Blockchain for IoT Security and Privacy: A Case Study of a Smart House

Mrs.G.Swetha,Assistant Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana,
E-Mail-id swetha.gottiparthy@cmrec.ac.in

Mr.K.Narender Reddy,Assistant Professor, Department of Information Technology, CMR Engineering College, Hyderabad, Telangana,
E-Mail-id k.narenderreddy@cmrec.ac.in

Abstract - Security and privacy for Internet of Things (IoT) networks continue to be a significant concern, primarily because of the vast scale and scattered nature of IoT networks. Although blockchain-based systems offer decentralised security and anonymity, they come with a high energy, latency, and processing overhead, making them unsuitable for the majority of IoT devices with limited resources. In our earlier work, we introduced a lightweight instantiation of a BC that was specifically designed for usage in the Internet of Things (IoT) by getting rid of the Proof of Work (POW) and the idea of coins. Our strategy, which was demonstrated in a smart home environment, has three key tiers: cloud storage, overlay, and smart house. In this essay, we go into more detail and define the different essential elements and features of the smart home tier. Every smart home has a "miner," which is a high-resource, constantly online device in charge of managing all communication both inside and outside the house. The miner also keeps a private and secure BC that is employed for monitoring and managing conversations. By carefully examining its security in relation to the core security objectives of confidentiality, integrity, and availability, we demonstrate the security of our proposed BC-based smart home system. Finally, we demonstrate simulation findings to demonstrate that our approach's overheads (in terms of traffic, processing time, and energy usage) are negligible compared to the security and privacy improvements it provides.

Introduction - Devices that are part of the Internet of Things (IoT) generate, analyse, and share enormous volumes of data that is sensitive to privacy as well as security and safety, making them attractive targets for various cyberattacks [1]. The Internet of Things (IoT) is made up of several new networkable gadgets that are lightweight and low energy. The issue of inexpensively enabling security and privacy is particularly difficult given that these devices must focus the majority of their available energy and compute on carrying out essential application functions. In terms of energy use and computing overhead, traditional security techniques are frequently expensive for the Internet of Things. Due to the complexity of scale, the many-to-one nature of the communication, and single point of failure,

many of the state-of-the-art security frameworks are highly centralised and hence may not be ideal for IoT [2]. Existing techniques to preserve user privacy frequently either reveal noisy data or inadequate data, which could potentially prevent some IoT applications from providing individualised services [3]. As a result, an IoT security and privacy precaution must be compact, scalable, and distributed. The distributed, secure, and private characteristics of the Blockchain (BC) technology, which serves as the foundation for Bitcoin, the first cryptocurrency system [4], give it the potential to address the aforementioned difficulties.

Core Components –

A. Transactions : Transactions are communications between nearby objects or overlay nodes. The smart home in British Columbia uses a variety of transactions, each of which serves a particular purpose.
Devices create store transactions in order to store data. To access the cloud storage, an SP or the property owner must create an access transaction. The house owner or SPs create a monitor transaction to periodically monitor a device's information. A genesis transaction is used to add a new device to the smart home, while a removal transaction is used to delete a device. The communication is encrypted in all of the aforementioned transactions using a shared key. To track down any content changes made to transactions while they are being transmitted, lightweight hashing [8] is used. A local private BlockChain is where all transactions to or from the smart home are stored (BC).

B. Local BC : Every smart home has a local private BC that records transactions and contains a policy header to impose the users' policy for incoming and outgoing transactions. The transactions of each device are chained together as an immutable ledger in the BC starting with the genesis transaction. Block header and policy header, which are both displayed at the top of Figure 1, are two of the headers that are present in each block of the local BC. To maintain the BC's immutability, each block's header contains the hash of the one before it. The policy header is employed to authorise devices and carry out the homeowner's control policy regarding his property. The upper right corner of Figure 1 depicts the four parameters in the policy heading. The requester PK in the received overlay transaction is referred to by the "Requester" parameter. This field is local for local devices. Similar to the "Device ID," which is displayed in the fourth row of the proposed policy header in Figure 1. The requested action in the transaction is listed in the second column of the policy header and can be one of the following: monitor to access real-time data from a specific device, access to access stored data of a device, store to store data locally, store cloud to store data on the cloud, access to store data on the device, or access to store data on the device. The policy header's third column contains the ID of a smart home device, and the last column lists the action that has to be taken for transactions that fit the preceding properties.

C. Home Miner - The processing of incoming and outgoing transactions to and from the smart home is done centrally by a device known as a "smart home miner." A

separate standalone device, such as F-secure [9], might be positioned between the devices and the home gateway, or the miner could be integrated with the Internet gateway of the house. The miner authenticates, approves, and audits transactions similarly to current central security apparatuses. The miner additionally performs the following extra tasks: genesis transaction generation, key distribution and update, transaction structure change, cluster formation and management. All transactions are gathered into a block by the miner, who then adds the entire block to the BC. The miner runs a local storage to offer more capacity.

D. Local Storage - A device used by devices to store data locally is known as local storage, such as a backup drive. The storage unit can be a standalone unit or incorporated with the miner.

Each device's data is kept in the storage as a ledger chained to its starting point using the First-in-First-out (FIFO) method of data storage.

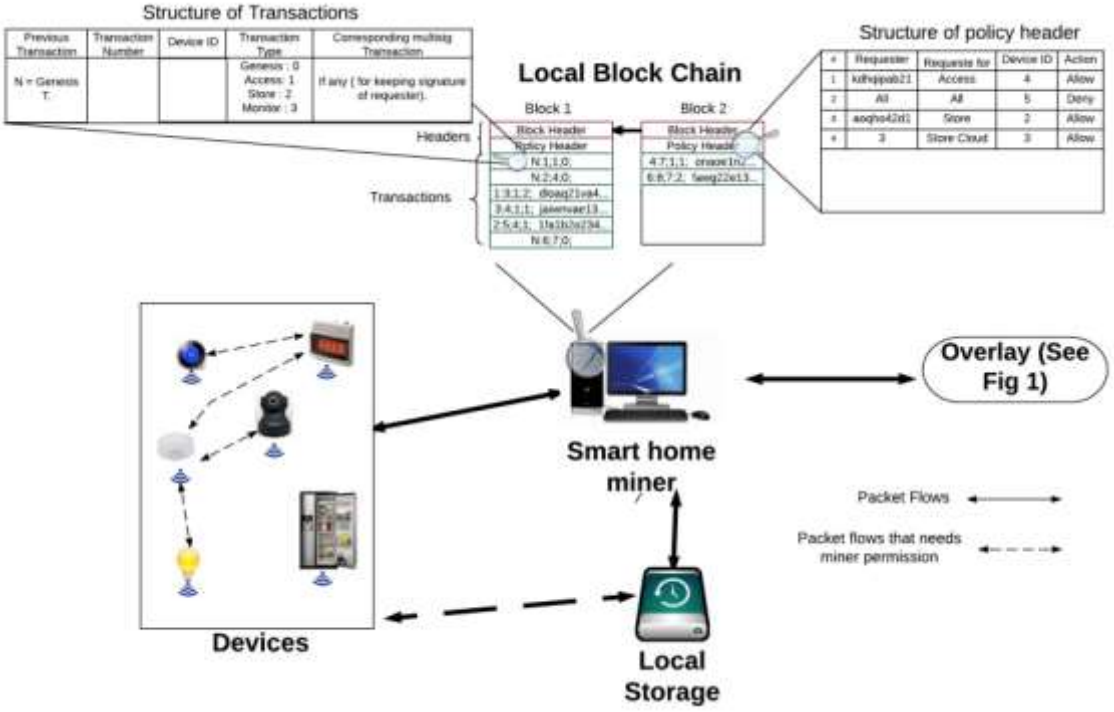

Figure 1 shows an overview of a smart home. IoT gadgets, local storage (see section II.D), miners (see section II.C), and the neighbourhood BC make up the smart house (see section II.B)

Evaluation And Analysis - The performance, privacy, and security of the smart home in BC are fully covered in this section.

A. Security Analysis: Each security design must take into account the CIA—Confidentiality, Integrity, and Availability—three fundamental security needs. Only the authorised user will be able to access the information, thanks to confidentiality message. When a message is transmitted, integrity ensures that it reaches its intended recipient without modification, and availability that each service or piece of data is accessible to the user at the appropriate time. Part III discusses the techniques used to fulfil the first two requirements. Devices are safeguarded from harmful requests to expand the availability of smart homes. This is accomplished by restricting the transactions that are approved to those

with which each device has a common key.

Before being sent to the devices, transactions received via the overlay are first approved by the miner. Furthermore, compared to currently available smart home gateway technologies, it can be argued that our BC-based framework only slightly increases transaction processing times. Moreover, a one-time delay for generating and distributing shared keys occurs during initialization. In conclusion, the extra delays are not considerable and have no effect on the accessibility of the smart home technology.

The methods used by our framework to meet the aforementioned security requirements are listed in Table I.

B. Performance Evaluation: In exchange for better security and privacy, BC-based design places a computational and packet overhead on the miner, smart home devices, and Internet of Things (IoT) infrastructure. With the Cooja simulator, we recreated a smart house scenario in order to assess these overheads [13]. We created a different simulation of a scenario that handles transactions without encryption, hashing, or BC in order to compare the overhead of the BC-based design. This baseline approach is referred to as the "base method". Since IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) is ideally suited to the resource limitations for a smart home scenario, we employed it as the underlying communication protocol in our simulation. We created three z1 mote simulations that resemble smart home equipment and transmit data to a home miner simulation that is also a z1 mote every 10 seconds. The results shown are an average over the three minutes that each simulation lasted. To store data and return the block number, a cloud storage is directly connected to the miner. It is important to note that in our simulation, the overlay latency and processing are not taken into account. We simulated storage and access transactions in order to provide an exhaustive assessment.

Requirement	**Employed SafeGaurd**
Confidentiality	Achieved using symmetric encryption.
Integrity	Hashing is employed to achieve integrity.
Availability	Achieved by limiting acceptable transactions by devices and the miner.
User control	Achieved by logging transactions in local BC.
Authorization	Achieved by using a policy header and shared keys.

Conclusion – IoT security is currently receiving a lot of interest from both academics and business. Due to significant energy consumption and computational overhead, current security solutions may not be appropriate for IoT. We previously presented a way that takes advantage of the Bitcoin BC, which is an immutable ledger of blocks, to solve these problems. A smart home was used as a case study to illustrate the concept. We addressed the numerous transactions and processes connected to the smart home tier in this paper as well as its various key components. We also provided a comprehensive examination of its privacy and security. Our simulation findings show that the overheads incurred by our strategy are negligible and tolerable for IoT devices with limited resources. Given the enormous security and privacy advantages on offer, we contend that these overheads are worthwhile. We believe that this study is the first to attempt to optimise BC in the context of smart homes. We will explore the applications of our framework to other IoT fields in our upcoming research.

Reference –

[1] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security,privacy and trust in internet of things: The road ahead," ComputerNetworks, vol. 76, pp. 146–164, 2015.

[2] R. Roman, J. Zhou, and J. Lopez, "On the features and challengesof security and privacy in distributed internet of things," ComputerNetworks, vol. 57, no. 10, pp. 2266–2279, 2013.

[3] A. Chakravorty, T. Wlodarczyk, and C. Rong, "Privacy preserving dataanalytics for smart homes," in Security and Privacy Workshops (SPW),2013 IEEE. IEEE, 2013, pp. 23–27.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] S. King, "Primecoin: Cryptocurrency with prime number proof-ofwork," July 7th, 2013.

[6] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things:Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.

[7] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder,Bitcoin and cryptocurrency technologies. Princeton University Pres,2016.

[8] A. Bogdanov, M. Knezevi ˇ c, G. Leander, D. Toz, K. Varıcı, and I. Ver- ´bauwhede, spongent: A Lightweight Hash Function. Berlin, Heidelberg:Springer Berlin Heidelberg, 2011, pp. 312–325.

[9] F.-S. sense, https://sense.f-secure.com/, [Online; accessed 19-November2016].

[10] H. Delfs, H. Knebl, and H. Knebl, Introduction to cryptography.Springer, 2002, vol. 2.

[11] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid andsmart home security: Issues, challenges and countermeasures," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954,2014.

[12]wired,https://www.wired.com/2016/10 /internet-outage-ddos-dns-dyn/,[Online; accessed 10-December-2016].

[13]Cooja,http://anrg.usc.edu/contiki/index .php/CoojaSimulator/,[Online;accessed 19-November-2016].

[14] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman, and R. Boreli, "An experimental study of security and privacy risks with emerginghousehold appliances," in Communications and Network Security (CNS),2014 IEEE Conference on. IEEE, 2014, pp. 79–84.

[15] V. Sivaraman, D. Chan, D. Earl, and R. Boreli, "Smart-phones attackingsmart-homes," in Proceedings of the 9th ACM Conference on Security &Privacy in Wireless and Mobile Networks. ACM, 2016, pp. 195–200.