International Journal of Smart Home
Vol.14, No.1 (2020), pp.9-16
http://dx.doi.org/10.21742/ijsh.2020.14.1.02

Threshold-Based Access Control for Smart Contracts Using IDoT Property in IoT Environment

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

[1]Dept. Information Management, Dongguk University at Gyeongju, Campus, Korea
[2]Dept. Techno-Management Cooperation Course, Dongguk University at Gyeongju, Campus, Korea
[1]song@dongguk.ac.kr, [2]jaekyulee@dongguk.ac.kr

Abstract

The Internet of Things (IoT) system has a physical limitation of the device and a limitation of storing and computing the collected data in one cloud. In order to solve the limitations of such a centralized system, prior researches integrating the IoT and blockchain technology are being actively conducted. In order to implement data sharing services, system efficiency and user privacy are indispensable. To enable data sharing, these limitations must be overcome. This paper flexibly and robustly configures user's access control through DACT using context attribute of Identity of Things (IDoT). In addition, the edge-type system configuration reduces the traffic overload caused by one cloud and combines the efficiency of the system. The system proposed in this paper can build a platform that can safely share users' energy consumption data in the energy data sharing system.

Keywords: *Internet of things, Tangle-Based blockchain, Edge, Data privacy, IDoT, Dynamic Access Control Table (DACT)*

1. Introduction

According to the top ten strategic technology trends for 2018, the Internet of Things (IoT) technology is emerging as a field for creating new value through the interaction between the real world and the virtual world in the 4.0 industry revolution [1]. The Statistica report also predicts that by 2025, nearly 75 billion devices will be interconnected [2].

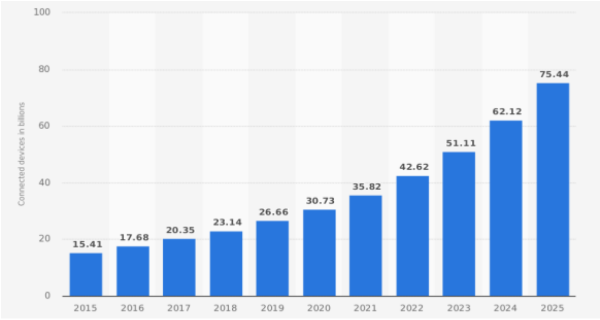


Figure 1. Internet of Things-number of connected devices worldwide 2015-2025(left)

Article history:
Received (December 1, 2019), Review Result (January 8, 2020), Accepted (February 19, 2020)

Print ISSN: 1975-4094, eISSN: 2383-725X IJSH

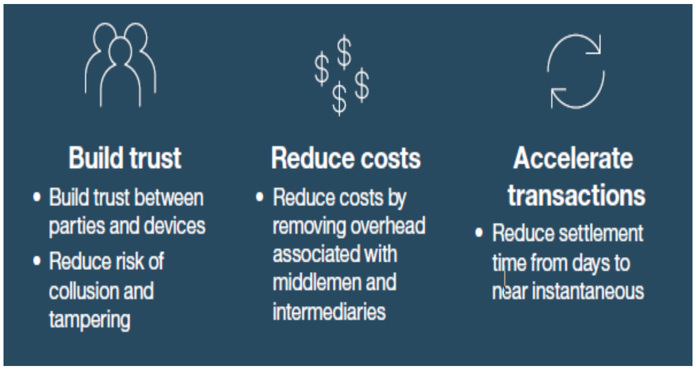

Build trust
• Build trust between parties and devices
• Reduce risk of collusion and tampering
Reduce costs
• Reduce costs by removing overhead associated with middlemen and intermediaries
Accelerate transactions
• Reduce settlement time from days to near instantaneous

Figure 2. Three key benefits of using blockchain for IoT(right)

This means that our society will soon enter the Hyper-Connected Society. A hyper-connected society is a society in which all things, such as people, objects, and space, are connected to each other through the Internet, where information is created, collected, shared, and utilized. This can create various value-added services through communication between not only human beings [3][4][5] but also all internet-connected objects, and provide breakthrough services in the industrial sector [6][7].

Currently, the basic network structure of the IoT is a cloud computing method of receiving information from a device and processing information requested by a server. However, this will not only exponentially increase the administration cost of the server to handle all the large amount of services requested in real-time in the hyper-connected network where a large number of devices are connected. Network users will not be able to use normal services. For example, the 2018 Mirai DDos botnet is documented as a case where companies such as PayPal, Netflix, and Twitter have harmed users with the above problem [8].

In order to solve this problem, many researchers have recently studied blockchain-based IoT (BIoT) technology by applying blockchain technology to the Internet of Things, which guarantees network scalability and transparency. According to an IBM report [9], the main advantages of applying blockchain technology to the IoT are:

First, participants share information with each other, creating trust in the relationships between people or things. From the consumer’s point of view, IoT sensors between multiple distribution managers and consumers can actually confirm the distribution process in the distribution process of goods, so that rewards can be rewarded when the conditions of execution of smart contracts are established.

Secondly, processing costs for transactions involving third-party trust or mediators can be reduced. For example, there is no need for a mediator who manages information about a person’s identity when using it to identify a person or when contracting or hiring. Furthermore, by accepting the signals from IoT sensors as data and applying them to the blockchain, the usage history of welfare and educational services that provide overseas travel or training provided by the company can be accurately identified.

Third, the transaction speed is increased by enabling immediate processing of daily transactions.

In addition, IBM is working on a Waston IoT project that combines blockchain and IoT technology, and the technology’s report also describes several examples. According to IDC, around 20 percent of IoT devices will have a blockchain service base by 2019 [10].

However, there are also problems to be solved in blockchain networks. First, the conditions under which transactions are created are not limited in a structure in which many things are connected to each other. Therefore, all transactions made in the blockchain are made in such a way that the consensus algorithm determines whether the transaction is illegal and approves the transaction. It is not suitable because the transaction time is delayed in the structure of the Internet of Things where many transactions are requested and processed in real-time. Secondly, the complete confidentiality of information about transactions made on the blockchain is not guaranteed. All transactions made in the blockchain are stored in the block so that the user's transaction patterns can be inferred based on sensitive personal information represented by the transaction information generated by the user [11].

Therefore, in order to solve these problems, in the BIoT environment where the blockchain and the IoT are combined, the user's identity is based on not only the unique address of the object but also dynamic information such as the location, distance, and time. It needs to be flexible. That is, in order to provide a variety of identifier attributes related to things, a concept of attribute values (contexts) related to things should be established to provide an accurate and secure system of transactions.

In this paper, we intend to provide various smart services that are connected in the future by linking the attributes of things with ID. Smart contracts are used to share transaction information collected from things in the BIoT structure. In order to execute the smart contract, various IDoT attribute values (5 values are illustrated in this paper) to control the user's access and design a new access control structure that only authorized users can execute the smart contract.

Chapter 1 of this paper describes the background and the necessity of the proposed system. Chapter 2 consists of the technology and previous studies that make up the proposed system, and Chapter 3 describes the composition and process of the proposed system. Chapter 4 consists of an analysis of the proposed system, and Chapter 5 consists of conclusions.

2. Related works

2.1. Fog computing

Fog computing is a structure that has been recently proposed to solve the delay and configuration complexity of cloud computing, and has a feature that provides faster responsiveness by distributing the load among users' devices or devices at the network edge [12]. It is a high-level virtual platform that provides networking services between compute, storage, and end devices and traditional cloud computer data centers, to increase the usability of sensor nodes. Cloud is a long way from us, but fog is a term that comes from around us, and many sensor and equipment companies are developing technologies. The basic data processing is possible, not just a sensing device [12].

Conventional edge computing distributes computing, storage, and other functions to network edge devices, and fog computing provides additional functions related to sensors and actuators of IoT devices. It is composed of a structure that reduces time. Fog computing research is focused on areas that require immediate response from users, especially wearable devices and healthcare services. Condry et al. Have proposed a mechanism to extend security and improve responsiveness in IoT environments through edge devices [13][14]. FAST supports smartphone-based fast situation detection by implementing a system based on fog computing to verify user safety [15]. Stantchev et al. Present a scenario and model for implementing smart healthcare services with fog computing [16]. EPHOES presents an architectural model through fog computing and a performance comparison with existing cloud services [17].

In addition to fog computing, research is being conducted to construct Internet of Things services through various configuration models. Baghli et al. Have proposed a 3-layer architecture for non-standard IoT services [18], and resource-based service composition methods using RESTful architecture are also being studied through various protocols [19][20]. Linthicum proposes a method of constructing a service to increase the responsiveness of IoT service through edge computing and fog computing [21]. Anumala et al. Proposed a configuration in which each device is in charge of distributed processing through a distributed architecture through peer-to-peer configuration between IoT devices [22].

As such, the basic concept of fog computing is to place a fog server between services and devices and provide computing, storage, and sensing / actuating-related services on the fog server.

2.2. Structure of IDoT

Identity of Things (IDoT) registers data corresponding to user information with a specific identifier (UID) to enable effective device-to-device communication in the IoT environment [23]. Data to be registered in the UID can be defined by a specific ID of the device, and any data related to the user can be handled and thereby accurately identified.

[Figure 3] is the structure of IDoT that borrows the concept of Identity of Users (IDoU) used in traditional systems and networks. This structure is divided into inheritance, association, knowledge, and context.

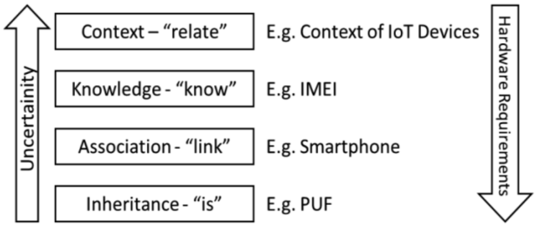


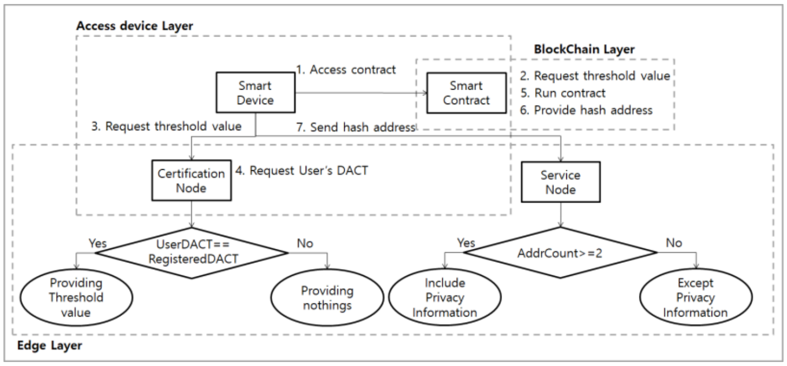
Figure 3. Identity in the internet of things

[Figure 3] "inheritance" means the same as human biometrics (fingerprint or retina). The use of biometrics is a PUF (Physical Unclonable Function), which has been used only in fields requiring strong security [4]. IoT devices are given personal gateways like smartphones, which are connected through "association." This transfers data to the cloud via predefined smartphones.

3. Threshold-Based access control using IDoT attributes

The system presented in this paper utilizes the smart contract function of blockchain to securely share transaction information. Processes in the blockchain layer can be broadly divided into Access network for Sensor Information, Transaction creation, and Provide Sensor Information.

A user attempts to access the network with a smart device to share transaction information. User accesses Smart Contract created by others. It runs by using the threshold value set in Smart Contract and accesses the fog network by using provided hash address. If the number of hash addresses owned at the time of access is 2 or more, all the threshold values of the smart contract are satisfied, and thus information including privacy information is provided.



DACT: Dynamic Access Control Table

Figure 4. Threshold-based smart contract process at the blockchain layer

[Figure 4] are largely divided into Access device Layer, BlockChain Layer, and Edge Layer. The access device layer is for users who want to access shared data using smart devices, and the blockchain layer is configured for data access and security. The edge layer is configured to provide data by identifying users accessing the data.

The threshold-based smart contract process in the blockchain layer is as follows.

(1) The user accesses the Smart Contract using the Smart Device.

(2) Smart Contracts require thresholds to drive contracts.

(3) the user requests a threshold from the Certification Node.

(4) The Certification Node requests IDoT information from the user. The Certification Node calculates the width of the pentagram following five IDoT information. If the width of the pentagram matches the value between the maximum and minimum widths of the registered pentagon, it is judged as an access approval. If approved, the threshold is provided to the user.

(5) The user runs the Smart Contract using the threshold.

(6) Receive hash address of shared data from Smart Contract.

(7) Deliver to service node providing shared data. The received Service Node shares data with the owner’s private information when the number of received hash addresses is two or more.

4. Analysis of the proposed system

The user sends a fingerprint, the access time, the location, the IMEI, and the access gateway values of the IDoT to the edge to access the shared data, and the edge determines whether the corresponding data values fall within the pentagon width threshold. It transfers the condition value of the smart contract as a means of granting access right after judgment. The user can run the smart contract using the received condition value and obtain the desired data.

In the blockchain-based IoT environment, we compared and analyzed users’ access control aspects. Comparative analysis consists of access control policy, types of access data, and data processing speed.

The IoT system, the BIoT, and a hybrid system [23] use two types of data for access control policy, but this paper expands and analyzes five types: fingerprint, time, place, IMEI, and access gateway.

The IoT system [25] controls user access using an ID and password, and the BIoT [26] and the hybrid system [27] control user access using an access control account and a secret key. This paper collects five pieces of real-time IDoT attribute information. After the five types of data are displayed in graph form, it is determined whether the width of the pentagon formed by the five types of data falls within the threshold, and then, the policy for determining access approval is applied.

The IoT system [25] has a centralized layer for determining whether to approve access, so the processing speed becomes slower as traffic increases. The BIoT [26], the hybrid system [27], and the one in this paper can slow down transaction processing because they have to go through a consensus process, but the process in this paper can determine the accessibility of nearby users at the edge to satisfy security.

In terms of security, the IoT system [25] has a low level due to the simple user access control method, and the BIoT [26] and hybrid system [27] have high security by using a secret key. This paper combines high security and flexibility of user access control by using five pieces of data from IDoT layer 4.

Table 1. Comparative analysis of previous studies and this paper

	IoT [25]	BIoT [26]	Hybrid [27]	This paper
Smart contract	×	○	○	○
Access control policy	ID/ password	Use account / secret key	Use account / secret key	IDoT layer 4 data
Amount of access data	2	2	2	5
Security	Low security	High security	Secured private blockchain	High security and flexibility of access control
Data processing speed	Fast processing when offline	Fast processing, even with many users	Slow processing speed (private + public) due to	Fast processing, even with many users

In this paper, we designed an IDoT-based threshold-based access control architecture as a condition for executing smart contracts. In addition, the user's access is flexibly configured by defining the static and dynamic attributes of the IDoT as thresholds.

5. Conclusion

In this paper, by linking the attributes of things with ID, it is possible to provide various smart services that are connected in the future. In order to share transaction information collected from things in BIoT structure, we designed a new access control structure that only authorized users can execute smart contracts using various IDoT attribute values. To this end, IDoT's four levels of data were classified into five categories to define threshold ranges and flexible access control for users. The accessor's fingerprint, device's IMEI, access gateway, and accessor's access time and location information are compared with the DACT registered by the accessor. The task of controlling the user's access is handled through fog computing at the edge layer in consideration of the traffic problems in the IoT environment. In addition, the traffic problem of rapid increase in users is designed to handle access authorization decision at the edge stage, not the cloud. And we measured the area by forming a pentagon based on five IDoT Information. It can control the accessor through the size of the area and compared this method with previous studies.

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] David W. Cearley, Brian Burke, Samantha Searle, and Mike J. Walker, "Top 10 strategic technology trends for 2018," Gartner, **(2017)**

[2] Statis Research Department, "Internet of Things - number of connected devices worldwide 2015-2025," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, **(2016)**

[3] Tragos Elias, Pöhls Henrich, Staudemeyer Ralf, Slamanig Daniel, Kapovits Adam, Suppan Santiago, Fragkiadakis Alexandros, Baldini Gianmarco, Neisse Ricardo, Langendoerfer Peter, Dyka Zoya, and Wittke Christian "Building the Hyperconnected Society," River Publishers, **(2015)**

[4] Alex Jinsung Choi, "Internet of things: Evolution towards a HyperConnected Society," IEEE Asian Solid-State Circuits Conference, **(2014)** DOI: 10.1109/ASSCC.2014.7008846,

[5] Hao Yin, Dongchao Guo, Kai Wang, Zexun Jiang, Yongqiang Lyu, and Ju Xing, "Hyperconnected network: A Decentralized Trusted Computing and Networking Paradigm," IEEE, **(2018)**

[6] Wikipedia, "Hyper connectivity," https://en.wikipedia.org/wiki/Hyperconnectivity, **(2019)**

[7] Kim Kwang-seok, Kwon Bo-ram, and Choi Yeon-kyung, "The fourth industrial revolution and hyper-connected society, changing future industry," KPMG Samjung, **(2017)**

[8] Wikipedia, "Mirai malware," https://en.wikipedia.org/wiki/Mirai_(malware), **(2019)**

[9] IBM, "Watson IoT and Blockchain Disruptor and game changer," **(2016)**

[10] Hugh Ujhazy and Simon Piff, "Blockchain Implications for Internet of Things," IDC, **(2017)**

[11] Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, and Antônio A. de A. Rocha, "A survey of how to use blockchain to secure Internet of things and the stalker attack," Hindawi, Security and communication Networks, **(2018)** DOI: 10.1155/2018/9675050

[12] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of things," Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp.13-16, **(2012)** DOI: 10.1145/2342509.2342513

[13] A. V. Dastjerdi and R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential," in Computer, vol.49, no.8, pp.112-116, **(2016)** DOI: 10.1145/2342509.2342513

[14] M. W. Condry and C. B. Nelson, "Using smart edge IoT devices for safer, rapid response with industry IoT control operations," Proceedings of the IEEE, vol.104, no.5, pp.938-946, **(2016)** DOI: 10.1109/JPROC.2015.2513672

[15] Y. Cao, S. Chen, P. Hou, and D. Brown, "FAST: A fog computing assisted distributed analytics system to monitor fall for stroke mitigation," Proceedings of the IEEE International Conference on Networking, Architecture and Storage (NAS), pp.2-11., **(2015)** DOI: 10.1109/NAS.2015.7255196

[16] V. Stantchev, A. Barnawi, and S. Ghulam, "Smart Items, Fog and Cloud Computing as Enablers of Servitization in Healthcare," International Journal of Sensors & Transducers, vol.185, no.2, pp.121-128, **(2015)**

[17] J. Li, J. Jin, D. Yuan, M. Palaniswami, and K. Moessner, "EHOPES: Data-centered Fog platform for smart living," Proceedings of the EHOPES: Data-centered Fog platform for smart living, In Telecommunication Networks and Applications Conference (ITNAC), pp.308-313, **(2015)** DOI: 10.1109/ATNAC.2015.7366831

[18] R. B. Baghli, E. Najm, and B. Traverson, “Towards a Multi-Leveled architecture for the Internet of things,” Proceedings of the Enterprise Distributed Object Computing Workshop (EDOCW), 2016 IEEE 20th International, pp.1-6, **(2016)** DOI: 10.1109/EDOCW.2016.7584391

[19] Dominique Guinard, Vlad Trifa, Friedemann Mattern, and Erik Wilde, “From the Internet of things to the web of things: Resource-oriented architecture and best practices,” International Journal of Architecting the Internet of Things, pp.97-129, **(2011)** DOI: 10.1007/978-3-642-19157-2_5

[20] Luigi Atzori, Antonio Iera, and Giacomo Morabito, “The internet of things: A survey,” International Journal of Computer networks, vol.54, no.15, pp.2787-2805, **(2010)** DOI: 10.1016/j.comnet.2010.05.010

[21] D. Linthicum, “Responsive data architecture for the Internet of things,” International Journal of Computer., vol.49, no.10, pp.72-75, **(2016)** DOI: 10.1109/MC.2016.302

[22] H. Anumala and S. M. Busetty, “Distributed device health platform using Internet of things devices,” Proceedings of the 2015 IEEE International Conference on Data Science and Data Intensive Systems(DSDIS), pp.525-531, **(2015)** DOI: 10.1109/DSDIS.2015.110

[23] Reyna Ana, Martín Cristian, Chen Jaime, Soler Enrique, and Díaz Manuel, “On blockchain and its integration with IoT. Challenges and opportunities,” Future Generation Computer Systems, vol.88, pp.173-190., **(2018)** DOI: 10.1016/j.future.2018.05.046

[24] Kwok-Yan Lam, and Chi-Hung Chi, “Identity in the Internet-of-Things (IoT): New Challenges and Opportunities,” Information and Communications Security, ICICS 2016, Lecture Notes in Computer Science, vol.9977, **(2016)** DOI: 10.1007/978-3-319-50011-9_2

[25] NICOLA BAROZZI, “17 blockchain disruptive use cases,” http://www.nicolabarozzi.com/blockchain/-8/11/2016-17-blockchain-disruptive-use-cases, Accessed: 2018-02-01., **(2016)**

[26] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol.4, pp.2292-2303, **(2016)** DOI: 10.1109/ACCESS.2016.2566339

[27] M. Aazam and E.-N. Huh, “Fog computing and smart gateway based communication for cloud of things,” 2014 International Conference on Future Internet of Things and Cloud, Barcelona, pp.464-470, **(2014)**