Hierarchical Trust Chain Framework for IoT Services

Hoan-Suk Choi*, Gyu Myoung Lee†, Woo-Seop Rhee*
*Department of Multimedia Engineering
Hanbat National University, 34158, Daejeon, Korea
Email: hkrock7904@gmail.com, wsrhee@hanbat.ac.kr
† Department of Computer Science
Liverpool John Moores University, Liverpool, L3 3AF, UK
Email: g.m.lee@ljmu.ac.uk

***Abstract*—**To support blockchain enabled Internet of Things (IoT) services, a lightweight approach is necessary in order to reduce the processing overhead and memory redundancy. We propose the hierarchical trust chain framework for secured and reliable IoT service provisioning, which consists of local trust chains and global distributed trust chain for scalable and trusted IoT services. The proposed framework provides the time slot based delayed verification algorithm and the blockchain configuration method based on the trust analysis mechanism.

Keywords—IoT Service; Trust chain; Trust; Blockchain; Hierarchical architecture;

I. INTRODUCTION

The recent technical evolutions of the Internet of Things (IoT) enabling interconnecting a large number of devices can provide very convenient and intelligent services in many application domains (e.g., home, office, factory and farm, etc.) in our daily life. But, the security and privacy problems still remain two of the main challenges in IoT environments, threatening user trust [1]. Also, the existing IoT platform-based centralized environments have scalability problems. Therefore, there are some ongoing researches which applied blockchain technologies to solve the security and scalability problems [2]. The blockchain technology provides hashed chain structure, distributed ledger and Public Key Infrastructure (PKI) based authentication and encryption to ensure the trust of distributed blockchain networks [3]. Exchange of value between nodes is a transaction. Successful transactions need to be fast, precise and easily agreed on by nodes participating in the transaction. As each transaction occurs and the nodes agree to its details, it's encoded into a block of digital data and uniquely signed or identified. Blocks are chained together to create an immutable chain, preventing any block from being altered or a block being inserted between existing blocks [4].

However, authors in [5] argued that adopting blockchain in IoT is not straightforward and entail several significant challenges. High resource demand for solving the Proof of Work (POW), long latency for transaction confirmation, low scalability that is a result of broadcasting transactions and blocks to the whole network. Thus, according to increasing transactions and size of the network, the efficiency of the blockchain dramatically decreases. In addition, as all nodes have to store the same blocks, it results in increasing block capacity and consuming a lot of storage space. Therefore, a distributed chain system with lightweight, secured and privacy preserving features is needed for IoT services.

In this paper, we propose the hierarchical trust chain framework for secured and reliable IoT service provisioning. The proposed framework has a two tiers trust chain structure which consists of the local trust chains and the global distributed trust chain. The local trust chain is managed by a decentralized local IoT network and it provides IoT home/office/factory services. The global distributed trust chain is managed by a distributed network which doesn't need fully meshed and it provides trusted services through logical trust service chains among multiple stakeholders in order to cope with sharing economy as collaborative consumption-based initiative. These two-tier trust chains act similar to blockchain respectively but are managed by the trust analysis mechanism, which is manipulated by trust information, to reduce blockchain processing overhead. In our previous work [6], we proposed the trust management system and resource model for social IoT based resource sharing services. It described relationship, trust profile, and usage information to evaluate trustworthiness. Also, [7] proposed a trust computation model for social IoT. It enables objects in social IoT to build associations in a trustworthy manner. A numerical model is developed to estimate trust of each object based on recommendation and reputation parameters. Based on these previous works, we can measure a level of trustworthiness of service components as well as participants and configure a trust chain based on authorized targets.

II. TWO-TIER TRUST CHAIN NETWORK CONCEPT

To provide trusted IoT services, the proposed trust chain networks consist of a two tiers structure between chain networks; the IoT device networks and the Distributed Trust Chain Edge Node (DTCEN) network. The IoT device networks contain the local trust chains and the DTCEN network contains the global distributed trust chain. Fig. 1 shows a layered concept of the proposed trust chain networks.

A. IoT Device Networks

The IoT device network includes various IoT devices as a local peer-to-peer network that is configured to provide various types of IoT services depending on specific domains (e.g., home IoT, office IoT and factory IoT, etc.). Each IoT domain has an IoT trust agent that manages all devices in a domain. To provide IoT services in a local domain, real-time data

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: NRF-2017R1D1A1B0303 5517)

collection, monitoring, access, store and control are very essential.

Therefore, the IoT trust agent requires the following functions; IoT data collection, trusted data generation from the collected data, the trust-based authentication and admission control of IoT devices, a trust evaluation algorithm, a local trust chain verification mechanism and local trust chain ledger management for the secured private chain.

B. Distributed Trust Chain Edge Node Network

In the DTCEN network, each DTCEN operates as a peer which configures the global distributed trust chain physically to connect between IoT service domains. An IoT service domain connected to the nearest DTCEN. It performs a lightweight verification algorithm to register and maintain transactions delivered across the multiple domains.

Therefore, DTCEN provides the following functions; distributed ledger management, a trust evaluation algorithm, security data block generation for transaction, a global distributed trust chain verification mechanism, service authentication and smart contract execution for the trust service chain.

The trust service chains are the overlay configured logical chains on top of DTCEN network to provide various application services. Application services can be provided by devices and users of the multiple domains. So, transactions, blocks and trust information sharing mechanisms across the multiple domains between the two layers are required.

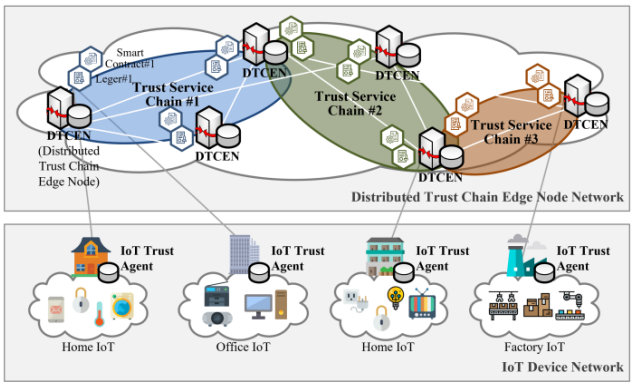

Fig. 1. Proposed two tiers trust chain networks with a layered concept.

III. HIERARCHICAL TRUST CHAIN FRAMEWORK

In this section, we propose the hierarchical trust chain framework with the local trust chains and the global distributed trust chain for scalable and trusted IoT services as shown in Fig. 2. The local trust chain provides a lightweight verification mechanism for real-time transaction processing for each IoT service and the global distributed trust chain can ensure trustworthiness of the logical trust service chains through the lightweight blockchain configuration method.

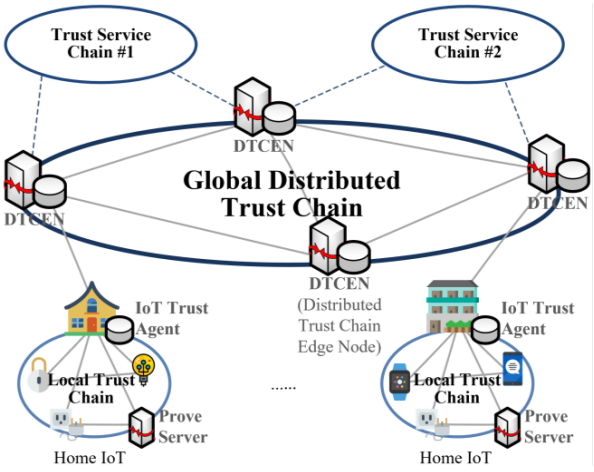

Fig. 2. A configuration model of hierarchical trut chains.

A. Local Trust Chain

The local trust chain is a private permissioned chain. The permissioned IoT devices by the trust analysis mechanism can join to a private chain. So, as the permitted peers (devices) in this local chain are trustable basically, it aims to ensure trustworthiness by the proposed lightweight verification algorithm rather than a complicated full-stack POW algorithm. For the trust analysis mechanism, the following trust information is used for determining a level of trustworthiness about a participant:

- Trust information for an IoT device includes the PKI certificate of a permissioned IoT device, the transaction creation number, the verified block number, etc.
- Trust information for an IoT trust agent and a prove server includes the transaction response rate, the transaction verification success rate, etc.

The proposed framework provides the verification algorithm for local trust chains as shown in the Fig. 3. An IoT trust agent and a prove server maintain transactions and blockchains per an IoT device. All devices generate a transaction and send it to the IoT trust agent and the probe server simultaneously. The IoT trust agent and the prove server check the integrity of this transaction using the shared key and a hash mechanism. After exchanging the checked results from each other, if the transaction data and its checked results are the same, the transaction is verified and added to a new block.

IoT services should be operated/updated at real-time. So, we propose the time-slot based delayed verification algorithm for local trust chains. The transaction occurring in a time slot T1 is verified upon in the next time slot, T2 to maintain the synchronization between transactions. As the nature of the IoT services, where many transactions occur in a short time, the IoT trust agent and the prove server add only the last verified transaction data to the block at the end of a time slot. This algorithm prevents from logical errors between several transactions and reduces block capacity and processing speed of block additions.

To maintain a certain level of trustworthiness of transactions and blocks from external attacks, parts of the existing blockchain solutions are applied. Each device is authenticated based on a PKI. Verified transactions are added to the new block including the hash value of the previous block. The generated blocks are stored in the IoT trust agent and the probe server respectively. Therefore, the shared key and the hash mechanism ensure security, privacy and trust of IoT devices, transactions and blocks. To reduce the block generation processing overhead, only filtered transactions are moving on to verification processing stage.

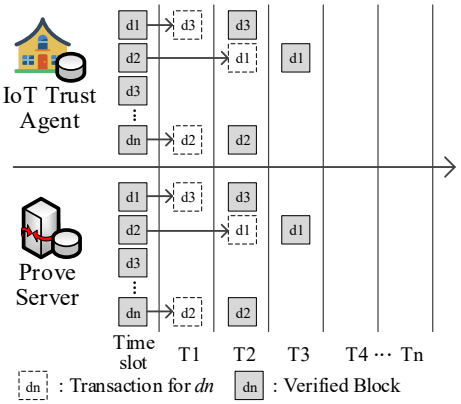

Fig. 3. Time slot based delayed verification algorithm for local trust chains.

B. Global Distributed Trust Chain

The global distributed trust chain is a private chain. It has the distributed features but does not need a full meshed structure, because the permissioned node using the trust analysis mechanism can only join to a private chain. To determine a level of trustworthiness, all nodes maintain the trust information of neighbor nodes, for example, the shared key about an edge node, the transaction creation number, transaction response rate and transaction verification success rate, etc.

Fig. 4 shows the proposed blockchain configuration method for the global distributed trust chain. Every node sends/receives the transaction and block to/from its neighbor nodes for the transaction verification and maintains the blockchain per a neighbor node. For example, Node B stores a copy of the blockchain data created by the neighbor nodes A, C, D and its own blockchain data of the directly connected internal chain. Blocks are appended to the blockchain without processing the POW, Therefore, the proposed mechanism significantly reduces the processing overhead and memory redundancy.

Trust service chains are configured in a form of overlay on top of the global DTCEN networks according to different types of IoT services. Initially, an edge node (i.e., DTCEN) sends the registration message and its trust information to neighbor nodes for registering to the trust service chain. If an edge node receives response messages from its neighbor nodes with trust information, it maintains trust information and block information of neighbor nodes.

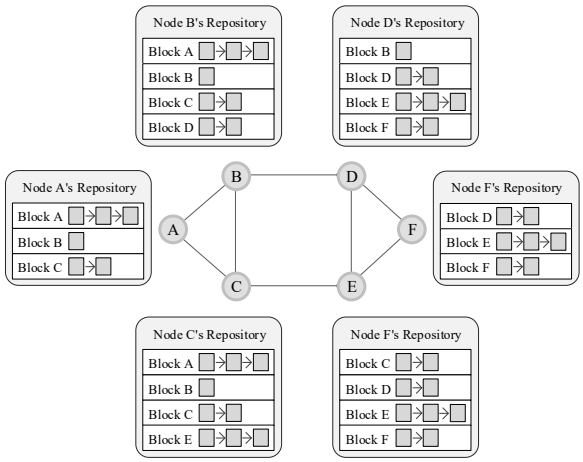

Fig. 4. Blockchains configuration method for the global distributed trust chain.

IV. Conclusion

As the IoT network has increased, the existing IoT service environments have security, privacy and scalability problems. In this paper, we have proposed the hierarchical trust chain framework with the local trust chains and the global distributed trust chain. To employ lightweight blockchain solutions for scalable and trusted services in the constraint IoT environments, we have proposed the timeslot-based delayed verification algorithm using the trust analysis mechanism for real-time transaction processing in local trust chains and the block chain configuration method in global distributed trust chain for improving efficiency.

For further research, we will focus on the development of enhanced trust analysis mechanisms including a trust evaluation and manipulation method for IoT devices and DTCENs as well as the performance evaluation of the proposed verification method.

References

[1] K. Christidis and M. Devetsikiotis, “Blockchain and smart contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp.2292-2303, June 2016.

[2] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab and L. Maglaras, “Blockchain technologies for the Internet of Things: research issues and challenges,” *IEEE Internet of Things Journal*, November 2018.

[3] T. M. Fernandez-Carames and P. Fraga-Lamas, “A review on the use of blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32979-33001, July 2018.

[4] IBM, “What is blockchain?,” Available: https://www.ibm.com/blockchain/what-is-blockchain.

[5] Ali Dorri, Salil S. Kanhere, Raja Jurdaky and Praveen Gauravaram, “Blockchain for IoT security and privacy: The Case Study of a Smart Home,” *IEEE PerCom2017* workshop on security privacy and trust in the internet of thing, March 2017.

[6] H. S. Choi and W. S. Rhee, “Social based trust management system for resource sharing service,” In Proceedings of the 2nd International Conference on Intelligent Systems, Metaheuristics & Swarm Intelligence (*ISMSI '18*). ACM, pp. 148-152, March 2018.

[7] U. Jayasinghe, N. B. Truong, G. M. Lee and T. Um, "RpR: a trust computation model for social Internet of Things," *IEEE UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld*, July 2016.