International Journal of Reliable Information and Assurance
Vol.7, No.2 (2019), pp.7-12
http://dx.doi.org/10.21742/ijria.2019.7.2.02

Using IDoT Attributes for Secure Power Data Sharing Based on Blockchain Dynamic Access Control

Jae-Kyu Lee[1] and You-jin Song[2]

[1]*Dept. Techno-Management Cooperation Course, Dongguk Univ., 123 Dongdae-ro, Gyeongju-si, Gyeongsangbuk-do, 38066, Korea*
[2]*Corresponding Author, Dept. Information Management, Dongguk Univ., 123 Dongdae-ro, Gyeongju-si, Gyeongsangbuk-do, 30866, Korea*
[1]*jaekyulee@dongguk.ac.kr*, [2]*song@dongguk.ac.kr*

Abstract

Data collected through devices are stored in a single cloud and processed in Internet of Things (IoT) environment. Because IoT has a limitation of computing and storage space of devices. In order to solve the problem of reliability of centralized system, previous researches have been carried out to link blockchain to the Internet. However, user privacy protection is an indispensable factor for sharing data through the Internet. However, these limitations are not overcome. In this paper, the access control of the user is made flexible and robust through Dynamic Access Control Table (DACT) using the context attribute of IDentity of Things (IDoT). The system proposed in this paper can build a platform to securely share users' power consumption data in the energy cloud.

Keywords: *Internet of Things, Blockchain based on tangle, Energy cloud, Data privacy, IDoT, Dynamic access control table (DACT)*

1. Introduction

The Internet of Things (IoT) will take the form of sharing data measured by sensors connected to each other and digitizing industries in various fields.

Current power grids are optimized for unidirectional power delivery. This makes it difficult to optimize the supply and demand of energy. In order to optimize the power grid, a power grid integrated with ICT technology, control technology and sensor technology is required in the power grid. The energy cloud is an efficient system that can purchase the necessary energy or sell the remaining energy through such a power grid.

Data reliability is still a key issue in the future of the Internet of Energy (IoE), and solutions to address data sharing and reliability issues in the energy cloud are becoming issues.

In this regard, blockchain technology can provide a solution to the data reliability problem. Blockchain has been applied in various fields and ensures the consistency and reliability of information. Blockchain has emerged as a key technology to change the way information is shared.

In order to prevent security threats such as forgery of energy trading data in previous researches, a system which adopts a blockchain [8] or a method of setting a consumption pattern

Article history:
Received (May 18, 2019), Review Result (June 14, 2019), Accepted (July 9, 2019)

Print ISSN: 2288-8950, eISSN: 2207-5143 IJRIA

suitable for a specific situation in consideration of parameters such as user's preference or household appliances . In this study, previous studies [7][8][9][10][11] are effective, but they have limitations on user privacy issues. IoT (Internet of Things) Because there is a limitation of computing and storage space of devices, data collected through devices are stored in a single cloud and processed. In order to solve the problem of reliability of centralized system, previous researches have been carried out to link blockchain to the Internet [3][4][5]. However, user privacy protection is an indispensable factor for sharing data through the Internet. However, these limitations are not overcome. In this paper, the access control of the user is made flexible and robust through DACT using the context attribute of IDoT (IDentity of Things). The system proposed in this paper can build a platform to securely share users' power consumption data in the energy cloud. To overcome the reliability limitation of the IoT system, we compare the results of this paper with previous studies [3][4][5] in which blockchain are interlocked.

In this paper, we propose a system structure that provides data reliability through blockchain considering user privacy in energy optimization system.

2. Related works

2.1. Internet of Things and IDoT

The Internet of Things is attracting attention as a core technology leading to a connected society by connecting people, goods, and places and providing various services by combining them with various fields. Things as core technology Internet security has always been an issue. Research is underway to analyze the characteristics of IDoT (IDentity of Things) to solve these security issues [1].

[Figure 1] is a structure of IDoT that borrows the concept of IDoU (Identity of Users) used in traditional systems and networks. This structure is divided into inheritance, association, knowledge, and context.

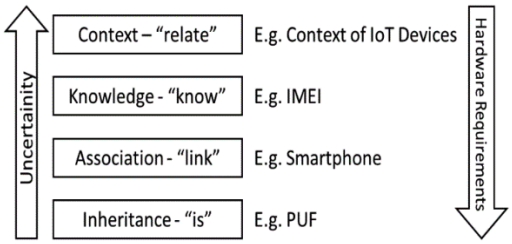

Figure 1. Identity in the Internet of Things

[Figure 1], "inheritance" means something like human biometrics (fingerprint or retina). Biometrics is a PUF (Physical Unclonable Function), and it is used only in fields requiring strong security, but it is one of popularized technologies [6]. Objects Internet devices are given a personal gateway like a smartphone, which is connected through "association". This transfers data to the cloud through pre-defined smartphones. And for "knowledge (knowledge)" e.g. smartphones, but the (International Mobile Equipment Identity) IMEI, IMEI Changing the smartphone is not as simple as changing your password. Finally, it is "context". This can have a significant impact on the security of the Internet. Objects Internet sensors are placed in groups that are related to each other. Attach various sensors to various parts of a person's body, and observe all bodies belonging to the person with sensors. Monitor and study the data collected by several sensors belonging to the same group. And comparing with the expected behavior

profile, IDoT of specific characteristic comes out. Contexts, unlike the previous ones, come from a variety of Internet objects that are related to each other [1].

In this paper, DACT is defined using IDoT and user authentication process is performed through defined DACT. Through the user authentication process using IDoT, the effect of service such as power trading is enhanced without infringing privacy of shared data.

2.2. Access control policy

Song, YJ et al. [2] emphasized the importance of generating new information, i.e., contextual information, by deducing information collected according to the user's situation in the Internet environment of things. In order to protect sensitive information that is sensed in the Internet environment of objects, information access control technique through context awareness is needed.

In this paper, user authentication is performed using DACT based on IDoT to protect user 's privacy in data sharing system. To do this, DACT consists of defined links and contexts. link is your smartphone. Context historically stores dynamic data such as user's access time and location, and effectively protects privacy by matching user's real-time dynamic data.

2.3. Tangle based blockchain

Unlike existing blockchains, Tangles developed by IOTA do not form blocks [12]. Tangle configures a distributed ledger only for each transaction. Also, the consensus process is not performed before saving. When a transaction occurs on the Tangle network, the user who generated the transaction chooses two transactions that lack the consensus number in their database. Then, the POW aggregation process is performed to verify the hash values of the transactions. The process of transaction processing in Tangle [Figure 2].

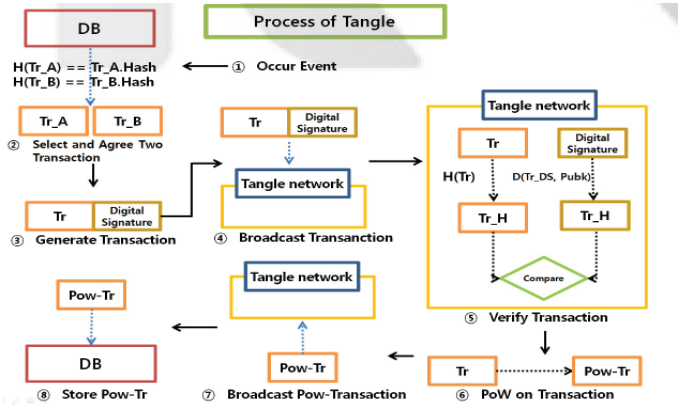

Figure 2. Process of tangle

Two transaction hash values that have already been agreed upon are included in the transaction and then stored. It is a storage structure that connects with a directional acyclic graph (DAG) instead of a chain structure like the existing blockchain. The DAG type in which transactions are stored is shown in [Figure 3].

Tangles have low difficulty of proof of work and low commission compared to blockchains. In addition, the lightweight hash algorithm Curl, developed by the IOTA Foundation, enables transactions to be processed faster than blockchains.

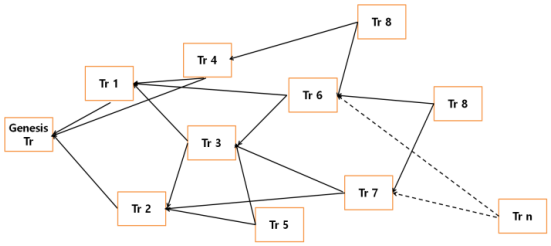

Figure 3. Off-chain storage structure of tangle

In this paper, we design the energy consumption data to be able to trade smoothly in real time using the tangled network.

Smart contract is a contract that is implemented to be executed when a certain condition is satisfied in a blockchain environment. The smart contract has a unique address and is executed when a message that satisfies the condition is sent to the address.

2.4. Blockchain connection for privacy protection in IoT environment

Truc Dinh et al. [3] presented how to use blockchains to solve data privacy problems in the Internet of Things (IoT). With Smart Contract, we have developed a system model with an unreliable access control mechanism that allows users to fully control their data and track how third-party services access the data. We also proposed a firmware update method using a blockchain to prevent fraudulent data due to modulation of IoT devices.

Yunru Zhang et al. [4] controlled data access using a block-chain model and an attribute-based cryptographic system in the Internet environment to protect personal information. I used the Permission Access Control Table to control access to the data. To achieve granular access control, a smart contract was used to generate an access control table (PACT). The owner first placed the smart contract in the access control table of the blockchain.

The architecture consists of an object Internet device, a data owner, a block-chain network, and a cloud. In addition, blockchain has been configured to control access to data using the access control table in terms of security.

3. System structure to protect user privacy of power consumption data

3.1. Architecture

Truc Dinh et al. [3] introduced a system for solving data privacy problems in object internet environment using blockchain [Figure 4]. Aggregators are users who generate data. Aggregator $A = \{a_1, a_2, \ldots, a_n\}$ represents an entity in which n components are aggregated. The data created by the aggregator is stored in off-chain storage and uses the hash of the stored data as a pointer. This information is recorded in the blockchain. Subscriber accesses off-chain storage using pointers in the blockchain when they want to browse the desired data. The vendor updates the firmware of each device of the aggregator to manage the system flexibly.

In this paper, we use off-chain storage in the form of a cloud and use a hash as a pointer. However, instead of specifying a pointer through a Vendor, the user specifies a hash pointer using DHT. Also, for privacy reasons, the subscriber designed the structure to obtain a hash pointer only after obtaining the agreement of the aggregator.

To efficiently utilize energy consumption, data must be analyzed through a smart meter. For this reason, it is shared so that user data, that is, MyData, can be collected, analyzed, and browsed.

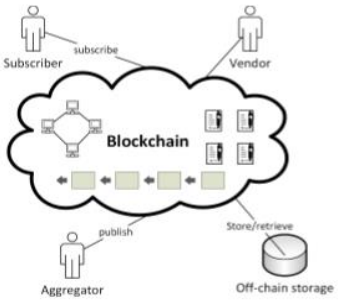

Figure 4. Blockchain type IoT system with off-chain storage

So the user has $A, B = \{IDoT_1, IDoT_2, \ldots IDoT_n\}$ and smart meter. The smart meter measures the amount of power and generates MyData. A When a user wants to browse MyData of user B, it is possible to browse from time to time. At this time, however, the privacy of user B is not maintained. We designed a system that can consume energy efficiently while sharing user's privacy while sharing power consumption data.

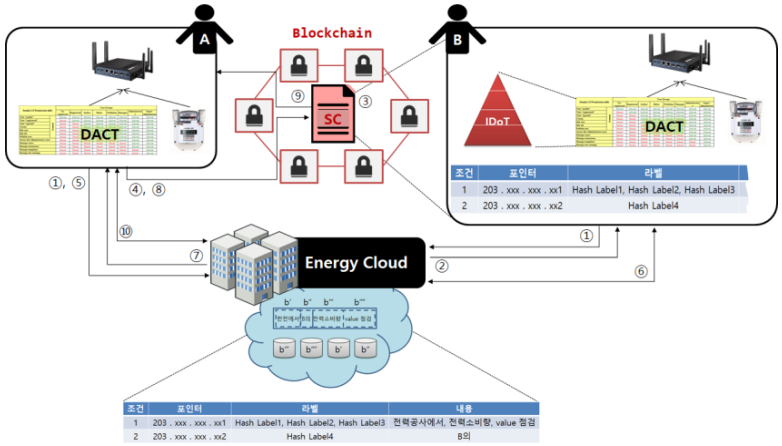

Figure 5. Secure energy data sharing cloud system based on blockchain

The system configuration is largely divided into user, energy cloud, and smart contract. Each configuration of the system is defined as follows.

1) User: Users define PACT based on IDoT for their own authentication. IDoT, which is defined in PACT, uses dynamic context and link. In the context configuration, the location information within a specific time and time is stored and used in a historical manner. Link uses the user's proprietary smartphone and desktop information.

2) Energy Cloud: The Energy Cloud owns each user's PACT to authenticate the user. This function allows users to go through certification procedures compared to PACT, which owns real-time IDoT information of users who want to access data.

3) Smart contact: In a blockchain network environment, the user creates a smart contact. The generated smart contact sets the hash pointer value specified by the user to the condition value.

4. Conclusion

In this paper, we added a blockchain to get out of the existing centralized system. This overcomes the limitations of centralized form. And through PACT based on IDoT's dynamic context, it has been designed to provide flexible and robust access control to users.

Acknowledgement

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2019R1F1A1056507).

References

[1] Kwok-Yan Lam and Chi-Hung Chi, "Identity in the Internet-of-Things (IoT): New challenges and opportunities," Information and Communications Security: 18th International Conference, ICICS 2016, pp.18-26, **(2016)**

[2] You-jin Song, Aria Seo, Jaekyu Lee, and Yei-chang Kim, "Access control policy of data considering varying context in sensor fusion environment of Internet of Things," KIPS Transactions on Software and Data Engineering, vol.4, pp.409-418, **(2015)**

[3] Truc Dinh, Trung Nguyen, and Hoang-Anh Pham, "Leveraging blockchain to enhance data privacy in IoT-based applications," 7th International Conference, Computational Data and Social Networks, pp.211-221, **(2018)** DOI: 10.1007/978-3-030-04648-4_18

[4] Yunru Zhang, Debiao He, and Kim-Kwang Raymond Choo, "Bads: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT," Wireless Communications and Mobile Computing, vol.2018, pp.9, Article ID 2783658, **(2018)**

[5] Hossein Shafagh, Anwar Hithnawi, and Simon Duquennoy, "Towards blockchain-based auditable storage and sharing of IoT data," CCSW '17 Proceedings of the 2017 on Cloud Computing Security Workshop, pp.45-50, **(2017)** DOI:10.1145/3140649.3140656

[6] Stefan Katzenbeisser, Ünal Kocabaş, Vladimir Rožić, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann, "PUFs: Myth, fact or busted? A security evaluation of Physically Unclonable Functions (PUFs) cast in silicon, international workshop on cryptographic hardware and embedded systems" CHES 2012: Cryptographic Hardware and Embedded Systems, pp.283-301, **(2012)**

[7] Yi Wang, Qixin Chen, Tao Hong, and Chongqing Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," IEEE Transactions on Smart Grid, vol.10, no.3, pp.3125-3148, **(2019)**

[8] Federico Lombardi, Leonardo Aniello, Stefano De Angelis, Andrea Margheri, and Vladimiro Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," Living in the Internet of Things Conference: Cybersecurity of the IoT - A PETRAS, **(2019)**

[9] Anish Jindal, Gagangeet Singh Aujla, and Neeraj Kumar, "SURVIVOR: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," Computer Networks, vol.153, pp.36-48, **(2019)**

[10] Muneeb Ul Hassan, Mubashir HusainRehmani, and Jinjun Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," Future Generation Computer Systems, vol.97, pp.512-529, **(2019)**

[11] Zhetao Li, Jiawen Kang, Rong Yu, Dongdong Ye, Qingyong Deng, and Yan Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol.14, no.8, pp.3690-3700, **(2018)**

[12] Serguei P, "The tangle," IOTA website, **(2017)**