Techno-Science Research Journal 6 (2018) 27-34

I.T.C

Content list available at ITC

Techno-Science Research Journal

Journal Homepage : www.itc.edu.kh

Techno-Science Research Journal

Security and Privacy for the IoT Network by Hyperledger

Ketya Huy[1*], Kimtho Po[2], Kimheng Sok[3], Virya Huy[1]

[1] *Department of Information and Communication Engineering, Institute of Technology of Cambodia, Russian Ferderation Blvd., P.O. Box 86, Phnom Penh, Cambodia.*
[2] *Department of Electrical and Energy Engineering, Institute of Technology of Cambodia, Russian Ferderation Blvd., P.O. Box 86, Phnom Penh, Cambodia.*
[3] *Faculty of Computer Science, University of Namur, rue Grandgagnage 21, 5000 Namur, Belgium.*

Abstract: *The Internet of Things is considered as the next big technology revolution after the invention of the Internet. Data of IoT are very useful and could produce such huge creativity for us to build many useful applications in our daily life. In Cambodia, the IoT is still a new technology for research and development. However, Security and Privacy are the main key issues for IoT and they are still facing some enormous challenges such as DDoS Attack on the centralized server, data leakage, and some IoT device products are a weakness in authentication, management and access control that is an opportunity to hackers can control their devices. So, the main objective of our research is to investigate how Blockchain and Smart Contracts can contribute to building trustworthy, secure and privacy-aware IoT systems. In this paper, we proposed a system architecture model of using a Blockchain called Hyperledger to secure the Internet of Things network in a smart classroom, and we developed the IoT platform for a smart classroom that including the mobile application as an end-user to remote or control devices in classroom, Blockchain and Smart Contracts of Hyperledger as the method to security and privacy for smart classroom, LoRa as a network for long-range communication and low power consumption IoT devices, The Things Network as a public LoRa server to communication over cloud server. After we investigated on Blockchain and Smart Contracts of Hyperledger to security and privacy for a smart classroom system, the results showed that it is very useful application for secure and privacy-aware IoT systems such as disintermediation, robustness, traceability, enhanced security, transparency, prevented DDoS attack on the centralized server, protected data leakage, eliminated a central authority, prevented dishonesty, data manipulation and prevented data fraud.*

Keywords: IoT; Blockchain; Smart Contract; Hyperledger; Ethereum; Bitcoin; LoRa; The Things Network; DDoS; Centralized system; Distributed system

1. INTRODUCTION

The Internet of Things is the inter-networking of physical devices, building, vehicles and other objects which consist of an embedded system with sensors, actuators, software, electronics and network connectivity that enable to collect and exchange data. Those data are very useful and could produce such huge creativity for us to build many useful applications in our daily life such as no matter in education, health care, environment, social or business sectors (N. Kumar, 2017). IoT is applied in many domains such as Smart Home, Smart City, Smart Healthcare and others (H. N. Saha, 2017). IoT has the power to change our world that the prediction has been made that there will be 50 Billion IoT devices by 2020 (Jacques, 2017), more or less it starts happening every single day that IoT devices start to go online. Since the IoT devices have been produced by different companies, using different standard architecture and protocol of communication, multiple interfaces, so interoperability among those devices, gateway, cloud and user application is the major problem in IoT network (N. Kumar, 2017). Besides interoperability, data that produced by the devices need to be protected, and use it a good way and correspond to the authorized one, which is why security, privacy, authentication, authorization, access control, data protection are another major thing to consider (Qayyum, 2017). Nowadays, IoT systems are based on the centralized client-server communication model (R. K. Kodali, 2017) that facing challenges such as DDoS Attack on the

[*] Coresponding authors:
E-mail: ketya.huy@gmail.com
Tel: +855-96-3303-096

centralized server (K. N. Mallikarjunan, 2016), a central authority and no user privacy. In this paper, we focus on IoT systems for a smart classroom. However, Security and Privacy are the main key issues for IoT such as single point of failure of the centralized system maintain availability and assure the integrity, some IoT device products are weakness in authentication, management and access control that is opportunity to hacker can control their devices, and unauthorized can readable or modifies data because users are using the default setting of IoT devices. So, the main objective of our research is to investigate how Blockchain and Smart Contracts (Antonopoulo, 2015) can contribute to build trustworthy, secure and privacy-aware IoT systems. Also, we proposed a system architecture model of using a Blockchain called Hyperledger to secure the Internet of Things network in the smart classroom, and we developed the IoT platform for the smart classroom. A blockchain and Smart Contract considered as one of the most revolutionary and disruptive technology nowadays, some may say it is the next generation of the Internet, and they are very popular on over the world (T. Ahram, 2017). The blockchain could be applied to many other solutions in the market (M. Conti, 2018). The blockchain is distributed ledger technology behind Cryptocurrency such as Bitcoin, Ethereum and others that keep a record of all transactions that take place across a peer-to-peer network. A cryptocurrency is a medium of exchange, such as the US dollar, but it's digital and uses cryptography or encryption techniques to control the creation of monetary units and to verify the transfer of funds. Also, Blockchain has many industries release it such as Bitcoin, Ethereum, Hyperledger and others (D. Vujičić, 2018). So, we chose one is Hyperledger for our research.

1.1 Blockchain

A blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable and updateable only via consensus or agreement among peers. A blockchain is a chain of blocks that each block contains ledger and each ledger contains transaction information. We can think a blockchain like a database that is spread over multiple sites, meaning that the storage information for the database is not all connected to a common processor. It maintains a growing list of ordered records, called blocks. Each block has a link to a previous block. A ledger is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network (Antonopoulo, 2015).

The below Figure 1 is shown the Blockchain.

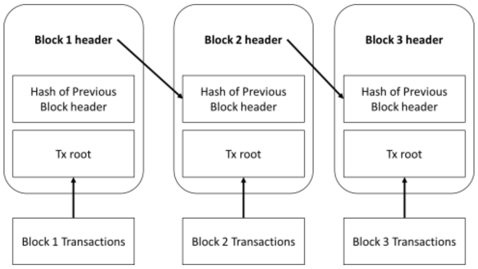


Fig.1. Blockchain

1.2 Smart Contracts

A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other (Antonopoulo, 2015). The contract is registered in a blockchain and all the legal clearing is made automated (Laskowski, 2017).

1.3 Hyperledger

Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies that client can create Blockchain and Smart Contracts for their solution. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing, and Technology.

2. MOTIVATION

In Cambodia, the IoT is still a new technology for research and development. We want to a classroom in Cambodia to become a smart classroom. In this paper, we studied in the classroom at the Institute of Technology of Cambodia in Cambodia will soon be transforming into the smart classroom. Nowadays, IoT systems are based on the centralized client-server communication model (A. Banerjee, 2018), all devices connected to the cloud server that provides huge storage and processing capacity which need expensive cost in building the infrastructure and maintenance, another main problem of the centralized system is the single point of failure when there is an attack on that centralized system (W. Peng, 2016). Which is why Blockchain and Smart Contracts with its secure and distributed nature come to play an important role in securing the IoT network (Devetsikiotis, 2016).

The motivation behind this paper is to investigate how Blockchain and Smart Contracts can contribute to building trustworthy, secure and privacy-aware IoT systems.

3. SMART CLASSROOM

3.1 Senario

Let’s take a classroom at the Institute of Technology of Cambodia and embedded with several sensors such as door lock, light sensor, and temperature sensor. Also, in the classroom have 5 device types such as air-conditioner, door, fan, lcd-projector, and light.

In the smart classroom scenario, before students and teachers entering the classroom every device inside the classroom is in an off mode. In the morning class starts at 7AM, the teacher arrived at the class and opens the classroom door attached with a smartphone for the door open or close. Teachers or students start to turn on the fan, air-condition, light, lcd-projector via smart phone if they needed. Also, sensors have deployed inside the classroom such as temperature sensor, and light sensor to detect if the room is cool enough or bright enough. All the data generates by the sensors will transmit to local server and cloud server which could be analyzed and alert to the authorized one about the environmental situation inside the classroom to manipulate the devices such as air-condition or light to save the energy, it can also be done autonomously by the device itself. After finished class, every device is turn off and some device needs to be kept in the saving mode depending on the time table. Some room are allowed students to enter to do something with the self-study.

3.2 Architecture

The below Figure 2 is shown the proposed system architecture for smart classroom.

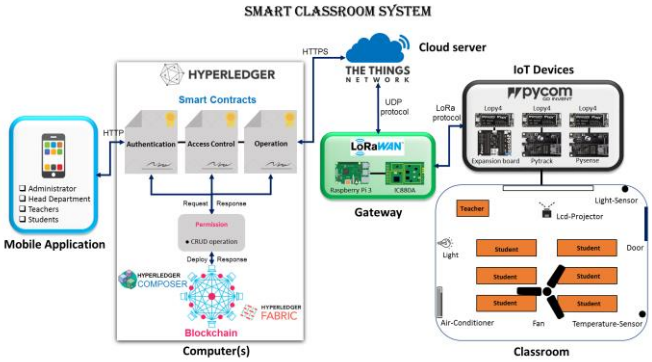


Fig.2. Smart Classroom System Architecture

In this system architecture have 4 user types such as Administrator, Head Department, Teachers and Students. Administrator and head department can use all function in the application such as register/control on users or devices, teacher can use all devices in the classroom such as air-conditioner, door, fan, lcd-projector and light but student cannot use door and lcd-projector. Those devices connected to micro-controllers to became smart devices by using LoPy4 with Expansion Board of Pycom products that operated in the frequency plan of 868MHz in Cambodia. Also, we need one or many computers to setup Blockchain and Smart Contracts of Hyperledger as a local server to security and privacy for a smart classroom system that Hyperledger has many projects, so we chose one is Hyperledger Fabric, and we need another tool is Hyperledger Composer. In Hyperledger Fabric and Composer, we created a blockchain network for our business network solution is smart classroom with 3 Smart Contracts to run on top blockchain of Hyperledger Fabric such as Authentication contract, AccessControl contract, and Operation contract. Those Smart Contracts use to do the transaction for smart classroom and all transaction history stored in blockchain that all blocks updateable only via Kafka consensus algorithm to agreement among peers. Permission is a CRUD operation to set the role what user can read, create, update or delete in the blockchain network that provided by Hyperledger. Blockchain gets live data from smart devices via cloud server of The Things Network by using LoRa protocol, and all devices in the classroom communicate with LoRaWAN gateway by using Raspberry PI3 with Concentrator IC880A that operated in the frequency plan of 868MHz in Cambodia. Also, sensors have deployed inside the classroom such as light sensor and temperature sensor by using LoPy4 with Pysense of Pycom products to detect if the classroom is cool enough or bright enough.

How does it work:

Users and devices account are registers by administrator or head department. When a user uses the mobile application to remote devices in the classroom, the user needs to login first that data send to authentication contract in Hyperledger to validate username and password from blockchain. After validation is correct, it moves to the next smart contract is access control that this contract used to set the role of the user and what a user can do in this application. And then the user can do something in this application via operation contract to remote devices in the classroom. When the user clicks turn on/off devices, the process will go to operation contract that it will get device information from blockchain and verifies with authentication contract to interact with smart contract code to remote on devices in the smart classroom via The Things Network. After The Things Network retrieves data from the smart contract, it will send data to LoRaWAN gateway. And then gateway will send data to micro-controller to turn on/off devices. All data transmitted in the application will store in blockchain. Also, sensors have deployed inside the classroom such as light sensor and temperature sensor to detect if the classroom is cool enough or bright enough, if sensors detect no cool enough or bright enough, so some sensors transmitted data to Hyperledger to turn on light or air-conditioner and then store data in blockchain, some devices turn off if it is cool or bright enough.

3.3 Network Communication

The below Figure 3 is shown the network communication of smart classroom.

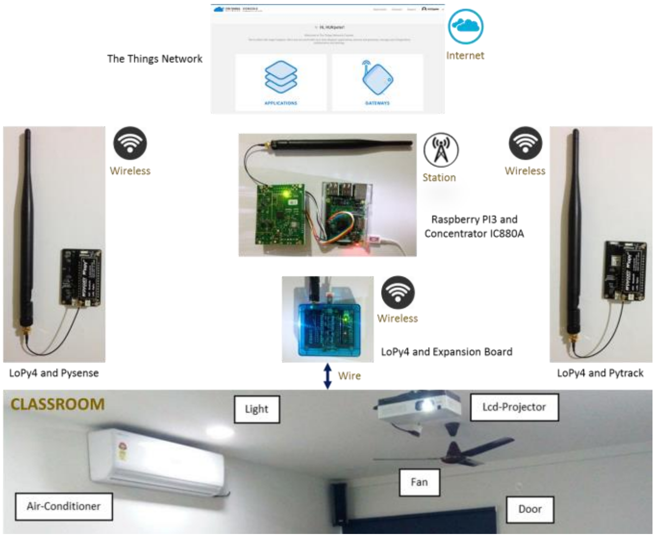


Fig.3. Network communication of Smart Classroom

In this paper, we used LoRa protocol to perform a network communication for IoT network (A. Augustin, 2016) with unlicensed spectrum 868 MHz of Europe in Cambodia. Also, we used Pycom products for LoRa nodes such as LoPy4 with Expansion Board as micro-controllers to use on top devices in classroom such as light, door, fan, air-conditioner, and lcd-projector, LoPy4 with Pysense as sensors such as temperature sensor and light sensor for collects data from classroom, LoPy4 with Pytrack as a GPS for collects location in classroom. We used Raspberry PI3 with Concentrator IC880A as a LoRaWAN gateway to communication with IoT devices (C. Garrido-Hidalgo, 2018), and we used The Things Network to secure and communicate with IoT devices and gateways over the cloud server.

3.4 Security and Privacy

Security and Privacy of a system usually rely on the following elements: confidentiality, integrity, availability (Qayyum, 2017). Data communication focuses on the ability for a device to transmit data to other devices over some distance. In order to ensure confidentiality, integrity, and availability of the transmit data, most communication protocols implement some new technologies, data encryption algorithm or used another cryptography to prevent the transmitting data from being read or modified by unauthorized parties (Z. Ren, 2017).

In this paper, we studied on Blockchain and Smart Contracts of Hyperledger (F. Benhamouda, 2018) as the method to security and privacy for the smart classroom system. A blockchain in this paper can reduce the top management overhead, and prevent a single point of failure of the centralized system maintain availability and assure the integrity of the transaction with the Kafka consensus algorithm for dealing with consensus, protect data privacy with cryptography algorithm. A smart contract in this paper is a set of rules under which parties to that smart contract agree to interact with our system. Smart Contracts enables smart devices to become independent autonomous conducts a variety of transaction and could keep track of the history of the devices in the blockchain ledger. Also, Hyperledger has many projects, so we chose one is Hyperledger Fabric and we need another tool is Hyperledger Composer.

a. Hyperledger Fabric

We created a permission blockchain framework implementation for our research by using Hyperledger Fabric that written smart contracts via chaincode in Go language. For the consensus algorithm, we used Kafka consensus. In Kafka consensus have 3 parties such as Endorser is driven by policy upon which participants endorse a transaction, Orderer accepts the endorsed transactions and agrees to the order to be committed to the ledger, and Validator takes a block of ordered transactions and validates the correctness of the results, including checking endorsement policy and double-spending.

The below Figure 4 is shown architecture of Kafka consensus algorithm.

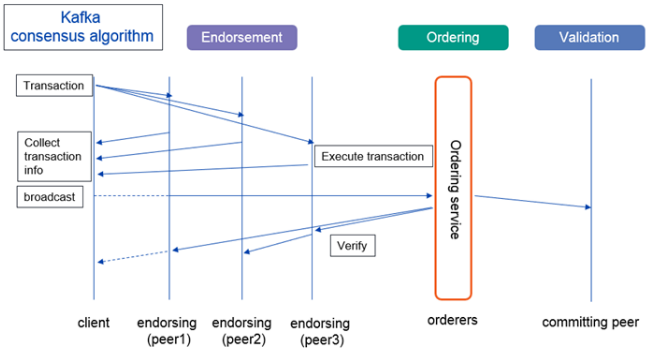
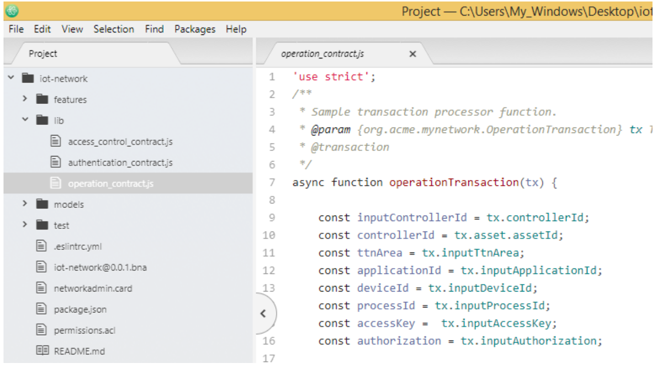


Fig.4. Kafka Consensus architecture of Hyperledger Fabric

b. Hyperledger Composer

After we created Blockchain and Smart Contracts for our solution via Hyperledger Fabric, we needed Hyperledger Composer to supports the existing Hyperledger Fabric Blockchain infrastructure and runtime, written Smart Contracts with JavaScript language and public APIs for clients use. We developed a Business Network Archive of the project is a smart classroom that including Model file contain participant and asset, Script file contains 3 Smart Contracts such as Authentication contract to verify users or devices in the application, AccessControl contract to set rule of users in the application, and Operation contract to interact devices in classroom.

The below Figure 5 is shown structure project of Hyperledger Composer for Smart Classroom.



```
'use strict';
/**
 * Sample transaction processor function.
 * @param {org.acme.mynetwork.OperationTransaction} tx
 * @transaction
 */
async function operationTransaction(tx) {

    const inputControllerId = tx.controllerId;
    const controllerId = tx.asset.assetId;
    const ttnArea = tx.inputTtnArea;
    const applicationId = tx.inputApplicationId;
    const deviceId = tx.inputDeviceId;
    const processId = tx.inputProcessId;
    const accessKey =  tx.inputAccessKey;
    const authorization = tx.inputAuthorization;

```

Fig.5. Structure project of Hyperledger Composer for Smart Classroom.

c. Advanced Encryption Standard (AES)

As you know a Blockchain is very strong for secure our system but we need to increase security level with encryption and decryption of Advanced Encryption Standard to protect data from no owner (Panchbhai, 2016) that data encrypted in Blockchain.

d. Password-Based Key Derivation Function 2 (PBKDF2)

We used Password-Based Key Derivation Function 2 to protect user password that it generates to hash function (Xiurong Chen, 2015). Hash function is only one way that it means we can't reverse it. Also, user password generated to PBKDF2 hashing and then its store in Blockchain.

3.5 Saving Energy

Beside Saving Energy and RoomSafetySecurity against malicious activity, the data from the sensor could also notify if the teacher has come to teach or not by reading the data from the door sensor and time, this could be applied as the policy is set to only the teacher could open the classroom door. So, the head of the department could know if the teacher comes to teach on time or not and could use it to evaluate the teaching performance as well as keep user privacy and give the right to users to have full control over their personal data. All the data generated by the IoT devices will be collected, analyses and give an insight for asset management and usage optimization for the good decision making.

In this paper, some sensors have deployed inside the classroom such as Lopy4 with Pysense as a temperature sensor or light sensor to detect if the room is cool enough or bright enough, and LoPy4 with Pytrack as a GPS to get a classroom location. All the data generated by the sensors will transmit to blockchain which could be analyzed and alert to the authorized one about the environmental situation inside the classroom to manipulate the devices such as air-condition or light to save the energy, it can also be done autonomously by the device itself.

4. RESULTS AND DISCUSSION

4.1 Results

The below Figure 6 is shown the result of our research about Security and Privacy for the IoT Network by using Hyperledger that we proposed a system architecture for a smart classroom, and we developed the IoT platform for the smart classroom. Our case study is a real classroom at the Institute of Technology of Cambodia in Cambodia. In this result, we conducted the classroom prototype by using cardboard as the classroom, and LED devices as real devices in the classroom such as air-conditioner, door, fan, light, lcd-projector. Also, we developed the mobile application to remote or control on smart devices. Those devices protected via Blockchain and Smart Contracts of Hyperledger that we created the Blockchain network for smart classroom, and we created 3 Smart Contracts such as Authentication contract to verify when user login to the application, AccessControl contract to set rule of users in the application, Operation contract to interact smart devices in the classroom. However, we used Blockchain and Smart Contracts of Hyperledger as a local server to security and privacy for our system that hackers hard to attack. Also, we used AES and PBKDF2 to increase security level on Blockchain to protect data from no account owner. For IoT network communication, we built LoRa with unlicensed spectrum 868 MHz in Cambodia for network communication of IoT that using LoRaWAN gateway to communication with IoT devices. For IoT devices, we used Pycom products that it is popular in Europe. After that, we used The Things Network as a public LoRa server via LoRaWAN to secure communication and get live data over the cloud.

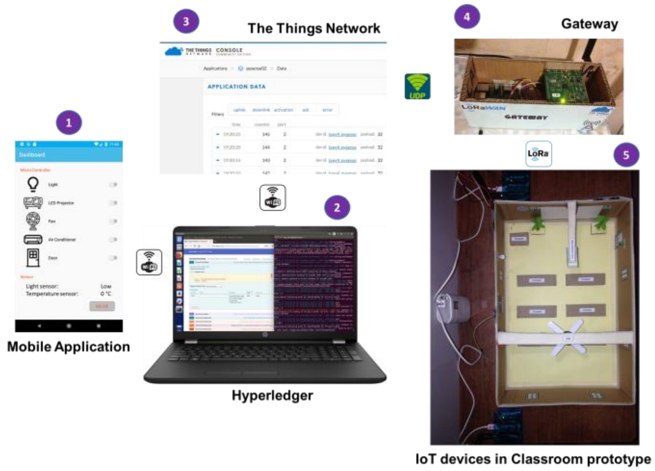


Fig.6. Our result about Security and Privacy for the IoT Network by Hyperledger.

The below Figure 7 is shown the result of saving energy for a smart classroom. Beside Saving Energy and RoomSafetySecurity against malicious activity, the data from the sensor could also notify if light sensor that using LoPy4 with Pysense inside the classroom to detect if the classroom is bright enough after that light is turn on, if light sensor detects in classroom is not bright enough after that light is turned off, it can also be done autonomously by the device itself, and sensors send data to Hyperledger to turn on/off light by using Smart Contracts and then it stores in Blockchain for data protection.

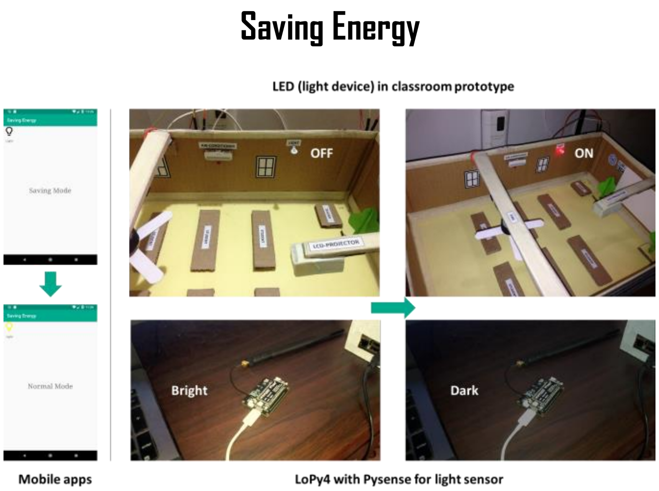

Saving Energy
LED (light device) in classroom prototype
Saving Mode
OFF
ON
Normal Mode
Bright
Dark
Mobile apps
LoPy4 with Pysense for light sensor

Fig.7. Our result about saving energy with light sensor in classroom and protect data via Hyperledger.

The below Table1 is shown the result of evaluation on a centralized system with a distributed system for our research. There are 3 types such as Threats are risk in our system, Centralized system as a traditional database, and Distributed system as a blockchain to solve problems of threats. Thus, blockchain is a very useful application for the security and privacy of IoT systems for the smart classroom.

Threats	Centralized System	Distributed System
DDoS attack	×	√
Data leakage	×	√
A central authority	×	√
Transparency	×	√
Enhanced security	×	√
Traceability	×	√
Robustness	×	√
Disintermediation	×	√
Data manipulation and fraud	×	√
Dishonesty	×	√

Table 1. Table Evaluation on centralized system with distributed system.

In this paper, we are testing with a computer as a centralized server and two computers as a distributed server that which one is better to build trustworthy, secure and privacy-aware IoT systems. Below is shown the solution that blockchain solved threats in Table1 such as:

DDoS attack: We used a computer as a centralized server, when we are shut down the computer all clients that access to this server is denied but if we used two computers as a distributed server, when we shut down one computer, another computer is work normal, so client's access to server normal. So, blockchain is always stable for network connection.

Data leakage: Blockchain has a write-only data structure and transactions are verified by consensus algorithm from other computers on the blockchain. Every new block gets appended to the blockchain by linking to the previous block's 'hash'. So, unauthorized cannot readable.

A central authority: Blockchain is no central body which governs whether a particular transaction should be recorded or not. Data is managed by a cluster of computers not owned by any single entity. So, the blockchain network has no central authority.

Transparency: Blockchain transaction histories are becoming more transparent through the use of blockchain. All computers work together to ensure they are all coming to the same conclusions, providing in-built security for the network and all network participants share the same documentation as opposed to individual copies that shared version can only be updated through consensus algorithm, which means every computer must agree on it. So, blockchain ensures the non-repudiation of users action, every transaction are recorded allow to audit and to trace back to its origin.

Enhanced security: Blockchain is high security than other record-keeping systems. In blockchain, transactions must be agreed upon before they are recorded. After a transaction is approved, it is encrypted and linked to the previous transaction. So, blockchain ensures the security of data by not having a single point of failure.

Traceability: Blockchain can be to trace record back to its origin. When we change information of data are recorded on a blockchain, the historical transaction data can help to verify the authenticity of assets and prevent fraud. So, blockchain as the ability to verify the history of documented recorded identification.

Robustness: Blockchain has a built-in robustness by storing blocks of record information that are identical across its network, the blockchain cannot be controlled by any single entity, has no single point of failure. Every node on a blockchain processes every transaction, so no individual node is crucial to the database as a whole, so it has extreme fault tolerance capabilities.

Disintermediation: Data in blockchain can be shared across the network without the need of an intermediary to validate or authorize it. These constraints can therefore be enforced directly by the nodes on the blockchain with a consensus mechanism to ensure that the nodes stay in sync. So, blockchain is the process of removing the middleman or intermediary in connection with a transaction or a series of transactions.

Data manipulation and fraud: Blockchain is its immutability. The use of sequential hashing and cryptography, combined with the distributed structure, make it virtually impossible for any party to unilaterally alter data on the ledger. So, blockchain is extremely hard to change.

Dishonesty: In blockchain, every user can be sure that the data they are retrieving is integrity, uncorrupted and unaltered since the moment it was recorded. So, blockchain ensures data integrity.

4.2 Discussion

Q1: Why did we use Blockchain and Smart Contracts of Hyperledger?

A1: Hyperledger is an open source collaborative effort created to advance cross-industry blockchain technologies that developers can create Blockchain and Smart Contracts for our solution.

Q2: Why did we use Pycom products for smart devices?

A2: Pycom product is very popular in 2018 at Europe and it has own feature such as update firmware, username and password on devices and others.

Q3: Why did we use Raspberry PI3 and Concentrator IC880A for LoRa gateway?

A3: Raspberry PI3 is the latest version in 2018, Linux software and exposed general-purpose input/output (GPIO) pins at the top of the board make it easy to connect with Concentrator IC880A that use LoRaWAN for IoT network.

Q4: Why did we use LoRa network with frequency plan 868MHz in Cambodia?

A4: For frequency plan 868MHz is not anyone uses in Cambodia.

Q5: Why did we use LoRa server of The Thing Network?

A5: Our system used LoRa protocol for IoT network and TTN is public LoRa server that it used LoRaWAN. TTN has many features such as register devices and gateways, get live data from the cloud server.

5. CONCLUSIONS

In this paper, we studied on Blockchain and Smart Contract by using Hyperledger Fabric and Composer for contributions to building trustworthy, secure and privacy-aware IoT systems for smart classroom because a blockchain is distributed nature, it can reduce the top management overhead, and prevent single point of failure of the centralized system maintain availability and assure the integrity of the transaction with Kafka consensus algorithm for dealing with consensus, protect data privacy with cryptography algorithm, and a smart contract is a set of rules under which parties to that smart contract agree to interact with IoT systems for enables smart devices to become independent autonomous conducts variety of transaction and could keep track of the history of the devices in the blockchain ledger.

Also, we proposed a system architecture model of using a Blockchain called Hyperledger to secure the Internet of Things network in the smart classroom, and we developed the IoT platform for the smart classroom that including the mobile application as an end-user to remote or control smart devices in the classroom, Hyperledger as the method to security and privacy for smart classroom, LoRa as a network for long-range communication and low power consumption devices of IoT, and The Things Network as a public LoRa server for communication over the cloud server. In fact, our research can apply to many IoT domains such as Smart Classroom, Smart Home, Smart Cities and others.

Finally, the results showed that Blockchain and Smart Contracts of Hyperledger is a very useful application to secure and privacy-aware IoT systems for Smart Classroom such as:

1. Disintermediation
2. Robustness
3. Traceability
4. Enhanced security
5. Transparency
6. Prevented DDoS attack on the centralized server
7. Protected data leakage
8. Eliminated a central authority
9. Prevented dishonesty
10. Data manipulation and prevented data fraud

However, there still some other aspects that need improvement for future work such as user and device register, saving energy with some sensors such as light sensor and temperature sensor.

REFERENCES

A. Augustin, J. Y. (2016). A Study of LoRa: Long Range & Low Power Networks for the Internet of Things. Sensors, vol. 16, no. 9, 1466-1484.

Antonopoulo, A. M. (2015). Mastering bitcoin. First edition. Sebastopol CA: O'Reilly.

C. Garrido-Hidalgo, D. H.-S. (2018). IoT Heterogeneous Mesh Network Deployment for Human-in-the-Loop Challenges Towards a Social and Sustainable Industry 4.0. IEEE Access, vol. 6, 28417-28437.

D. Vujičić, D. J. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. IEEE International Symposium INFOTEH-JAHORINA (INFOTEH), 1-6.

Devetsikiotis, K. C. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, vol. 4, 2292-2303.

F. Benhamouda, S. H. (2018). Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation. IEEE International Conference on Cloud Engineering (IC2E), Orlando, FL, 357-363.

H. N. Saha, A. M. (2017). Recent trends in the Internet of Things. IEEE Annual Computing and Communication Workshop and Conference (CCWC), 1-4.

Jacques, B. (2017). The Internet of Things: Assessing Its Potential and Identifying the Enablers Needed to Capture the Opportunity. IGI Glob, 15.

K. N. Mallikarjunan, K. M. (2016). A survey of distributed denial of service attack. IEEE International Conference on Intelligent Systems and Control (ISCO), 1-6.

Laskowski, H. K. (2017). A Perspective on Blockchain Smart Contracts: Reducing Uncertainty and Complexity in Value Exchange. IEEE International Conference on Computer Communication and Networks (ICCCN), 1-6.

N. Kumar, J. M. (2017). Review on security and privacy concerns in Internet of Things. IEEE International Conference on IoT and Application (ICIOT), 1-5.

Panchbhai, M. M. (2016). Review on realization of AES encryption and decryption with power and area optimization. IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), 1-3.

Qayyum, M. H. (2017). Internet of Things: A study on security and privacy threats. IEEE International Conference on Anti-Cyber Crimes (ICACC), 93-97.

R. K. Kodali, V. J. (2017). IoT based smart security and home automation system. IEEE International Conference on Computing, Communication and Automation (ICCCA), 1286-1289.

T. Ahram, A. S. (2017). Blockchain technology innovations. IEEE Technology & Engineering Management Conference (TEMSCON), 137-141.

W. Peng, S. L. (2016). A secure publish/subscribe protocol for Internet of Things using identity-based cryptography. IEEE 5th International Conference on Computer Science and Network Technology (ICCSNT), 628-634.

Xiurong Chen, X. L. (2015). A modified PBKDF2-based MAC scheme XKDF. TENCON 2015 - 2015 IEEE Region 10 Conference, Macao, 1-6.

A. Banerjee, F. S. (2018). Centralized framework for controlling heterogeneous appliances in a smart home environment. IEEE International Conference on Information and Computer Technologies (ICICT), DeKalb, IL, 78-82.

M. Conti, S. K. (2018). A Survey on Security and Privacy Issues of Bitcoin. IEEE Communications Surveys & Tutorials, 1-1.

Z. Ren, X. L. (2017). Security and privacy on internet of things. IEEE 7th International Conference on Electronics Information and Emergency Communication (ICEIEC), 140-144.