Securing IoT Using Blockchain

Dr.S.Brindha[1], Ms.P.Abirami[2], Ms.R.Aishwarya[3], Ms.N.V.Ragavi[4], Mr.A.C.Shriehari[5]
[1]*Head of the Department, Department of Computer Networking, PSG Polytechnic College, Coimbatore*
[2]*Professor, Department of Computer Networking, PSG Polytechnic College, Coimbatore*
[3, 4, 5]*UG Students, Department of Computer Networking, PSG Polytechnic College, Coimbatore*

***Abstract*— The rise in popularity of IoT devices has resulted in security flaws and exploitation. The interoperability and computational power of IoT devices have also been impacted due to security concerns. As a result of their decentralization and secure design, Blockchain technologies are gaining popularity for IoT security solutions. Does the existing security in home automation face challenges and vulnerabilities in automated living? and will they be immune to IoT attacks and our security solution using Blockchain is proposed. An evaluation of Blockchain and Hyperledger frameworks was conducted, leading to the development of IoT device security through Hyperledger Fabric. Hyperledger Fabric, an open-source Blockchain framework, was implemented on AMD64 and ARM64 architectures using docker swarm to support multi-host configurations. In this paper, we propose the implementation and comparative study of security solutions using decentralized Blockchain.**

Index Terms*— *Internet of things, Blockchain, Home automation, Hyperledger fabric

I. INTRODUCTION

The popularity of network embedded systems and wireless network communication drives a rapid increase in IoT device deployment every year. The convenience of the automated world gives users complete control over the surroundings and integrated with more technical information that are better to operate and attractive to users [2]. More IoT devices are connected to different systems in our society, it is important to secure and isolate sensitive devices. They are characterized into sensor and actuators that usually have small processor that handles control. These devices are liable to both hardware and software (firmware) attacks. The devices connected to a smart hub and operating under a wi-fi connection are of the vulnerable to different types of security attacks [1].

II. MOTIVATIONS AND BACKGROUND

A. Motivations

Connected to the internet, every smart device becomes an entry point for unauthorized external actors, exposing personal data and home integrity is compromised via these devices, which are proliferating. The automated system can put the data or property at risk if it is not secured properly. People are often unaware of protections are available or skip the protocols to enjoy a more streamlined experience, resulting in automated smart home devices lacking adequate security measures [3]. In some scenarios, instead of breaching a single individual's smart device to nab their data, hackers will take the database of a smart- device company to pilfer the data of all its users. Massive data breaches can expose the data of users with smart devices. Ordinary citizens will have to deal with an increase in attempts at fraud, phishing, and password theft, especially through fraudulent websites that purport to offer information that is also accessible via a security flaw in the automated world [1]. They are mostly connected to the Internet via domestic Wi-Fi networks, which are easily compromised, especially now that automation devices and household appliances are cyber-connected, opening up new avenues for cyber-attacks. [1] [2].

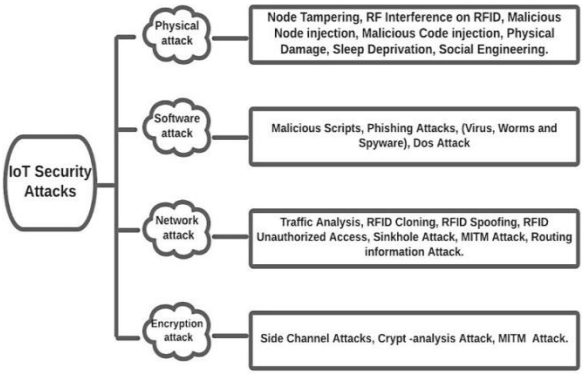

Figure-1: Attack scenario classification in network embedded systems

B. Background

Attack scenarios can be classified based on their target in- network embedded systems into system attacks, network attacks, and device firmware, hardware attacks as shown in Fig. 1. The physical harm attack that brings failure to the physical devices, data theft attack that does identity threats; device control, and shutdown are the various targeted attacks in such scenarios [1].

Encryption attacks consist of breaking the system encryption, which can be done by side channel, cryptanalysis, and man-in-the-middle attacks that also presented a multi-layered security approach to address the IoT structure layers and encryption system vulnerabilities and security issues [2]. There is also a protocol-based attack including the communication and network protocol namely flooding attack, SSL stripping, pre-shared key attack, selective forward attack, hash attack, and wormhole attack [1] [3].

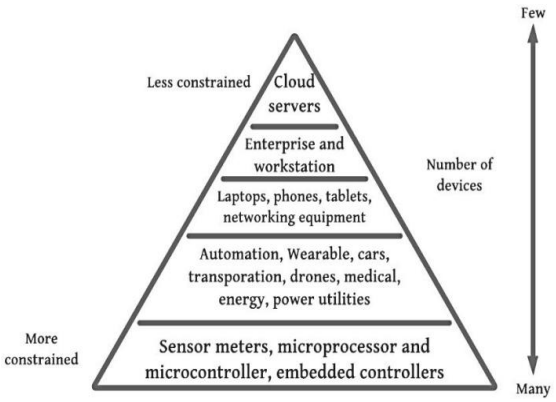

Figure-2: IoT device pyramid

As mentioned in the above Figure 2. In the IoT pyramid at the very top are the cloud servers, which are the centralized system controllers owned by third parties (Amazon, Microsoft, IBM, etc.). These solutions mostly depend on a centralized cloud server architecture to store data storage, authentication, communication, and any required services. Using centralized IoT solutions has security and trust issues since users have to trust proper handling of data and no mass surveillance [3]. In physical access, the attacker can have the highest level of access to the automated device in home automation if they get access to it; this has the highest level of vulnerabilities. Another attack scenario takes the advantage of the market for second-hand IoT devices. Users might also buy a used device that could end up with a device that has been compromised to spy on people that can be compromised through supply chain hacks. In such scenarios, attackers can compromise a supplier company's network and Trojan their software updates, allowing the threat to spread to any device that receives the tainted update and is connected to that network [4].

III. RELATED WORK

Blockchain records and duplicates data across a distributed network, and new entries are added to the end of the record [5]. A node in a Blockchain network is responsible for maintaining and validating blocks. P2P (peer-to-peer) network architecture is used, which achieves decentralization and ensures no single point of failure. Existing Blockchain-based IoT security solutions fail to address latency, applicability, and resource constraints, instead focusing on secure firmware updates, configuration management, and energy transactions. Eavesdropping refers to passive wiretapping, which involves listening. Active wiretaps, on the other hand, involve inserting something into the conversation. The attack does not need any contact. It is possible to wiretap a communication covertly so neither the sender nor the receiver will realize the wiretap has taken place.

Depending on the communication medium used, different types of wiretapping can be used

- Cable- A local LAN allows anyone with access to the cables to intercept all signals. Every LAN connector (For example, a computer board) has a unique address.
- Microwave- A microwave signal is not transmitted over a wire, but instead transmitted over the air, so anyone can see it.
- Satellite Communication- Even though satellite communication is intended for a limited area, certain signals can be intercepted over a large area.
- Interception- Whether passive or active, wireless traffic interception is always a threat.
- Wireless Service Theft- Furthermore, rogue users may exploit a network connection because DHCP assigns clients an IP address and allows them to connect to the host.

Figure 3. When the user enters the login credentials in the IoT device, the attacker can wiretap the data access in the unsecure network connection. This type of attack can take place even when the data is processed.

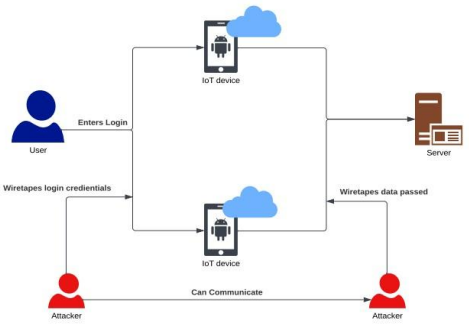

Figure-3: Existing system wiretapping

Table-1 compares the types of Blockchain with its details, example, and characteristics, the reason we need Hyperledger fabric network.

TYPE	DETAILS	EXAMPLE
Public Blockchain (Permission less)	Transactions can be accessed and created by participants, and nodes can be executed by any valid participant.	Ethereum, Bitcoin
Private Blockchain (Permissioned)	Controlled by a few parties who add participants	Hyperledge, Ripple

TABLE 1: BLOCKCHAIN COMPARISION

IV. AUTHENTICATED BLOCKCHAIN FOR IOT APPLICATIONS

The Hyperledger Fabric Blockchain framework is being proposed as a solution for secure access control and the foundation of a trust model for IoT objects. Its decentralized feature allows agents to direct contact each other without third party [5]. In comparison to Ethereum, the modular Blockchain platform uses container technology to host smart contracts, resulting in a more secure private (permissioned) blockchain. That is accessible by the authorized parties only.

Ethereum application network is very transparent, and transactions happening over the network is visible. In comparison, Hyperledger has more control mechanisms that allow participants to access the ledger.

A. Fabric Network

The Hyperledger Fabric (HLF) organizes a collection of nodes into organizations that form a network that interfaces with external applications; Organizations (ORG) in HLF are treated as Blockchain network members. Nodes within the HLF network are managed by the MSP which acts as the identity manager, providing valid digital signatures. Default Hyperledger can differentiate nodes based on organizational characteristics; each organization has its own root certificate. As shown in Figure 4 the fabric test network is created.

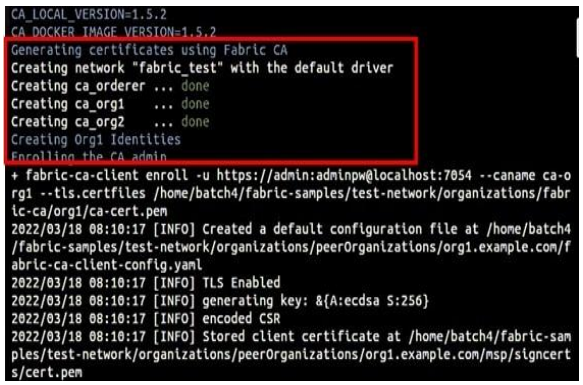

Figure-4: Fabric Network Screenshot

B. Cryptogen

Cryptogen is a binary tool that is created during the HLF installation on the host system. It generates key cryptographic materials for entities in the HLF network. The cryptographic materials generated by cryptogen include Identity management material as well as TLS for communication between entities as shown in Figure 5.

Figure-5: Cryptogen Screenshot

C. Transaction Flow

The flow of transactions is requested when a client application creates a transaction request which is sent to endorsers for endorsement. The endorser peers will simulate the transaction using smart contracts and if valid endorse it with a response sent to the client application[4]. Ordering, as shown in Figure 6, the endorsed transactions are sent to the orderer, who then packages the transactions using an ordering service in this case in the organization.

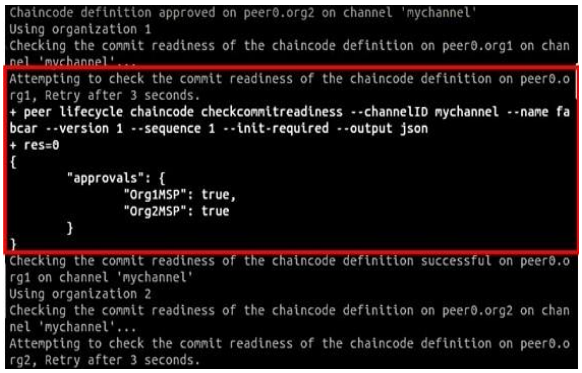

Figure-6: Transaction Flow Screenshot

D. Membership Service Provider

It is a managing authority for digital certificates, user access and provides authentication for users of the network. Every access of HLF must be accounted for because it is a private Blockchain and MSP helps through generating certificates using cryptogen. In HLF, certificate authorities generate certificates with private and public keys that are assigned to the respective entities to form a keyset used to establish identity. Verification of the allocated private keys is done by the MSP by checking the private key against the saved public keys of participating peers as shown in Figure 7.

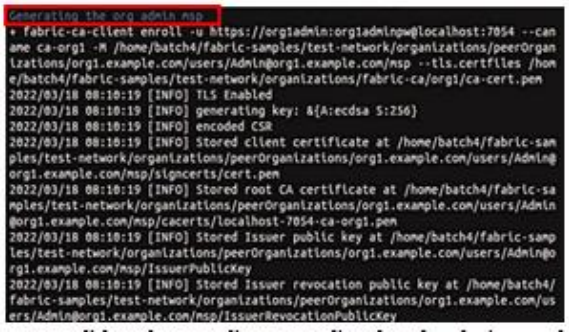

Figure-7: Membership Service Provider Screenshot

E. Hyperledger Composer

Hyperledger Composer is a comprehensive, open development toolset and framework for creating Blockchain applications. It ensures that transactions are validated according to policy by the designated business network participant by supporting the existing Hyperledger Fabric Blockchain infrastructure and runtime [5]. Composer is a programming model that contains a modeling language, and a set of APIs to define and deploy business networks; applications that allow participants to send transactions that exchange assets. The Hyperledger composer works primarily in the following areas:

• Assets: houses and listings
• Participants: buyers and homeowners
• Transactions: buying or selling houses and creating and closing listings

In which participants can have their access to transactions restricted based on their role as either a buyer. The realtor can then create an application that allows buyers and sellers to view available listings and make offers through a simple user interface.

V. EVALUATION

The main objective of taking Hyperledger fabric over Ethereum is because the mode of operation is permissioned that means, a private Blockchain that does not allow public participants to join the network without permission. It is a reliable Blockchain platform that enables people to develop personalized Blockchain for their various needs that is a modular architecture that provides a lot of flexibility and futuristic solutions for enterprise Blockchains. Ethereum is a transparent network in which each transaction is visible to anyone on the network that does not provide confidentiality. In Hyperledger the transactions are visible only to the admin in that network. In that case, we have implemented Hyperledger Fabric-based application for home automation website, in which when a particular node or an organization is attacked then only that particular organization is at threat. The admin in that network can view and remove that particular compromised organization so that it will not be a launch pad for subsequent attacks in the network. The result is shown in Figure 8.

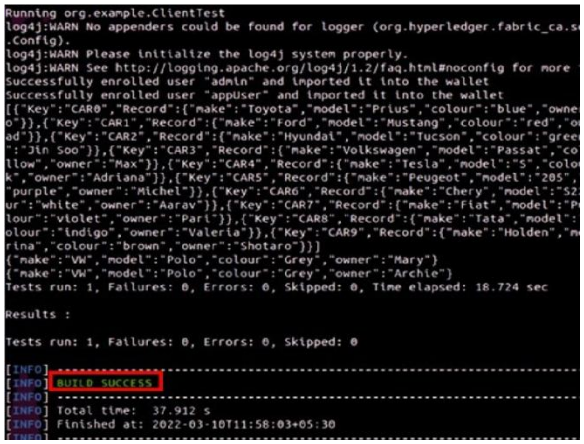

Figure-8: Evaluation Screenshot

VI. CONCLUSION

In this paper, the proposed Hyperledger fabric Blockchain framework is used as a solution to secure access control and root of a trust model for IoT devices that are connected in home automation. The wiretapping attack is executed and with our study, we conclude that when Hyperledger based web application is used instead of a centralized automated websites for home automation, medical websites it reduces the risk of attacks and provides secure encryption that is proved more secure during our study.

REFERENCES

[1] Sreenivas Sudarshan Seshadri, David Rondriguez, Mukunda Subedi, Kim-Kwang Raymond Choo, Sara Ahmed, Qian Chen, and Junghee Lee, “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, issue.5, Mar. 2021.

[2] Dr. S. Brintha Thiyagaraj, P.Abirami, Amitha. S, Chellina. A. S. and Shrutika Pawar. S, "Peer to Peer Solar Energy Sharing using Blockchain in IOT", International Journal of Research Publication and Reviews J., vol. 2, issue. 3, pp. 433-436, Mar. 2021.

[3] Y. Yang, L. Wu, G. Yin, L. Li and H. Zhao, "A survey on security and privacy issues in Internet-of-Things", IEEE Internet Things J., vol. 4, no. 5, pp. 1250-1258, Oct. 2017.

[4] T. Alladi, V. Chamola, B. Sikdar, and K. R. Choo, "Consumer IoT: Security vulnerability case studies and solutions", IEEE Consum. Electron. Mag., vol. 9, no. 2, pp. 17-25, Mar. 2020.

[5] S. Sridhar and S. Smys, "Intelligent security framework for IoT devices cryptography based end-to-end security architecture", Proc. Int. Conf. Inventive Syst. Control (ICISC), pp. 1-5, Jan. 2017.

[6] Ali, M.S. et al. (2019). Applications of Blockchains in the Internet of Things: A Comprehensive Survey. IEEE Communications Surveys and Tutorials, 21 (2), 1–34.