Blockchain-Based Access Control for IoT in Smart Home Systems

Chapter · September 2020

DOI: 10.1007/978-3-030-59051-2_2

CITATIONS
0

READS
236

3 authors:

Bacem Mbarek
Masaryk University
18 PUBLICATIONS **58** CITATIONS
SEE PROFILE

Mouzhi Ge
Deggendorf Institute of Technology
88 PUBLICATIONS **1,240** CITATIONS
SEE PROFILE

TomáŠ Pitner
Masaryk University
104 PUBLICATIONS **335** CITATIONS
SEE PROFILE

Blockchain-Based Access Control for IoT in Smart Home Systems

Bacem Mbarek(✉), Mouzhi Ge, and Tomas Pitner

Faculty of Informatics, Masaryk University, Brno, Czech Republic
bacem.mbarek@mail.muni.cz, mouzhi.ge@muni.cz, tomp@fi.muni.cz

Abstract. Smart home systems are featured by a variety of connected smart household devices, where Internet of Things (IoT) is one of the critical enablers in the smart home environment. Since these smart home IoT devices are working collaboratively, the access control among the IoT devices becomes more and more important because non-authorised access can result in resource misuse, home breach threats or private information disclosure. Thus, an effective access control in smart home systems is essential to prevent from unauthorized use of the available resources. However, most of the access control schemes in smart home systems are still lack of decentralized peer trust and hard to control the security and credibility of the smart home IoT network. This paper therefore proposes a Blockchain-based Access Control (BAC) solution by integrating the Blockchain technique to IoT networks, where the agent-based policy is proposed to improve the efficiency of the Blockchain management. In order to validate the BAC solution, we demonstrate the implementation process of the proposed BAC in the parental control scenario and also evaluate performance and feasibility in a simulated smart home.

Keywords: Blockchain · Smart home systems · IoT · Access Control

1 Introduction

Nowadays, smart home systems are developed to enable home automation and increase the quality of life [18]. These systems are usually featured by using a smart phone application to interconnect and control different home devices such as lights, power plugins, cooking devices, temperature and humidity sensors as well as security systems [25]. In order to implement the home device interconnections, Internet of Things (IoT) is widely used as one typical wireless communication technique [17]. IoT is a concept of interrelated physical objects or devices that have been used in different application domains such as in smart cities, vehicular networks, military, and healthcare [11]. In the smart home context, the main goal of IoT is to connect different kinds of objects such as refrigerator, washing machines, TV, laptop, or cars [33] to facilitate people's daily life.

While the smart home system brings comfort and convenience to the home environment, it is also found to be vulnerable and exposed to different non-authorised access threats [12]. For example, if an attacker targets the functionality of the access control system by modifying the authentication headers in the

S. Hartmann et al. (Eds.): DEXA 2020, LNCS 12392, pp. 17–32, 2020.
https://doi.org/10.1007/978-3-030-59051-2_2

packets, this attack can create a fake identity and access without legal authorization to the IoT devices deployed in a home environment. In order to prevent such threats, access-control mechanisms are being investigated as policy enforcement components or main gateways to secure communications between IoT devices [30]. However, current access-control mechanisms used in IoT are with limited flexibility and inefficient to secure the resource constrained smart home devices [22]. These smart home devices are commonly prone to malicious attacks and require mutual authentication to guarantee the confidentiality and security of data shared in the IoT network [15]. As a typical IoT network, smart home systems urge to be a highly secure, independent and distributed platform [11]. In order to tackle this issue, the emergent Blockchain technology can be used to transform the way that data will be shared in IoT networks [2].

In this paper, we therefore propose a Blockchain-based Access Control solution, named as *BAC*, which controls the access to smart home devices and ensures secure communications between the IoT devices and the householders. In particular, we address the drawbacks of regular Blockchain access control protocols in terms of the time cost involved in the necessity of contact with the owner of the resource for each new access, by using agent-based software as an authenticated key for access control management. The contribution in this paper is twofold. First, we highlight the problem of the time cost involved in getting an access permission with the standard Blockchain platform. Second, we present an agent-based method to monitor inappropriate activities of users in the Blockchain. While we consider that Blockchain is capable of controlling the secure access and efficient data sharing in smart home systems, the *BAC* can be also applicable for diverse scaled IoT applications. Further, the collaborations of smart home devices can benefit from Blockchain to enhance the processes of authentication and coordination of data collection as well as optimizing the usage of the available resources [14,35]. In order to validate the proposed BAC solution, we demonstrated its applicability in the parental control scenario in smart home systems.

The remainder of the paper is organized as follows. Section 2 presents an overview of Blockchain with common definitions. Section 3 proposes BAC solution by integrating the Blockchain into smart home. To evaluate the proposed solution, Sect. 4 describes a typical smart home scenario and implement BAC in smart home systems. Section 5 concludes the paper and outlines future directions for this work.

2 Related Work

While the increasing use of IoT devices in smart home allows for real-time, low-cost data acquisition, the smart home IoT network is exposed to challenging security and access threats such as spoofing user identity, cloning access control cards, or submission of false information [18]. In order to prevent such threats, access-control mechanisms are being investigated to secure communication among the IoT devices. However, most current mechanisms used in comput-

ing systems can be inappropriate for resource constrained environments including IoT-based home automation systems [1]. Although the smart home is a specific environment, the overall nature of security threats is similar to other domains. We describe three types of threats and their consequences in smart home systems as follows.

Confidentiality Leaking: An attacker may try to access the sensitive information in the smart home. For example, the confidentiality threats could lead to house stealing by hacking information about air conditioning system parameters or light system operation to determine whether a house is occupied or not. Thus, the confidentiality should be considered to ensure the safety of IoT systems [36].

Access Phishing: An attacker can confuse the home system by letting the system agree that there is an using emergency alerts and opening doors and windows to allow an emergency exit. Therefore, without appropriate access control schemes, the smart home can be in danger [30].

Unauthorized Access: An attacker can use unauthorized devices in the IoT network by for example cloning some access card. Since many smart home devices can be physically attacked, an attacker may start an energy depletion attack, a form of denial of service. Thus, using simple access control system through password and key management is not enough. Dynamic key updating scheme is necessary to protect smart home network [16].

A variety of solutions have been proposed to solve the access control problems in smart home by identifying the malicious activities and exploring secure access control management mechanisms among house members [8,9,30]. In [19], the authors proposed a platform, named FairAccess, to secure the IoT network based on the token method, where Fairaccess only supports the Blockchain authorization based on access tokens using smart contracts. However, their proposal has some issues, for example, the time involved in obtaining access licenses takes long, the time cost is mainly in the necessity of contacting with the owner of the resource for each new access or for each token expiration. In [8], the authors also employed Blockchain in access control. They proposed a Blockchain-based smart home framework that is used for handling all the internal communications inside home and external communications from or to the home. In [30], authors proposed a private Blockchain as central intelligent home administrator. Their proposed model addresses the problems related to DoS attacks by controlling all incoming and outgoing packets to smart home devices. In [9], authors proposed a managing IoT device using Blockchain platform that is manipulated by Ethereum Blockchain with smart contracts for tracking meter and setting policies. It can be used to turn on and off air conditioner and light bulbs in order to save energy.

From the Blockchain perspective, authors in [7] proposed a combination of private and public Blockchains. The private Blockchain was employed to handle data flow in SHS, whereas the public Blockchain was to manage data flow over cloud storage. Their approach is composed of three layers: smart home systems (SHS), overlay network and cloud storage. To improve further the security between IoT devices and the Blockchain, different researchers proposed the inte-

gration of cloud computing in Blockchain platforms to manage a large number of IoT devices. In [21], the authors implemented a cloud server as a centralized and decentralized combined architecture and an intermediate between IoT devices and the Blockchain. In [37], the authors combined Blockchain and off-Blockchain storage to construct a personal data management platform focused on data privacy. Similarly, in [20], the authors proposed a secure service providing mechanism for IoT by using Blockchain and cloud. However, the unstable connection between cloud servers and IoT devices could cause communication delay as well as prevent the proposed model from achieving optimal performance and security scores. In [9], authors have demonstrated how Blockchain can be used to store IoT data with smart contracts. In [24], authors have proposed a new framework in which Blockchain is used to support the distributed storage of data in IoT applications. In [5], authors have proposed various protocols that enable the synchronization of IoT endpoints to the Blockchain. To this end, the authors have used several security levels and communication requirements. They have also analyzed the traffic and the power consumption created by the synchronization protocols via numerical simulations. Extended reviews of using Blockchain to store IoT data with a focus on open problems of anonymity, integrity, and adaptability as well as to architect Blockchain-based IoT applications are available in [4]. Therefore, the development of a smart home based on Blockchain system with scalable communication network is required for ensuring the safety of users as well as the transmission of aggregated IoT data.

3 BAC: Blockchain-Based Access Control Model

In order to provide an effective access control solution for smart home systems, we integrate Hyperledger Fabric-based Blockchain [10] to IoT network to secure the peer and trust and use agent-based policy model to improve the Blockchain efficiency. The agent-based policy aims to reduce or eliminate human interventions in the Blockchain, as every agent in the IoT device has the capacity to autonomously process Blockchain transactions. In addition, the Blockchain can organize the user behaviors by using a mobile agent which to detect inappropriate user activities with the used IoT device.

3.1 System Setting and Roles

In the system, the Blockchain is composed of three roles: 1) endorsing peers, 2) the ordering service, and 3) committing peers. Each householder is a transmitter/receiver that sends requests to a manager controller in the channel through the Blockchain platform. Inside the Blockchain, the smart contract is a code fragment that executes the terms of a contract [32]. A channel can be defined as a sub-network for peers communication. In the smart home context, it can be communication between IoT devices, and family members. Using different channels can divide transactions according to different boundaries according to some service logic. In the smart home systems, the transactions can be considered as an activity request or a collaboration order.

- **Endorsing peers** are the manager members in the Blockchain channel. The endorsing peers will endorse a transaction proposal, for example, the endorsement can be carried out based on specified family policies. When enough endorsing peers support a transaction proposal, it can be submitted to the ordering service to be added as a block. During the commissioning and configuration of the Blockchain network, the smart home system should firstly select the endorsing peers.
- **Ordering service** collects transactions for a channel into proposed blocks for distribution to peers. Blocks can be delivered for each defined channel. The smart home ordering service is to gather all the endorsed transactions, perform the ordering in a block, and then send the ordered blocks to the committing peers.
- **Committing peers** includes all the members of the Blockhain. The committing peers run the validation and update their copy of the Blockchain and status of transactions. Each peer receives the block, as a committing peer, can now attach the new block to its copy of the transactions. Committing peers have also the responsibility of updating the shared ledger with the list of transactions.

When a householder agrees to enter a transaction, he determines the parameters of this transaction by specifying its request, its location, authentication key. Each transaction is stored in a smart contract and transmitted to the house managers as playing the rules of endorsing peers of the Blockchain platform. The received transaction is verified by checking their smart contract. Then, the endorsing peers verifies the received transaction by executing the static agent policies. After, the verification of the received transaction by the house managers and the creation of the Block by the ordering server, the endorsing peers will submit a mobile agent to the requested user of IoT sensors to detect the inappropriate activities during the utilization of connected device.

3.2 Agent-Based Policy for the Blockchain Management

In the smart home systems, there can be different frequent activity requests such as turn on or off the light. For those frequently occurred requests, it is inconvenient to manually approve each request for the endorsing peers. In order to increase Blockchain efficiency for smart home IoT network, the Blockchain platform will create two kinds of agents: (1) a static agent, and (2) a mobile agent. Both the static and mobile agents are dedicated to every new transaction. The endorsing peers can monitor the selected node by using those agents. While the static agent is used to verify the received transaction, the mobile agent is to check the user activities. The mobile agent also can control the connected devices in real time, for example, if activities from some IoT device are inappropriate, the mobile agent can turn off this IoT device. The positions of these agents and their functions are depicted on Fig. 1.

Static Agent is a static agent that will be implemented in each peer device of the Blockchain. Once the peer device receives a transaction such as a activity request, The peer device will use the static agent to verify and check the received transaction. Those Agents intend to replace manual verification. Then, the static agent will carry on each received transaction. The static agent compares the received transaction T to its predefined policies P_s. Then the static agent compares P_s with T. If $P_s \neq T \pm \varepsilon$, then the transaction will be rejected. If $P_s = T \pm \varepsilon$, then the transaction will be accepted.

$$T = \begin{cases} 1, & \text{accepted} \\ 0, & \text{if } P_s \neq T \pm \varepsilon \end{cases} \tag{1}$$

Mobile Agent is the agent that is created by the householder managers to control access to their household devices. The mobile agent is a standalone software entity that can start various tasks when visiting different computing nodes: such as collecting data, contorting access management tools, as well as monitoring and detecting inappropriate using of household devices. According to the request of the endorsing peers, a mobile agent can migrate to the selected house, transfer their code and data, allow them to efficiently perform computations, gather information and accomplish tasks. The agent can be encrypted by asymmetric authentication (by the public key of the selected peer).

The Blockchain platform will create a mobile agent dedicated to every requested IoT device. The mobile agent will migrate to the requested IoT device. Then, the mobile agent will execute its code in the IoT device controller. The mobile agent collects the behaviours of user B that is detected by each user and reported by the sensors. Then the mobile agent compares B with P, where P is the declared policies given by Blockchain platform. If $B \neq P \pm \varepsilon$, then a potential inappropriate activities (P) is suspected. The mobile agent also checks the user time connection T to the IoT device, and compares it to the policy declared time T_B. If $T < T_B$, then a potential inappropriate activity can be reported. The mobile agent detects the inappropriate activities as depicted in Eq. (2), where ε represents some measurement error threshold.

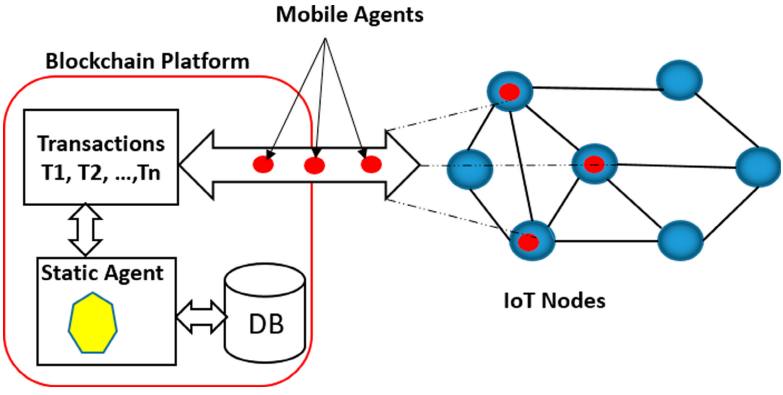

Fig. 1. Architecture of blockchain agents-based model

$$P = \begin{cases} 1, & \text{if } B \neq P \pm \varepsilon \text{ or } T < T_B \pm \varepsilon \\ 0, & \text{otherwise} \end{cases} \quad (2)$$

Figure 1 shows the overall architecture of integration between agent-based Blockchain and IoT networks. In this architecture, although Database (DB) is place, the analysis engine is out of the scope of this paper. It can be seen that the role of the static agent is used to manage access control for a transaction. After allowing and giving a permission for a transaction, a mobile agent will be created by the Blockchain platform and will migrate to the requested IoT node to control user behaviours with the connected device.

3.3 System Algorithm Design for Smart Home

Algorithm 1 presents the BAC solution by using Blockchain components and software agents as a method for enabling and access control in smart home. To

Algorithm 1. Hyperledger Fabric Blockchain-based Access Control (BAC)

EP: endorsing peers
Tr: Transaction
SA: Static agent
MA: Mobile agent
BC: Blockchain platform
C: Children
OS: Ordering Service:
DB: Data Base
P: Declared policies given by BC
B: Collected behaviours of user
T: User connection time
T_B: Policy declared time
res: proposal response
CE: Collected Endorsements
while Tr received **do**
  Verify(T, EP(SA)) {EP verifies T by executing SA}
  Send(res, EP, C) {EP sends res to C}
  Request(EP, OS) {EP requests block creation form OS}
  Verify(CE, OS) {OS verifies CE}
  Send(Block, OS, BC){OS sends the created Block to BC}
  Add(Block, BC(DB)) {BC adds the Block into its DB}
  Send(MA, EP, C) {EP sends MA to C}
  while MA received **do**
    if $B \neq P \pm \varepsilon$ **then**
      inappropriate activity is detected
    else if $T < T_B$, **then**
      inappropriate activity is detected
    else
      appropriate activity
    end if
  end while
end while

adapt Blockchain to the specific needs of IoT, we integrated 2 software agents: the static and mobile agents. First, the static agent is responsible of transactions verification. Second, the mobile agent is able to detect inappropriate activities. Once on the peer (children), the mobile agent will be acting as a Local Intrusion Detector (LID) as well as a Delegated Authenticator (DA) on behalf of endorsing peers (Parents). To this end, it will use the local processing resources of the peer to investigate its behavior. The mobile agent compares its declared policies P with the user behaviour $B \neq P$, then inappropriate activity is detected. The mobile agent also compares its policy declared time T_B with the user connection time T.

4 Validation of BAC in Smart Home Systems

In order to validate our solution, we demonstrate the application of BAC in the parental control scenario, which is a typical and important case in smart home systems [27]. We use the smart home setting for demonstration and evaluation purposes, while BAC is application agnostic and well-suited for diverse IoT applications and networks. Our demonstration is show how to design and implement a secure and efficient model that can manage access control between children and their parents based on the Blockchain.

Considering that in the smart home, sensors are coupled to a number of household devices to turn on or off the digital devices, which can be controlled remotely and give access to the children. Those control sensors are coupled to household devices in the smart home to monitor and control home appliances. Control sensor consists of activating or deactivating household devices and monitoring the user behavior about how appliances are used. For example, Children need request for permission before using any connected household devices. Parents will receive the transaction and react to it by allowing or rejecting usage by executing access control policies. The parents can control remotely the connected home appliances through their mobile phone or tablet or a wireless remote. Two agent-based control will be used in our system: static agent and mobile agent.

The *static agent* will be implemented in each parent manger device to verify received transactions that their children request. After executing each policies code, the static agent is also responsible for accepting or declining the received transaction. After giving access to children, the *mobile agent* will migrate to the target devices. The mobile agent is able to control the activities of children and detect e.g. the inappropriate behaviour. The mobile agent can visit each of the connected home appliances and execute customized code on each control sensor. Therefore, the mobile agent can analyse user behaviour through the connected home appliances. Apart from monitoring user behaviour, when a malicious activities are detected, the mobile agent can also turn off the device and denied further access.

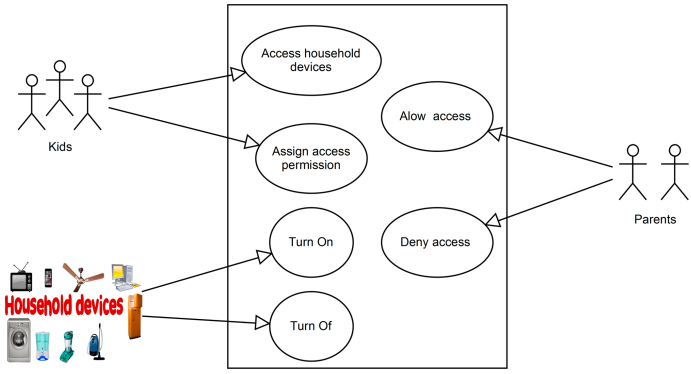

Fig. 2. Roles in blockchain-based model: use case diagram

4.1 System Implementation Process

While the BAC can enable the parents to set digital rules remotely with their devices to control child's activity on the house, digital parental access control helps to keep children safe when they're using household devices and to track their activity when using the connected devices. As shown in Fig. 2, devices at home such as television, computer and video games are connected to a private Blockchain channel and accessible only when the parents give access to their child's. Moreover, parents have a remote controllers (e.g. mobile phone, hand clock, computer) which are connected to the private Blockchain channel.

When a children enters into a transaction, he determines the parameters of this transaction by specifying its location, name of household items that he will interact with it, usage time, etc. Each transaction is stored in a smart contract and transmitted to the endorsing peers of the Blockchain platform. As shown in Fig. 3, the following steps occur during access request time.

1. The children store the endorsement requests in the smart contract and submits it to their endorsing peers, in the smart home context, the endorsing peers are usually the parents.
2. The static agents located in the parents devices can approve or reject the status after checking for consistency by aligning the smart contract.
3. The static agents send the proposal response to the IoT device applicant. Each execution captures the set of read and written data (also called the RW set), which is flowing in the Hyperledger fabric. Moreover, the Endorsement System Chaincode (ESCC) signs the proposal response on the endorsing peer. The RW sets are signed by each endorser. Every set will include the number of the version of each record.
4. The children send the proposal response to the ordering service, which is located on the Blockchain platform as a clustering code to create Blocks).
5. Afterwards, the ordering service verifies the collected endorsements and creates the Block of transactions.

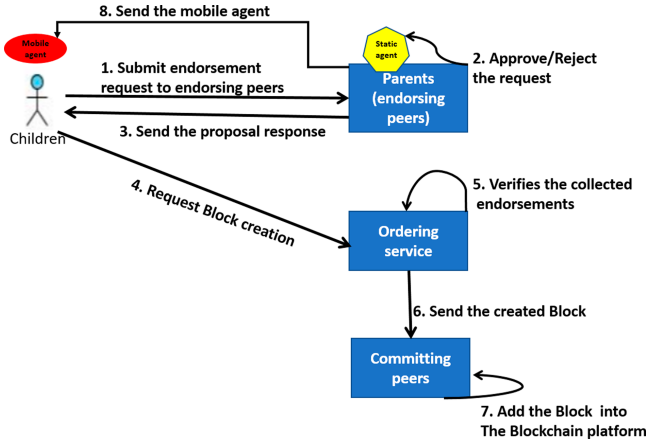

Fig. 3. Order-execute architecture to storage data in the Hyperledger Fabric Blockchain platform

6. The ordering service sends the Block to the committing peers which can include the parents or other family members who will be notified for validation.
7. If the validity is fulfilled, the Blockchain platform adds the checked Block into the data base of the Blockchain. Then, the Blockchain emits the notification to all peers.
8. After the validation of transaction, one of the parents static agent (in a chosen sequential manner) creates a mobile agent and sends it to the child who made the request and track his activities.

We have implemented a system prototype of the proposed BAC based on the open source Blockchain platform: Hyperledger Fabric [10], which has been reported as one of the most suitable platforms for the IoT applications [31]. In the smart home environment, all nodes such as the IoT endpoint for parents and children in the network use the SHA-1 hash algorithm and 2MB as data block sizes. Also, the IoT home devices are linked by the hyperledger in Blockchain, the foundation of the Blockchain in smart home is designed to control children activities with the household devices. To implement this in practice, first, householders should be Blockchain channel members. Besides that, there are two ways for endorsing peers to verify and check the authenticity of the children's requests and transactions: by their smart contract and by the mobile agent report. We created a smart contract program that is used by the children to send its transaction to the endorsing peers, which in our case the peers are the IoT endpoint from parents. A transaction invokes a smart contract called chaincode, which defines an application running on the Blockchain [3]. When the transition is issued, the mobile agent is used to monitor the behavior of the IoT device usage. For example, a child can request to watch TV for half an hour by smart contract. After the parents agree this transaction by endorsement, the mobile agent

is used to monitor if watching TV in this transaction is more than half an hour or not, in case longer than half an hour, the mobile agent can turn off the TV based the defined policy.

We deployed the initial prototype to test the feasibility of the solution, and planned tests by running simulations of different scenarios of tracking children's activities in smart home. We described the implementation process of the Blockchain components and their characteristics as follows. Each peer in the Blockchain channel runs as an image in the docker container and contains the smart contract modeled as JavaScript Object Notation (JSON). The smart contract is designed and implemented by using the Hyperledger Composer, which is an extensive, open development tool set and framework to facilitate the implementation of Blockchain applications. The peer processes and orders transactions on a first-come-first-serve basis across the network. The notification generated from the blockchain network is emitted to the client using WebSockets [28]. Each Block contains a key and the key of the previous block. Therefore, the database collects Blocks that are cryptographically linked together to form a sequence of chains. The connector between Blocks helps user to trace back the different stored transactions and to know the history changes that happened in the state database. The ordering node is employed with the practical byzantine fault tolerance (PBFT) algorithm [6] to ensure the consistency of every copy of the leger.

4.2 Performance Evaluation

To analyze the performance of our proposed BAC solution, we used Hyperledger Caliper software [26], which is a benchmark tool developed within the Hyperledger project. This tool can produce reports containing various performance indicators, such as transactions per second, transaction latency and resource utilization. For performance evaluation, this study is mainly focused on the task execution time. In the simulations, we varied two kinds of variables to observe the transaction execution time. One variable is the number of IoT devices in the smart home, and the other one is the number of transactions with a fixed number of smart home IoT devices.

In the setting of varying the number of IoT devices in the smart home, we configured the system with a range of 50 to 250 IoT devices with the interval of 50 devices. This range is chosen because of real-world applicability. For smart buildings, we estimate that the total number of IoT devices is usually less than 200, and the IoT devices or sensors in smart home in most cases are less than 50 pieces. Considering Hyperledger Fabric nodes setup, Those IoT devices contain 2 endorsing peers that are both parental controller devices, 4 committing peers including endorsing peers and others are smart IoT devices or sensors at home. We run our simulations for 60 s. The execution time is mainly spent on processing transactions, peer communications and updating the Blockchain. The transaction is the exchange of messages between sender and receiver where a peer (e.g. children) access request, asking the manager peers (e.g. parents) for the access of the household device (e.g. TV). In our simulation, to read one transaction in the

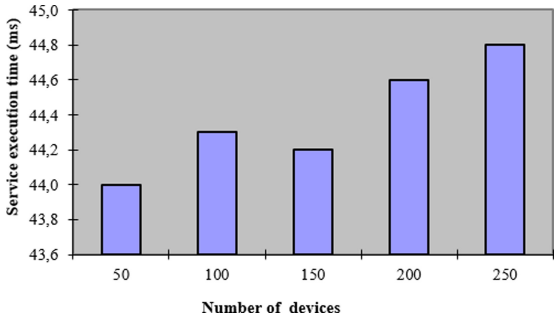

Fig. 4. Average execution time of each transaction by varying the number of IoT devices

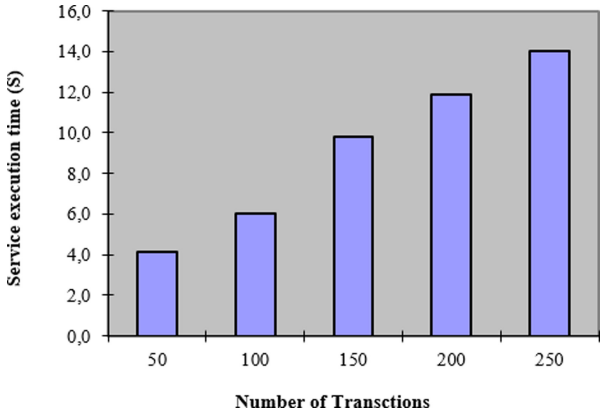

Fig. 5. Execution time of processing all the transactions by varying the number of transactions

Blockchain, the average time is around 39 ms. To compute the time execution of each transaction, we are using the simulation tool Hyperledger Caliper [26] to record the average time. We observed that for the one transaction the average execution time is 44 ms.

Figure 4 shows the evaluation result of the execution time for accessing usage to IoT devices. We can obtain the average execution time of one transaction by varying the number of IoT devices directly from the simulator. The main observation is that when increasing the number of IoT devices, the execution time is between (43 ms) and (45 ms), indicating that the execution time for transaction is very reasonable and implementable. Also, it can be seen that the variation of IoT device quantity has limited effects on our solution and thus the proposed BAC can potentially support even large IoT networks. One of the reasons is that in smart homes each transaction may only involve a small set of peers. Thus enlarging the network may not enlarge the scale of the transaction. Moreover, the implemented static agent helps to verify fast the received transactions.

The agent-based method in our solution can provide more efficient transaction execution.

In the setting of varying the number of transactions in the smart home, we configured the system with a fixed number of 50 IoT devices because we estimate most smart homes have less than 50 devices. Thus our performance testing can be set to be a larger scale case. Same as the previous setting, 2 IoT devices with parents as endorsing and committing peers and 2 more IoT devices as committing peers. The rest of the IoT devices are the IoT devices or sensors available in the house. We reported the observations in Fig. 5.

Figure 5 shows the total time that is used to successfully complete all the designed transactions in the Blockchain. In this setting, all the householder members who submit transactions have a designated target smart contract function. As we expected, more transactions will take more execution time. However, the average execution time per transaction is decreasing as the number of the transactions increase. This may be explained by the fact that Blockchain provides a way to execute many transactions at the same time in an efficient way [23]. For instance, when the number of transactions is equal to 50, the total time to process all the transactions is 4 s and thus each transaction needs 0.08 s on average, while for 250 transactions the total execution time is 14 s, where each transaction needs 0.056 s. It can be seen that each transaction needs less time when more transactions are carried out. One possible reason is that executing smart contract for many transactions simultaneously spend less execution time than executing smart contract program separately for each transaction. Thus, when the density of the transaction is high, instead of processing the full cycle for each transaction, the smart contract takes the full list of transactions as input values. Likewise, each receiver peer may process the list of multiple sequential transactions into one Block by using the smart contract executable program. Therefore, with the increase number of transactions, the time that is used to execute each transaction will decrease.

During the simulation, we also found that collaborations among the smart home IoT devices can achieve results that exceed their individual capabilities. In smart homes, different IoT devices may need to work collaboratively to finish one task [35]. In this context, because of the commonly limited processing, storage, and communication capabilities of these devices as well as the dynamic, open, and unpredictable environments in which they operate, implementing effective collaboration mechanisms remain a challenging concern [34]. For example, in order to finish one cooking task, the kettle, the cooking machine and the oven may need to work collaboratively, interactively or in a sequence. Potential solutions can be inspired from the extensive studies to enable the collaboration between distributed autonomous entities in the context of Multi-Agent Systems (MAS). MAS have proven flexibility, autonomy, and intelligence to solve complex problems within highly dynamic, constrained, and uncertain environments [13,29]. In our proposed BAC solution, agent-based design is used to automate the approval, monitoring and controlling activities. We believe that

the agent-based design can be further developed to coordinate the communication among IoT devices and enhance the efficient automation in smart home systems.

5 Conclusion

In this paper, we have proposed a Blockchain-based access control (BAC) mechanism for IoT in smart home systems. The BAC solution is mainly featured by integrating the Blockchain to IoT networks with agent embedded systems. This solution is designed for the smart home IoT devices. In the BAC solution, we have modelled the agent-based policy for the Blockchain management and designed the algorithms for smart home access control. In order to validate our solution, we have implemented the BAC for a typical parental control scenario in smart home, and demonstrated the detailed processes and interactions, across from request, to endorsement and verification as well as monitoring activities in parental control. Based on the performance evaluation, it can be seen that the execution time for accessing the service in IoT devices is reasonable and the system interactions such as transaction processing are efficient. This also indicates that the BAC solution can be implemented in the real-world smart home systems. Furthermore, although the BAC solution is proposed in the context of smart home, it can be potentially used in the other scaled IoT networks with access control concerns and requirements.

As future works, we first plan to conduct more experiments with various real-world IoT applications. In most smart home systems, since the number of IoT devices is only scaled to a small limitation, we believe our solution can be effectively implemented. Further, a user study will be conducted in a real-world smart home environment, and we will also intend to investigate the interoperability and the cost of implementing our solution compared to other solutions.

References

1. Al-Shaboti, M., Welch, I., Chen, A., Mahmood, M.A.: Towards secure smart home IoT: manufacturer and user network access control framework. In: 32nd International Conference on Advanced Information Networking and Applications, Krakow, Poland, pp. 892–899 (2018)
2. Ali, G., Ahmad, N., Cao, Y., Asif, M., Cruickshank, H.S., Ali, Q.E.: Blockchain based permission delegation and access control in Internet of Things (BACI). Comput. Secur. **86**, 318–334 (2019)
3. Brandenburger, M., Cachin, C., Kapitza, R., Sorniotti, A.: Blockchain and trusted computing: problems, pitfalls, and a solution for hyperledger fabric. arXiv:1805.08541 (2018)
4. Conoscenti, M., Vetro, A., De Martin, J.C.: Blockchain for the Internet of Things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6. IEEE (2016)
5. Danzi, P., Kalor, A.E., Stefanovic, C., Popovski, P.: Analysis of the communication traffic for blockchain synchronization of IoT devices. In: 2018 IEEE International Conference on Communications (ICC), pp. 1–7. IEEE (2018)

6. De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., Sassone, V.: PBFT vs proof-of-authority: applying the cap theorem to permissioned blockchain (2018)
7. Dorri, A., Kanhere, S.S., Jurdak, R.: Towards an optimized blockchain for IoT. In: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, pp. 173–178. ACM (2017)
8. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623. IEEE (2017)
9. Huh, S., Cho, S., Kim, S.: Managing IoT devices using blockchain platform. In: 19th International Conference on Advanced Communication Technology, pp. 464–467. IEEE (2017)
10. Hyperledger: Hyperledger fabric (2019). https://github.com/hyperledger/fabric
11. Johnsen, F.T., et al.: Application of IoT in military operations in a smart city. In: 2018 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1–8. IEEE (2018)
12. Kavallieratos, G., Chowdhury, N., Katsikas, S.K., Gkioulos, V., Wolthusen, S.D.: Threat analysis for smart homes. Future Internet **11**(10), 207 (2019)
13. Kong, Y., Zhang, M., Ye, D.: A belief propagation-based method for task allocation in open and dynamic cloud environments. Knowl.-Based Syst. **115**, 123–132 (2017)
14. Kum, S.W., Kang, M., Park, J.: IoT delegate: smart home framework for heterogeneous IoT service collaboration. TIIS **10**(8), 3958–3971 (2016)
15. Lyu, Q., Zheng, N., Liu, H., Gao, C., Chen, S., Liu, J.: Remotely access "my" smart home in private: an anti-tracking authentication and key agreement scheme. IEEE Access **7**, 41835–41851 (2019)
16. Mbarek, B., Ge, M., Pitner, T.: Self-adaptive RFID authentication for Internet of Things. In: 33rd International Conference on Advanced Information Networking and Applications, Matsue, Japan, pp. 1094–1105 (2019)
17. Mbarek, B., Ge, M., Pitner, T.: An efficient mutual authentication scheme for Internet of Things. Internet Things **9**, 100160 (2020)
18. Mocrii, D., Chen, Y., Musilek, P.: IoT-based smart homes: a review of system architecture, software, communications, privacy and security. Internet of Things **1**, 81–98 (2018)
19. Ouaddah, A., Abou Elkalam, A., Ait Ouahman, A.: Fairaccess: a new blockchain-based access control framework for the Internet of Things. Secur. Commun. Netw. **9**(18), 5943–5964 (2016)
20. Rehman, M., Javaid, N., Awais, M., Imran, M., Naseer, N.: Cloud based secure service providing for IoTs using blockchain. In: IEEE Global Communications Conference (2019)
21. Rifi, N., Rachkidi, E., Agoulmine, N., Taher, N.C.: Towards using blockchain technology for IoT data access protection. In: 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), pp. 1–5. IEEE (2017)
22. de Rivera, D.S., Bordel, B., Alcarria, R., Robles, T.: Enabling efficient communications with resource constrained information endpoints in smart homes. Sensors **19**(8), 1779 (2019)
23. Selimi, M., Kabbinale, A.R., Ali, A., Navarro, L., Sathiaseelan, A.: Towards blockchain-enabled wireless mesh networks. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 13–18 (2018)

24. Shafagh, H., Burkhalter, L., Hithnawi, A., Duquennoy, S.: Towards blockchain-based auditable storage and sharing of IoT data. In: Proceedings of the 2017 on Cloud Computing Security Workshop, pp. 45–50. ACM (2017)
25. Stojkoska, B.L.R., Trivodaliev, K.V.: A review of Internet of Things for smart home: challenges and solutions. J. Clean. Prod. **140**, 1454–1464 (2017)
26. Sukhwani, H., Wang, N., Trivedi, K.S., Rindos, A.: Performance modeling of hyperledger fabric (permissioned blockchain network). In: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), pp. 1–8. IEEE (2018)
27. Vilas, A.F., Redondo, R.P.D., Rodríguez, S.S.: IPTV parental control: a collaborative model for the social web. Inf. Syst. Front. **17**(5), 1161–1176 (2015)
28. Wörner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with bitcoin. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, pp. 295–298. ACM (2014)
29. Wray, K., Thompson, B.: An application of multiagent learning in highly dynamic environments. In: AAAI Workshop on Multiagent Interaction Without Prior Coordination (2014)
30. Xue, J., Xu, C., Zhang, Y.: Private blockchain-based secure access control for smart home systems. KSII Trans. Internet Inf. Syst. **12**(12) (2018)
31. Yu, Y., Guo, Y., Min, W., Zeng, F.: Trusted transactions in micro-grid based on blockchain. Energies **12**(10), 1952 (2019)
32. Yuan, Y., Wang, F.Y.: Towards blockchain-based intelligent transportation systems. In: IEEE 19th International Conference on Intelligent Transportation Systems, pp. 2663–2668 (2016)
33. Zaidan, A.A., Zaidan, B.B.: A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations. Artif. Intell. Rev. **53**(1), 141–165 (2020)
34. Zaidan, A.A., et al.: A survey on communication components for IoT-based technologies in smart homes. Telecommun. Syst. **69**(1), 1–25 (2018)
35. Zhang, Y., Tian, G., Zhang, S., Li, C.: A knowledge-based approach for multiagent collaboration in smart home: from activity recognition to guidance service. IEEE Trans Instrum. Measure. **69**(2), 317–329 (2020)
36. Zhang, Y., He, Q., Xiang, Y., Zhang, L.Y., Liu, B., Chen, J., Xie, Y.: Low-cost and confidentiality-preserving data acquisition for internet of multimedia things. IEEE Internet Things J. **5**(5), 3442–3451 (2018)
37. Zyskind, G., Nathan, O., et al.: Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops, pp. 180–184. IEEE (2015)