A BLOCKCHAIN-BASED ACCESS CONTROL SOLUTION FOR IoT

Huynh Thanh Tam[*], Nguyen Dinh Thuc[+], Tan Hanh[*]
[*] Posts and Telecommunications Institute of Technology, HCM, Vietnam
[+] University of Science, VNU-HCMC, Vietnam

***Abstract*—This paper proposes a security framework for Internet of Things (IoT) based on blockchain. The solution provides the two features: (1) Access control for IoT devices, which allows users to pay a fee to the device's owner to access the device for a certain period of time. When the access time expires, the connection will automatically be denied by a proxy of the owner; And (2) Decentralized storage service, providing storage space for IoT data. Device owners have to pay for the system to rent storage space. The total amount of payment depends on the size of the data and storage time. The stored data on the storage system are automatically discarded when the storage time has expired. We also present a mechanism for privacy-preserving data sharing on peer-to-peer networks between owners and the storage system. We use blockchain technology to manage IoT devices, access information, and data storage information. The Proof of Authentication consensus is used to provide a lightweight block verification. To store data of IoT devices, we use the interplanetary file system (IPFS) which is a peer-to-peer distributed file system. Our solution provides flexibility in time-based access control comparison with other blockchain-based access control solutions.**

***Keywords*— Blockchain, IoT, access control.**

I. INTRODUCTION

IoT devices are indispensable components in smart city systems, smart homes, etc. According to forecasts of IDC [1], more than 150 billion devices will be connected across the globe by 2025. Worldwide data will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB by 2025, of which 90 ZB will be created on IoT devices. However, most IoT devices are limited in computing power, storage memory capacity, and network bandwidth. In addition, with various types of devices used in the network, making the deployment of security solutions faces many difficulties and challenges.

Currently, many solutions have been proposed to improve the security and privacy of IoT. Most solutions are usually implemented based on centralized and hierarchical structures. However, with the rapid growth of IoT devices, along with the needs of device owners (called owners) such as device management, resource sharing, data storage. That may create many challenges in managing, privacy-preserving data, ensuring system availability. These problems can be solved based on the blockchain technology.

In this paper, we propose a decentralized security framework for IoT, in which owners can manage and allow users to connect their devices in a period of time depending on the amount of payment. Moreover, because of the limited storage space in the owners' servers, they may conduct a payment to store long term in the peer-to-peer storage system, the total amount of payment depends on the size of the data and storage time. Particularly, considering in the context of a smart home area where has some public areas such as kindergarten, sport areas, parking, park. In the kindergarten, the owner has camera devices to monitor children. Parents can access the camera to view their children's activities by submitting a transaction to the owner. The deadline is fixed when the transaction is mined and added to the blockchain. Similarly, in order to store camera data in the decentralized storage system, the owner's kindergarten has to share securely their data to the administrator of the system. The information of shared data is also published on the blockchain. We also present a scheme for guaranteeing the privacy, integrity, and authentication of sharing data on the peer-to-peer network from owners to the storage system.

Comparison with the other blockchain-based access control solutions, our solution has some advantages in setting access time for users. And the IoT data is stored on demand of owners, is guaranteed confidentiality and privacy in sharing and storing processes, owners and users can access data via a peer-to-peer network. The rest of this paper is organized as follows. Section II introduces the blockchain technology and IPFS. In section III IoT security issues are presented. Section IV introduces an overview of the blockchain-based security solutions for IoT. Our solution is described in section V. Section VI shows our evaluation. Finally, our conclusions are given in Section VII.

II. BLOCKCHAIN AND IPFS

A. Blockchain

Blockchain, was first proposed in 2008 by Santosi Nakamoto [2], is a technology in which blocks are linked together to form a chain as a linked list, each block has two main components, the block header contains management information of block as well as chain. And the block body

Contact author: Huynh Thanh Tam,
Email: tamht@ptithcm.edu.vn
Arrival: 8/2020, Revised: 9/2020, Accepted: 10/2020

holds a list of transactions. Each block is associated with a previous block through a hash pointer. This hash value also uses to verify the integrity of the content of the previous block. The first block of the chain is called the genesis block [3][4]. An example of a blockchain is shown in Figure 1.

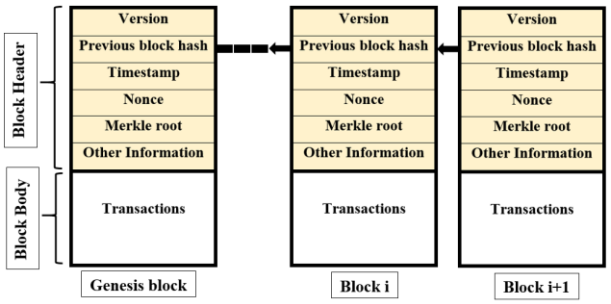

Figure 1: An example of a blockchain.

Blockchain is a decentralized system in which the nodes communicate directly with each other through a peer-to-peer network. All valid transactions are mined and securely recorded in the ledger which is stored at miner nodes. In order to synchronize data in the ledger, the two popular consensus algorithms are Proof of Work and Proof of Stake.

B. IPFS

IPFS was proposed by Juan Benet in 2014 [5], which is a peer-to-peer distributed file system. Each IPFS node owns a key pair (public and private key), in which the public key is used to generate NodeID, and the private key is used to sign in the IPNS service. When two nodes initialize a connection, they exchange their public key and NodeID with each other and then check the validity between the NodeID and the public key being exchanged, if the information is not correct, the connection is terminated. Basically, there are three types of nodes, namely: client node, retrieval miner node, and storage miner node. Each miner node owns a distributed hash table (DHT) to support routing and discovery of content and peers on the network. In order to lookup or store objects, nodes can use four remote procedure calls including PING, STORE, FIND_NODE, and FIND_VALUE. Currently, the S/Kademlia DHT, an extension of kademlia protocol, is used to build the routing table [6].

By default, files are only cached temporarily and removed by the garbage collection feature of IPFS. Hence, in order to improve the redundancy of data on the network, some storage miner nodes (called cluster nodes) are configured the cluster feature. Then important files are pinned and replicated between these cluster nodes. Normally, cluster nodes have a large storage space and high-speed processing capacity [7].

III. IOT SECURITY ISSUES

Internet of Things is a network that connects any possible objects/things (tablets, smart phones, smart watch, etc.). IoT could be applied in many fields, such as smart home, smart city, smart agriculture, smart health, etc. The 3-layer architecture of IoT and the corresponding protocols at these layers are shown in Table I [8][9][10].

Table 1. IoT architecture.

Layer	Feature	Protocol
Application layer	Provide specific applications for users	HTTP, XML, JSON, etc.
Network layer	Receive and process data from the Perception layer. Establish connections and transfer data to devices in the network	IPv6/IPv4, IEEE 802.15.4 6LoWPAN, MQTT, etc.
Perception layer	Collect data from the surrounding environment and transfer data to the Network layer	IEEE 802.11/15, Z-Wave, WirelessHart, etc.

Some security requirements for IoT, including Privacy, Confidentiality, Integrity, Authentication, Authorization, Accounting, Energy efficiency [10][11][12]. The security issues and affected security properties of IoT are presented in Table 2.

Table 2. Attack types and security issues of IoT [10]

Attack types and security issues of IoT	I	II	III	IV
(1) Perception layer				
1. Jamming adversaries			✓	
2. Insecure initialization	✓		✓	
3. Insecure physical interface	✓		✓	
4. Low-level Sybil and spoofing attacks			✓	
5. Sleep deprivation attack				✓
(2) *Network layer*				
1. Replay or duplication attacks			✓	
2. Insecure neighbor discovery		✓		
3. Buffer reservation attack.		✓		
4. RPL routing attack	✓	✓		
5. Sinkhole and wormhole attacks			✓	
6. Sybil attacks	✓	✓		
7. Secure communication and Transport security	✓			
(3) *Application layer*				
1. Constrained Application Protocol			✓	
2. Insecure interfaces.	✓	✓	✓	
3. Insecure software/firmware	✓		✓	

I: Privacy, Confidentiality, Integrity.
II: Availability.
III: Authentication, authorization, Accounting.
IV: Energy efficiency.

IV. OVERVIEW OF THE BLOCKCHAIN-BASED SECURITY SOLUTIONS FOR IOT

The blockchain-based security solutions for IoT can be classified into 3 categories: access control, device management, data security.

A. Access control

Access control is a security mechanism for monitoring and controlling access to resources. Traditional solutions often use an access control list installed on a centralized server, connection requests will be sent to this server for checking the validity before granting permission. However, when the number of IoT devices connected in the network increases significantly, and the owners need to control their devices and data, the centralized model raises privacy concerns, complex configuration, and a single point of failure. Blockchain-based access control solutions can solve these problems.

The authors in [13] proposed a security framework for smart home, consisting of three core tiers that are: smart home, cloud storage, and overlay. The home owner generates and stores access control policies in the policy header of the genesis block. The latest block's policy header is considered the latest policy update. The policies include: (1) Granting access to other devices in the smart home; (2) Granting access from the overlay network to the smart home; (4) Granting access the local storage/cloud storage; (3) Granting storage to the local storage/cloud storage. The policy header has four parameters: The "*Requester*" parameter refers to the requester PK in the received overlay transaction, or is "*Device ID"* for local devices. The second parameter is used to indicates the requested action in the transaction (such as *store*, *store cloud*, *access*, *monitor*). The third field is the *ID* of a device inside the smart home, and finally, the last column indicates the action that should be done for the transaction (*Allow*, *Deny*).

The authors in [14] proposed a Smart Door Lock system based on blockchain. In order to open the smart door, a user has to perform a transaction which contains information as follows: (1) the OPEN control message, and (2) the GPS information of the node is used to measure a distance (*d*) between the smart door lock and the node. If the *d* is lower than the preset range, the smart door will open. The result of the operation is also broadcasted to the blockchain network.

Ouaddah et al. [15] built a distributed privacy-preserving access control framework called FairAccess that allows owners to control access to their devices. In particular, blockchain is used to stores all access control policies for each pair (resource, requester) in form of transactions. When device A wants to perform an operation on device B, it sends a request to the owner of device B. Then, the owner defines an access control policy and transfers it to the blockchain through a GrantAccess transaction. In case of successful validation, device A receives an access token which is considered a license to access device A. Device A uses this token in a GetAccess transaction. Then when device A accesses device B, device B verifies the signature and the validation of the token based on the blockchain ledger. Owners can also make a new GrantAccess transaction to update or revoke a permission on their resources.

In the ControlChain architecture of [16], the authors use 4 different blockchains to store access control rules, relationships, contexts and accountability information. This architecture provides a secure way to establish relationships between users, devices and group of both, allowing the assignment of attributes for these relationships and their use in the access control authorization. Outchakoucht et al. [17] combined blockchain and machine learning algorithms to create a decentralized access control framework and to provide a dynamic optimized and self-adjusted security policy. In the solution of [18], managers, as miner nodes, are responsible for registering and setting access control policies for their devices by using smart contracts. The management hub nodes, is not part of the blockchain, is the intermediary to translate messages from devices into RPC messages and forward them to the blockchain network, and the nodes can also return query results on the blockchain to the IoT devices. The policy rules in the proposed solution can expire automatically after a certain time.

In [19], in order to connect an IoT device, a user had to perform a smart contract. Then, both the user and the device receive an authentication token. The user uses this token in an authentication message signed by the user's private key. The IoT device verifies the signature in the authentication message along with checks the validation of the token and the source IP before exchanging data. The authors in [20] proposed an attribute-based access control scheme using blockchain for IoT. In which, each device is described by a set of attributes by attribute authorities. Blockchain is used to record the distribution of attributes. To get the access authorization, the device involved must prove its ownership of corresponding attributes that satisfy the policy.

B. Device management

A device management system includes the following basic tasks: managing firmware; identifying and authenticating devices; monitoring and updating configurations for devices.

Huh et. al. [21] proposed a configuration management solution for IoT devices using the ethereum blockchain platform. In this solution, each device owns an ethereum account and uses Meter contract to send technique parameters (such as electricity index, temperature, etc.) periodically to the blockchain. Policy contract is used to configure policies for devices, and devices regularly check its related data on the blockchain to update the corresponding parameters. For instance, when the meter of an air conditioner reaches 150KW, the air conditioner will switch from normal mode to saving mode.

Concerning secure firmware update: In [22], a manufacturer deploys a smart contract to store the hash value of the latest firmware version in the ledger. IoT devices can query the information of a new firmware via smart contracts, and then download this firmware on a distributed peer-to-peer filesystem such as IPFS. In the

proposed solution of Lee et al. [23], IoT devices act as Normal nodes in the blockchain network, they can send requests or respond to firmware update requests from other nodes in the network. The vendor operates Verification nodes, which is responsible for maintaining the latest firmware information. The vendor node is outside of the blockchain network but keeps a secure channel connected to the Verification node to provide the latest firmware. When a normal node submits a request transaction to require a firmware update. This transaction contains the current version information of the requesting node. In case the current firmware is not up-to-date or not integrity, the Verification node will send a metadata file containing a peer list of the firmware sharing network. Then, the requesting node will download and update the latest firmware.

Concerning IoT devices management: In a device identity protocol of Lombardo [24], each device owns a public key. In order to verify a device's identity, the device has to send encrypted challenge and response messages to other devices on the network. The authors in [25] proposed TM-Coin to manage TCB measurements of IoT devices. The verifier can launch remote attestation of sensed data from the devices using the TCB measurements published on the blockchain without attesting to the TCBs of the devices. In [26], blockchain is used to store cryptographic hashes of devices' firmware. That aims to prevent fake devices joining to the network. The authors in [27] proposed the BIFIT (blockchain-based identity framework for IoT) to automatically extract signatures for IoT devices in smart homes and to create blockchain-based identities for their appliance owners. The information of device's signature and owner's identification is used to authenticate in use. The correlations between appliances' signatures and owners' identities are used in authentication processes. According to the solution in [28], each device is identified by a blockchain address and has a minimal set of attributes such as MAC/IP addresses, serial number, manufacturer, life cycle, and owners of the device. Using smart contracts to register devices, or change the ownership of devices. All information related to devices can also track in the ledger.

C. Data security and secure communication

Hashemi et al. [29] proposed a user oriented data dissemination and distribution system. In this system, blockchain is used at the Data store system layer to store the access control data from the Messaging service layer. In the proposed security framework for smart cities of the authors in [30], blockchain is integrated at the communication layer to provide security and privacy of transmitted data. And the database layer in this framework uses private ledgers to ensure scalability, performance, and security for real-time applications in smart cities.

In the modum.io AG start-up [31], in order to ensure quality control and regulatory compliance over the transport of medical products, the temperature of each parcel during the shipment is sent from sensors to blockchain for storage. In addition, the temperatures can be assessed automatically and notify the sender and recipient by smart contracts. And external parties can audit data through the ledger of the blockchain. Some other proposed solutions in [32][33][34], blockchain is used as a storage tool of IoT systems to record data in plaintext, cipher or hash values.

V. OUR SOLUTION

In this section, we propose a security framework for IoT based on blockchain that provides the two features including:

Access control: The basic idea is to control connections based on the time fixed on the blockchain. Particularly, the owner of devices registers the information of their devices on the blockchain network, all information concerning devices are encrypted by a symmetric cryptosystem to ensure privacy. To connect a device, a user has to conduct a request transaction to the owner, then the owner sends the decryption key securely to the user via a transaction, and the deadline for access is fixed on the blockchain. After having information of the device, the user establishes a connection to the device, the connection is verified by a proxy server of the owner based on information of the ledger. The connection will be automatically rejected when the deadline is over.

Decentralized storage service: Servers of the owner can only store IoT data in a certain time because of the limited storage space. The oldest data will be deleted to reserve free space to store new data. In some cases, important files should be stored long term, besides these files can be accessed from a lot of users. If the owner uses a hosting service that operates on a centralized model, data security issues and system availability will not be guaranteed [35]. To overcome the limitation, our solution provides a decentralized storage service based on IPFS. We use some IPFS storage nodes with large storage capacity for data synchronization, these nodes also join the public IPFS network. Currently, the ipfs.io is one of the largest public IPFS networks, is built by the Protocol Labs [35]. The owner can register the decentralized storage service to store IoT data for a long period of time. In order to transfer IoT data from the owner to the storage system, we also present a mechanism for privacy-preserving data sharing on peer-to-peer networks. All information about the service is recorded in the ledger.

We consider in the context of a kindergarten in a smart home area, with camera devices as IoT devices that need to be managed. We build a private blockchain with the Proof of Authentication consensus, in which each block has a structure as follows:

Block Header: The header includes three fields

- *Block_ID* is used to identify the block.
- *Previous hash* is the hash value of the parent block.
- *Timestamp* shows that the blocks are connected in chronological order.

Block Body: A block body contains the sequence of transactions. Each transaction is signed by the sender. The Genesis block contains a list of public keys of miner nodes. The proof-of-authentication consensus works as follows:

(1) When a miner node generates a new block. It generates a signature on this block, and then it broadcasts this block along with the digital signature to the network.

(2) The other miner nodes verify the signature by using the list of public keys of the miners in the ledger. If the signature is valid the new block will be added to the chain.

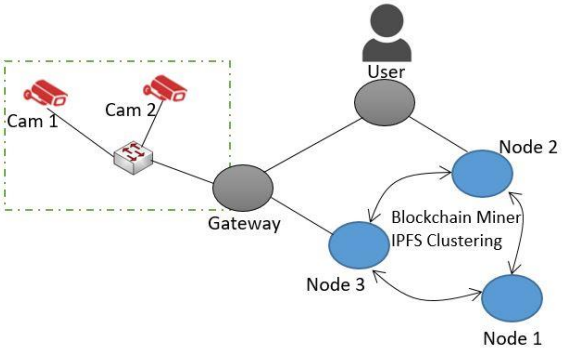

Figure 2: The general architecture of the system.

The architecture of our system is depicted in Figure 2, including components as follows: (1) Blockchain Miner node; (2) IPFS Storage node; (3) Gateway node; (4) User node; (5) Camera device. A node with high performance can assume two roles, a blockchain miner and an IPFS storage node.

Blockchain miner node: The node is responsible for mining new blocks for the private blockchain.

IPFS storage node: The node has a high storage space, is enabled the clustering service for data replication between cluster nodes. All data is pinned to ensure always available on the network.

Gateway node: The gateway is a normal node of the blockchain network, and is also an IPFS client node of the IPFS network. Moreover, the node acts as a proxy for managing connections from outside to camera devices of the kindergarten. The node can also store videos from IoT devices.

Camera device: The device does not belong to the blockchain and IPFS networks, and is connected to the Gateway node.

User node: The node represents for user's devices that is used to perform blockchain transactions and connect to the camera devices of the kindergarten. The node can also join the public IPFS network if it wants to get data shared from the owner's camera devices.

A. Device registration process

The sequence diagram of the device registration process is shown in Figure 3. The owner of the kindergarten has to submit a transaction to the blockchain network called *TX::Reristration_Cam*. The contents in this transaction including:

#TX::Registration_Cam
From: PU_{DO} *to* PU_{SYS}
CAM_ID: <ID_Camera>
$C1 = E_k(Cam\_Information)$
Sig: Signature

Where PU_{DO} is the public key of the owner, is also considered a wallet address of the owner on the blockchain network; PU_{SYS} is the public key of the blockchain system; *CAM_ID* is an identification of a camera; $Cam\_Information$ is the necessary information to connect to the camera device, which is encrypted by a symmetric algorithm *E* along with a key (*K)*, the output result is assigned to $C1$. The *Sig* field is the signature of the owner in this transaction. After mining success by miners, data is recorded in the ledger.

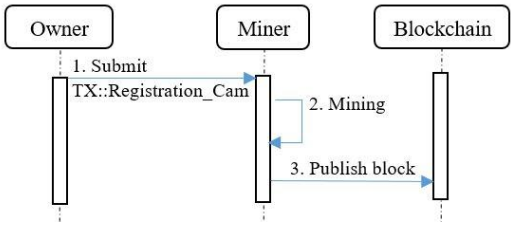

Figure 3: The sequence diagram of the device registration process.

B. Access management process

As shown in Figure 4, the steps of the access management process including:

(1) The user submits a transaction *TX::View_Request* to the owner. The user must specify the Camera ID (*CAM_ID*) and the period of access time. By default, the user can only view a camera for a certain period of time (*T*). The time *T* can also be determined based on the cost the user pays to the owner. The transaction information is shown in Table 3a: Where PU_U is the public key of the user. *Sig* contains a signature of the user on the transaction.

(2) The transaction is verified by miners.

(3) A miner publishes a new block on the blockchain network.

(4) A client application is used to query transactions corresponding the DO's public key in the ledger. After receiving a transaction *View_Request* informed by the client application, the owner makes a transaction *View_Reply* to the user with contents as shown in Table 3b:

Table 3. The contents of transactions.

(a)	(b)
#TX::View_Request	***#TX::View_Reply***
From: PU_U *to* PU_{DO}	*From:* PU_{DO} *to* PU_U
CAM_ID: <ID_Camera>	$C2 = E_{PU_U}(K)$
Time: T	*Deadline: Systime+T*
Sig: Signature	*Sig: Signature*

Where, the key *K* is encrypted by an asymmetric cryptography and the public key of the user. Therefore, only the user can know the key *K*. The result is assigned to C2; *Deadline* is the end time of the connection.

(5) and **(6)** are similar to the steps (2) and (3) above. Noted that the deadline will be fixed at the step (6).

(7) The gateway node checks transactions *View_Reply* to build an access management table, as shown in Table 4.

Table 4. The connection management table.

Connection Management table		
CAM_ID	**User**	**Deadline**
1	PU_{U1}	9:00 10/06/2020
2	PU_{U2}	10:00 10/06/2020
...	…	…

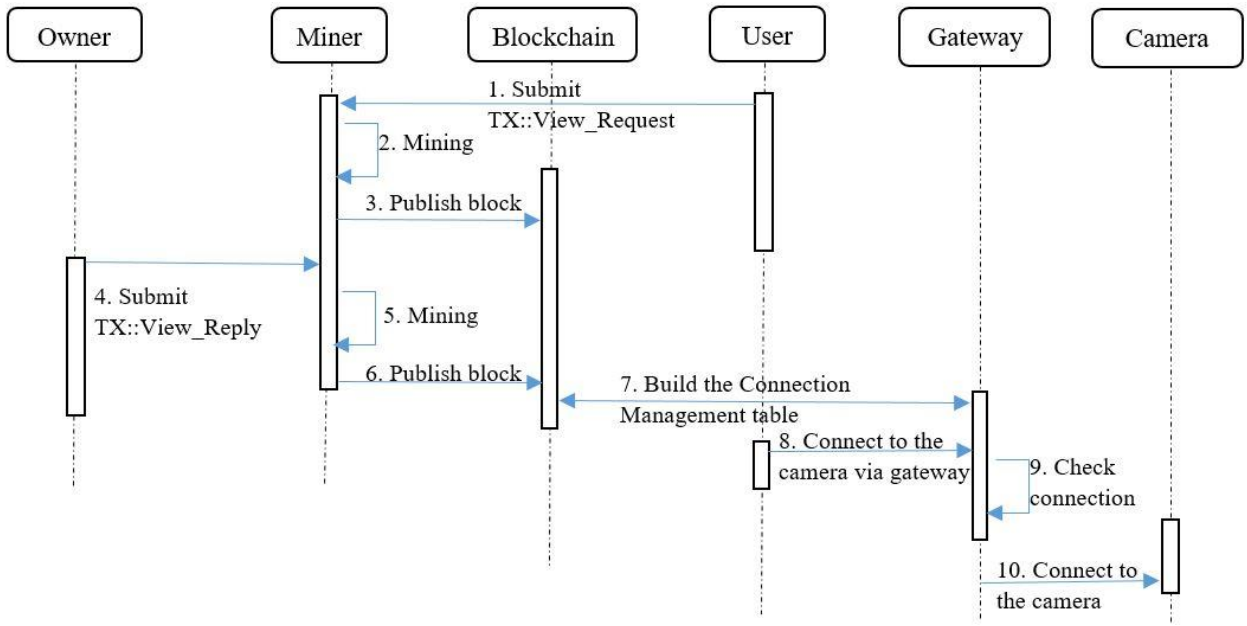

Figure 4. The sequence diagram of the access management process.

The table will be updated at each mining round of the blockchain network.

(8) The user performs the two decryption processes to get the key *K* and *Cam_Information*:

$$K = D_{PR_U}(C2)$$

$$Cam\_Information = D_k(C1)$$

Where D_{PR_U} denotes the decryption algorithm of an asymmetric cryptosystem with the input is the private key of the user PR_U and $C2$; D_k denotes the decryption process of a symmetric cryptosystem, the input is the key *K* and $C1$. Then, the user uses the *Cam_information* to connect to the Gateway node in a format specified by the owner. For instance,

"http://ip_gateway/Cam_ID/timestamp/public_key/signature_on _this_link"

(9) The checking process includes two steps, as shown in Figure 5. Step1: The Gateway node checks whether the public key of the connection exists in the connection management table (CMT) or not? If the public key already exists, the node verifies the signature in the connection link; Step 2: The node checks whether the time is still valid or not. The time checking is performed every 60 seconds.

(10) The connection is established to the camera.

C. Storage registration process

Because of the limitation of the storage space of the gateway. Hence, the owner can transfer data to the decentralized storage system. We propose a mechanism for privacy-preserving data sharing on the peer-to-peer network, as shown in Figure 6. The sequence of steps are as follows:

(1) Encrypt and sign: This step includes the following activities:

(i) The owner encrypts data of camera devices with a secret key and the selected symmetric cryptography. The output is denoted by *D1*.

(ii) The owner issues a certificate to mask the integrity of the data. $CA = sig_{Pr_{DO}}(Hash(D1))$.

(2) The owner uploads $D1$ and CA to the IPFS.

(3) The IPFS network returns a path of the encrypted data and the certificate.

(4) Create and submit a transaction (*TX::Store_Request*) to the blockchain network. This transaction has the following necessary information:

(i) Sender (PU_{DO}), Receiver (PU_{SYS})

(ii) The path of the encrypted data and the certificate on the cloud.

(iii) The certificate of the data

(iv) The Storage time

(5) and **(6)** are the process of mining and publishing block of the blockchain network.

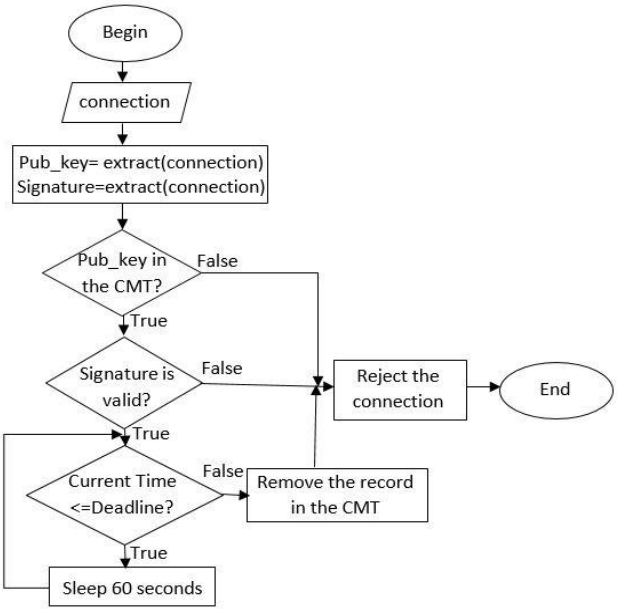

Figure 5. The flowchart of checking connections

(7) The Admin of the system get the link on the blockchain.

(8) The Admin pins the link on the IPFS cluster nodes.
(9) The Admin submits a transaction *TX::Store_Reply* to the blockchain network with information as follows:
(i) Sender (PU_{SYS}), Receiver (PU_{DO}).
(ii) The link of data on the IPFS.
(iii) Status: Completed.

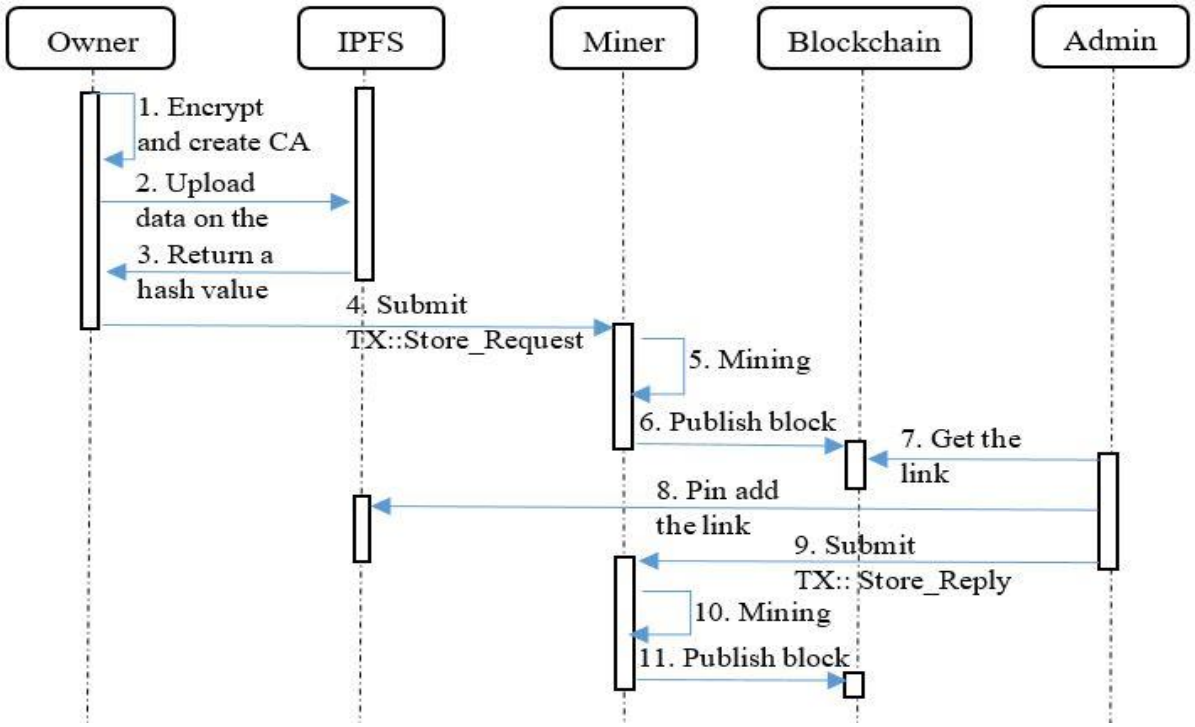

Figure 6. The sequence diagram of the storage service.

(10) and **(11)** are similar to the steps (5) and (6) above.
The Storage time depends on the cost the owner paid to the system and the size of data. The cluster node has a tool that automatically deletes data that is out of date on the IPFS.

VI. EVALUATION

We use the confidentiality, integrity, and availability (CIA) model for evaluation of our system security.

Confidentiality: Sensitive data such as device information, camera data are stored on the ledger and IPFS in encrypted form. The connection from a user to a camera device can be protected by using a Secure Sockets Layer (SSL).

Integrity: For the blockchain network, the data is guaranteed integrity by the immutable of the ledger. For the IPFS network, files in IPFS are identified by their hashes. These hash values are used to verify the integrity of files. The certificates of files are also used to validate the possession of files. Concerning the integrity of the Connection Management Table, this table is stored at the proxy node, in case this table is edited by adversaries, the connections are affected for a certain period of time because this table is reloaded from the bockchain ledger at each mining round.

Availability: The clustering feature of IPFS ensures that stored data is replicated on IPFS storage nodes. Besides, the blockchain ledger is kept at miner nodes. In cases some nodes of IPFS and Blockchain do not work, our service will still be provided by other mine nodes.

VII. CONCLUSION

Access control plays a crucial role for IoT, blockchain-based solutions bring more advantages than other solutions. Our solution is efficient in managing access based on access times, and providing a decentralized storage service for IoT. Data stored on the storage system is guaranteed privacy by symmetric cryptosystems. Owners or users can join the public IPFS network, and access data through the peer-to-peer network. The Proof of Authentication is a suitable selection for our private blockchain network which improves miners' performance.

Acknowledgment. This research is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number NCM2019-18-01.

REFERENCES

[1] A. Patrizio, "IDC: Expect 175 zettabytes of data worldwide by 2025," Network World, 2018.
[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and cryptocurrency technologies: A comprehensive introduction," Princeton University Press, 2016.
[3] Z. Zheng, S. Xie, H. N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," in International Journal of Web and Grid Services, 2016.
[4] T. T. Huynh, T. D. Nguyen, and H. Tan, "A Survey on Security and Privacy Issues of Blockchain Technology," in 2019 International Conference on System Science and Engineering (ICSSE), IEEE, pp. 362-367, 2019.

[5] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXiv preprint arXiv:1407.3561, 2014.
[6] T. T. Huynh, T. D. Nguyen, and H. Tan, "A Decentralized Solution for Web Hosting. In 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), IEEE, pp. 82-87, 2019.
[7] IPFS cluster, "https://cluster.ipfs.io" (accessed June, 2020).
[8] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," Journal of Network and Computer Applications, 88, 10-28, 2017.
[9] A. Kamble, and S. Bhutad, "Survey on Internet of Things (IoT) security issues & solutions," in 2018 2nd International Conference on Inventive Systems and Control (ICISC), IEEE, pp. 307-312, 2018.
[10] M. A. Khan, and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, 82, pp. 395-411, 2018.
[11] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, 32, pp. 17-31, 2015.
[12] M. L. Das, "Privacy and security challenges in Internet of Things," in International Conference on Distributed Computing and Internet Technology, Springer, Cham, pp. 33-48, 2015.
[13] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), IEEE, pp. 618-623, 2017.
[14] D. Han, H. Kim, and J. Jang, "Blockchain based smart door lock system," in 2017 International conference on information and communication technology convergence (ICTC), IEEE, pp. 1165-1167, 2017.
[15] A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," In Europe and MENA cooperation advances in information and communication technologies, Springer, Cham, pp. 523-533, 2017.
[16] O. J. A. Pinno, A. R. A., Gregio, and L. C. De Bona, "Controlchain: Blockchain as a central enabler for access control authorizations in the IoT," in GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, pp. 1-6, 2017.
[17] A. Outchakoucht, E. S. Hamza, J. P. Leroy, "Dynamic access control policy based on blockchain and machine learning for the internet of things," Int. J. Adv. Comput. Sci. Appl, 8(7), 417-424, 2017.
[18] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," IEEE Internet of Things Journal, 5(2), pp. 1184-1195, 2018.
[19] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for IOT access control and authentication management," in International Conference on Internet of Things, Springer, Cham, pp. 150-164, 2018.
[20] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," IEEE Access, 7, pp. 38431-38441, 2019.
[21] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in 2017 19th international conference on advanced communication technology (ICACT), IEEE, pp. 464-467, 2017.
[22] K. Christidis, and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, 4, pp. 2292-2303, 2016.
[23] B. Lee, and J. H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," The Journal of Supercomputing, 73(3), pp. 1152-1167, 2017.
[24] H. Lombardo, "Blockchain Serves as Tool for Human, Product and IoT Device Identity Validation" [online] Chain of Things, (2017).
[25] J. Park, and K. Kim, "TM-Coin: Trustworthy management of TCB measurements in IoT," in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, pp. 654-659, 2017.
[26] N. Kshetri, "Can blockchain strengthen the internet of things?" IT professional, 19(4), pp. 68-72, 2017.
[27] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic identity framework for the internet of things," in 2017 International Conference on Cloud and Autonomic Computing (ICCAC), IEEE, pp. 69-79, 2017.
[28] A. S. Omar, and O. Basir, "Identity management in IoT networks using blockchain and smart contracts," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, pp. 994-1000, 2018.
[29] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users," in 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), IEEE, pp. 13-24, 2016.
[30] K. Biswas, and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS), IEEE, pp. 1392-1393, 2016.
[31] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in 2017 IFIP/IEEE symposium on integrated network and service management (IM), IEEE, pp. 772-777, 2017.
[32] Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," in Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS), Dec. 2017, pp. 1–6.
[33] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Peer to peer for privacy and decentralization in the Internet of Things," in Proc. IEEE/ACM 39th Int. Conf. Softw. Eng. Companion (ICSE-C), May 2017, pp. 288–290.
[34] B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for IoT data," in Proc. IEEE Int. Conf. Web Services (ICWS), Jun. 2017, pp. 468–475.
[35] T. T. Huynh, T. D. Nguyen, and H. Tan, "A Decentralized Solution for Web Hosting," In 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), IEEE, pp. 82-87, 2019.
[36] The IPFS network. Online resource. https://ipfs.io (accessed April, 2020).

GIẢI PHÁP KIỂM SOÁT TRUY CẬP TRUY CẬP DỰA TRÊN BLOCKCHAIN CHO IOT

Tóm tắt—Bài báo này đề xuất một nền tảng bảo mật cho vạn vật kết nối internet (IoT) dựa trên blockchain. Giải pháp cung cấp hai tính năng: (1) Kiểm soát truy cập cho các thiết bị IoT, cho phép người dùng trả phí cho chủ sở hữu thiết bị để truy cập một thiết bị trong một khoảng thời gian nhất định. Khi hết thời gian truy cập, kết nối sẽ tự động bị ngắt bởi proxy của chủ sở hữu; Và (2) Dịch vụ lưu trữ phi tập trung, cung cấp không gian lưu trữ cho dữ liệu IoT.

Chủ sở hữu thiết bị phải trả tiền cho hệ thống để thuê không gian lưu trữ. Tổng số tiền thanh toán phụ thuộc vào kích thước của dữ liệu và thời gian lưu trữ. Dữ liệu được lưu trữ trên hệ thống lưu trữ sẽ tự động bị xóa khi hết thời gian lưu trữ. Chúng tôi cũng trình bày một phương thức chia sẻ dữ liệu đảm bảo tính riêng tư trên mạng ngang hàng giữa các chủ sở hữu và hệ thống lưu trữ. Chúng tôi sử dụng công nghệ blockchain để quản lý các thiết bị IoT, thông tin truy cập và thông tin lưu trữ dữ liệu. Giao thức đồng thuận Bằng chứng xác thực được sử dụng để cung cấp xác minh khối nhẹ. Để lưu trữ dữ liệu của các thiết bị IoT, chúng tôi sử dụng hệ thống tệp liên hành tinh (IPFS) là một hệ thống tệp phân tán ngang hàng. Giải pháp của chúng tôi cung cấp sự linh hoạt trong việc kiểm soát truy cập dựa trên thời gian so với các giải pháp kiểm soát truy cập dựa trên blockchain khác.

Từ khóa: *Blockchain, IoT, kiểm soát truy cập*

Huynh Thanh Tam is currently a lecturer of the Faculty of Information Technology at Posts and Telecommunications Institute of Technology, Ho Chi Minh City Campus. His research interests include blockchain, IoT, and decentralized storage.

Email: tamht@ptithcm.edu.vn

Nguyen Dinh Thuc is currently a lecturer of the Faculty of Information Technology at University of Science, VNU-HCMC, Vietnam. His research interests include cryptography, information security, and machine learning.
Email:ndthuc@fit.hcmus.edu.vn

Tan Hanh is currently a vice president of Posts and Telecommunications Institute of Technology. His research interests are machine learning, information retrieval, and data mining.
Email: tanhanh@ptithcm.edu.vn