PROJECT SYNOPSIS

OF

Blockchain Based Device Authentication for The IoT Devices

Submitted By:

Sayantan Banerjee – 11500221018

Soumik Pal – 11500222125

Sayan Bhattacharya– 11500221042

Arindam Dandapat- 11500221027

Academic Year - 2024-25

Under the guidance of

Mr.Asim Kumar Panda

Dept. of Information Technology

MAULANA ABUL KALAM AZAD UNIVERSITY OF TECHNOLOGY

(Formerly known as WBUT)

B.P. PODDAR INSTITUTE OF MANAGEMENT AND TECHNOLOGY

PODDAR VIHAR, 137 VIP ROAD

KOLKATA-52

Signature of the Guide

CONTENTS

ACKNOWLEDGEMENT

Words do fall short when it comes to paying off gratitude, still we wouldlike to convey our sincere thanks to our guide - Mr.Asim Kumar Panda for allocating us to this project-“ Blockchain Based Device Authentication For The IoT Devices” and also for guiding us throughout the development process. We would further like to thank each and every onewho directly or indirectly helping us in doing this project successfully.

OBJECTIVE –

The increasing number of IoT devices presents significant security challenges, including device counterfeiting, unauthorized access, and data breaches. Existing authentication methods often rely on centralized authorities, which can be vulnerable to attacks. Blockchain technology offers a decentralized, immutable, and transparent solution to address these issues.

ABSTRACT -

This project aims to enhance IoT device authentication using a blockchain-based approach with Hyperledger Fabric. By leveraging the decentralized, permissioned nature of blockchain, we ensure secure, tamper-proof registration and authentication of devices. Smart contracts written in Go enforce security policies, preventing unauthorized access and ensuring device trustworthiness.

The system addresses challenges like device impersonation and data tampering, providing a scalable, secure IoT infrastructure. This solution promotes transparency, integrity, and privacy in connected device ecosystems.

INTRODUCTION –

The Internet of Things (IoT) has revolutionized the way devices connect and communicate, but this rapid growth has introduced significant security challenges, particularly in device authentication. Traditional authentication methods often rely on centralized systems, making them vulnerable to attacks and single points of failure.

This project, Blockchain-Based Device Authentication for the Internet of Things, aims to enhance security through a decentralized approach using Hyperledger Fabric and the Go programming language. By employing Hyperledger Fabric, we create a secure and tamper-proof environment for device authentication, leveraging its modular architecture for customized privacy and consensus mechanisms.

Using Go, we will implement smart contracts (chaincode) to manage device identities and authentication processes on the blockchain. This innovative solution not only strengthens the security of IoT networks but also ensures trust and transparency among connected devices, paving the way for a more secure IoT ecosystem.

REVIEW OF THE RELATED WORK –

When implementing blockchain-based device authentication for the Internet of Things (IoT) using Hyperledger Fabric and Go, various algorithms are employed to ensure security and integrity. These algorithms are crucial for several aspects of the authentication process, including identity verification, access control, and data protection.

Algorithms and Their Functions

1. Hash Functions:
   SHA-256: This widely used algorithm calculates hashes of data, creating unique identifiers for devices and verifying data integrity.
   Keccak-256: The underlying algorithm for the Ethereum blockchain, Keccak-256 is often utilized for generating addresses and verifying transactions.

2. Digital Signature Algorithms:
   ECDSA (Elliptic Curve Digital Signature Algorithm): A commonly used algorithm for digital signatures, it authenticates devices and verifies the authenticity of transactions.
   ED25519: A modern elliptic curve signature algorithm known for its speed and efficiency, it is particularly suited for lightweight applications and IoT devices.

3. Encryption Algorithms:
   AES (Advanced Encryption Standard): This symmetric-key encryption algorithm encrypts sensitive data to protect information stored on the blockchain and in transit.
   RSA (Rivest-Shamir-Adleman): An asymmetric-key encryption algorithm used for public-key cryptography, it facilitates key exchange and digital signatures.

4. Consensus Algorithms:
   PBFT (Practical Byzantine Fault Tolerance): This consensus algorithm ensures high fault tolerance, enabling honest nodes to agree on the state of the blockchain, and is commonly used in Hyperledger Fabric.
   Raft: Another consensus algorithm gaining popularity due to its simplicity and efficiency, it is also implemented in Hyperledger Fabric.

PROPOSED WORK -

The proposed work should be progressed in the following way-

- **System Design:** Create a high-level architecture using Hyperledger Fabric for device authentication, detailing key components.
- **Smart Contract Development:** Implement smart contracts in Go for device registration and authentication processes.
- **Device Integration:** Integrate the blockchain-based authentication with various IoT devices for seamless communication.
- **Testing and Evaluation:** Conduct testing to validate functionality, performance, and security, comparing it with traditional methods.
- **Documentation and Future Work:** Document the development process and outline potential enhancements for scalability and additional features.

FUTURE SCOPE -

The future of blockchain-based device authentication for the Internet of Things (IoT) is promising as the number of connected devices continues to rise. Blockchain's decentralized, immutable, and transparent features enhance device trust by preventing counterfeiting and tampering through immutable records and transparent provenance. It also streamlines secure device provisioning via smart contracts, reducing fraud and automating enrollment processes.

Additionally, blockchain improves protection against unauthorized access with granular controls and tamper detection. It promotes supply chain transparency, ensuring device authenticity and supporting interoperability across different IoT ecosystems. Finally, blockchain addresses privacy concerns by securing user data and facilitating consent management, making it a transformative solution for IoT security.

SOFTWARE REQUIREMENT -

- Go Language
- Python
- Docker
- Hyperledger Fabric

HARDWARE REQUIREMENT -

- Esp32
- Arduino
- RASPBERRY PI
- Microcontroller

CONCLUSION -

In conclusion, the proposed solution for device authentication using blockchain technology in IoT devices effectively addresses security concerns. Utilizing Go for backend development ensures high performance and scalability, while Python simplifies prototyping and data management. Docker enhances application deployment, and Hyperledger Fabric provides a secure and private blockchain framework. On the hardware side, ESP32 and Arduino facilitate efficient device communication, while Raspberry Pi offers powerful processing capabilities. This combination of software and hardware creates a robust and adaptable system, ensuring secure authentication and enhancing trust in the growing IoT ecosystem.

REFERENCES -

1. https://ciet.ncert.gov.in/storage/app/public/files/19/Webinar%20ppt/itmsday3.pptx.pdf

2. https://www.webology.org/data-cms/articles/20220310121920pmwebology%2018%20(6)%20-%20222%20pdf.pdf

3. https://www.h-x.technology/blog/how-secure-internet-of-things-with-blockchain

4. https://openaccess.city.ac.uk/id/eprint/32678/

5. https://www.mdpi.com/1424-8220/19/10/22