Internet Of Things(IOT) Security Enhancement Using Blockchain Technology

[1]Dr.Shweta Marigoudar,Associate Professor,GM University,Davanagere
[2]Ms. Bhoomika BV, MCA 3rdsem, GMU, [3]Ms. Devaramani Kavya, MCA 3rdsem, GMU,
[4]Mr. Harsha G R, MCA 3rdsem, GMU, [5]Mr. Punith Yadav J S, MCA 3rdsem, GMU,
[6]Ms. Roopashree N, MCA 3rd sem, GMU, [7]Mr. Siddesh K, MCA 3rd sem, GMU
[8]Ms. Chandana T, MCA 3rd sem, GMU

ABSTRACT

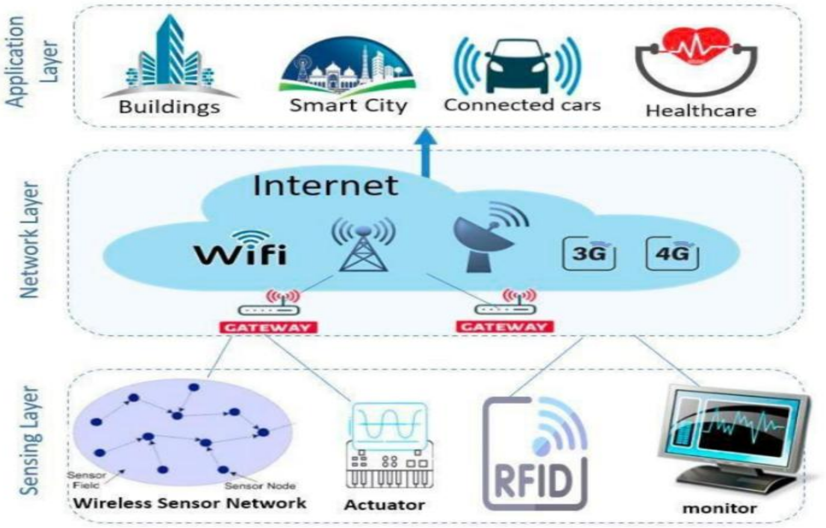
The Internet of Things (IoT) has become an essential part of our daily lives, especially in the rapidly expanding field of smart home applications. As this technology continues to grow, it raises concerns about the security, transparency, and privacy of user data. To address these issues, blockchain technology has shown potential as a solution to improve the IT infrastructure of smart homes. One promising blockchain solution is Hyperledger Fabric, which can enhance the security of smart home systems,can address these vulnerabilities by providing key security features like confidentiality, integrity, authentication, and data security.It also suggests that, with Hyperledger Fabric's features, IoT security deficiencies such as data breaches, unauthorized access, and the risk of data tampering can be significantly reduced.Blockchain, particularly Hyperledger Fabric, can address these vulnerabilities by providing key security features like confidentiality, integrity, authentication, and data security. The approach uses the MQTT protocol for IoT data transfer, ensuring secure communication between devices. By implementing this within a demo Hyperledger network with simulated IoT devices, the solution demonstrates how blockchain can effectively resolve security issues in IoT systems.

INTRODUCTION

Today, **IoTdevices** are everywhere, in smarthomes, wearable devices, smart cities, healthcare, automotive, environment, smart water, and grid applications, etc. IoT devices data are actively transferred over the internet, they are always accessible.

The technology that enables this intensive data transfer between human beings and devices is called IoT. IoT devices are uniquely identified in the network. These devices are generally designed to operate with small memory, limited processing capacity, and low power. Networks act as a bridge between IoT devices and users.

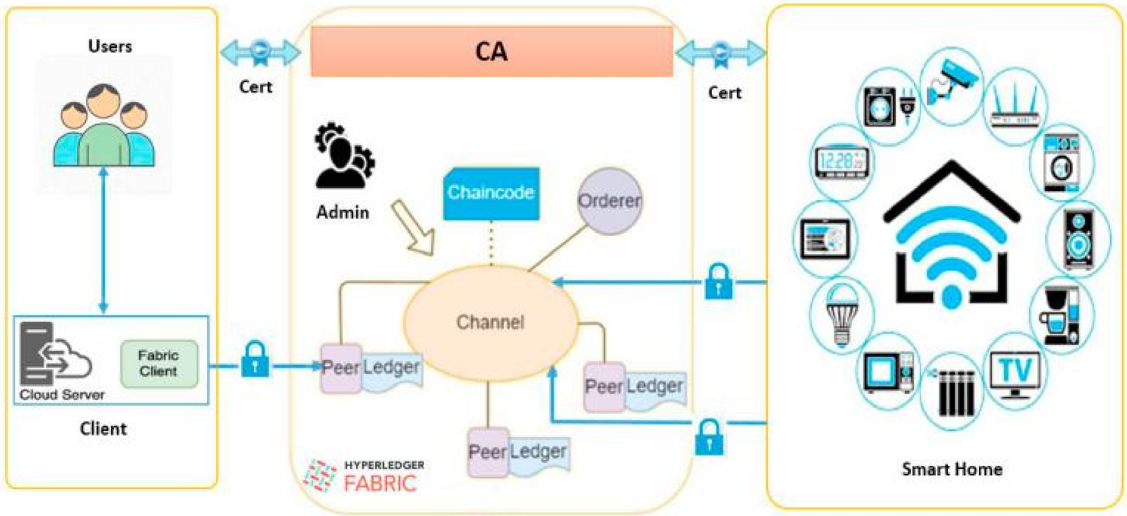
There are protocols for to transfer of data received from IoT devices. The most widely used one is MQTT (Message Queuing Telemetry Transport), it is a light-weight, publish-subscribe protocol for machine-to-machine communication.IoT devices by nature are small memory, low powered, and limited processing capacity; faced with security weaknesses in the fields of identity verification, authorization, and accounting. It is unfortunately easy to capture and manipulate the data transmitted by many IoT devices.



So, to avoid above insecurity problems in IoT devices, **Blockchain technology** is the solution. By Blockchain Technology, Tempering can be avoided. Blockchain is a decentralized, immutable and shared ledger that keep track of transactions on a peer-to-peer network (P2P). One of the most important concepts of blockchain is blocks. Each block contains an encrypted value containing the block information preceding it. Another important contribution of blockchain technology is the transparency it adds to business processes. This increases the trust between stakeholders and ensures accountability. It allows all stakeholders to monitor the blockchain network in realtime. Data privacy is an important feature of restricted blockchain networks. In restricted blockchain networks, only users authorized by the node's administrator can view data. This ensures that data coming to the blockchain network is protected. The public key structure of blockchain networks, which protects data modification, largely eliminates integrity problems. The participants and the consensus mechanism of a blockchain network are other factors that increase data security. Blockchain technology is used on many digital currencies including widespread Bitcoin and Ethereum cryptocurrencies using smart contracts. In the field of corporate blockchain applications, Hyperledger Fabric network is frequently used. In blockchain technology, a **hash value** is a unique string of characters (a fixed-length alphanumeric code) generated by a **hash function**. The hash value represents data (such as a block of transactions) in a way that it is computationally difficult to find two different inputs that produce the same hash.

Hyperledger Fabric

Hyperledger Fabric: An open-source, permissioned blockchain platform ideal for enterprise applications. It offers secure, decentralized data management, allowing businesses to build customizable blockchain networks.Hyperledger Fabric is used in smart homes to secure and automate the interaction between **IoT devices** (e.g., smart thermostats, security cameras, lighting systems) and **home management systems**.



The proposed system design based on Hyperledger Fabric Network.

The above proposed system design. A blockchain system is created using Hyperledger Fabric. The four essential components of the architecture are users, clients, the Hyperledger Fabric blockchain network, and smart homes. Homeowners and regular users are the two categories of users. Each smart home contains a single Homeowner.

LITERATURE REVIEW

The paper “SECURING IoT WITH BLOCKCHAIN” explores the integration of blockchain technology with Internet of Things (IoT) systems to address security challenges. The authors propose an approach to securely connect IoT devices to a blockchain network, specifically using Hyperledger Fabric.

Internet of Things (IoT) and Smart Homes

The paper begins by discussing the rapid growth and importance of IoT in various aspects of modern life, with a particular emphasis on smart home applications.IoT enables the connectivity of numerous devices within an environment, offering valuable insights and services that enhance daily life.However, the authors highlight that alongside these advancements, smart homes face significant challenges in ensuring information security.

Centralized IoT Architecture and Its Limitations

The current IoT architecture is predominantly centralized, which poses several security risks.The authors explain that this centralized structure makes IoT systems vulnerable to various attacks, particularly Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks.Other limitations of the centralized approach include high costs, privacy concerns, and the risk of a single point of failure.

Blockchain Technology as a Solution

To address these security challenges, the paper proposes the use of blockchain technology.Blockchain is presented as a distributed and decentralized ledger that can enhance security, transparency, and trust in IoT systems.The authors argue that blockchain can address issues related to data manipulation, unauthorized access, and privacy concerns in smart home environments.

Requirements for Blockchain Adoption in Smart Homes

The paper outlines specific requirements for adapting blockchain to smart home systems. These include considerations for both software and hardware components.The authors emphasize the importance of selecting the right blockchain platform and consensus mechanism based on factors such as the number of miners, transaction frequency, and block insertion frequency.

Proposed Approach Using Hyperledger Fabric

- The authors propose a blockchain-based approach using Hyperledger Fabric, a permissioned blockchain platform.
- The proposed architecture consists of four layers: Cloud Storage Layer, Blockchain Platform Layer, Application Layer, and IoT Devices Layer.

- The paper provides a detailed explanation of each layer and its role in enhancing smart home security.

- The paper presents an architecture that integrates IoT devices with a Hyperledger Fabric blockchain network. This approach uses MQTT (Message Queuing Telemetry Transport) protocol for data transfer from IoT devices to the blockchain network.

Implementation

The proposed approach is demonstrated using a simple Hyperledger Fabric network setup with four organizations on separate physical machines, communicating via Docker Swarm Network. Simulated IoT devices trigger events that inform the network of state changes.

Security Analysis

The authors discuss how their proposed approach addresses various dimensions of network security.
Confidentiality: Ensured through Hyperledger Fabric's privacy control and datasecurity features.
Integrity: Maintained by the distributed ledger structure of blockchain.
Availability: Provided by the distributed nature of the Hyperledger network.
Authentication and Authorization: Achieved through Hyperledger Fabric user identification and MQTT protocol.
Accountability: Enabled by the traceability of all transactions in the blockchain.

Future Research Directions

- The paper concludes by suggesting areas for future research, including further testing of the access control system in real-world settings and the incorporation of additionaltechnologies like identity authentication to enhance the overall security of smart home environments.

- Overall, the literature review provides a comprehensive overview of the current state of IoT security in smart homes, the potential of blockchain technology to address these challenges, and a detailed proposal for implementing a blockchain-based security solution using Hyperledger Fabric.

Objectives

1. **Enhance Scalability of Hyperledger Fabric in IoT Environment.**

- Optimize the blockchain network to handle high volumes of IoT-generated transactions.
- Improve throughput and reduce latency under increased device loads.

2. **Simplify Integration of IoT Devices with Hyperledger Fabric.**

- Develop a seamless approach for integrating diverse IoT devices with the blockchain.
- Minimize architectural and protocol-level disruptions during implementation.

3. **Improve System Adaptability and Maintainability.**

- Create a modular architecture that supports future scalability and integration efforts.
- Reduce the technical overhead involved in onboarding new devices or services.

4. **Ensure Secure and Efficient Data Handling.**

- Establish secure communication and data transmission between IoT devices and the blockchain.
- Ensure data consistency and integrity without overwhelming the network.

Methodology

1. **Requirement Gathering & System Assessment**

- Analyze the current IoT system architecture to identify integration points.
- Determine transaction volume, latency requirements, and device heterogeneity.

2. Optimized Network Design

Use Channel Partitioning:

- Create separate channels for different IoT device clusters to parallelize workloads and reduce congestion.

Implement Private Data

- **Collections:** Allow selective sharing of data to reduce network overhead and improve performance.

Adjust Block Size and Batch Timeout:

- Fine-tune Hyperledger Fabric parameters to optimize transaction processing times.

3. Edge-Blockchain Integration

- Use **Edge Computing** to preprocess data near IoT devices, reducing the load on the blockchain network.
- Introduce **gateway nodes** or lightweight agents to act as intermediaries between IoT devices and Fabric peers.

4. Standardization&Modular Architecture

- Develop middleware using **standardized APIs** and **MQTT protocols** to facilitatecommunication between IoT devices and the blockchain.

API: API is like a **messenger** that lets two apps or systems talk to each other.
APIs make it easy for developers to use features from other software without building everything from scratch.

MQTT is a lightweight messaging protocol, often used in IoT (Internet of Things).
MQTTis **fast**, **low-power**, and perfect for devices with **limited resources** like sensors, wearables, and smart gadgets.

- Use containerization (e.g., Docker) and orchestration (e.g., Kubernetes) to deploy modular components that can be easily scaled or updated.

5. Interoperability & Protocol Bridging

- Implement protocol adapters or translators to support devices using non-standardcommunication methods.
- Use an **IoT integration framework** (like Node-RED or Apache Camel) to abstract device logic from blockchain interaction logic.

IoT integration framework: it is a structure or system that helps connect and managedifferent IoT devices (like smart sensors, appliances, or machines) so they can work together, share data, and communicatewith apps or cloud services.

6. Testing and Validation

- Conduct **scalability testing** (load testing, performance benchmarking) under simulated IoT traffic conditions.
- Perform **integration testing** to verify the functionality of middleware and edge-node communications with Hyperledger Fabric.

7. Monitoring,Feedback, and Optimization

- Use monitoring tools like **Prometheus** and **Grafana** for real-time performance tracking.

Prometheus:it is a **monitoring tool**. It collects **metrics** (like CPU usage, memory usage,error rates, etc.) from your systems and applications over time.Think of it as a **data collector**for how your system is performing.

Grafana:it is a **visualization tool**. It takes the data that Prometheus (or other tools) collectsandturns it into beautiful **dashboards and graphs**.

- Analyze bottlenecks and fine-tune Fabric configurations and edge strategies accordingly.
- Set up automated alerts for anomalies in transaction processing or device communication.

CONCLUSION

Further enhance our IoT and Hyperledger Fabric architecture, several key implementations can be explored. First, focus on **scalability** by expanding the number of IoT devices and blockchain participants to test the system's performance under heavy loads, ensuring it can handle increased latency and throughput.

Integrating **edge computing** will enable IoT data preprocessing at the device level, reducing latency and alleviating the blockchain's processing load. Additionally, implementing **smart contracts (Chain code)** within Hyperledger Fabric can automate critical tasks such as device authentication, data validation, and event-triggered responses, enhancing system efficiency.

LIST OF ABBREVATION

- IOT = Internet of Things
- P2P = peer-to-peer network
- MQTT = Message Queuing Telemetry Transport
- DoS= Denial-of-Service
- DDoS= DistributedDenial-of-Service

REFERENCES

1) Jyoti D. and Amarsinh V.: Security Attacks in IoT: A Survey (2017).

2) Alfonso P.: Blockchain and IoT Integration: A Systematic Survey. Sensors, 1424-8220 (2018).

3) Rui Z., Rui X. and Ling Liu.: Security and Privacy on Blockchain (2019).

4) Moniruzzaman, Md, et al. (2020) "Blockchain for smart homes: Review of current trends and research challenges."

5) Nitin N.: Choice of effective messaging protocols for IoT systems:MQTT (2017).

6) Yin, Shan, Yueming Lu, and Yonghua Li. (2015) "Design and implementation of IoT centralized management model with linkage policy."

7) Mishra, Saumya, and Aditi Paul. (2020)"A critical analysis of attack detection schemes in IoT and open challenges." 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON).

8) Chelloug, Samia Allaoua, and Mohamed A. El-Zawawy. (2017) "Middleware

9) Mishra, Saumya, and Aditi Paul. (2020)"A critical analysis of attack detection schemes in IoT and open challenges." 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON).

10) Chelloug, Samia Allaoua, and Mohamed A. El-Zawawy. (2017) "Middleware for internet of things: Survey and challenges." Intelligent Automation & Soft Computing.

11) Khan, Minhaj Ahmad, and Khaled Salah. (2018) "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems.

12) Atlam, Hany F., et al. (2018) "Blockchain with internet of things: Benefits, challenges, and future directions." International Journal of Intelligent Systems and Applications