BlockChain-A Countermeasure for Security and Privacy in Domotics

Priyajot
Shri JJT University, Jhunjhunu, Rajasthan, India

Pramod Kumar
Shri JJT University, Jhunjhunu, Rajasthan, India
Corresponding author: Priyajot, Email: priyajotsingh77@gmail.com

Due to improvements in information & communication technology & growth of sensor technologies, Internet of Things is now widely used in smart homes for optimal resource management & ubiquitous sensing. In smart homes, many IoT devices are linked together via gateways. Importance of gateways in smart homes cannot be overstated, but their centralised nature exposes them to variety of security threats, including integrity, certification, & availability. In this paper, we propose blockchain-based smart home gateway network to address these security vulnerabilities. This network guards against likely smart home gateway attacks. In smart home setting with limited resources, devices such as sensors & actuators are connected & communicated in dispersed manner. One of problems in this sector is data storage & safe transmission since information is sensitive & contains lot of personal information from home network. Authors of this study have created3-tier architecture IoT-Fog-Cloud for safe & efficient data processing. Data may be analysed & monitored in real time with fog computing. Identity is one of thread models for IoT-based smart homes. Finally, this article focuses on Blockchain Technology, which has potential to overcome IoT application security problems. We built suggested network using Ethereum blockchain technology & tested it against industry standards for security, such as security response time & accuracy. We also propose some possible solutions to these security & privacy problems in IoT based on blockchain to illustrate how blockchain helps to IoT.

Keywords: Internet on Things, Blockchain, Domotics, Security, Privacy, Gateway.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 55–61. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-7

1 Introduction

The IoT is most hopeful technology to emerge previous decade. Industry produces large number of smart gadgets that can connect to various networks. Smart gadgets can sense their surroundings & interact with other smart devices innetwork. Kevin Ashton initially proposedInternet of Things inlecture about supply chains [1]. IoT is one of building blocks for creating smart house or city. Low-power embedded systems, fog computing, cloud computing, big data, machine learning, & networking are all being combined. Internet has grown so popular intwenty-first century thatnumber of devices linked tonetwork has reached billions, makingworld's populationminority. As billions of devices become linked, massive amount of data & information is created & exchanged between them. Asresult, processing& storing that data has become difficult problem in IoT. IoT offer slot of promise for developing numerous applications that will improve people's daily lives.Internet of Things makes traditional networks& applications more real-time, allowing for deployment of various sensors & smart devices to be monitored in real time. Data analysis may be done withhelp of some associated technology, which speeds upsystem's operation. Usage of fog computing, also known as edge computing, speeds up processing& computation by performing functions at network's edge [2].

Health care, smart parking, smart grid, smart lighting, smart product management, air pollution, forest fire detection, & earthquake early detection are some of uses of Internet of Things. Our main goal is to create smart IoT-based home system. Blockchain is made up of eight distinct components, each with its own set of specifications. Ledger is immutable & distributed historical record, & block chain's objective is to build one. Peer network is used to store, update, & maintain ledger. This ledger is replicated by each node in network. Goal of this network is to reach consensus oncontent of each update. This eliminates requirement for centrally copied ledger & assures that all ledger copies are identical. Membership Services department is in charge of user permission, authentication, & identity management. Smart house is private residence that transmits & receives data in real time. Through different household gadgets such as TVs, lighting, & refrigerators, it delivers automated & intelligent services. These devices are part of home-based communication system that allows gadgets to interact with one another & without side world without requiring human intervention. User's control range of home gadgets to monitor & manage themselves according on their preferences & home network configuration [3].

This transition, however, has resulted in smart home ecosystem that is heavily reliant on gateways. Smart homes use centralised networks to link several devices, posing major security threats. Smart TVs & refrigerators, which are essential components of smart homes, have been hacked inpast to send dangerous emails like phishing & spam. One example is hacking of newborn monitoring cameras at house in Texas, USA, in order to record vulgar sounds. These smart home devices are often exposed due tousage of unencrypted passwords on their wireless networks, making them perfect target for DDoS attacks. These difficulties occur as result of centralised IoT system structure, & security concerns such as data forgery & tampering, access to unauthorised devices, & inappropriate device control are rising as IoT era expands, due to attacks on IoT server & gateway systems. In IoT applications, several smart devices are employed. Majority of these smart gadgets are low-resource devices with limited processor & memory capacity. As noted before, numerous security issues occur in each oflayer architectures. Security & privacy issues must be addressed in order to make IoT application realistic enough for end users to trust it [4].

2 Overview of BlockChain

Public electronic ledger, similar torelational database, that users may freely share & that produces immutable record of their transactions, each of which is time-stamped & connected to one before it. Each thread block is digital record or transaction that permits unlimited or limited number of users to participate indigital ledger. When fresh data is added into blockchain, it can never be altered or

removed, ensuring data integrity. Every transaction that has ever occurred insystem has been recorded on blockchain & can be verified. From standpoint of network, Blockchain is distributed file system in which members maintain copies of file & agree on modifications through consensus. Each block contains collection of transactions as well as main data such as previous block's timestamp & cryptographic signature (hash), current block's hash, & other data. Hash of previous block links current block to previous block, & subsequent blocks will require hash of current block as well, resulting inchain of blocks. If anything in block is altered, hash can be computed & value discovered that differs from one supplied, leading block to be refused.

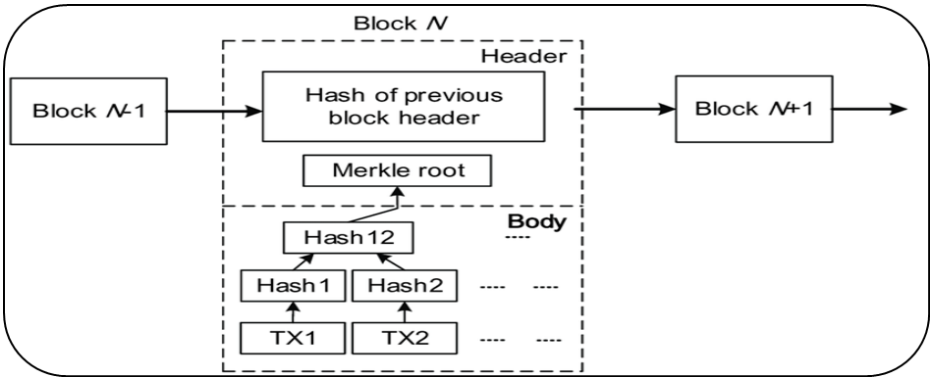

Fig. 1. Blockchain Structure

Table 1. Smart appliance descriptions in Smart Home application

IoT Home Appliance	Description
Smart Coffee maker	It can be used as smart plug. Wireless or Bluetooth connection option available. Smart coffee maker allows easily schedule, Monitor & update from anytime & anywhere.
Indoor Lighting System	Intelligent lighting bulbs are connected in mesh networks wirelessly with other lighting system. They can be used for different Benefit like energy management, easy to monitor through mobile or tablet & remote control is also possible.
Smoke detector	Smart home gas detection or monitor of different levels in kitchen is much needed. Smart gas sensor like MQ series & Others are used to monitor gas linkage & detect fire inside home.
Smart Door Lock	The smart device is capable of sensing activity around door & act accordingly. Different authentication techniques are embedded with device for validating purpose.
Smart Camera/ Motion Sensor	In smart home system, smart camera plays vital role to monitor elder person's condition in room. Monitoring the Home users activity inside home from remotely make easy to take call in emergency.
Water Management	Using smart water controller reduces waste of water by which it will lower bill also. Most importantly it can be accessed Remotely by mobile devices or through tablet.

Health & Fitness Devices	Some of essential smart health & fitness devices like Blood pressure monitor, Heart rate monitor, Sleep tracker, smart watch, and Activity tracker help to get real-time information. It makes easy to make decision in case of emergency & live healthy Life.

3 Review Of Literature

A public blockchain & private blockchain are two sorts of blockchains. Permission less blockchain is public blockchain. Anyone may effectively & usefully participate.

They can participate by viewing or adding to blockchain. Because it is decentralised, this public chain does not havesingle entity in charge ofnetwork. That is to say, once data on blockchain has been verified, it cannot be altered. This public blockchain is advantageous because it allows users to freely enter& see data, ledger is distributed rather than centralised, it is immutable to prevent data manipulation, & it is safe due to 51 percent rule.

In [5] demonstrates that bulk of peers known to Bitcoin network reside in its own system. This means thatpeer-to-peer network is not properly connected, which might result in relay issues for newly generated blocks on Blockchain.

The authors show in [6] that when large number of nodes are controlled byattacker with high computational power (or not), overall computational power in Blockchain with few miners can reach fraction that is deemed high relative to total computational power in small system. Integrity of system might be jeopardised in this instance due toattacker's capacity to induce forks on purpose.

Inselfish mining attack, as described in [7], malicious mining pool decides to keepblocks it discovers unpublished. As result, split in Blockchain is created. Public branch with miners is one of branches, while private branch with damaging pool is other. It keeps mining on private branch until both branches are same length, at which point it broadcasts it. As result, it may become longest branch, & other miners might adopt it. Public branch, along with all data it holds, may be deleted after period. Damaging pool may gain advantage based on miner's ratio between both branches.

Another assault, known ashistory-revision attack, was mentioned byauthors in [8]. Attacker has far more computing power than other nodes in such assault. Then, using Proof of Work's hard terms, he may construct fork & destructive branch while bypassing original branch. Other miners may then accept it, resulting in Blockchain's history being converted.

Security considerations for domotics gateways

The domotics is made up of several gadgets that are all managed & monitored through gateway. Network design like this might expose data inhome, lead to privacy breaches, create gadget failures, & endanger individuals. Whenperson is exposed tosmart home network set up in each house hold, data acquired by gadgets intargeted manner might be leaked. It is difficult to connect many heterogeneous devices due tolack of security standards for smart homes & gadgets. As result, many services are difficult to provide to users. Security of smart home gateways is essential, & standards for gateway security are given below [9]:

- **Confidentiality:** Networks set up in smart homes gather& retain variety of data, including sensitive information provided by inhabitants. Only authorised staff should have access to this information, which is important aspect of smart home security. We utilise blockchain with encryption technique & customise it using key to keep features of smart homes private.

- **Integrity:** When data is transferred& received across configurations, there must be no falsification during transmission. Hash function lowerschances of this data being tampered with & enables for tracking & verification of exactly what data is saved.
- **Validation:** Authentication prevents attackers from acting maliciously with in conventional network from outside in smart home network settings. Blockchain is used to validate legitimacy of network members, & it can be verified at any time to ensure appropriate smart home network design [10].

4 The Technical Challenges & Advances of BlockChain

Scalability: Almost all existing Blockchain systems, such as Bitcoin, Ethereum, Ripple, & their associated consensus methods, have limited scalability. Decentralised nature of blockchain technology poses tough restriction. Each network node processes each transaction & maintains copy of ledger's current state. Two major scalability concerns aretime it takes to place transaction into block & time it takes to reach consensus.

Throughput: Bitcoin has transaction rate of about 7 transactions per second, whereas Ethereum has rate of around 20 transactions per second. VISA, for example, processes 1668 transactions per second, whereas PayPal handles 193. As result, Bitcoin & Ethereum's throughput must be raised in order for them to compete with more popular systems like VISA & PayPal. When frequency of Blockchain transactions approaches that of VISA, blockchain networks' throughput must be raised.

Latency: Creating or mining block containing transactions in Bitcoin network presently takes approximately 10 minutes, whereas ("Bitcoin, Litecoin, Namecoin, Dogecoin, Peercoin, Ethereum stats,") Ethereum takes about 14 seconds. More time must be spent on block creation & validation in order to ensure that transaction inputs have not been used previously, resulting in double-spending attacks. Existing blockchain systems must improve block generation & validation speeds in order to perform transactions while maintaining security.

Bandwidth & Size: Bitcoin blockchain is now 190.65 GB in size, whereas Ethereum blockchain is 330.61 GB in size. Bitcoin blockchain might grow in size if throughput reaches level of VISA network. Bitcoin's average block size is currently 1 MB. Instead of block size restriction, Ethereum utilises gas limit method. Generation of Bitcoin 1 MB block, which contains on average 500 transactions, takes on average 10 minutes. If Bitcoin blockchain is to control more transactions, it must overcome size & capacity problems [11].

5 Security & Privacy Issue in BlockChain

A blockchain is distributed database of records, or public ledger, of all completed & shared transactions or digital events among members. Blockchain technology was created as result of Bitcoin crypto currency.

Bitcoin is used to carry out transactions inpeer-to-peer network. Usage of Blockchain in non-financial applications has piqued curiosity of scientific community as well as industry professionals during last decade. Because of its safe foundation, Blockchain offers wide range of possible uses, as illustrated in Figure 2. [12] ADEPT (Autonomous Decentralized Peer to Peer Telemetry) is system developed by IBM & Samsung that leverages aspects of bitcoin's fundamental architecture to build distributed network of devices for decentralised IoT. To executesmart house, we require private Blockchain architecture, which comes in three flavours: public, private, & consortium. Here, nodes will be restricted; not every node will be able to join in this Blockchain, & data access will be managed with rigorous authority. Many sensors & actuators are connected to data gathering & processing in smart home IoT ecosystem. Incase of smart home automation, there are limited amount of nodes, therefore permission Blockchain is good fit. Different consensus methods that address development of IoT applications in Blockchain networks are discussed in detail. As result,

such Blockchain categories are designed to be modified in order to preserve compatibility with existing applications. Scalability is benefit of permission Blockchain. In such environment, data is kept on every computer in network, & every node participates in verification of all transactions. In this Blockchain, just limited numbers of fixed participants are necessary to operate, making it much easier forgroup of users to cooperate & change rules or reverse transactions. Open Blockchain is permission Blockchain network in which end users must register in order to submit or perform transactions that have been published insystem. Security & privacy for IoT-based home automation may be addressed by adopting permission-based Blockchain, in which each node must authenticate to network [13].

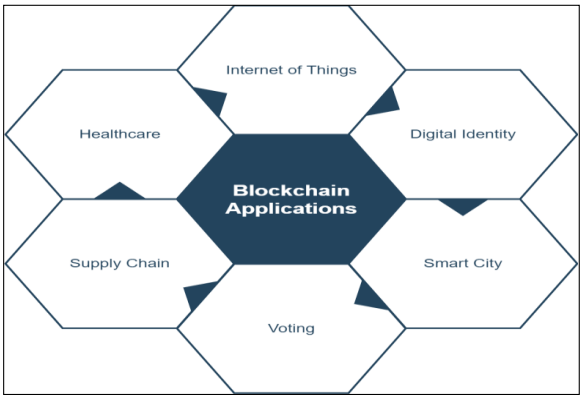

Fig. 2. Open Blockchain's Basic Architecture

Due to large number of dispersed sensors linked innetwork, user registration is required to authenticate IoT device to network. All of sensors are linked to Raspberry Pi, which serves as fog computing & performs local operations. Once transaction has been validated bynodes, it is stored in all of network's nodes. We can make smart house truly usable by utilising Blockchain idea. IoT enabled smart home network has following security problems, which blockchain can address [14]:

- The devices are identified byunique hash number.
- Users are authenticated viadecentralised authentication method.
- Business logic is enabled viaaccess control mechanism enabled bysmart contract.
- Every transaction available to each& every node after verification& validation is referred to as trust management.

6 Blockchain's Future.

Blockchain has lot of interesting potential applications. It's technology that get slot of attention & meets criteria for lot of other fascinating developing technologies. IoT, AI, smart gadgets, & self-driving automobiles are justfew examples. It might serve as enabler for all of technologies described above, as well as others. Consider concept of smart refrigerator that would automatically recordphrase "More Milk" as soon as it ran out. When discussing such implementation, most individuals become frightened & afraid because they are concerned about security & how to safeguard it. What guarantees security & immutability of system's data? [15]

Another aspect worth mentioning is ever-decreasing cost of devices & ever-increasing need for processing power. All of this is possible with blockchain. It is already involved in number of developing technologies, & by expanding; it is allowing new technologies to arise since it is making more& more things feasible every day [16].

7 Conclusion

We offer detailed study of security issues of IoT-based smart home architecture using Raspberry Pi, Fog computing for data processing, & Docker containers to execute various applications in this article. Despitefact that numerous security& privacy protocols exist, they are not relevant to IoT-based architecture due to resource constraints & use of lightweight devices to connect to smart home system. Then we discovered few attack models. Following solutions are provided by this architecture to address heterogeneous IoT & centralised gateways that makeup smart home's secrecy, integrity, & authentication problems. In smart home gateways & heterogeneous IoT, SHA2 encryption method is used to overcome secrecy & authentication issues. In addition, blockchain technology is utilised to ensure thatdata kept ingateway is secure. By efficiently moulding raw data, data transformation method is applied in architecture. Finally, we believe that in IoT-based smart home setting, Blockchain security & privacy may be accomplished [17]. Scalability problem is overcome by utilising permission Blockchain. Anonymity or privacy goal can be achieved by keeping fingerprint of digital asset rather than digital asset itself. Cross fault tolerance, or XFT, can be used to create dependable & secure distributed systems. In future study, we'll try to investigate more attack models, security, & privacy of IoT-based smart home automation by implementing this Blockchain on Hyper ledger utilising Docker as container in real application.

References

[1] D. Geneiatakis et al., "Security & privacy issues for IoT based smart home", in *40th In.l Conven. on Inform. Commun. Tech. Electro. Microelectronics*, 2017, pp. 1292–1297.

[2] Jose and R. Malekian, "Improving smart home security: Integrating logical sensing into smart home", *IEEE Sensors J.*, vol. 17, no. 13, pp. 4269–4286, 2017.

[3] C. Lin et al., "Homechain: Blockchain-based secure mutual authentication system for smart homes", *IEEE Int. Things J.*, vol. 7, no. 2, pp. 818–829, 2019.

[4] W. Felter, A. Ferreira, R. Rajamony and J. Rubio, "An updated performance comparison of virtual machines & linux containers", in *Performance Analysis of Systems & Software*, 2015, pp. 171–172.

[5] S. S. Panda et al., "Study of Blockchain Based Decentralized Consensus Algorithms", in *IEEE Region 10 Conference (TENCON)*, 2019, pp. 908- 913.

[6] P. K. Sharma et al., "SoftEdgeNet: SDN based energy-efficient distributed network architecture for edge computing", *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 104–111, 2018.

[7] N. Y. Kim et al., "Survey on cyber physical system security for IoT: issues, challenges, threats, solutions", *J. Inf. Process Syst.*, vol. 14, no. 6, pp. 1–10, 2018.

[8] X. Huang et al., "Software defined networking for energy harvesting internet of things", *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1389–1399, 2018.

[9] C. M. S. Magurawalage et al., "Energy-efficient & network-aware off loading algorithm for mobile cloud computing", *Comput. Netw.*, vol. 74, pp. 22–33, 2014.

[10] S. Rathore, B. W. Kwon and J. H. Park, "BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network", *J. Netw. Comput. Appl.*, vol. 143, pp. 167–177, 2019.

[11] B. C. Choi et al., "Secure firmware validation & update for consumer devices in home networking", *IEEE Trans. Consum. Electron,* vol. 62, pp. 39–44, 2016.

[12] K. Palani, E. Holt and S. Smith, "Invisible & forgotten: Zero-day blooms in IoT", in *Int. Conf. on pervasive computing & communication workshop*s, 2016.

[13] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in IoT: mirai & other botnets", *Computer*, vol. 50, pp. 80–84, 2017.

[14] I. C. Lin and T. C. Liao, "Survey of Blockchain security issues & challenges", *I.J. Netw. Secur.,* vol. 19, pp. 653–659, 2019.

[15] M. M. Salim, S. Rathore and J. H. Park, "Distributed denial of service attacks & its defences in IoT: survey", *J Supercomput.*, vol. 10, pp. 1–44, 2019.

[16] M. Rychowicz et al., "Fair Two party Computations via Bitcoin Deposits", *Proc. Int'l. Conf. Financial Cryptography & Data Security*, Springer, 2014, pp. 105–21.

[17] Y. Sompolinsky and A. Zohar, "Accelerating Bitcoins Transaction Processing", *Fast Money Grows on Trees, Not Chains*, 2013.