Advancing Security and Data Protection for Smart Home Systems through Blockchain Technologies

Conference Paper · July 2022

DOI: 10.5220/0011310800003266

3 authors:

Ciprian Paduraru
University of Bucharest
50 PUBLICATIONS **157** CITATIONS
SEE PROFILE

Rareș Cristea
University of Bucharest
7 PUBLICATIONS **11** CITATIONS
SEE PROFILE

Alin Stefanescu
University of Bucharest
68 PUBLICATIONS **813** CITATIONS
SEE PROFILE

Advancing security and data protection for smart home systems through blockchain technologies

Ciprian Paduraru, Rares Cristea and Alin Stefanescu
University of Bucharest, Romania
ciprian.paduraru@fmi.unibuc.ro, rares.cristea@unibuc.ro, alin@fmi.unibuc.ro

Keywords: smart home, IoT, blockchain, services, security, Hyperledger

Abstract: Internet of Things (IoT) systems are becoming ever-present in our lives and the demand recently increased with the explosion of external services offered by healthcare, smart city or smart home providers. However, the connection of private IoT-driven smart home systems and passing data to these external services can pose significant privacy issues, such as information theft or attacks to control, monitor, or harm personal resources. In our paper, we address the identified security issues through a comprehensive architecture based on blockchain technology, namely the Hyperledger Fabric platform. We underscore the value that a permissioned blockchain brings in addressing performance issues both architecturally and through fog computing, and propose a pipeline to mitigate known security threats through static and live monitoring techniques.

1 INTRODUCTION

Smart home systems are often defined as a set of interconnected devices in a private home that send and receive data in real time. Typically, they automate various household tasks via smart devices such as TVs, lamps, or fridges. These devices use a dedicated home communication system between appliances and other environments, usually wirelessly. Users can access these products to monitor, control the device behaviour or extract useful information.

Motivation for using a blockchain technology. Due to space constraints, the reader new to the blockchain field is invited to check the basic technical aspects in the existing literature (Ma et al., 2019), (Antwi et al., 2021), (Zhang, 2020). Smart home systems consist of heterogeneous devices made interoperable by creating gateway connections. In the absence of security standards for their connection, it is difficult to assess the security of the network and whether the privacy of the data collected by the devices is vulnerable to attacks. Centralized architectures (gateways) are vulnerable to data forgery, tampering, denial-of-service attacks, etc. An example of this is the hacking of toddler surveillance cameras (Schiefer, 2015). From this type of studies, at security level, we identified the following requirements:

- Confidentiality: since the networks used in smart homes could collect and store sensitive information, access to this data should be restricted to authorized individuals. Blockchain is capable of providing a solution when paired with encryption algorithms. (Dotan et al., 2021), (Zhang et al., 2019), (Zou et al., 2020), (Abdelmaboud et al., 2022).
- Data integrity: Connected devices communicating with each other must maintain data integrity and prevent forged information from flowing through the network.
- Authentication: It is important to prevent attackers from connecting to the network and then acting maliciously.

Contributions of the paper.

- To the best of the authors' knowledge, this is the first work that brings together all current smart home system requirements into a unified architecture and framework, while proposing a blockchain-based solution to mitigate security threats. APIs and infrastructures for data collection, processing, and collaboration between third parties such as marketplaces, service providers, smart cities, and external collaboration in general, are also discussed.
- We propose an open-source full-stack system based on a customizable permissioned blockchain solution, i.e., Hyperledger Fabric [1]. Although technologies change over time, we still consider it

[1] https://www.hyperledger.org/use/fabric

a novelty, as we believe that the fundamental ideas behind this solution will be useful over time.

- We propose a user-customizable fog computing method that allows homeowners to select and use their own devices either in their own homes or controlled cloud resources for advanced computing activities.

2 RELATED WORK

The work in (Ammi et al., 2021) is closely related to ours. The purpose is to provide a technical perspective on how a smart home system having a permissioned blockchain can be deployed on a Hyperledger Fabric. They use a cloud storage (virtual servers) to store resources - which we think it is not really suitable for real-time computing devices in terms of responsiveness, as also suggested, for example, by the work in (Moniruzzaman et al., 2020). Instead, our solution uses the InterPlanetary File System (IPFS) framework (Steichen et al., 2018) to store only cryptographic hashes of data addresses in the blocks. Then, the data may physically exist either in a local storage for critical operations or in the cloud for big data management. Additionally, their work does not take into account dynamic user management (e.g., visitors, healthcare providers who might ask for triggers), policy and security management, or integration to various external systems such as application marketplaces or data services. (Lee et al., 2020) proposes a blockchain-based solution for smart homes at the gateway level to mitigate security issues. Their study is based on a decentralized architecture that uses Ethereum to support the security requirements of confidentiality, authentication, and data integrity in the smart home gateway. Overall, their methods work by analyzing the data flow at the center of the smart home gateway, including scenario configurations and security considerations for various attacks on the network. In (Lee et al., 2017), the authors propose a secure firmware verification for embedded devices to prevent "patch file forgery" attacks using a blockchain architecture. Their proposed technique guarantees that the firmware on embedded devices is not tampered with while being up-to-date. In (Dorri et al., 2017), the authors propose a blockchain-based method to define an architectural identification management system for IoT devices, the FairAccess Framework. The novelty of the paper is the solution they use for identity verification when accessing resources between interconnected devices. The authors use smart contracts to express and verify contextual control policies when making authorization decisions. In (Ouaddah et al., 2017), the authors consider the fact that traditional access control methods are costly in terms of power consumption and processing overhead, which is a problem for embedded devices. They also believe that public blockchains are not suitable due to the limited resources of the devices. As for other implementation platforms and languages used, the work in (Calo et al., 2018) and its extension in (Hossain et al., 2020) use Ethereum and Solidity. They address the use cases of smart home systems and emergency services. The goal of both papers is to provide a practical introduction to the use of Ethereum and smart contracts, without research implications or other contributions. Each IoT device is registered on the network via the blockchain. As for the application of Hyperledger Fabric (HF) to our solution, we were encouraged by the recent application of this technology. For example, in (Antwi et al., 2021), the authors use HF for the healthcare industry. In (Zhang, 2020) and (Ma et al., 2019), HF is used as a deployment platform for supply chain financial management. Some of the benefits are the provision of a certificate authority and the protection of privacy and data using the *channels* concept.

3 SMART HOME SYSTEMS

Having gathered the requirements of smart home systems from literature and industrial applications, in this section we try to present the basic details about blockchain technologies that might be suitable for our targeted application domain.

3.1 Requirements for the smart home systems and blockchain motivation

The application of centralized access control mechanisms in the IoT domain and the ever-increasing number of connected devices can affect scalability, trust, and security management. Given the theory and recent applications of blockchains, we believe that incorporating blockchains into the architecture of smart home ecosystems can help in many ways. First, it can support management and data exchange between devices in a decentralized manner. This is a kind of prerequisite for IoT in general, as the goal is to achieve scalability and security, which is not possible with centralized architectures where a single server manages user permissions, performs verifications, and makes various queries from the set of interconnected devices. The data in the blockchain nodes, which can be used by different devices, descentralized and encrypted, can meet the security requirements of confi-

dentiality, integrity, and authentication in smart home systems. This eliminates the need for an external intermediary, which may be vulnerable to attacks.

3.2 Motivations for a permissioned blockchain and Hyperledger

Different open-source platforms are available and widely used in literature, such as Ethereum (Buterin, 2013), Hyperledger (Cachin, 2016), and Corda R3 (Polge et al., 2021).

Some of the key requirements for a blockchain-based smart home environment are to share user data only with a closed list of entities rather than with the public and to provide different levels of control for different types of users. Users can be either humans or IoT-connected devices within the smart home. This is only possible with an approved framework such as Hyperledger or Corda. These two also provide fine-grained access control, meaning participants can be restricted via policies and channels for reading, creating or updating data. In addition, the consensus mechanisms in Hyperledger Fabric and Corda can be set up to include only a subset of participants, and this has two major implications: (a) user privacy can be maintained by an approved list of parties and (b) it can be executed faster than Ethereum's Proof of Work (PoW) consensus mechanism, making it impractical for applications that require rapid response, such as smart home systems (Xu et al., 2017), (Polge et al., 2021), (Krishnapriya and Sarath, 2020). These functions can meet the confidentiality, scalability, and availability requirements of smart home systems. In light of the requirements of the GDPR, which are generally difficult to meet with a blockchain solution, Hyperledger offers users the right to delete data by creating a transaction that simply marks certain data as deleted. This is an advantage over its peers. This additional feature and the fact that Corda is more focused on financial services tipped the scales in our final decision to use Hyperledger Fabric as the deployment platform for the proposed solution. On the other hand, one of the drawbacks of the platform is that, while trying to be as open as possible, i.e., allowing users to customize things like credentials, consensus algorithm, private data and channels, developers need to put more effort to properly implement and connect interfaces. Therefore, there is an engineering price to pay.

4 PROPOSED ARCHITECTURE

This section first discusses the basic architectural principles for connecting smart home systems to blockchains and how these types of systems can interact with external, i.e., outside their own ecosystem, applications and users. Then, the intricacies of the different layers that have been shown to help with computational overhead are presented, as well as the implementation details of security management and interactivity methods.

4.1 Key ideas in applying blockchain technology for smart home systems

The basic idea of the underlying blockchain technology is that *users*, who can be either people (owners of the home ecosystem or external), agents, devices, etc., create *transactions* for the operations they perform. The transaction is approved using *miners* and consolidated into blocks. The purpose and motivation of a blockchain is to track the operations performed on the shared ledger so that privacy and other metrics can be tracked. For example, an automated agent could query the ledger to understand if the sequence of operations may potentially lead to a data loss of which the human user (owner) was unaware. Or the agent could detect the sequence of operations that were expensive and resulted in poor battery performance of a set of embedded devices. At this point, one might ask what is the difference between a classical method of logging the operations in a file and using the overhead of a blockchain. We answer this with two main arguments: (a) the transactions are validated by consensus, i.e., multiple parties, using a blockchain, which prevents the possibility of hacking the log files, (b) the data is stored in a structured format with timestamps and sequence of operations, which makes it easy to track and can be automatically followed by queries.

Our choice for a permissioned blockchain was also reinforced by arguments given in (Ammi et al., 2021) and (Moniruzzaman et al., 2020), which we summarize below:

- Sensitive data should be kept private, i.e., the user does not have to share their data with the public. Also, third parties should not be trusted without the user's explicit permission.

  Transaction latency is an important factor, as confirmation of transactions in the smart home use case must occur within seconds, not minutes. From our evaluation of the HF, the expected performance in standard production environments can exceed 100,000 transactions per second (Xu et al., 2021). In such environments, data is usually updated by more than one user.
- Connecting with smart cities, external applications and services, other identities in identities in

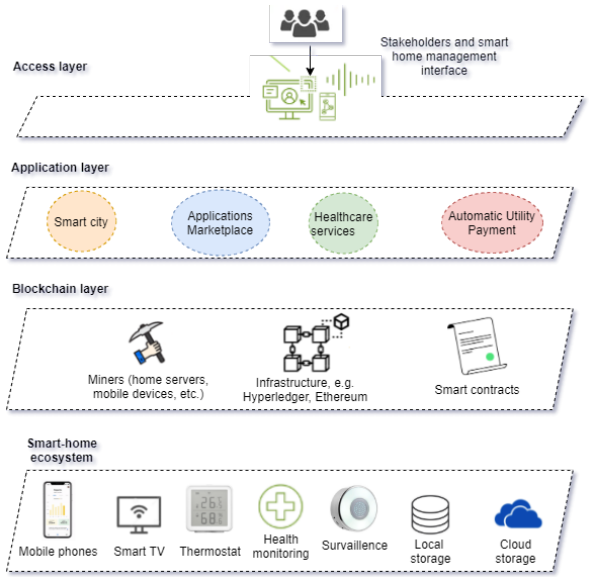

Figure 1: The four layers architecture and related entities for fulfilling the requirements of a modern smart home ecosystem and its interaction with users, vendors, blockchain technology, and external services

general requires the use of blockchain solutions in the form of communities or consortia. This is the reason for choosing a permissioned blockchain instead of a private one.

After reviewing the literature and requirements, in Fig. 1 we present an architecture that connects individual smart home systems to common ecosystems as required by industry and users. In the proposed architecture, we also architecturally link the current requirements with blockchain mechanisms. Within a smart home system, *user* can be understood as either people, devices, or AI agents.

The base layer consists of the devices and storage layers that are present in one's home. These may be devices in the areas of entertainment, health, sensors, etc. The data from these devices can be stored either locally, in the cloud, or on a decentralized platform based on blockchain technologies. The permissioned blockchain platform, which is the second layer, contains three main components.

- One or more *Miners* in the user's house and helps to keep the shared ledger of operations in a good state, i.e., checking new transactions from the connected devices and adding them to blocks by applying the consensus algorithm. As further explained in our paper, the set of miner devices can be adjusted by the user by simulating the capabilities of fog computing.
- A framework that enables the use of high-level blockchain operations and authentication. In our case, we used Hyperledger Fabric, but other systems such as Ethereum can also be used.
- A list of smart contracts - *chaincodes* in the terminology of HF - that can be used to implement business logic using rules and facilitate the decentralization of transactions. Specifically, in our use case, they define how devices interact and exchange data with other applications inside and outside the user home ecosystem.

Table 1: Mapping some of the core blockchain concepts to smart home use case

Concept	Description	Examples
Assets	resources and devices managed by the blockchain network	window sensor, thermostat, smart TV, wireless toothbrush, vacuum cleaner
Participants / users	actors who own the assets or act on them from outside	homeowners, children, visitors, healthcare providers, data mining agents
Transactions	set of activities that take place within the network, managed by smart contracts (chaincode in HF terminology) that act on assets or identity management	change status of the lights, raise temperature, add or reject a new user, collect metrics from the toothbrush, start or stop vacuum cleaner

4.2 Mapping smart home entities to blockchain terminology

Table 1 presents our proposed mapping of the three main concepts, i.e., *assets*, *participants*, and *transactions* from the blockchain terminology, and in particular the Hyperledger Fabric Model, to the use cases needed by the smart home systems.

Fig. 2 shows the proposed blockchain network integration for our use cases in smart home systems. .The organizations in our framework are divided into three main categories:

1. Internal smart home system organization: grouping the managers of the home itself and their assets (devices).
2. Marketplaces and external application providers: Grouping of external applications and interactions with which a smart home system might interact (e.g., stores, smart cities, intelligent traffic management, etc.). Currently, these services are grouped into a single organization, but in a real-

life environment, these could be expanded and split into different organizations.

3. External users, such as visitors or healthcare providers, who connect to assets in the home to temporarily use resources or collect metrics.

One of the main ideas to achieve safer and faster response times in HF technology is to use different communication channels between groups of entities and/or organizations. Each of these channels stores its own ledger and status, can be managed by one or more organizations, and has its own rules for confirming activities and membership. Applying this HF concept to smart home systems facilitates the management and tracking of communication between groups with different activities.

Fig. 3 shows the low-level details of how the blockchain network gets requests approved by the HF infrastructure. Note that in our proposed framework, administrators have the option to choose different computing capacities for processing endorsement peers (EP), principals (OP), or commit peers (EP). Internal hardware assets such as computers, laptops, cell phones, smart TVs, etc. (including those that participate in the smart home infrastructure as *assets*) can be used as physical deployments for these peers. In addition, a single physical entity can serve multiple roles, i.e., a computer could be either EP, OP, and CP. Cloud devices or externally rented devices can also be assigned as peers. This determination could be made through the administrators' UI interface.

Initializing the system from a high-level perspective within our framework is done as follows. The configuration of the organization, policies, admin users, and channels that enable basic communication and identity management in-house is first created by a configuration script. This information is added to the block *genesis* of the blockchain when it is instantiated. Later, when new assets or users are added to the smart home environment, change requests are received by the admin interface. When approved, they are recorded as transactions and added to the ledger in new blocks. Organizations and channels can also be added on the fly. Similarly, requests must be approved and executed by administrators, resulting in transactions, and eventually new blocks are added to the ledger. This is the case, for example, when a new health monitoring system is added to the smart home assets, allowing doctors to monitor some of the embedded devices monitored in the home. In this way, a new organization for healthcare providers and channels for communicating with these devices is created at runtime. Other examples include applications downloaded from a marketplace or external services related to smart city management.

4.3 Managing the home ecosystem

Our framework assumes that owners and administrators have a user interface that is accessible from a computer, smartphone, or voice control device. This would be the entry point for controlling permissions, access, and monitoring of devices and privileges of other users. Also, through the interface, users can customize the details of the miners that participate as resources in the operations of the blockchain infrastructure. As shown in Fig. 2, communication between the interface UI and the devices and other external entities within our framework is handled through REST API, relying on a central gateway that we refer to as *Central Hub* in our framework. If needed, multiple gateways and hubs can be connected hierarchically to enable fast transmission and communication. The external users connect to the smart home infrastructure through the central hub using a communication proxy component.

For data storage, we found that large files and data cannot be stored on the blockchain because the blocks could be bloated with data that needs to be mined, and this would significantly impact the computational and communication overhead. One solution mentioned in (Steichen et al., 2018) is to use the InterPlanetary File System (IPFS) framework. IPFS is a peer-to-peer file sharing system that could solve the problem of efficiency in storing and sharing large data. We also adopt this solution and instead of storing large amounts of data in transactions and blocks, we only store references and cryptographic hashes of data in the blocks. A concrete example could be camera sensors in a smart home system that could potentially send large amounts of data on a regular basis for automatic analysis by various systems. Rather than copying this type of data deep into a transaction or block within the blockchain, our proposed solution stores the data on the camera device itself or on the device performing the computational analysis by using IPFS and creating a reference to it, which is then used as a hash/reference within the blockchain-based framework. However, some of the local data storage is backed up to the cloud if the user chooses so. For example, it is advisable to store the user identity wallets in a database that is backed up in the cloud.

5 EVALUATION

Our application dataset, source code is open sourced at *https://github.com/unibuc-cs/IoT-application-set*. Since the framework is currently only a prototype that is not deployed in production environments, it

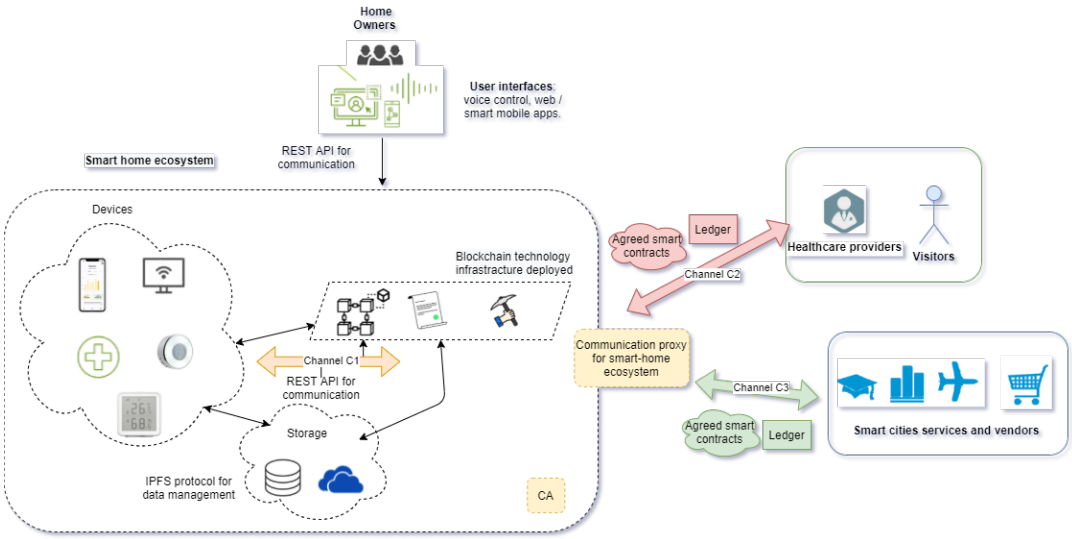

Figure 2: The three main levels of organization we propose: the smart home ecosystem, visitors and facilities that need to capture certain metrics, smart cities, and vendors. In production, these could be further divided hierarchically into sub-organizations or grouped into consortia of other organizational levels. Interaction between the smart home organization and others occurs through channels, each with agreed-upon smart contracts implemented in chaincode and its own ledger of operations, separated for performance and security reasons. The Certification Authority (CA) component is used to recruit and enroll new users to the systems. Note also that in our framework, new organizations and communication channels can be added spontaneously along with the smart contracts. For example, a property manager could install a new application that performs automatic grocery shopping.

is difficult to evaluate real metrics. We follow the methodology of evaluation in (Lee et al., 2020) and (Antwi et al., 2021) and present how our framework addresses common issues related to performance and security threats instead of simulated metrics.

A. Applications dataset and performance aspects

The current prototype implementation of the framework has an initial collection of five simulation applications that are either independent or communicate with each other via a central hub connection: a smart TV, a smart window and lighting system, an automatic plant watering system, a smart water heater, and a wirelessly accessible toothbrush. In the application marketplace, we offer two new applications that can be installed by the user: an entertainment lighting system and a smart vacuum cleaner connected to the sensors and cameras of the smart home system. These applications are created in different languages such as C++, Rust, or Python. An organization called *DentalServices* can access and monitor the smart toothbrush and send notifications to the interface UI, simulating health services. An automatic payment application is externally connected to the system to monitor the power consumption of the applications.

Users with administrative rights (homeowners) can granularly select which of the devices in the house are allowed to participate in mining processes within the blockchain network, i.e., commits, orders, and endorsements from peers, through the UI interface. Either personal cell phones, computers or IoT devices can be part of these processes. We strongly believe that this access feature can provide vertical scalability (i.e., adding new devices at runtime) for the use case of smart home environments, as operations can be further partitioned as needed. Performance can be monitored live via the UI dashboards by integrating Splunk[2] tool, which we describe below.

B. Security evaluation

To mitigate security threats, we apply protection at two different levels in our framework:

1. Proactive measures - e.g., automated inspection of chain codes through static analysis using the work in (Yamashita et al., 2019).
2. Live monitoring of network performance and security through automated triggers or visualization dashboards using Splunk.

As shown below, many of the threads can only be detected by correlating data across the blockchain.

We first describe how to respond to common attacks on distributed systems:

- Denial of Service (DoS): can disrupt network availability by flooding the network with requests, and is generally difficult to prevent proactively.

[2]https://www.splunk.com

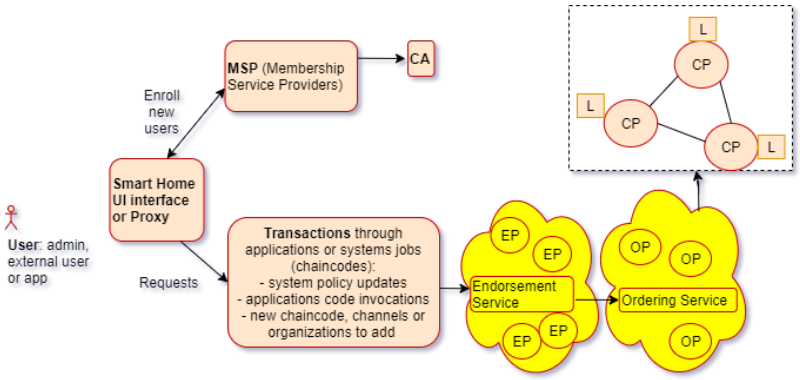

Figure 3: The processes that take place in an internal smart home organization: New users are registered by requesting access from an MSP and from an assigned certificate authority (CA), which creates a certificate for the new user. When various requests are received from external organizations either through the admin UI interface or through the smart home's proxy, they are first converted into transaction proposals. The transactions are then endorsed by the assigned endorsement peers (EP), timestamped by the ordering peers (OP), and finally committed to the general ledger by the committing peers (CP).

This risk can be mitigated by capturing two key performance metrics: transactions throughput and latency. Within our framework, we propose automated triggers using Splunk integration that constantly check these metrics and raise alarms at UI of homeowners when certain thresholds are exceeded, such as when the number of transactions from one of the users or applications has increased by more than twice the number of operations or the CPU time it takes to resolve.

- Consensus Manipulation: the consensus mechanism can be attacked with classic DoS, but also with transaction reordering attacks. At the moment, HF uses only Crash Fault Tolerant (CFT) consensus algorithms (Liu et al., 2016), so it cannot detect malicious actors. According to the documentation of HF, there are plans to add Byzantine Fault Tolerant (BFT) algorithms (Liu et al., 2016), which should theoretically detect on average 1/3 of malicious actors. However, at the moment, the triggers and dashboards provided by our system and Splunk that query and report leadership election attempts and transaction latencies are able to detect malicious actors at runtime.

Second, we describe how the framework responds to common blockchain attacks that we identified in our use case at HF:

- Smart Contract Exploitation: may target and affect business logic and/or network performance. To mitigate this risk before injecting a new or updated chaincode into the system, our framework has implemented a system checker chaincode that launches the Hyperledger Lab Chaincode Analyzer static analysis tool and uses the work in (Yamashita et al., 2019) to detect some of the potential risks. Runtime monitoring uses metrics, triggers and dashboards similar to those used in DDoS attack response. For example, alerts can be automatically triggered if some of the chaincode calls take much longer than expected or average, or if the CPU and memory requirements have unexpectedly increased.
- MSP Compromise: This attack is more of a HF specific threat, but its roots could be in the other frameworks as well. To mitigate this risk, our proposed system provides automatic triggers and alerts. For example, it would be suspicious if a particular user attempted to make a high number of connections to a channel or application within a certain time period, resulting in latency and/or throughput issues.

6 CONCLUSION AND FUTURE WORK

After in-depth analysis, we conclude that permissioned blockchain has the potential to improve security and trust in such systems. We also found that some architectural choices could increase performance, security, and tracking capabilities: configurable fog-like computing capabilities, use of the IPFS protocol as much as possible instead of deep-copying data, and smart organization of users into groups as well as private communication channels and ledgers. As future work, we will contact industrial partners to apply the concepts and our open source framework. We plan to further develop the connection between different smart home providers as a consortium and provide an interface proxy API and generic

smart contracts to connect them. As for the security of smart contracts, we believe that the current state can be improved through formal verification and fuzzing techniques before deploying new chain code.

ACKNOWLEDGEMENTS

This research was supported by the European Regional Development Fund, Competitiveness Operational Program 2014-2020 through project IDBC (code SMIS 2014+: 121512).

REFERENCES

Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., and Karim, F. K. (2022). Blockchain for IoT applications: Taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, 11(4).

Ammi, M., Alarabi, S., and Benkhelifa, E. (2021). Customized blockchain-based architecture for secure smart home for lightweight IoT. *Information Processing & Management*, 58:102482.

Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Habib ur Rehman, M., and Kerrache, C. A. (2021). The case of HyperLedger Fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications*, 2(1):100012.

Buterin, V. (2013). Ethereum white paper: A next generation smart contract & decentralized application platform. Technical report, Ethereum Foundation.

Cachin, C. (2016). Architecture of the Hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers (DCCL'16)*, pages 1–4.

Calo, S., Verma, D., Chakraborty, S., Bertino, E., Lupu, E., and Cirincione, G. (2018). Self-generation of access control policies. In *Proc. of SACMAT'18*, pages 39—-47. ACM.

Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2nd IEEE PERCOM Workshop On Security Privacy And Trust In The Internet of Things*, pages 618–623. IEEE.

Dotan, M., Pignolet, Y.-A., Schmid, S., Tochner, S., and Zohar, A. (2021). Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Comput. Surv.*, 54(5).

Hossain, M., Waheed, S., Rahman, Z., and Hossain, M. (2020). Blockchain for the security of internet of things: A smart home use case using Ethereum. *International Journal of Recent Technology and Engineering*, 8.

Krishnapriya, S. and Sarath, G. (2020). Securing land registration using blockchain. *Procedia Computer Science*, 171:1708–1715. 3rd Int. Conf. on Computing and Network Communications (CoCoNet'19).

Lee, B., Malik, S., Wi, S., and Lee, J.-H. (2017). Firmware verification of embedded devices based on a blockchain. In *Proc. of QShine'16 conference*, volume 199 of *LNICST*, pages 52–61. Springer.

Lee, Y., Rathore, S., Park, J., and Park, J. (2020). A blockchain-based smart home gateway architecture for preventing data forgery. *Human-centric Computing and Information Sciences*, 10:9.

Liu, S., Viotti, P., Cachin, C., Quéma, V., and Vukolic, M. (2016). XFT: Practical fault tolerance beyond crashes. In *12th USENIX Conf. on Operating Systems Design and Implementation (OSDI'16)*, pages 485—-500. USENIX Association.

Ma, C., Kong, X., Lan, Q., and Zhongding, Z. (2019). The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance. *Cybersecurity*, 2.

Moniruzzaman, M., Khezr, S., Yassine, A., and Benlamri, R. (2020). Blockchain for smart homes: Review of current trends and research challenges. *Comput. Electr. Eng.*, 83:106585.

Ouaddah, A., Elkalam, A., and Ouahman, A. (2017). Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In *Proc. of EMENA-TSSL'16*, pages 523–533. Springer.

Polge, J., Robert, J., and Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, 7(2):229–233.

Schiefer, M. (2015). Smart home definition and security threats. In *9th Int. Conf. on IT Security Incident Management and IT Forensics*, pages 114–118. IEEE.

Steichen, M., Fiz, B., Norvill, R., Shbair, W., and State, R. (2018). Blockchain-based, decentralized access control for IPFS. In *Int. Conf. on Internet of Things (Things'18)*, pages 1499–1506. IEEE.

Xu, X., Sun, G., Luo, L., Cao, H., Yu, H., and Vasilakos, A. V. (2021). Latency performance modeling and analysis for hyperledger fabric blockchain network. *Information Processing & Management*, 58(1):102436.

Xu, X., Weber, I., Staples, M., Zhu, L., Bosch, J., Bass, L., Pautasso, C., and Rimba, P. (2017). A taxonomy of blockchain-based systems for architecture design. In *IEEE Int. Conf. on Software Architecture (ICSA'17)*, pages 243–252. IEEE.

Yamashita, K., Nomura, Y., Zhou, E., Pi, B., and Jun, S. (2019). Potential risks of Hyperledger Fabric smart contracts. In *Int. Workshop on Blockchain Oriented Software Engineering (IWBOSE'19)*, pages 1–10. IEEE.

Zhang, J. (2020). Deploying blockchain technology in the supply chain. In *Computer Security Threats*, chapter 5. IntechOpen.

Zhang, R., Xue, R., and Liu, L. (2019). Security and privacy on blockchain. *ACM Comput. Surv.*, 52(3).

Zou, Y., Meng, T., Zhang, P., Zhang, W., and Li, H. (2020). Focus on blockchain: A comprehensive survey on academic and application. *IEEE Access*, 8:187182–187201.