Customized Blockchain-Based Architecture for Secure Smart Home Based Hyperledger Fabric and Hyperledger Composer for Lightweight IoT

|  |  |
| --- | --- |
| 1Meryem Ammi and2Shatha Alarabi  Department of Information Security  Naif Arab University for Security Science  Riyadh, Saudi Arabia  1[mammi@nauss.edu.sa](mailto:mammi@nauss.edu.sa)  2[4370882@nauss.edu.sa](mailto:4370882@nauss.edu.sa) | Elhadj Benkhelifa  Cloud Computing and Application Lab  Staffordshire University,  Stoke on Trent, ST16 1FG  [e.benkhelifa@staffs.ac.uk](about:blank) |

*Abstract*—Internet of Things (IoT) security and privacy remain a major challenge, due to the huge scale and distributed nature of IoT networks. In Smart homes context, the information system is based mainly on sharing information through smart devices (IoT) embedding sensors. Indeed, each sensor generates data to be processed or assembled by a central system. This data, while transmitted over the internet to other users or servers, can be compromised for its privacy, user confidentiality and/or service availability. This paper proposes a novel Blockchain-based solution for secure smart home systems, using a combined hyperledger fabric and hyperledger composer. This solution is proposed to overcome reported security limitations in commonly used permissioned blockchains approaches. The proposed architecture contains four layers: Cloud storage, Hyperledger fabric, Hyperledger composer, and smart home layer. Another important aspect of the proposed solution is the mapping of the attributes of a smart home to those from the hyperledger composer. This mapping allows for a customized, designed-for purpose solution, which can meet the security requirements for IoT based smart homes. The proposed architecture was implemented and tested for improved smart home’s integrity, confidentiality, availability, authorization and privacy as well as some inherited features, including transparency and interoperability.

*Index Terms*—Internet of Things, IOT, Smart Homes, Blockchain, Information system, Hyperledger Fabric, Hyperledger composer, Security

# INTRODUCTION

With the development of critical technologies in the Internet of things (IoT), IoT applications (e.g., smart home, smart healthcare, smart grid, smart city etc) become widely used [1]. Cisco predicts to over 50 billion devices to be connected by the year of 2020 [2]. IoT consists of devices that generate, process, and exchange vast amounts of data; some of this data can be highly sensitive and require high levels of security and privacy preserving. Though, IoT devices are hugely susceptible to cyberattacks that may impact data integrity by modifying the stored data for malicious purposes [29]. Therefore, IoT solutions must enable devices to work together with secure communication protocols. One primary challenge for securing IoT systems is dealing with ownership and identity of IoT devices along with their data authentication, integrity and privacy.

The Blockchain (BC) technology, introduced in 2008, has underpinned the first cryptocurrency system "Bitcoin" [3]. Since Bitcoin’s release, the popularity of the cryptocurrency has only kept on growing. This growth is attributed to the security and transparency of the BC approach [30]. BC, serves as the decentralized, distributed, shared, and immutable ledger that stores the registry of assets and transactions across a peer-to-peer (P2P) network. BC is not only applied in the cryptocurrency field but can also be applied in a myriad of other applications, such as healthcare, data verification, IoT and others [30] [4].

Developing smart homes will be elementary for smart cities. IoT is the underlying technology for smart homes, yet, the proliferating of IoT connected devices requires securing these devices and communication network. These connected devices and objects in IoT can be exploited by cyber-criminals, taking over control or get access to the user’s personal and financial information stored in the related smart home devices [28].

Within smart home applications, the user can interact with electronic device connected to his/her home network; whether this command is conducted by voice, remote control, tablet or smartphone. Each smart home has a controller responsible for handling all the communication within the household and/or outside. This makes it highly vulnerable to security threats, which can intercept the communication between devices and gain access to sensitive information stored in the user’s devices, or injecting malwares to user’s smart home IoT devices.

In order to deal with these security challenges related to smart homes, alterative options can be explored. The BC technology becomes an attractive technology for addressing the security and privacy challenges in the IoT and Smart Homes [11]. The absence of a central control, in BC, guarantees usability and reliability by utilizing assets from all operating nodes, which in turn overcomes the issue of one single point of failure. Moreover, the inherent anonymity feature in BC is highly relevant for most IoT application deployments, such as in Smart Homes, where the users’ identity must be kept anonymous. The BC approach also offers a protected network over untrusted parties with various and heterogeneous devices, which is highly required in IoT systems.

Accordingly, adopting the BC technology as a secure platform for IoT devices and mapping its basic architecture into an adapted architecture for the IoT system is not a straightforward application [32, 33, 34], where a number of considerations have to be taken into account. For instance, mining in BC can be computationally demanding, while the IoT applications are resource constrained and need low latency. Moreover, IoT networks contain a large number of devices; therefore, the BC scales operate poorly as the number of devices is increased. In addition, the BC’s underlying protocols make overhead traffic, which is unwanted for the bandwidth limited IoT devices.

This paper proposes a novel BC-IoT solution for secure Smart Homes, improving the users’ experience. In this solution we propose the use of a Hyperledger Fabric and composer to improve the performance of the proposed BC-IoT architecture. The proposed integrated solution meets the security requirements for smart homes, including confidentiality, integrity, authorization and availability as well as the inherited feature of BC transparency.

The novelty of the proposed solution combines hyperledger fabric and hyperledger composer, which to the best of the authors; knowledge, has not been attempted previously. This solution is proposed to overcome reported security limitations in commonly used permissioned blockchains approaches. The proposed architecture contains four layers: Cloud storage, Hyperledger fabric, Hyperledger composer, and smart home layer. Another important aspect of the proposed solution is the mapping the attributes of a smart home to those from the hyperledger composer. This mapping allows for a customized, designed-for purpose solution, which can meet the security requirements for IoT based smart homes.

The remainder of the paper is organized as follows. Section II presents related work. In section III, we present the proposed solution followed by evaluation and experimental results within section IV. We conclude the paper in section IIV.

# Related Work

There are several published researches on smart homes and the great potentials IoT holds for this application [4-7, 25, 26]. Ouaddah et al. [32] reviewed the challenges and opportunities of access of control in the IoT, where the main two key challenges smart home IoT devices are: integrity and confidentiality. Al-Kuwari et al. [5], for instance, presented, through their study, one of the most important applications of IoT systems for Smart homes. In smart homes, users can monitor various things including temperature, humidity, lighting, and air quality to make it ensuring an optimized usage of resources as well as human comfort. The study provided a simple design for intelligent home monitoring, especially with respect to solar energy and automation. The system used by EmonCMS relies on a cloud server to collect data from connected sensors to control home appliances. NodeMCU and ESP2866 were integrated for data processing, and then loaded to an EmonCMS server. Thus, a complete system for home automation through the Internet is created.

Often a centralized IoT model can be considered as useful, however as more and more devices are connected, issues will arise and the use of blockchain can assist with using a decentralized approach. The decentralization of an IoT network can provide the ability to solve numerous security issues that are present within a central model and can become a potentially essential component of Smart home security [13]. However, by reviewing several studies to give consumers an insight into IoT in smart home and related security risks, it turns out that the Internet system presents users with many security risks. It is possible to consumers are exposed to identity theft or invasion of the home through Internet devices their own things and exploit their personal data. However, despite the risks to smart homes, "normal" consumers do not care much about security risks, perhaps because the Internet-connected device is not accessible in the same way as other forms of communication. This study pointed that ordinary consumers do not care much about the security risks, but large governments that seek to automate all businesses, and large companies are concerned about security risks because it threatens all its future work.

Reyna et al. [8] discussed in a study the challenges of the IoT in terms of security such as data reliability and have analysesd how BC can overcome many IoT related security challenges, boosting the trust environment within a distributive information exchange system. The same study discussed various implementation of blockchain in IoT, as reported in literature. the study also pinpointed several issues that must be taken into consideration in order to successfully integrate blockchain in IoT, such as consensus as a part of mining process of inclusion paradigm, as well as the scalability and capacity storage [8]. Kreku et al. [9] presented a study that aims to evaluate blockchain in IoT applications. The evaluation considered two main metrics; power consumption and the transaction timeliness in the blockchain inclusion within IoT using a simulation, by ABSOULT-virtual modeling system.

Gallo et al. [10] proposed a DeCyMo system as a solution of common vulnerabilities in IoT for smart homes and other industrial applications. The proposed system in [10] is based on the idea of decentralization and distributed architecture of the blockchain. The blockchain was exploited for transaction validation without any central trusted control of authority. In DeCyMo, users who have an interest in IoT information, does not need Tackling security issues, DeCyMo provides a trusted environment based authenticated nodes, which eliminate the MQTT protocol that minimizes attack surfaces of the system. Dorri et al. [11] proposed a blockchain approach in a smart home scenario, being one of the most popular IoT applications. The approaches of the lightweight instantiation of the blockchain were examined in a smart home setting as a decentralized approach that provides security and privacy, as well as overcome the energy, delay, and computational overhead that blockchain commonly added to the limitation of the IoT devices.

The proposed integrated solution, as explained later in section III, meets the security requirements for smart homes, including confidentiality, integrity, authorization and availability as well as the inherited feature of BC transparency [27, 34]. The novelty of the proposed solution combines hyperledger fabric and hyperledger composer, which to the best of the authors; knowledge, has not been attempted previously. This solution is proposed to overcome reported security limitations in commonly used permissioned blockchains approaches. Another important aspect of the proposed solution is the mapping the attributes of a smart home to those from the hyperledger composer. This mapping allows for a customized, designed-for purpose solution, which can meet the security requirements for IoT based smart homes as stated in [32]. Androulaki, et al. [12] discussed the fabric hyperledger, describing its structure and the logical decision making in designs. The authors explored hyperledger fabric as a solution for the limitations that common permissioned blockchains suffered from such as trust model, consensus, smart contract, the sequential execution, and deterministic nature of the transaction and confident issue in term of all peers runs every single contract. Fabric has a unique execute -order-validate methodology. The process of transaction is divided into three main procedures, (1) executing transaction as well as assessing its correctness, and endorses it based on it on the other blockchains, (2) ordering via censuses protocol and then (3) validation of transaction per application of determining trust assumptions. Consequently, the fabric comprises two main common replication approaches, passive and active approaches. This Fabric architecture separates the transaction execution from the consensus and uses a policy-based endorsement. Furthermore, the study in [12] evaluated the fabric in terms of Bitcoin digital currency and revealed that fabric achieved more than 100 peers scale in the specific common settings with a standard 3500 transaction per second. Sukhwani et al. [13] used the Stochastic Reward Net for modeling the performance of hyperledger fabric version v1.0+, and measuring the throughput, utilization, and length of the queues at each peer and each stage when the transaction rate increases. Mit [14] compared the hyperledger fabric platforms with the traditional solution to enable advanced platform without a trusted third party using the smart contract. The study found that hyperledger fabric has an advantage feature against the conventional; that Fabric enables trust among peers, data, and transactions confidently; thus, it is considered as a secure and consistent platform by its unique design. The obvious weakness of the conventional platform is the scarcity of the distributed transaction without a third party.

# The Proposed APPROACH

The main objective of this paper is to explore “how can we use blockchain technology to secure the sensitive data of a smart home user in IoT”. To achieve this goal, a blockchain-based approach is proposed to secure sensitive data and to track the transactions among IoT devices and among the cloud as well. In other words, when any transaction is sent by a user for sensor data acquisition, any IoT devices in the cloud that intercepts or forwards the transaction information stored on immutable blocks that ensure Integrity of the data. Having an adaptive blockchain-based approach will capture all the information associated with the transaction lifecycle will allow home users to track any abnormal communications. Hence, in this section, we will explain the key elements of the proposed approach. First, the architecture of the proposed approach is explained, which will highlight the reason behind using permissioned blockchain that uses hyperledger fabric platform in conjunction with hyperledger composer. Then, the smart home model upon which the integrated solution will be implemented and tested is detailed. After that, the BC network model that is mapped to the smart home model is explained in details. In order to simulate a real case of the proposed approach, a Smart Home Scenario within the BC is shown. And finally, we show how we have Create API to Call Blockchain Application.

## The proposed Architecture

There are different models of BC [15], however for this paper, a permissioned BC will be used for the following reasons

* The traditional database cannot meet the needs of smart homes.
* More than one user needs to be able to update the data.
* There is no third party can be trusted by all participants.
* The sensitive data must be kept private.

Within permissioned BC, there exist at least three different implementations [16], the most appropriate for the purpose of this paper is the Hyperledger, more specifically, the Hyperledger Fabric, for the following reasons

* Permissioned and private: In smart homes, it is important to protect sensitive data from any manipulation by attackers.
* Modularity: Hyperledger fabric has modular architecture that enables enterprises to plug in their preferred encryption, consensus, and ordering service [17].
* Transaction Speed: Transaction confirmation in seconds instead of minutes. The expected performance is 100,000 transactions per second in the standard production environment [18].
* Safety: For handling identity management and managing strong authentication, Hardware
* Security Module enhances protection for keys and sensitive data by providing PKCS11 for a key generation [19].

Therefore, the proposed approach is permissioned blockchain using hyperledger fabric platform in conjunction with hyperledger composer. As we mention before hyperledger fabric, which has an advantage feature that enables trust among peers, data, and transaction confidently; thus, it is considered as a secure and consistence platform by its unique design. In addition, hyperledger fabric Identities for Lightweight IoT devices.

The proposed approach, shown in Figure 1 consists of four layers, cloud storage layer, hyperledger fabric layer (blockchain network), hyperleadger composer layer, and application layer (smart home).

* **The Cloud Storage Layer**: We added a cloud storage layer in our proposed approach due to advantages related to its efficiency and availability. Indeed, devices within a given smart home need some computing resources and storage capacity offered by the cloud. In our case, we use virtual servers hosted on cloud to store large data such as distributed ledger and the transactions between nodes in the blockchain network. More specifically, the user connects to the cloud server via a secure shell protocol (SSH) to setup secure authentication. In addition, the cloud can be accessed by smart home application enabling homeowners to follow their transactions and securely store them.
* **Hyperledger Fabric Layer:** Hyperledger fabric is a business blockchain framework with a modular architecture. In our proposed approach, fabric represents the blockchain network. As represented in fabric architecture, it has three service categories: membership, blockchain and chaincode. Membership service aims at offering an abstraction of a membership operation architecture, responsible for issuing and validating certificate and user authentication by abstracting cryptographic mechanisms and protocols [21]. Blockchain service is a core component of blockchain technology responsible for ledger storage, p2p network, consensus and distributed ledger. Chaincode is the smart contract encapsulated in a secure and isolated sandbox, processing and validate transactions. A chaincode typically handles business logic agreed to by members of the network.

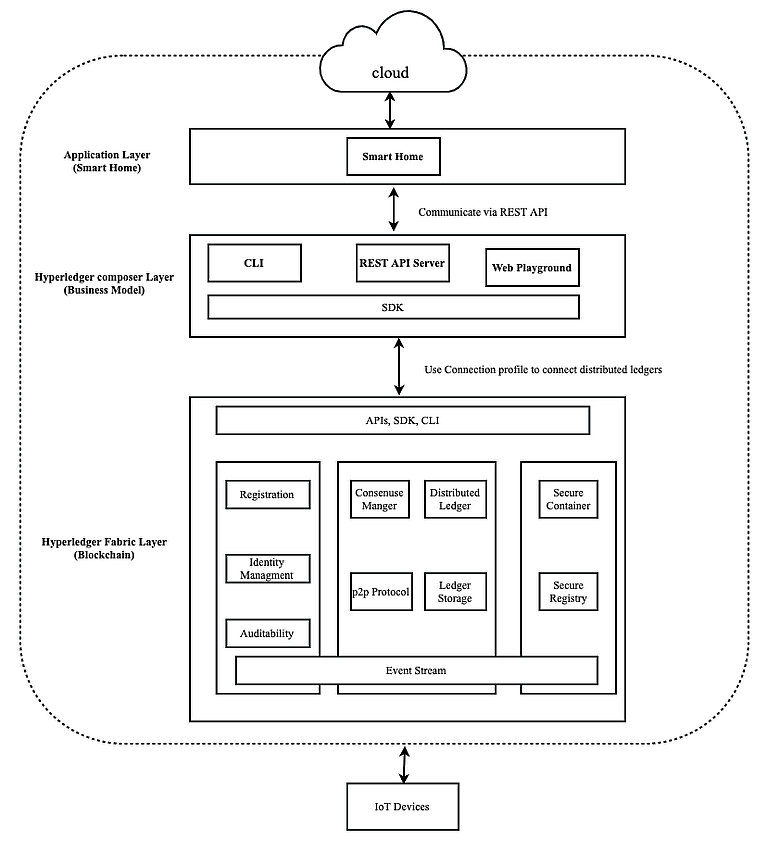


Figure 1 Proposed Approach Architecture

* **Hyperleadger Composer Layer**: Hyperledger composer is a set of tools that enable building blockchain applications on top of hyperledger fabric and testing of the business logic running on a blockchain. This layer is composed of some high-level components summarized in Table1. When creating a hyperledger composer application, the focus is put on the abstract concepts used rather than the low level of blockchain concepts (e.g., blocks, smart contracts).
* **Application Layer:** This layer contains web application of smart home to enable home members to control transactions and control IoT devices in the smart home environment.

Table 1 Hyperleadger Composer Component

|  |  |
| --- | --- |
| Component | Work |
| CLI | Facilitate developers and operators with efficient deployment and management of business network definitions. |
| REST server | Generated by Loopback connector to create the REST APIs for integration with application. |
| Web UI | Playground that define and test business network quickly |
| SDK | Set of Node.js APIs to perform operations (Create, Read, Update, Delete) of resource in blockchain distributed ledger. |

## Smart Home Model Adopted in the Proposed Approach

To implement the proposed solution, it is important to map the three basic concepts of the hyperledger composer (i.e., assets, participants, and transactions) to smart home elements (i.e., users, sensors, and transactions). In order to create the smart home application, we used the composer to create a business network definition comprised of a model, script, and access control files. Figure 2 shows the business network definition.

* **Model File** — A definition of the resources present in the network. These resources include Assets, Participants, and Transactions. Table 2 shows the definition and example of a model in the blockchain business network.
* **Script File** — Logic for the transaction functions, which is the chain code of our application.
* **Access Control File** — Contains various rules, which define the rights of different participants in the network. This includes, but is not limited to, defining what assets the participants can control. This file help homeowner to define the rules and how can access smart home devices.

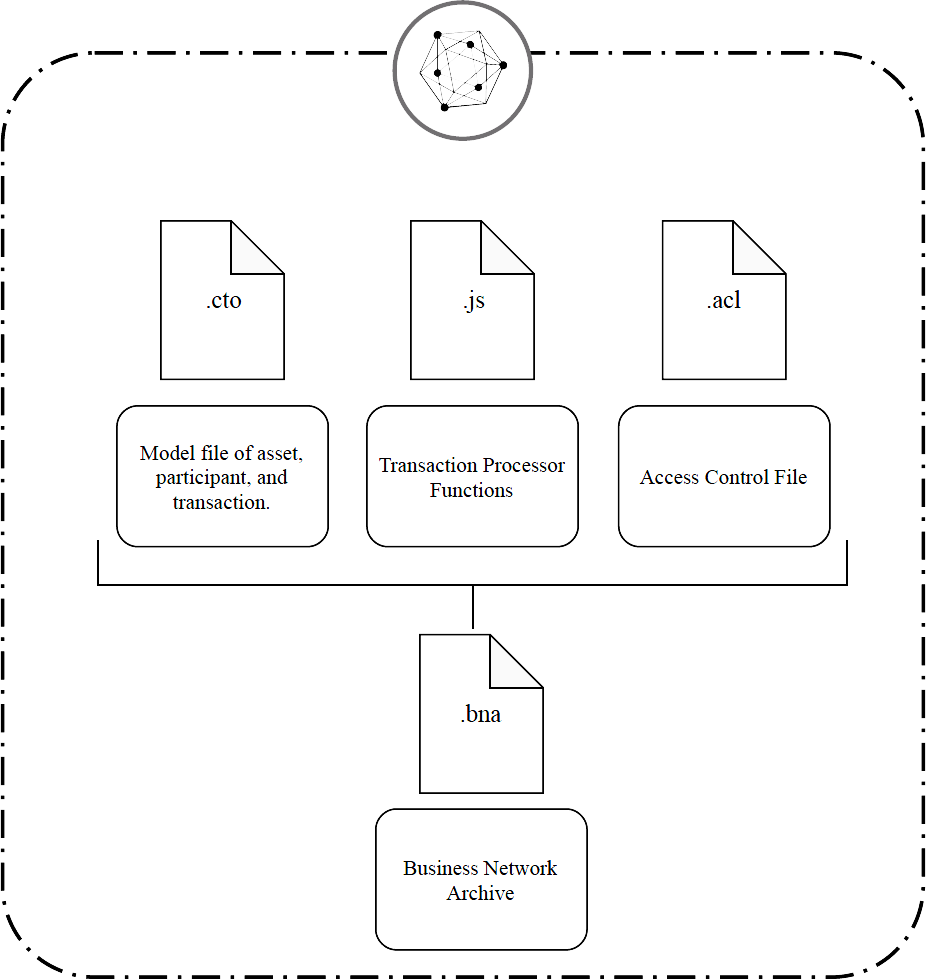


Figure 2 Business Network Definition Structure

The Composer layer runs in its own isolated runtime, and it is connected to the fabric network through the means of connection profiles. After defining asset, participant, and transaction of Business Network Definition (BND) archive files (.bna files) that is generated to allow deployment to hyperledger fabric layer in the proposed approach as shown in Table2.

Table 2 Definition and Example of Model in Blockchain Business Network

|  |  |  |
| --- | --- | --- |
|  | Definition | Example |
| Asset | The resources of value that are  owned and managed by the  network. | light sensor, thermostat sensor |
| Participants | The actors owning or acting  on the assets. | homeowner |
| Transactions | The activities to be carried out  on the assets on behalf of the  participants. | Set Temperature, Change  Light Sensor Status |

## Blockchain Network Model Mapping to Smart Home IoT Devices

Figure 3 shows blockchain network of hyperledger fabric layer that illustrates the transaction life cycle of the model. Indeed, the user application is registered and enrolled with the home’s certificate authority (CA) and receives back necessary cryptographic material, which is used to authenticate to the network and peers authenticate , endorse , order , validate and commit transaction in the blockchain network as described in [21].

Hyperledger fabric was designed to be modular, scalable and has a secure foundation for blockchain adaptation solutions. In Figure 3 there are roles defined within hyperledger fabric network:

1. **User:** How to access to applications to propose transactions on the network.

2. **Peers**: Maintain the state of the network and a copy of the ledger. There are three types of peers in network.

* Endorsing peer: Endorsers simulate and receives a transaction proposal for endorsement, grant or deny endorsement of transaction proposal by validating with endorsement policy.
* Ordering peer: Approves endorsement of transaction orders them into a block and delivers the blocks to the committing peers.
* Committing peer: Committers verify endorsements and validate transaction results, ordered transactions, maintains **ledger and state.**

**3. Ordering Service:** The ordering service packages transactions into blocks to be delivered to peers on a channel. It guarantees the transaction delivery in the network. It communicates with peers and endorsing peers.

4.**Membership Service Provider (MSP):** The MSP is implemented as a Certificate Authority to manage certificates used to authenticate member identity and roles. No unknown identities can transact in the hyperledger Fabric network. It manages user IDs and authenticates all participants on the network [22].

Confidentiality can be only ensured by endorsing peers in the network. Different identities of peers can be arranged to different participants in the network depending on the policy agreed by all the participants in the blockchain network and all done by MSP that uses Fabric CA to generate the keys and certificates needed to authenticate peers. Peers have an identity assigned to them via a digital certificate from a particular certificate authority CA. While blockchain network is a distributed network, network and rules might be set up by one trust party in the beginning. In our approach after authenticating users to join the network. The access control file limits their access to allow them querying only relevant data, thus providing permissioned and secure environment. However, the access rule should be agreed by each node in the network and blockchain is an immutable database, if the administrator or regulator tries to change the rule or do something harmful, every peer in the network could see the record of each action.

A close up of a map

Description automatically generated

Figure 3 Blockchain Network Model Adopted to Smart Home

## Smart Home Scenario within Blockchain Adaptation

In order to experiment with and test the proposed approach, a practical scenario of a smart home transaction handling and how to interact with hyperledger fabric using hyperledger composer is presented. More specifically, this implementation will use a browser UI to modify and test chaincode and deploy our changes. After that, we generate API to allow our application to integrate through a REST-ful interface of IoT devices. The experimental scenario will simulate a smart thermostat that provides the temperature data as the first IoT device. The other one is a smart light bulb to provide light on or off smart function. Similarly, in a real-world scenario, this will be a temperature sensor that could be connected to a real thermostat like Nest or other smart home devices via AP0I. To keep homeowners and family members safe from any external interference or hacking attempt to controlling any smart home device, they must first find out if they have permission to adjust the smart device by running a transaction defined in a chai/ncode that runs on the hyperledger fabric. Hence, the chaincode will check the value recorded in the ledger for the temperature gauge to determine if the smart thermostat adjustment is allowed or not. Secondly, we will add smart light bulbs to check the current state of smart light and adjust it to ideal settings based on the terms of the chaincode. The following steps discuss the approach’ implementation in further details:

* **Cloud Storage**

We host Virtual Servers on IBM LinuxONE Community Cloud, to make our proposed solution lightweight on smart home devices, However, to ensure security, we use Secure Shell (SSH); it is a cryptographic network protocol that provides a secure channel over an unsecured network in a client–server architecture.

* **Smart Home Model**

In the previous section, we described the Business Network Definition and its resources, briefly. Here we describe how we used hyperledger composers and developed our smart home model, also how we deployed it on the blockchain network. Figure 4 illustrates how business network definition is developed with three main files: Model file, Transaction processor which represents our smart home model, and deployed finally on hyperledger fabric blockchain network. Hyperledger Composer uses an object-oriented modeling language that is used to define the domain model which is (asset, participant, transaction) in business network definition.



Figure 4 Development and Deployment of business network on blockchain

* **Model file**

Figure 5 show sensor as the asset that has two types thermostat and light sensor to collect the data and send them to the participant in the network according to their transaction.

* **Transaction Processor Functions**

This is a script file which represents the chaincode. It is invoked to change the state of a resource in the associated resource registry. Figure 6 illustrates a transaction processor function that updates the state of the sensor when it is transferred from one participant to another.

* **Access Control File**

Access control language (ACL) declares access control rule of interaction between asset, participant, and transaction. After defining ACL rules that restrict which users/roles are permitted to manipulate (create, read, update or delete) resources in the business network. Figure 7 shows our file that will check if the home user is an admin or non admin [20].

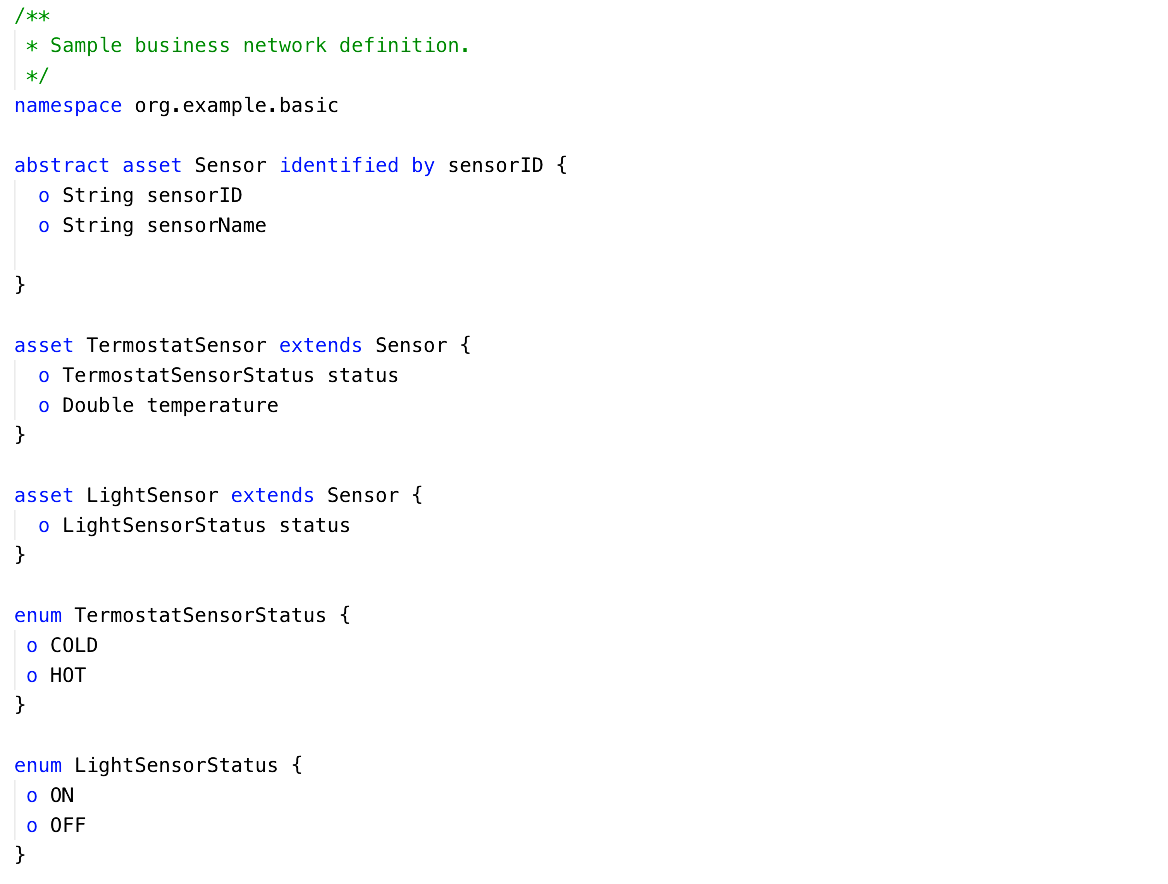


Figure 5 Model File Example



Figure 6 Script File Example

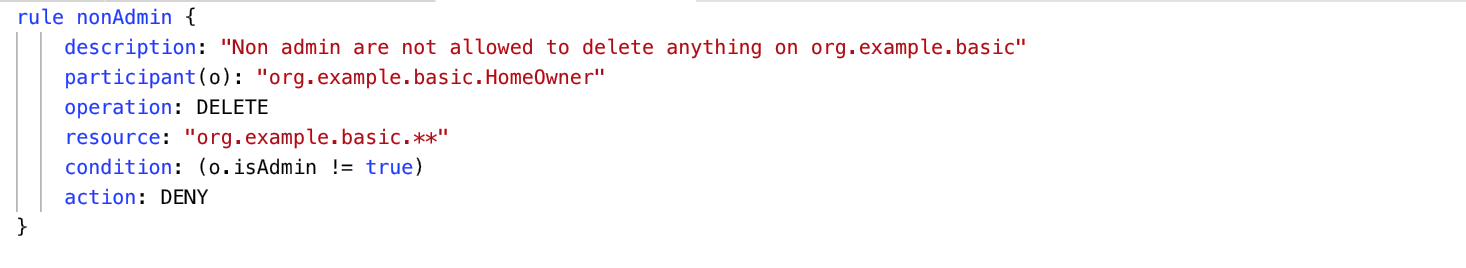


Figure 7 Access Control File Example

## Deployment the solution on the Fabric Blockchain Network

After defining business network definition archive files (.bna files) that are generated to allow the deployment of a blockchain network, in the deployment process, administrators have permission to install hyperledger fabric chaincode for a new business network onto peers. Members do not have permission to install chaincode. In order to deploy a business network to a set of peers, identity has to be provided that has administrative rights to all of those peers of all these rules defined on the access control file. More specifically, deploying a business network archive (.bna) file requires using an ID card (which includes connection profile and credentials) to deploy it to the distributed ledger. However, each deployment and modification will be recorded in the immutable blockchain database. By this, every transaction done by the smart home members is monitored and traceable and each data generated by sensors will be recorded. Consequently, this provides the integrity of the home members sensitive data. Our approach deploys the blockchain network on the cloud using Docker. Indeed, this Docker is designed to make it easier to create, deploy, and run applications by using containers. In our case, hyperledger fabric uses docker images to run the following four processes:

1. Fabric-peer is for peers endorsing and committing.
2. Fabric-couchdb is a key value database used to store its state.
3. Fabric-orderer used for ordering service that takes the responsibility for ordering the endorsed transaction.
4. Fabric-ca is a certificate authority that takes over the registration of identities and issuance of enrollment certificate.

Figure 8 shows a workflow of transactions on the blockchain network for our smart home approach. It represents two processes that the homeowner can do to submit transaction and update data in the blockchain network.

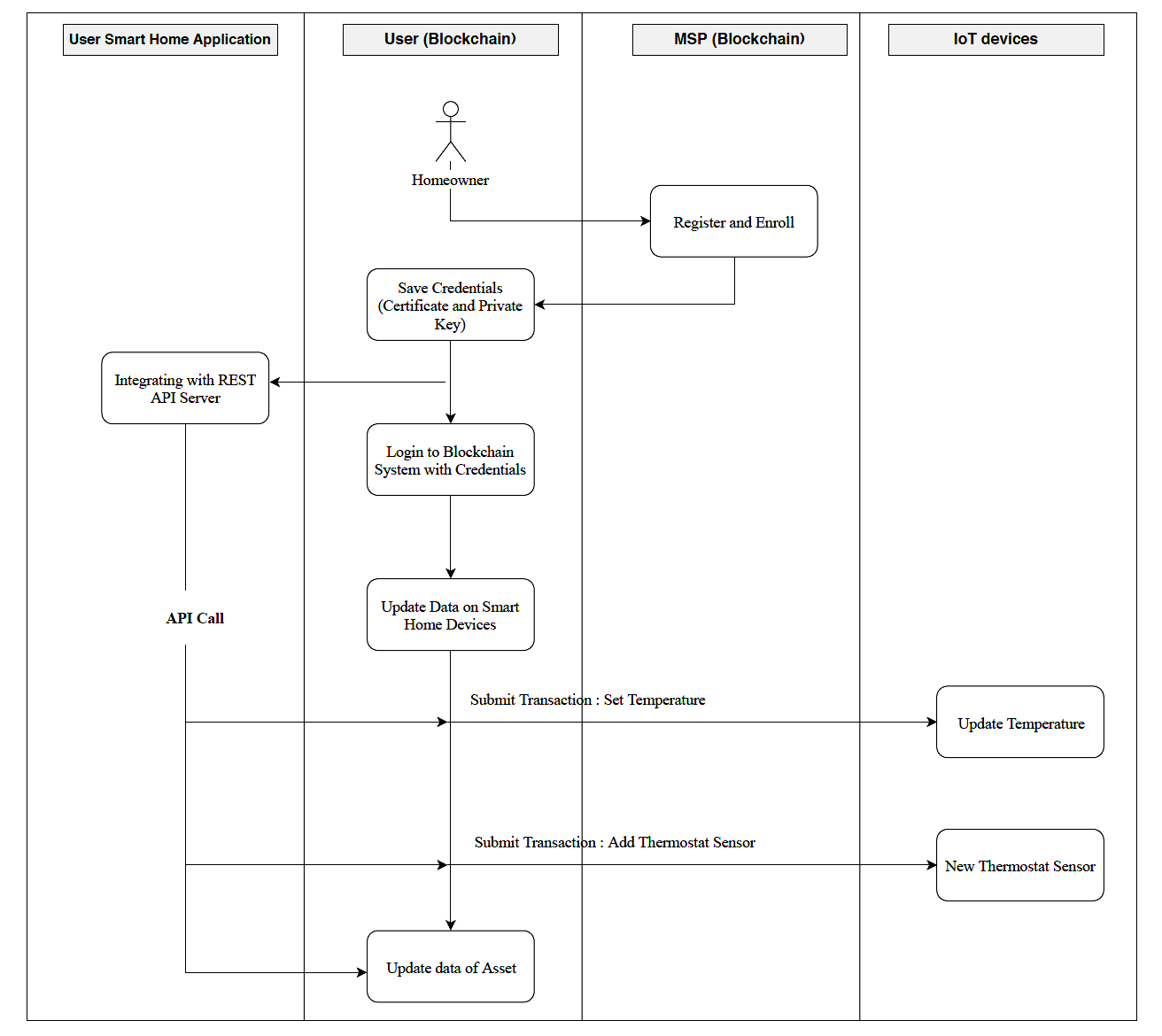


Figure 8 Workflow of Transactions on Blockchain Network within Smart Home

Figure 9 shows the sequence diagram of the proposed model which illustrates the data transactions flow in blockchain network model

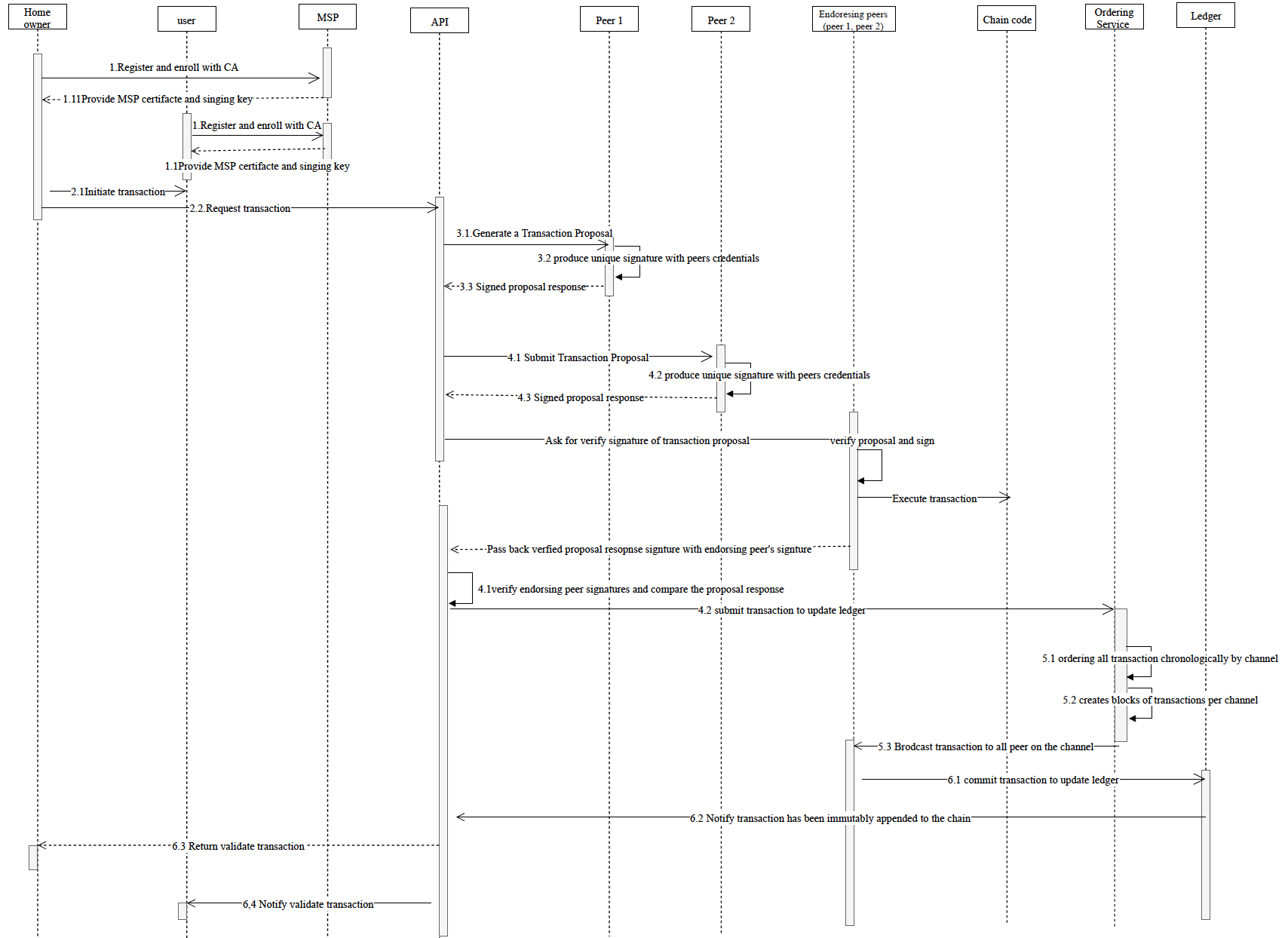


Figure9 sequence diagram of transaction flow in the blockchain network

The steps described in Figure 9 are explained as follows:

1. Application user send registration and enrollment to Membership Service Provider (MSP) with their certificate authority (CA) and wait for MSP issue them confidential, which includes certificate and private key. Those confidential is used to authenticate themselves to the blockchain network in the future.
2. The client sends a transaction proposal (TxProposal) to the peers defined by the endorsement policy (all running the same smart contract, say SC1), consisting of theclientID, payload, and transactionID, along with a cryptographic signature of the client on the transaction header. The payload contains the chaincodeID, operation and inputparameters.
3. Homeowner sends a transaction proposal to an endorsing peer. This initiation is referred to *Peer1* and *Peer2*, who are individually representative of homeowner and users. Endorsement policy states that both peers must endorse any transaction, therefore the request goes to peer1 and peer2. Then SDK generates a transaction proposal to each peer. The proposal is a request to invoke a chaincode function so that data can be read and/or written to the ledger. Afterwards, *Peer1* and *Peer2* sign proposal with their own signature, which is derived from cryptographic credentials.
4. The signed proposal sends to endorsing peers to verify the digital signature of users. The endorsing peers will simulate a transaction by executing a chaincode function. From this process we get a set of key/value versions that were read in the chaincode(read set) and a set of key/value that were written in the chaincode (write set). Finally passing back the proposal response to the SDK.
5. SDK verify the proposal response and endorsing peer signature. Then, SDK checks if the transaction fulfils endorsement policy then submits the transaction to the Ordering service. This service is responsible to broadcast the ordered transactions to all the peers on the channel.
6. Order Service receives all the pending transactions in the network and order them chronologically, then creating blocks of transaction.

Now we will explain creating block process, The blockchain is structured as sequential log of interlinked blocks, where each block contains a sequence of transactions, each transaction representing a query or update to the world state. What is important is that block sequencing, as well as transaction sequencing within blocks, is established when blocks are first created by ordering service. Each block’s header includes a hash of the block’s transactions, as well a copy of the hash of the prior block’s header. In this way, all transactions on the ledger are sequenced and cryptographically linked together. This hashing and linking makes the ledger data very secure. Even if one node hosting the ledger was tampered with, it would not be able to convince all the other nodes that it has the ‘correct’ blockchain because the ledger is distributed throughout a network of independent nod.

1. Transaction encapsulated in a block pass to committing peers. Once the peers have received the transactions, they will validate it according to the endorsing policy of the channel, and authenticate the signatures with respect to the transaction payload. This process ensures that the correct allotment of specific peers have signed the result of the transaction proposal. In addition, peers check the versioning of the read set to ensure the data integrity and protect against double-spend attack. Finally, for each valid transaction the write sets are committed to the current state database and the block is appended to the chain. The ledger is updated, and event is emitted to notify homeowner and users that the transaction has been successfully proceed.

Figure 10 explains the general structure of blockchain in hyperledger fabric, blockchain containing list of blocks ,the first block in the blockchain, the genesis block it is the starting point for the ledger, though it does not contain any user transactions. Each block has block data which contains all its transactions. Each transaction hold header , Signature that created by the client application , Proposal , Response and Endorsements a list of signed transaction responses from each required organization sufficient to satisfy the endorsement policy. In Addition, blocks has block header which contains block number , current block hash and previous block hash. Current Block Hash mean the hash of all the transactions contained in the current block. Previous Block Hash it is a copy of the hash from the previous block in the blockchain.

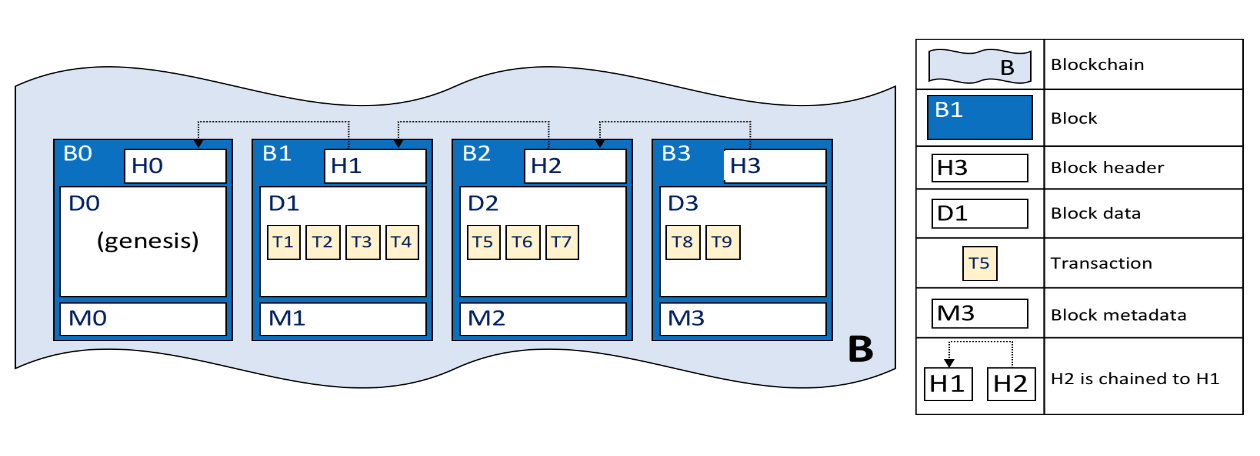


Figure10 general structure of Hyperledger blockchain

*D. Create API to Call Blockchain Application*

The smart home application can be integrated with a blockchain through Loopback API. By this integration, it is possible to pull data from the smart home application and convert it to assets or participants in a blockchain network. Hyperledger composer provides a tool to generate Node.js server that exposes the business network as a REST API. This REST API server in Figure 10 represents the role of the gateway, subscribing to the events emitted from the deployed business network and publishing them to client applications. REST server should be configured to be secured with HTTPS and TLS (Transport Layer Security), so that all data transferred between the REST server and all of the REST clients are encrypted. Hence, the smart home application uses REST API to test and submit the transaction of the IoT devices through the browser UI [20].

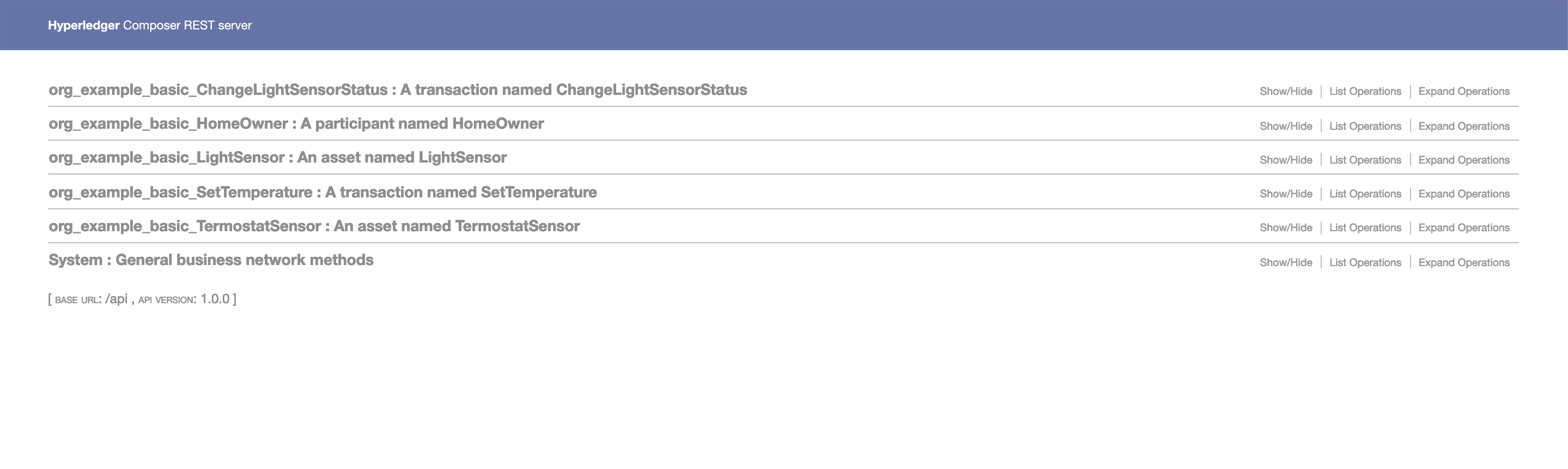


Figure 10 REST API Generated by Hyperledger Composer

Final step in the implementation process after generating a REST API server, is the integration with IoT devices in the smart home. Indeed, our implementation does not contain any hardware devices, and this is one of our future works, however, we used NodeRED as a simulator to simulate our IoT devices. Node-RED is a lightweight Open Source integration technology, written in JavaScript. It uses a graphical flow to integrate different nodes, where nodes can receive data, transform data and output data.

For our smart home application, we design the Node-RED flow which represents how the transactions are processed inside the smart home. The purpose of this Node-RED flow is to allow IoT data to flow in Smart home devices. All data generated will be tracked by sensors and all the transactions will be added to our blockchain network. Likewise, for the thermostat sensor, we used a RaspberryPi Sense Hat simulator and we can control it via the dashboard that appears on the smart home application. in the end, we will submit all home transactions through NodeRED’ dashboard which interacts with the blockchain network

via API.

Figure 11 shows the Node-RED flow work we are using in our demo application. This flow sets up the HTTP parameters to call the REST API of the Hyperledger fabric network, sets to the POST command to write a temperature even into blockchain as a transaction. Also, this flow uses GET command required to query all of the Temperature transactions on the blockchain. Consequently, this method uses all IoT connected devices on the smart home. This flow constructs a variety of Node-RED Dashboard UI elements that is to select and control the smart home devices took while collecting IoT environmental sensor readings. Finally, Figure 12 illustrates our smart home application with sensors that store data in a hyperledger blockchain.

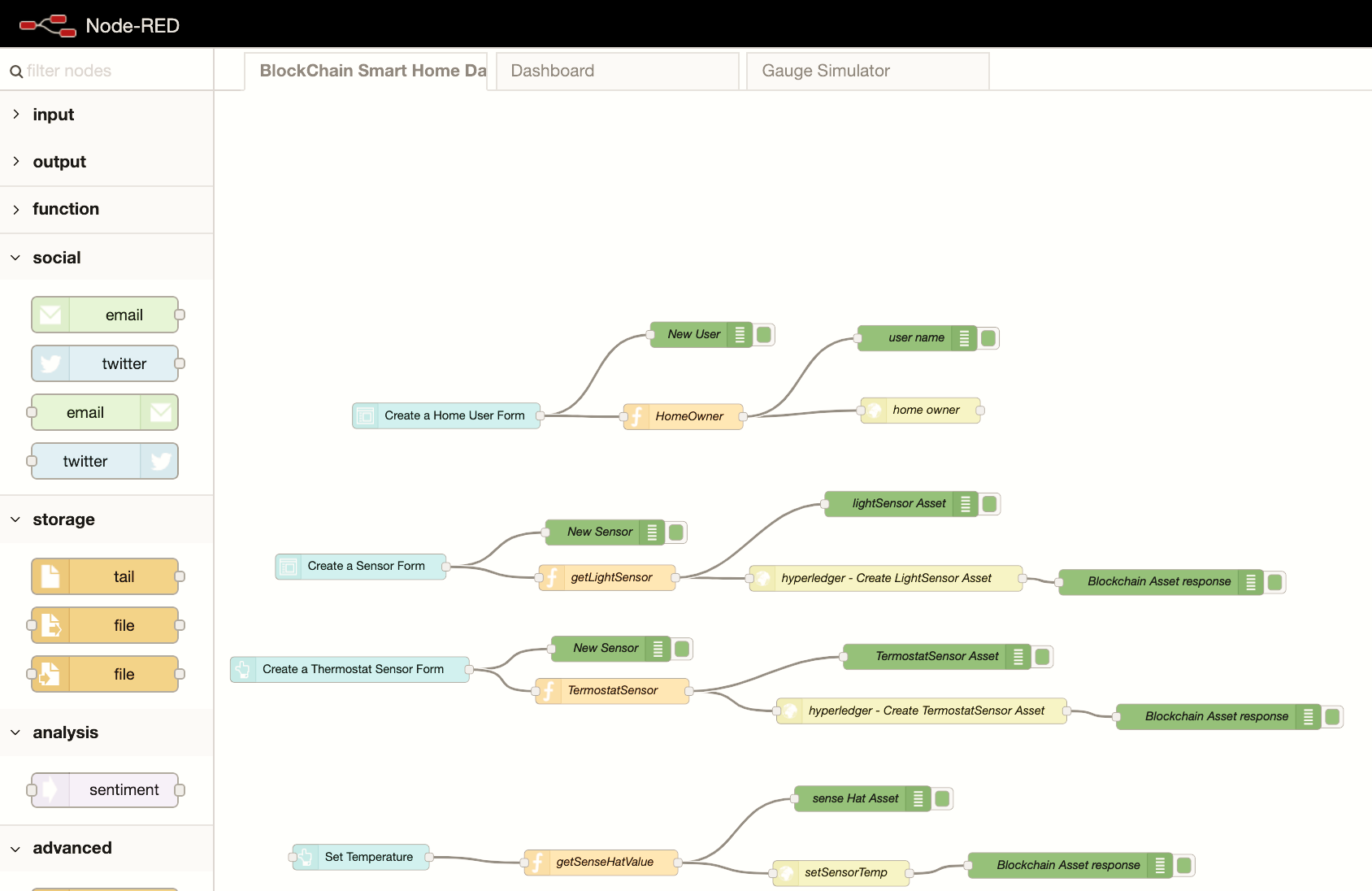


Figure 11 Node-RED Workflow Used in Demo Application

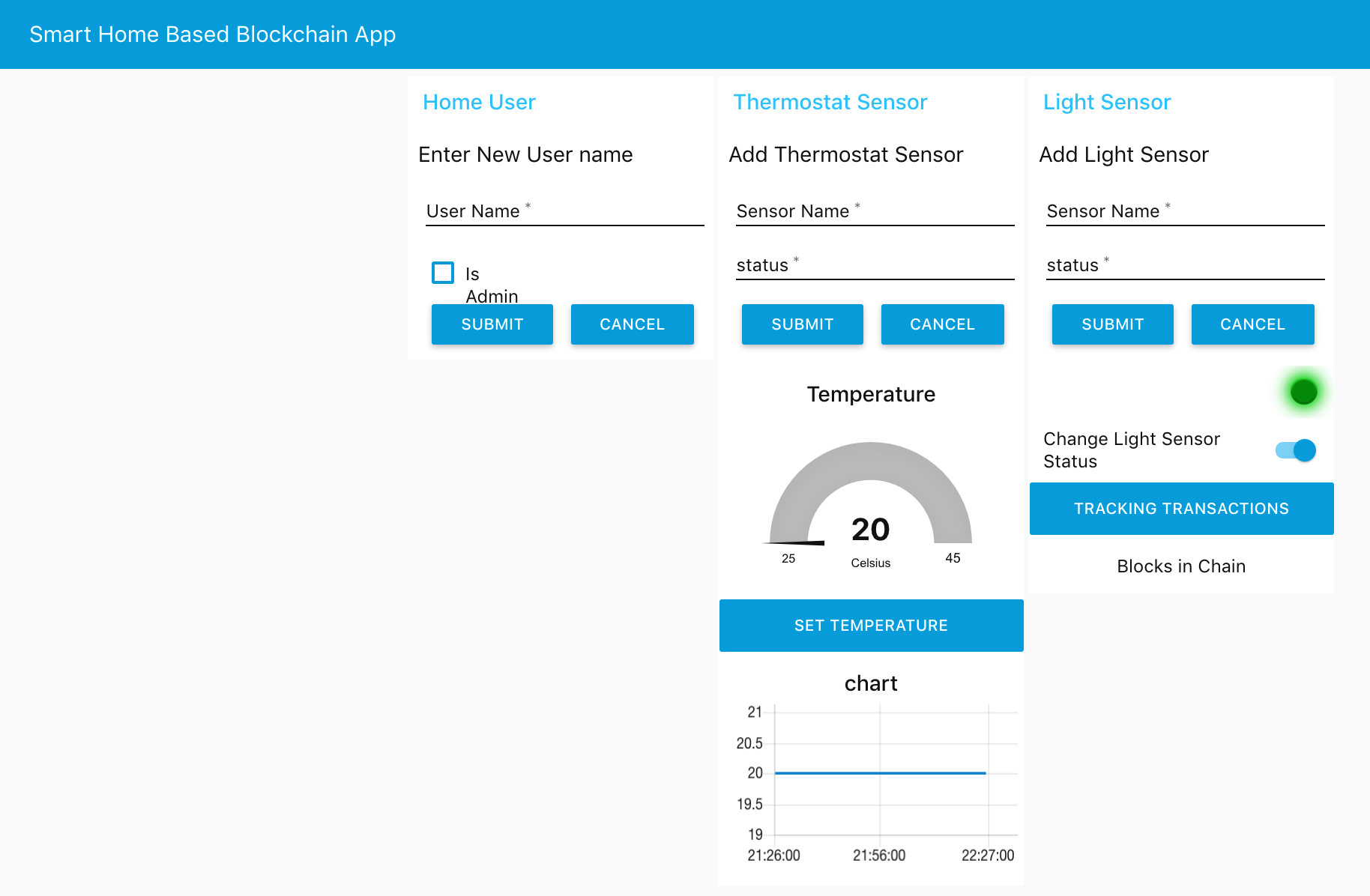


Figure 12 Our Smart Home Application

# Results and Discussions

This section provides the implementation of the proposed adaptive approach and the simulation scenario of the smart home based blockchain application. Furthermore, this section will focus on testing our smart home application using a Composer playground. We also present the security analysis of our proposed adaptive approach from different perspectives: confidentiality, integrity, availability, authorization, and transparency.

## Confidentiality and Authorization

In this paper, our main objective is to achieve the confidentiality and privacy of IoT devices on the smart home using blockchain technology. According to the proposed architecture, the cloud storage layer ensures confidentiality for the smart home when users connect to the cloud server via secure shell protocol (SSH) to setup authentication for users. SSH protocol is a method for securing remote login. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. Also, the Hyperledger fabric layer will ensure confidentiality using MSP. Moreover, in Hyperledger, the composer layer provides access control that contains various rules, which define the rights of different participants in the network, which limit unauthorized access to the network. In our simulation scenario, confidentiality is achieved by combining the two aspects. Access control file in the business network definition that is deployed on a blockchain network and membership service provides access control service to any data recorded.

Hyperledger fabric layer on our architecture uses MSP to provide security on the blockchain network. Membership service provider maintains the identities of all nodes in the system and is responsible for issuing node credentials that are used for authentication and authorization. Since Fabric is permissioned, all interactions among nodes occur through messages that are authenticated, typically with digital signatures. The membership service comprises of a component at each node, where it may authenticate transactions, verify the integrity of transactions, sign and validate endorsements, and authenticate other blockchain operations. MSP aims to offer an abstraction of cryptographic mechanisms and protocols. Thus, MSP is responsible for issuing and validating certificates, and user authentication. Fabric CA is an implementation of the MSP that provides a mechanism for registering users from a network member and issuing them digital identities (X.509 certificates). Fabric CA, typically, runs inside a Docker container. Each Fabric CA is configured with a backend database that stores the registered identities, as well as their X.509 certificates. However, to test the simulation scenario, all the files of identity cards are issued by MSP, which is used to identify users and connect them the blockchain network securely. Also, the connection profile used to connect our hyperledger fabric layer with hyperledger composer layer defines all the necessary configuration parameters, which contains the TCP/IP addresses and ports for the peers and certificate authority. Credential is made up of X.509 certificate and private key. Figure 13 shows screenshot of the files and certificates

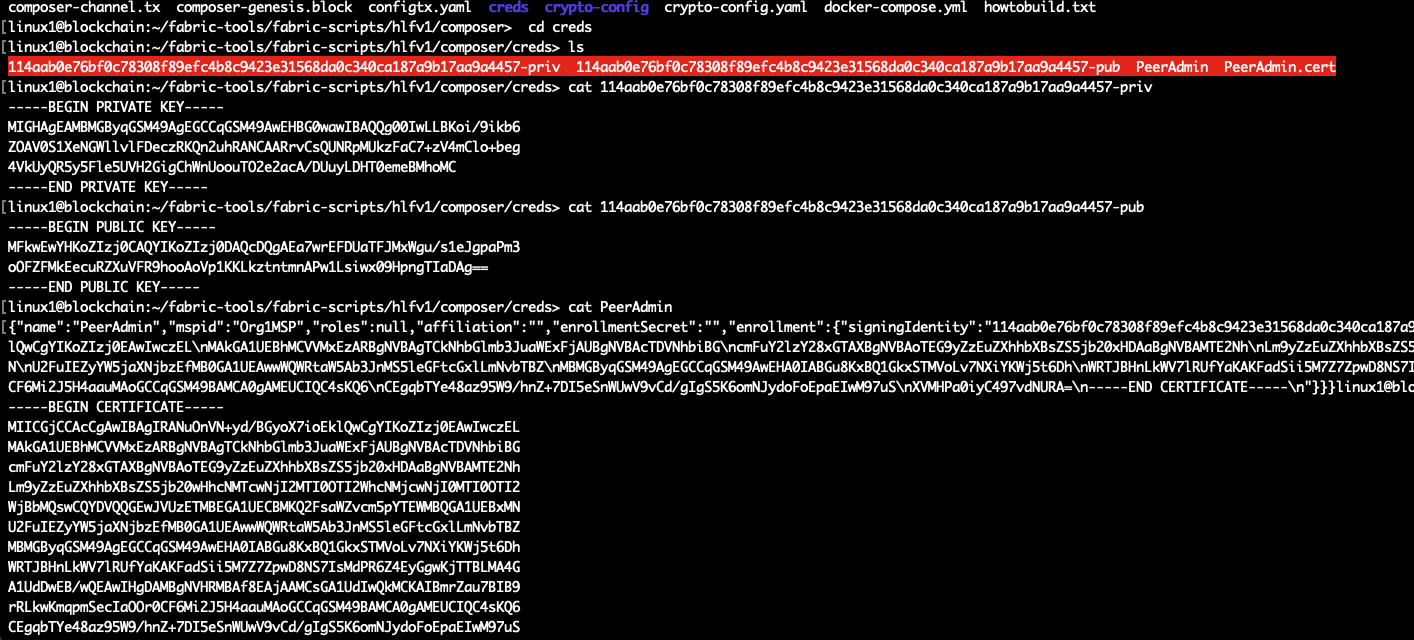


Figure 13 Screenshot of the files and certificates

The hyperledger composer implements the concept of role-based security through permissions that are embeded right into its architecture to handle both authentication and authorization. A participant’s access to resources is controlled based on the identity that is issued to that participant. In the smart home test scenario, we restricted data access to non admin participant and defined that on ACL file. It is important to mention that while using access control it is impossible for any participant who is not admin in network to create or delete an asset. However, this will ensure the privacy and security of the generated data of IoT devices. Also, it denies any malicious activity on the smart home environment. Figure 14 illustrates that non admin participant is denied to create an asset on the network.

## Integrity and Availability

Securing smart home IoT-based system means realizing the integrity and availably of data. Firstly, integrity is the assurance that the accuracy and consistency of data is maintained. No unauthorized modifications, destruction or losses of data will go undetected. The nature of the blockchain structure supports data integrity for all IoT transactions in smart homes. Blockchain is designed to be resistant to data modification, which provides an immutable data record that is tamper-proof. Secondly, availability is about the assurance that any network resource (data/bandwidth/equipment) will always be available for any authorized entity. Such resources are also protected against any incident that threatens their availability. To increase smart home availability, devices are protected from malicious requests by using access control. Hence, any participant without a rule, will be eliminated from the smart home network because as in private blockchain, only authorized and validated users can access the network.

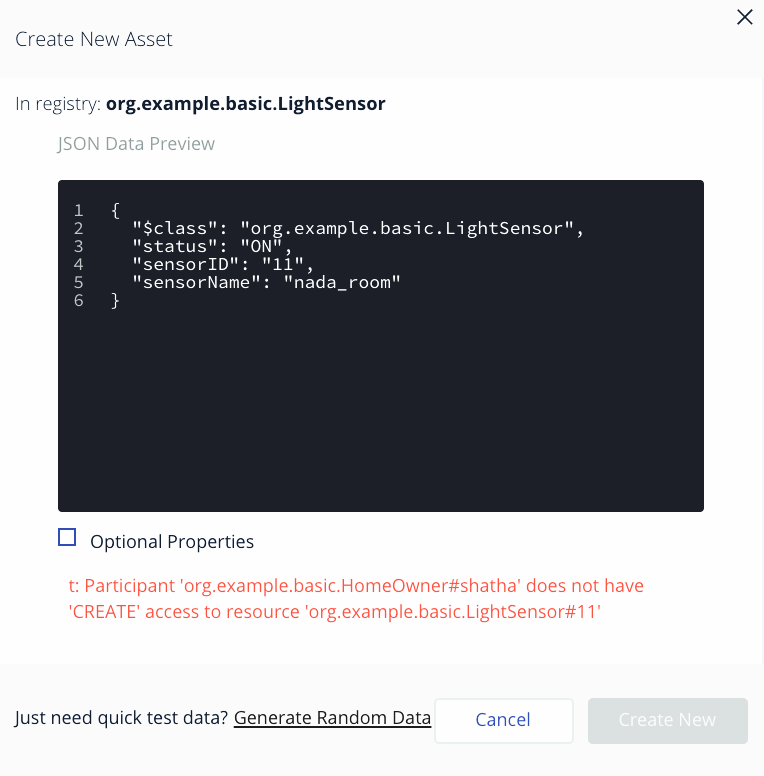


Figure 14 Non-Admin Participant Deny to Create Any Asset on the Network

## Transparency

Transparency covers visibility and operability of the approach. By utilizing blockchain technology, we can ensure accuracy and transparency across all transactions, leading to a safer and more efficient process for delivering goods and services to consumers. Hyperledger fabric ensures transparency via Immutable Database. Indeed, if any data is stored in the hyperledger fabric, then the data cannot be altered in any way, neither edited nor deleted. By consequence, deceiving the system by external users and other hyperledger participants will be hard to achieve. When it will become hard to forge data to benefit oneself then trust and transparency will be increased automatically. Even though the ability to gain access to the information also depends on the access control and identity of the participant, the capability to record data and access data is unprecedentedly effortless and trustful compared to the traditional database system. To ensure transparency of the proposed approach, we will focus on the model file described in terms of *Participant*, *Asset*, and *Transaction*.

* **Participant**

Hyperledger Composer comes with a web user interface which is a web playground as describe in our architecture. Hyperledger Composer Playground is where we can model and test our network before generating REST API server. The proposed smart home simulation scenario explains the roles on smart home and devices that need to submit transaction as defined on the model files. First, we will test the homeowner the participant on the model file. Figure 15 will show the creation of participants with different home members names and if he is an admin or not. However, all this transaction will be recorded and visible on our blockchain network. In this example, we added a new participant username is the identifier of this example, which is shathaAlarabi. The class field indicates which role is created. Another field is Admin, which indicates if the participant is considered as admin or not. After confirmation of creating a new participant’s transaction, data will be recorded to the blockchain with transaction **id,** which is the hash generated and timestamp. Figure 16 is a JSON format of the transaction data.

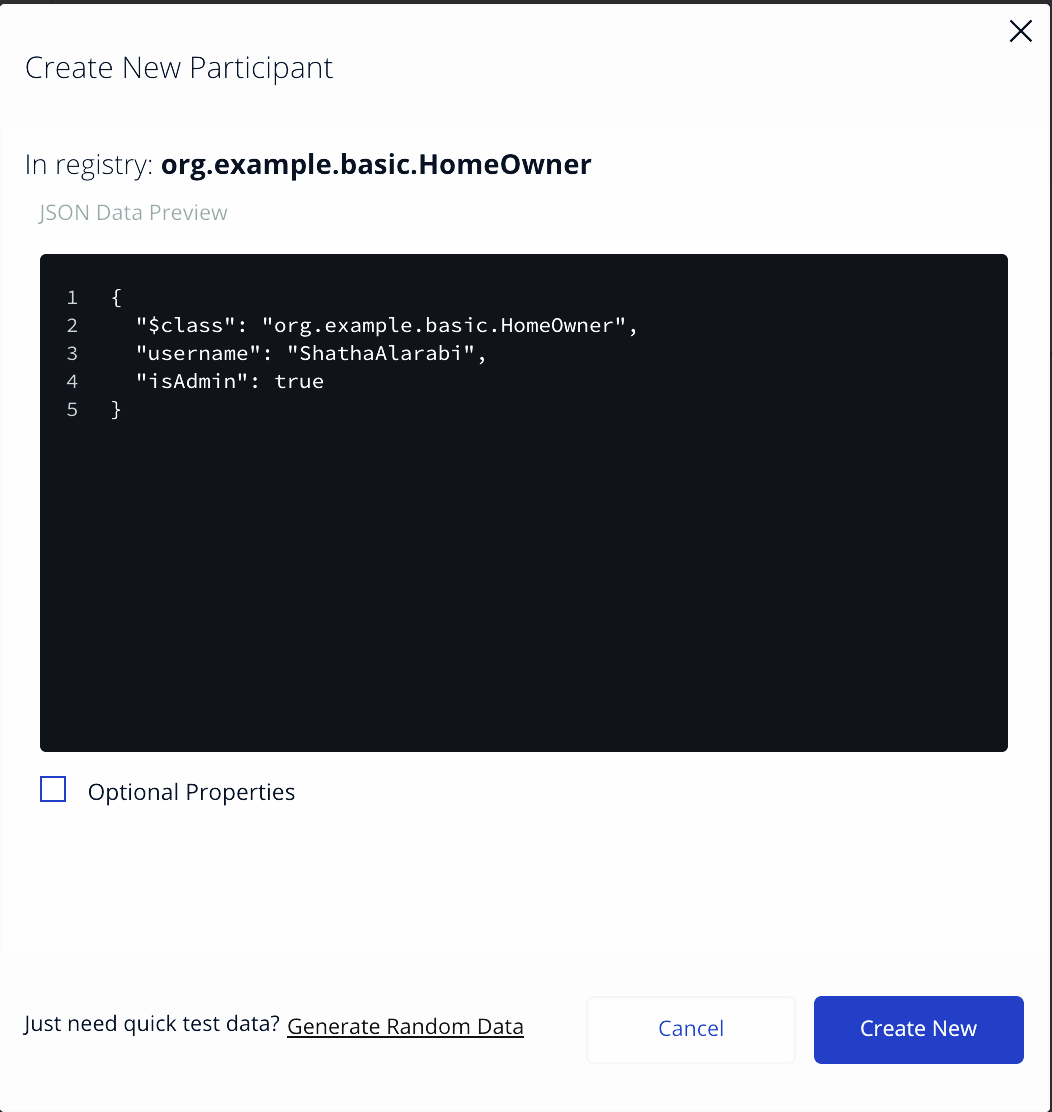


Figure 15 Create a New Participant

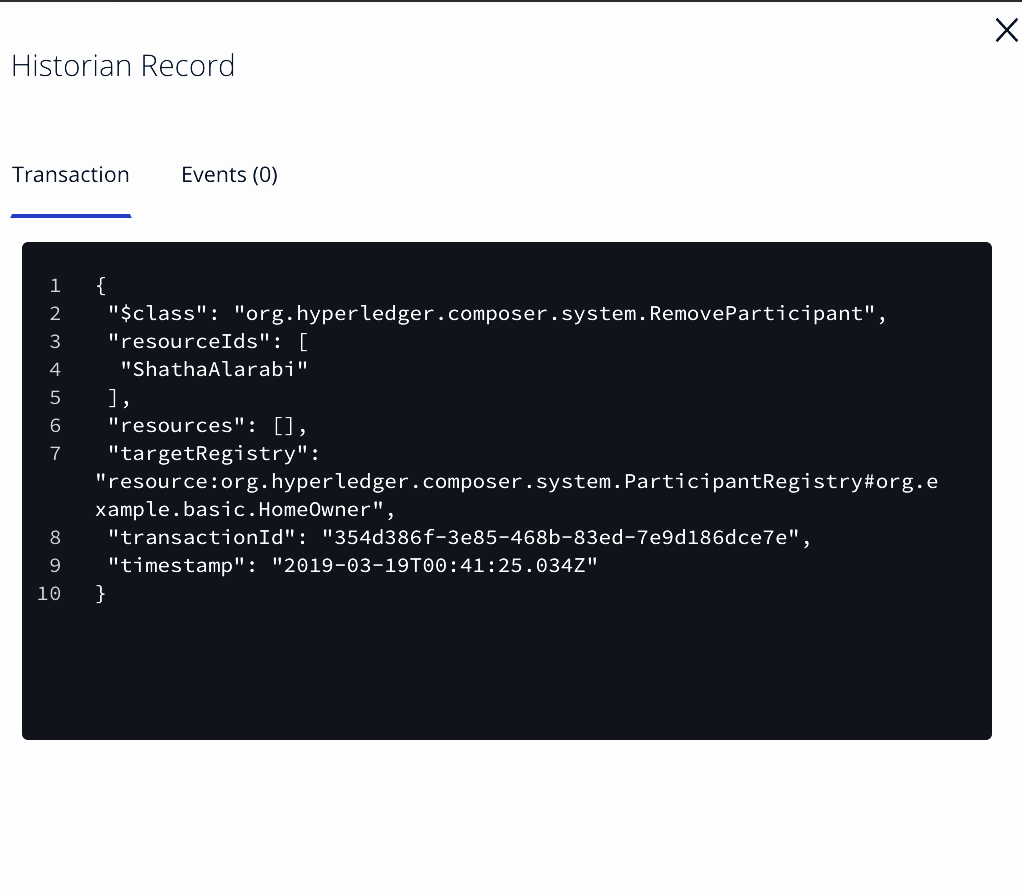


Figure 16 Record of the Successfully Created Participant

Any action to create or remove participants, in the smart home simulation scenario, is recorded with transaction id and time, in historian record, which is a specialized registry that records successful transactions, including the participants and identities that submitted them. The historian stores transactions as HistorianRecord assets, which are defined in the Hyperledger Composer system namespace. All created participants will be able to interact with other devices and submit transactions. All data recorded on the blockchain network is tamper-proof, which increases the trust and privacy of the home member sensitive data, see Figure 17.



Figure 17 Historian Record of Adding Participants on Blockchain

* **Asset**

Here we test the Asset Registry API. The Asset Registry is used to manage a set of assets stored on the blockchain. In our smart home application, we have two types of assets: thermostat sensor and light sensor. Asset registry supports the creation, update, and deletion of assets with access control. This example creates a new thermostat sensor, which is shatha-room. sensorID is a unique identifier of the example. Additional asset information such as state of the thermostat that if temperature is less than 15 degrees, then it changes the status field to COLD, otherwise the status field will be HOT (See Figure 18). After confirmation with the creating of a new thermostat sensor, JSON format transaction data will be recording to the blockchain with all the input data (see Figure 19). The asset registry features the item-level transparency of the entire smart home, which means all the items have their own information resided in the blockchain system. Compared to the easy tampering of the traditional database systems, blockchain ensures the trust of data by its distributed network feature.

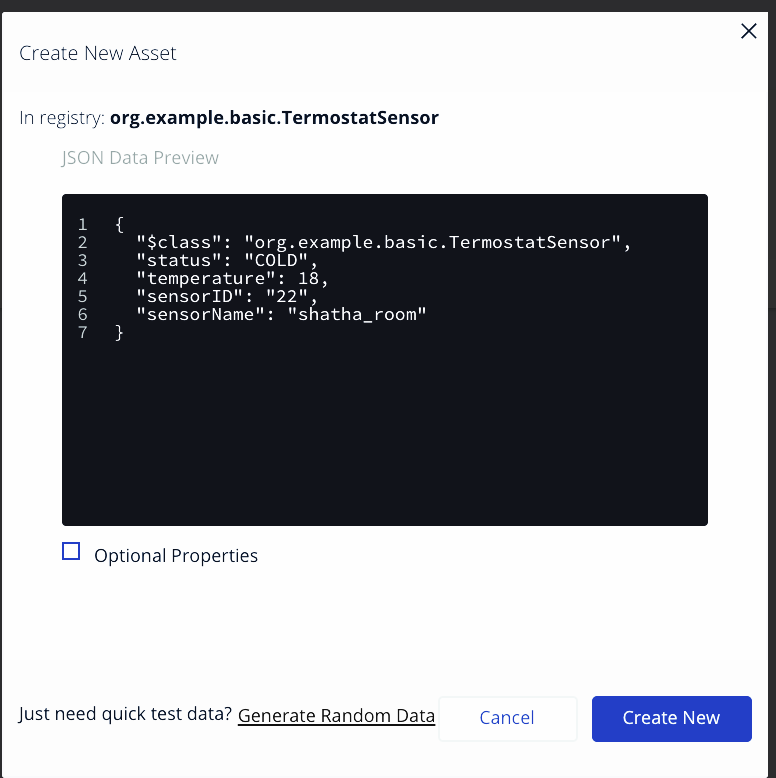


Figure 18 Creating a New Thermostat Sensor

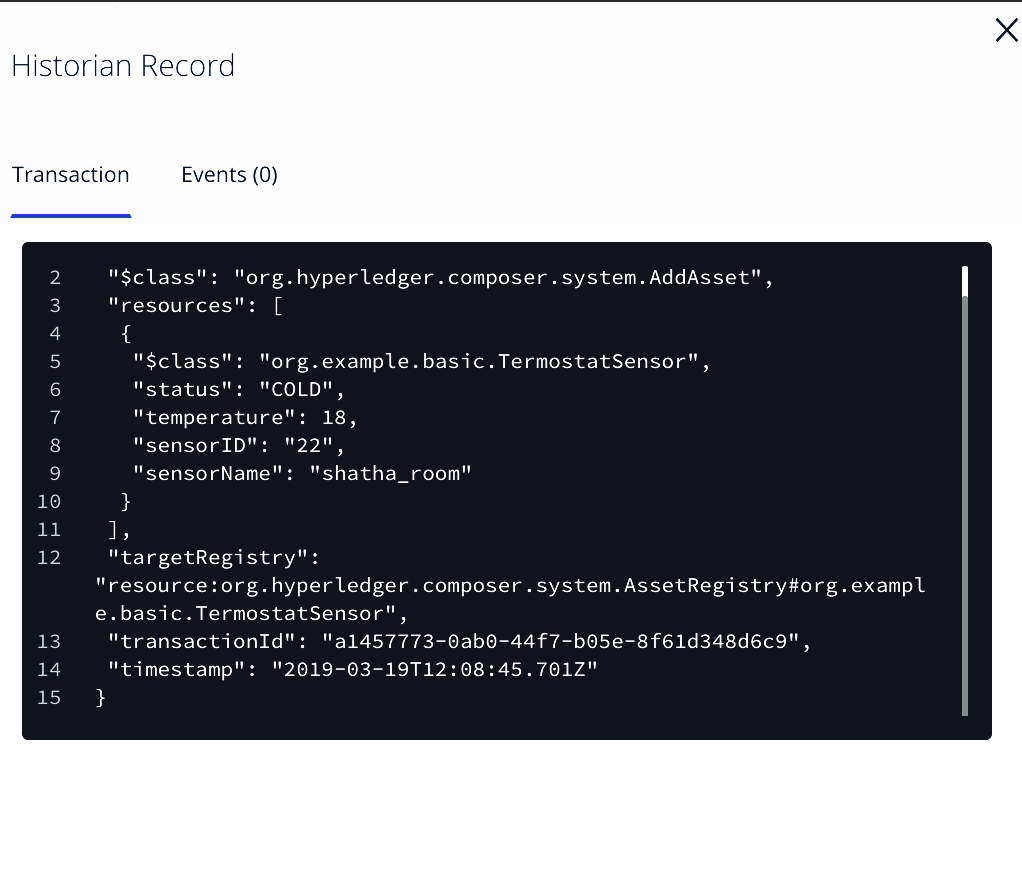


Figure 19 New Asset Being Created in the Asset Registry

* **Transaction**

The transaction represents an interaction between asset and participant. After creating assets and participants, it is possible to submit transactions by the home members. There are two defined interactions in our scenario: (1) Set Temperature and (2) Change Light Sensor Status. Figure 20 shows that Homeowner Shatha intends to change the Temperature of shatharoom by submitting the Set Temperature transactions. In submitting a transaction, we change the temperature to 20 degrees and add the SensorID of shatharoom that need to change its temperature as well as adding the participant who submits this transaction. the temperature of the thermostat sensor will then be updated. All transactions between homeowners and IoT devices will be recorded into the immutable blockchain network. Table 3 summarizes how the proposed solution achieves the above security requirements.

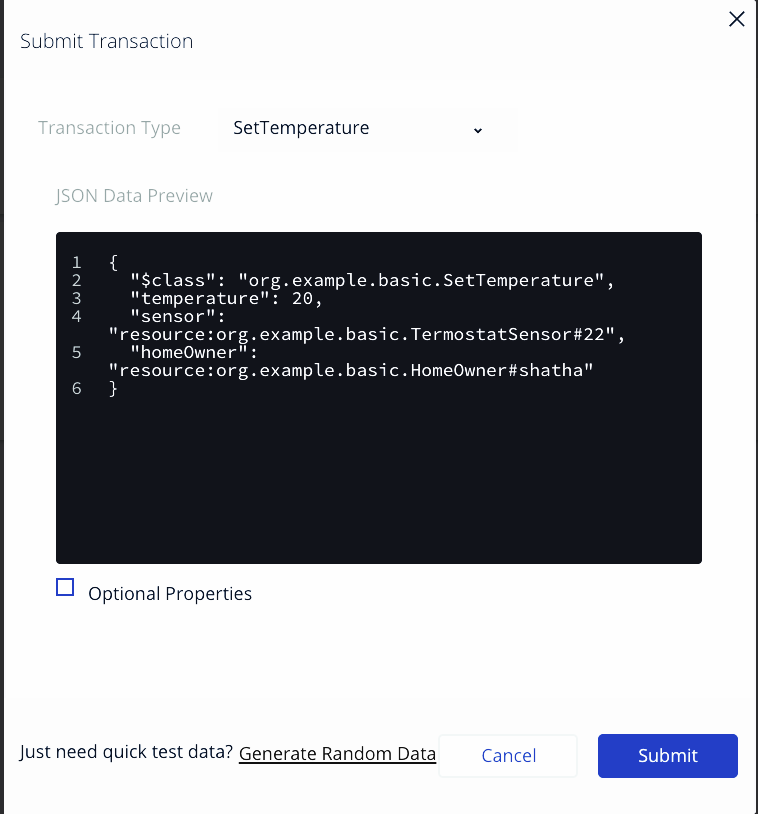


Figure 20 Submit Set Temperature

|  |  |
| --- | --- |
| Requirement | Safeguard |
| Confidentiality | Achieved using MSP and Access Control |
| Integrity | Achieved using hashing and digital signature |
| Availability | Achieved using MSP and Access Control |
| Transparency | Achieved using Hyperledger Composer Historian |
| Authorization | Achieved using Access Control |

Table 3 summarizes how our approach achieves the above security requirements

**Interoperability**

In our proposed architecture we can find REST API server generated by Hyperledger composer tools, once we create and test our blockchain network, we can integrate it with other web/mobile application by using a REST API this what make our network Interoperability. This allows homeowner to pull data from web/mobile application and convert it to assets or participants in a Composer business network. In the implementation of simulation scenarios, Table 4 illustrates all the REST API collection for the scenario designed. The table contains methods to manipulate all the assets, participants, transactions and system related activities. Besides, it can be configured to authenticate the participants in the business network, ensuring that credentials and permissions are enforced.

Table 4 REST API collection

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Resource | Methods | Description |
| Asset | Light sensor | GET, POST, HEAD, PUT, DELETE | Find, create, update, delete in-stance(s) of the Light Sensorasset |
| Asset | Thermostat sensor | GET, POST, HEAD, PUT, DELETE | Find, create, update, delete in-stance(s) of the Thermostat Sensorasset |
| Participant | Home owner | GET, POST, HEAD, PUT, DELETE | Find, create, update, deleteinstance(s) of the homeownerParticipant |
| Transaction | Set Tempertature | GET, POST | Find all instances or create a new instance of the Set Temperature transaction |
| Transaction | Change Light Sensor Status | GET, POST | Find all instances or create anew instance of the ChangeLight Sensor Status transaction |

Figure 21 shows a user interface for testing API of creating a thermostat sensor. All the input parameters should be including as JSON format data in the body. When deploying REST API server in a production environment, the REST server can be configured to be secured with HTTPS and TLS (Transport Layer Security). Once the REST server has been configured with HTTPS and TLS, all data transferred between the REST server and all of the REST clients is encrypted [20].

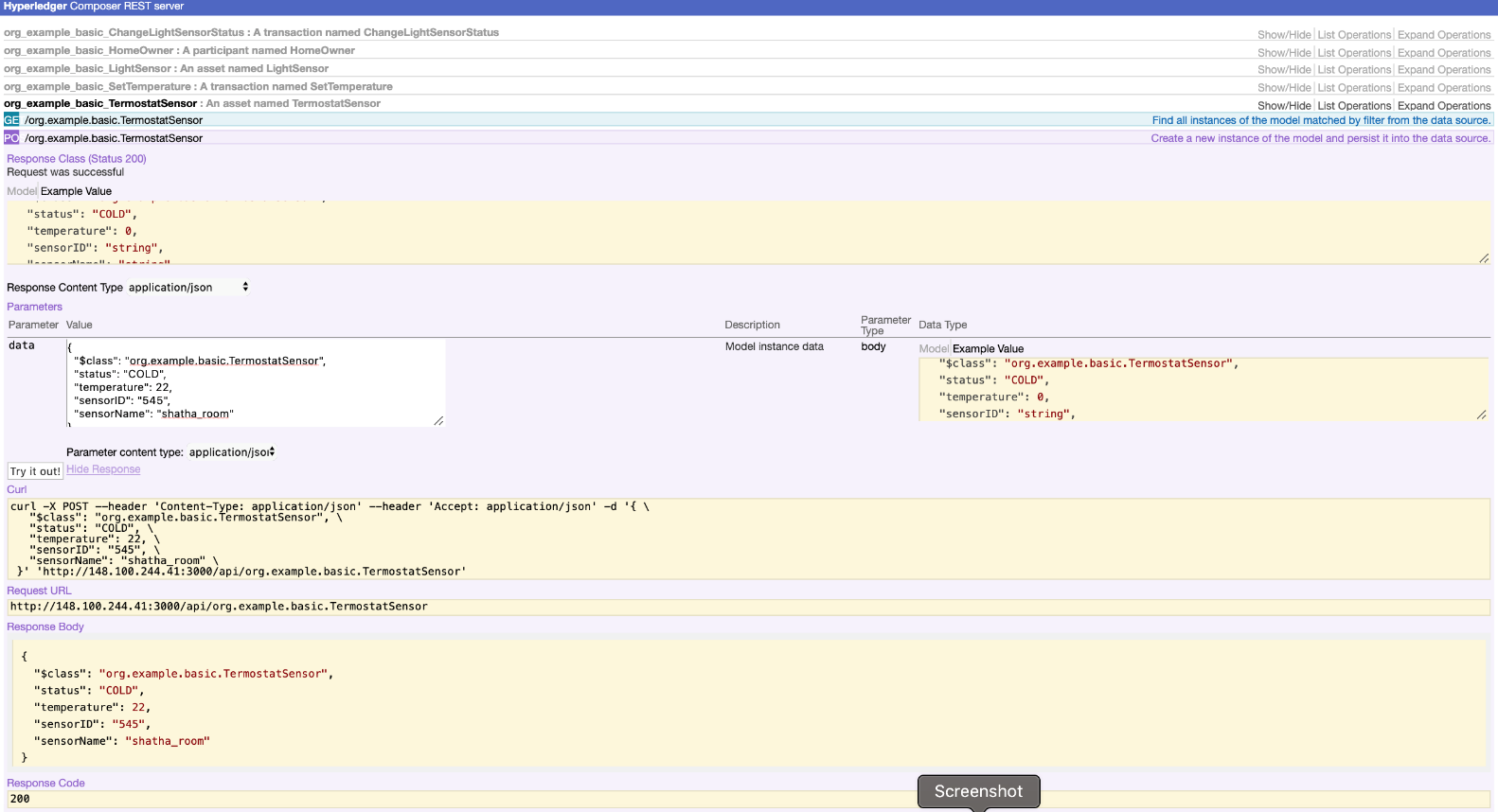


Figure 21 User interface of API test field

*Overall Security Analysis*

The motivation of the presented solution was hypothesized on the assumption that blockchain technology is a suitable solution for securing IoT devices that preserves data privacy. According to the implemented scenario which implements our adaptive architecture of the smart home on blockchain network, the security requirements need now to be checked. Indeed, utilizing blockchain technology expected to meet confidentiality, integrity and availability. Also, with our solution we achieved transparency and interoperability, which is important security requirement needed to ensure IoT environment.

In this regard, the solution ensures transparency and visibility in blockchain network by using hyperledger composer that record the registry of asset, participants and transaction. However, any home member submits transaction for any smart home devices this transferred data is recorded into blockchain that is immutable database and it is temper-proof which makes it almost impossible for any attacker to change those data. In addition, those stored transactions are tractable across smart home to enable strong backwards tractability.

In the solution proposed, we used permissioned blockchain technology by hyperledger fabric and composer to provide confidentiality and authority. The results of our application prove that the confidentiality is achieved with membership service and access control mechanism. Any home member should be authorized before access the data using permission and predefined rules. Access control roles are stored as smart contract in the blockchain to ensure immutability. Moreover, with blockchain nature of recorded list that linked using hash function which makes it more secure.

Moreover, the interoperability is an important feature to ensure. Our proposed approach based blockchain can integrate with other applications. The scenario verifies the possibility to interoperate with web or mobile application by generating REST API server for operating and handling entry and access of data.

In summary, the results verify that the adaptation of blockchain technology that we adopted can yield to significant security and privacy benefits needed for smart home members, while keeping transparency and achieving interoperability.

# Conclusion and Future Works

IoT is an emerging communications paradigm with the aim of connecting all kinds to different devices to the internet with the further aim of gathering data generated by the sensors on these devices. IoT has numerous implementations in various domains such as: Healthcare, Energy Production and distribution. The general purpose of IoT is to transform the way people live by making smart, intelligible devices perform daily tasks. Smart homes are an increasingly popular application of IoT that people pay close attention to in recent years. Its smart concept can bring people a lot of convenience, for instance, the safety guarantee brought by the intelligent monitoring system and the better living environment brought by the intelligent lighting system, all under the control of the home owners, As the adoption rate of IoT devices constantly increasing, more and more devices are becoming connected via the internet. Unfortunately, the majority of these connected devices and applications are not being designed to address current and future security issues. In turn, a lot of issues arise such as confidentiality, authentication, data integrity, etc and therefore efficient security measures are needed to protect IoT devices and networks. This paper investigates Blockchain technology and the ways it can be used to secure IoT based smart homes. In this paper, we propose a novel approach whereby, the proposed blockchain-IoT solution is designed to map the Smart home architectural attributes, so that we achieve a customized architecture that ensures enhanced smart homes security. Experiments with the proposed approach of the four layers architecture, combining hyperledger fabric and the hyperledger composer, have verified its effectiveness in satisfying all defined smart home security requirements, as well as taking advantage of the inherited blockchain features, including transparency, interoperability, which have also been verified. Future work will experiment with more complex smart home settings and security threat scenarios to prove the robustness of the proposed solution.

References

1. Zhou, Wei, et al. "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved." IEEE Internet of Things Journal 6.2 (2018): 1606-1616.
2. Dave Evans. How the Next Evolution of the Internet Is Changing Everything. Cisco Internet Business Solutions Group (IBSG), (April), 2011.
3. Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.
4. Minhaj Ahmad Khan and Khaled Salah. Iot security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 2017.
5. Majid Al-Kuwari, Abdulrhman Ramadan, Yousef Ismael, Laith Al-Sughair, Adel Gastli, and Mohieddine Benammar. Smart-home automation using iot-based sensing and monitoring platform. In 2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018), pages 1–6. IEEE, 2018.
6. Ashley Mancini. Security Awareness: Internet of Things in the Home. PhD thesis, Utica College, 2017.
7. Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, and Michele Zorzi. Internet of things for smart cities. IEEE Internet of Things journal, 1(1):22–32, 2014.
8. Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, and Manuel Díaz. On blockchain and its integration with iot. challenges and opportunities. Future generation computer systems, 88:173–190, 2018.
9. Jari Kreku, Visa Antero Vallivaara, Kimmo Halunen, Jani Suomalainen, M Ramachandran, VM Muñoz, V Kantere, G Wills, and RJ Walters. Evaluating the efficiency of blockchains in iot with simulations. In IoTBDS, pages 216–223, 2017.
10. Pierluigi Gallo, Uy Quoe Nguyen, Giorgia Barone, and Phan Van Hien. Decymo: Decentralized cyber-physical system for monitoring and controlling industries and homes. In 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), pages 1–4. IEEE, 2018.
11. Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on, pages 618–623. IEEE, 2017
12. Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, page 30. ACM, 2018.
13. Harish Sukhwani, Nan Wang, Kishor S Trivedi, and Andy Rindos. Performance modeling of hyperledger fabric (permissioned blockchain network). In 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), pages 1–8. IEEE, 2018.
14. Sven Mitt. Blockchain Application - Case Study on Hyperledger Fabric. page 8, 2018.
15. Enbo Chen. An approach for improving transparency and traceability of industrial supply chain with blockchain technology. 2017.
16. Enbo Chen. An approach for improving transparency and traceability of industrial supply chain with blockchain technology. 2017.
17. Philipp Sandner. Comparison of Ethereum, Hyperledger Fabric and Corda.[online]Availablat:https://medium.com/@philippsandner/comparison-of-ethereumhyperledger- fabric-and-corda-21c1bb9442f6. Accessed 25 Jun 2017.
18. hyperledger Fabric. "Hyperledger Fabric". [online] Available at: [https://hyperledgerfabric](about:blank). readthedocs.io/.
19. Experfy Insights. Top Six technical advantages of Hyperledger Fabric for blockchain networks. [online] Available at:https://www.experfy.com/blog/top-six-technicaladvantages- of-hyperledger-fabric-for-blockchain-networks. Accessed 26 Des 2017.
20. Hyperledger Composer. "Hyperledger Composer ". [online] Available at:https://hyperledger.github.io/composer/. Accessed 15 june 2020.
21. hyperledger Fabric. "Hyperledger Fabric". [online] Available at: [https://hyperledgerfabric.readthedocs.io/](about:blank).
22. IBM Developer. Blockchain basics: Hyperledger Fabric. [online] Available at:https://developer.ibm.com/articles/cl-blockchain-hyperledger-fabrichyperledger-composer-compared/. Accessed 1 july 2018.
23. Nikos Komninos, Eleni Philippou, and Andreas Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Communications Surveys & Tutorials, 16(4):1933–1954, 2014.
24. SSH . "SSH Protocol". [online] Available at: [https://www.ssh.com/ssh/protocol/](about:blank). Accessed 1 march 2020.
25. Kshetri, N. Can Blockchain Strengthen the Internet of Things? IEEE. It Prof. 2017, 19, 68–72. doi:10.1109/mitp.2017.3051335
26. Dodd, N. The Social Life of Bitcoin. Theory Cult. Soc. 2018, 35(3), 35–56. doi:10.1177/0263276417746464
27. A. Rejeb, J. G. Keogh and H. Treiblmaier, "Leveraging the Internet of Things and Blockchain Technology in Supply Chain Management," Future Internet, vol. 11, no. 161, pp. 1-22, 2019.
28. Kamanashis Biswas and Vallipuram Muthukkumarasamy. Securing smart cities usingblockchain technology. InHigh Performance Computing and Communications; IEEE14th International Conference on Smart City; IEEE 2nd International Conference onData Science and Systems (HPCC/SmartCity/DSS), 2016 IEEE 18th InternationalConference on, pages 1392–1393. IEEE, 2016.
29. Gupta, Abhishek, et al. "RETRACTED: Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: A survey." (2019): 118-148.
30. Yetis, Ramazan, and Ozgur Koray Sahingoz. "Blockchain Based Secure Communication for IoT Devices in Smart Cities." 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG). IEEE, 2019.
31. Ouaddah, Aafaf, Mousannif, Hajar, Abou Elkalam, Anas, Et Al. Access Control In The Internet Of Things: Big Challenges And New Opportunities. Computer Networks, 2017, Vol. 112, P. 237-262.
32. Zhu, Qingyi, Seng W. Loke, Rolando Trujillo-Rasua, Frank Jiang, and Yong Xiang. "Applications of Distributed Ledger Technologies to the Internet of Things: A Survey." ACM Computing Surveys (CSUR) 52, no. 6 (2019): 1-34.
33. CASINO, Fran, DASAKLIS, Thomas K., et PATSAKIS, Constantinos. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 2019, vol. 36, p. 55-81.
34. TRAN, Nguyen Khoi, BABAR, M. Ali, et BOAN, Jonathan. Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. Journal of Network and Computer Applications, 2020, p. 102844.