol. 7, pp. 176935–176951, 2019, doi: 10.1109/ACCESS.2019.2956748.

4.T. L. N. Dang and M. S. Nguyen, “An Approach to Data Privacy in Smart Home using Blockchain Technology,” in 2018 International Conference on Advanced Computing and Applications (ACOMP), Nov.2018,pp.58–64.doi: 10.1109/ACOMP.2018.00017.

5. M. Ammi, S. Alarabi, and E. Benkhelifa, “Customized blockchainbased architecture for secure smart home for lightweight IoT,” Information Processing & Management, vol.58,no.3,p.102482,May2021,doi:10.1016/j.ipm.2020.102482 .

6. L. Yang, X. Y. Liu, and W. Gong, “Secure smart home systems: A blockchain perspective,” IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2020, pp. 1003–1008, Jul. 2020,doi:10.1109/INFOCOMWKSHPS50562.2020.9162648.

7. A.Mukherjee, M. Balachandra, C. Pujari, S. Tiwari, A. Nayar, and S. R. Payyavula, “Unified smart home resource access along with authentication using Blockchain technology,” Global Transitions Proceedings, vol. 2, no. 1, pp. 29–34, Jun. 2021, doi: 10.1016/j.gltp.2021.01.005.