

# **Blockchain in IoT enabled Smart Home Network**

## **Abstract**

Network security is a vast topic that combines processes, devices, and technologies. Network security is the group of rules and configurations. The network nowadays has become complex, which is changing the threatened environment. Similarly, smart homes are also becoming prone to security threats. In this system we are going to investigate the various security threats related to smart home networks and Blockchain Technology will be used to mitigate the security issues of the smart home. By using the Blockchain, not only security issues, we can also overcome the single point of failure of IoT devices. The combination of IoT and blockchain offers various potential benefits and allows a smart device to function autonomously without the need for a centralized authority. It can also track how devices communicate with each other.

## **Introduction**

Smart Home automation is gaining popularity among the current application of the Internet of Things. Sensors are employed within the home via wireless connectivity to be accessible remotely by the home owners to operate these devices. Due to vast increase in the smart home IoT devices in the market such as power switch's, light bulbs, locks etc., numerous security concerns are arising due to the storage and processing power of these devices.

To avoid these security threats, we are decided to apply Blockchain technology mainly Consortium Blockchain, a decentralized database based on cryptographic technique, is gaining an enormous attention to attain security of IoT devices.

One of the methodologies adopted in blockchain-based smart home automation consists of three layers: the cloud layer, the gateway layer, the device layer. The device layer comprises sensor devices that gather and collect information in the smart home communication network via different IoTs installed in a smart home. The gateway layer holds the data produced by the Device Layer. It makes it available to users as required. The cloud layer stores data processed by every gateway and the gateway ID in the blockchain [1].

In [2], the consortium blockchain was incorporated with cloud computing and the smart home architecture was presented in to achieve confidentiality, integrity, scalability, and availability to keep smart homes safe and secure. The proposed scheme showed the blockchain implementation in a smart home network for manipulating the transactions and uses green

cloud computing. The technique implements green service using as a green broker to lessen the factors affecting environmental condition, i.e., managing the selection of energy-efficient service providers, of the proposed mode.

According to [3] instead of using users as a node they had used each IoT sensors as a node and authorise users using RESTful API. This suggested architecture enhances the privacy and security by implementing the core blockchain process along with the further security checks that enhances integrity and confidentiality in the system.

A Smart Contract is a computer program that directly and automatically controls the transfer of digital assets between the parties under certain conditions. In [4] Smart contract models are based on secured and immutable distributed ledgers; IOT devices on network can share data more securely across stakeholders, embed agreed-upon business terms to automate transactions, verify identification and authentication, and reduce costs by eliminating the intermediaries. The health of the IOT network is improved by letting devices register and validate themselves, automatically executing contracts, and reducing the threat of attack since there is no central system to be attacked.

## **Problem Statement**

Adopting Blockchain based home automation technology to reduce numerous security problems which arises due to equipment's small power and storage, making people vulnerable to various cyber-attacks, including ransomware.

## **Objectives**

- Design of a smart home architecture using Consortium Blockchain.
- Designing a working prototype of a Smart Home Mobile App for the proposed architecture.
- Implementing hardware design for a simple secure smart home architecture by utilizing commonly available IoT devices to evaluate.

## **Existing System**

The IoT based home automation consist of several smart devices for different applications of lighting, security, home entertainment etc. All these devices are integrated over a centralized network established by gateway.

Most of the existing blockchain-based architectures are quite complex to implement, as public blockchain is based on an open network and can suffer from scalability issues.

## **Proposed System**

To avoid these security threats and scalability issues, we have decided to adopt Blockchain technology. One of the methodologies in this is Consortium Blockchain, a decentralized database based on cryptographic technique, is gaining an enormous attention to attain security on IoT devices.

## **Advantages**

- Blockchain can improve efficiency and speed, as it can complete time-consuming processes and automate them, maximizing efficiency.
- It is secure and encrypted by design with so many independent nodes to verify the updates to the chain before the updates.
- Encryption with blockchain can help secure the IoT-based devices, making it impossible to overwrite existing data records.
- The block can be verified and inspected by all parties, which can help improve trust and access to the data.
- It allows data to be submitted peer-to-peer without centralizing the controls.

## **Disadvantages**

- Blockchain has a difficult process of implementation, and scalability is an issue.
- It needs huge storage; most of the blockchain consumes too much energy.
- Blockchain is highly energy-dependent, and it is not a distributed computing system.

## **Hardware Requirement**

- Arduino UNO
- Relays
- LED's, Buzzer
- Jump wires
- Bread board

## Software Requirement

- Android Studio, Arduino IDE
- Programming Language: JAVA, Spring framework, C++ programming
- EOSIO blockchain platform

## References

- [1] A. Johari and R. Alsaqour, "Blockchain-Based Model for Smart Home Network Security," *International Journal of Computer Networks and Applications*, vol. 9, no. 4, pp. 497–509, Jul. 2022, doi: 10.22247/ijcna/2022/214509.
- [2] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," *Int J Distrib Sens Netw*, vol. 15, no. 4, Apr. 2019, doi: 10.1177/1550147719844159.
- [3] S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, "Investigating Smart Home Security: Is Blockchain the Answer?," *IEEE Access*, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.
- [4] J. Singh, "Internet of Things with Smart Contract," *Int J Res Appl Sci Eng Technol*, vol. 10, no. 5, pp. 4505–4509, May 2022, doi: 10.22214/ijraset.2022.43446.
- [5] N. R. Pradhan and A. P. Singh, "Smart contracts for automated control system in Blockchain based smart cities," *J Ambient Intell Smart Environ*, vol. 13, no. 3, pp. 253–267, May 2021, doi: 10.3233/ais-210601.
- [6] M. Alshaikhli, T. Elfouly, O. Elharrouss, A. Mohamed, and N. Ottakath, "Evolution of Internet of Things from Blockchain to IOTA: A Survey," *IEEE Access*, vol. 10, pp. 844–866, 2022, doi: 10.1109/ACCESS.2021.3138353.
- [7] B. Kumar Mohanta, "INTERNET OF THINGS ENABLE SMART HOME SECURITY ISSUE ADDRESS USING BLOCKCHAIN."
- [8] Y. Kumar Sharma and J. Rajasthan, "A Comparative Performance Study on Smart Home Automation and Security System Using Blockchain Technology," 2021.