Empowering Blockchain For Secure Data Storing in Industrial IoT

Muhammad Firdaus* and Kyung-Hyune Rhee**

*Department of Information Security, Graduate School
Pukyong National University

**Department of IT Convergence and Application Engineering
Pukyong National University

e-mail: mfirdaus@pukyong.ac.kr, khrhee@pknu.ac.kr

Abstract

In the past few years, the industrial internet of things (IIoT) has received great attention in various industrial sectors which have potentially increased a high level of integrity, availability, and scalability. The increasing of IIoT is expected to create new smart industrial enterprises and build the next generation smart system. However existing IIoT systems rely on centralized servers that are vulnerable to a single point of failure and malicious attack, which exposes the data to security risks and storage. To address the above issues, blockchain is widely considered as a promising solution, which can build a secure and efficient environment for data storing, processing and sharing in IIoT. In this paper, we propose a decentralized, peer-to-peer platform for secure data storing in industrial IoT base on the ethereum blockchain. We exploit ethereum to ensure data security and reliability when smart devices store the data.

1. Introduction

The integration of IoT and industry, also known as the industrial internet of things (IIoT) has received great attention in various industrial sectors which has potential increasing a high level of integrity, availability, and scalability. The increasing IIoT is expected to produce extraordinary economic growth opportunities by conducting digital transformation to create new smart industrial enterprises and build the next generation smart system in many areas, including manufacturing, energy, transportation, agriculture, retail, and many more.

However existing IIoT systems rely on centralized servers for data storing, processing and sharing are vulnerable to a single point of failure and malicious attack, which exposes the data to security risks and storage [1]. Therefore, data security becomes critical concerns for IIoT [2]. To address the above issues, blockchain is widely considered as a promising solution, which can build a secure and efficient environment for data storing, processing, and sharing in IIoT [3], [4]. Blockchain can be a decentralized cloud storage network that has been introduced with many advantages over the datacenter-based storage.

In this paper, we propose a decentralized, peer-to-peer platform for secure data storing in industrial IoT base on ethereum blockchain. We exploit ethereum to ensure data security and reliability when smart devices store the data since ethereum can effectively maintain a tamper-proof ledger shared by the participating smart devices without the need of a trusted third central organization. The rest of this paper is organized as follows. We present the related works concerning the IIoT system and blockchain technology. Then, we describe the system that empowering blockchain for securing data storage in the IIoT system. Finally, we conclude this paper.

2. IIoT and Blockchain

The past years have witnessed the rapid development of the IIoT, which is reshaping various industrials such as agriculture, environmental monitoring, and security surveillance [5]. The IIoT system which consists of smart devices is adequate for using sensors to collect data around or using embedded cameras to capture the images or videos, which should be captured and stored or processed securely. In [6], the authors provided several research opportunities and challenges such as using cryptography and other techniques to ensure privacy and security in IIoT. Shrouf et al. [7] presented a reference for IoT-based smart factories' architecture and they decide the main characteristics of the factories especially from the perspective of sustainability.

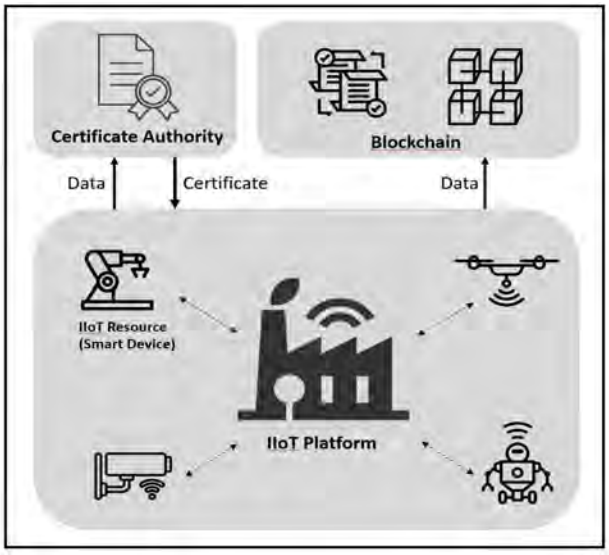
In 2008, Nakamoto proposed a peer-to-peer (P2P) digital currency system named bitcoin for economic transactions based on blockchain technology [8]. Blockchain can guarantee data security and efficiency by enabling anonymous and trustful transactions and removing all kinds of intermediaries. Refers to [9], authors discuss the possibilities of integrating blockchain into IoT applications, called BIoT. They provide a detailed analysis of the important aspects of the development of BIoT applications.

3. Blockchain-based for Secure Data Storing in IIoT

We consider a blockchain-enabled IIoT system, which consists of two stages, the authentication of the IIoT smart devices which will collect the data with sensing tasks and blockchain system that guarantees data storing in a distributed ledger and secure manner.

3.1 Smart Devices Authenticated in IIoT Network

In this scheme, each smart device registers to the certificate authority (CA) and obtains its public and private keys (pk^m, sk^m), $\forall m \in M$, to become an authenticated smart device. The private key is used to encrypt data to ensure that collected data sent to the blockchain network is valid and can not be forged. Next, the smart device will send it to the CA, which will check whether the data come from a legitimate smart device and data is real. After verification, the signature of CA and encrypted data will return to the smart device, and can be sent to the blockchain as a storage request.



(Figure 1). System Model

3.2 Blockchain-Enabled Secure Data Sharing

The blockchain is capable to securely exchange and store the data from components in IIoT systems without the need for an intermediary. Smart devices generate transactions using its sensor to collect data, which should be captured and stored securely. Eventually, these transactions are relayed to blockchain systems for storing the data into/from the distributed ledger, i.e. the underlying blockchain. We exploit ethereum as required data storage service and build a private blockchain, which includes $N\ \{n = 1, 2, N\}$ Ethereum nodes for storing and sharing data. We then classify them into the following two categories.

1) Mining Nodes: They are used to verify data sharing transactions and compile them into

Algorithm 1: Blockchain-Enabled Secure Data Storing Among Smart Devices

1. Initialize private blockchain and setup N Ethereum nodes;
2. Deploy smart contract on blockchain;
3. Blockchain start mining;
4. **for** SD m in M **do**
5. Run Gen (1^n) to obtain (pk^m, sk^m);
6. CA stores identity (m, pk^m);
7. **end for**
8. **for** SD m in M **do**
9. Collect data ;
10. Generates data collection (U_m);
11. Hash collected data H (U_m);
12. Send { U_m,$Sign\ sk^m H(U_m)$} to CA ;
13. **if** $Vrfy$ $pk^m\{U_m || Sign\ sk^m H(U_m)\} == 1$ **then**
14. **if** $U_m == collection[m]$ **then**
15. $U_m^* = Sign\ sk^m\{H(U_m)\}$;
16. Return $\{U_m, Signsk^{CA}(U_m^*)\}$ to SD m;
17. **end if**
18. **end if**
19. **if** SD m receives signature from CA **then**
20. Send transaction request $\{U_m, Signsk^{CA}(U_m^*), pk^m\}$ to blockchain;
21. **if** verifiy signature and identity is true **then**
22. Upload transaction to blockchain and wait for confirmation ;
23. **end if**
24. **end if**
25. **end for**

blocks. They need to consistently use machine computing resources to solve computing problems and submit blocks to the blockchain network.

2) Non-mining Nodes: Since the non-mining node is only responsible for receiving and broadcasting data sharing transaction request, it does not need the same amount of resources if compared to a mining one.

4. System Model

We explain the whole process of secure data storing among smart devices by using pseudo-code in Algorithm 1. As shown in Algorithm 1, to be more specific, we first run Gen (1^n) to generate public and private keys pair (pk^m, sk^m) for each smart device (SD), where 1^n is a security parameter (Line 5). And CA would store SDm id and public key (m, pk^m) in a list (Line 6). SDs starts to collect data using different kind of sensors. After the end of collecting data, SDs will send their data collection (U_m) and signature to CA (Line 9-12). CA can decrypt it and judge whether it is the SDs m data according to the result $Vrfy$ $pk^m\{U_m, Sign\ sk^m H(U_m)\}$. If the result is 1, the request is sent by SDm, otherwise not. Besides, after decryption, it is also necessary to compare U_m with the data on the device itself to avoid fake data. Therefore, if $Vrfy$ $pk^m\{U_m, Sign\ sk^m H(U_m)\} = 1$ and U_m = collection[m], then CA will add its signature to the request and return it to the SD m (Line 13-18). SD can package the request $\{U_m, Sign\ sk^{CA}(U_m^*), pk^m\}$, then send it to the blockchain. After non-mining nodes receive transaction requests from SD, blockchain will verify the signature on the request and decide whether to submit the transaction to the blockchain network based on the verification results (Line 26-28). The submitted transaction will be mined and written in a new block by mining nodes.

5. Conclusions

We presented a blockchain platform for secure data storing in industrial IoT. Smart devices generate transactions by collecting data using its sensors. These transactions are relayed to blockchain systems for storing the data into the distributed ledger. We propose ethereum as the required data storage service and build a private blockchain, which includes mining nodes to verify data sharing transactions and non-mining nodes for receiving and broadcasting sharing transactions.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2018R1D1A1B07048944) and partially was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information

Technology Research Center) support program (IITP-2020-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation)

[References]

[1] Do, H.G. and Ng, W.K., 2017, June."Blockchain-based system for secure data storage with private keyword search," in 2017 IEEE WorldCongress on Services (SERVICES) (pp. 90-93). IEEE.

[2] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang,"Consortium blockchain for secure energy trading in industrial Internet of Things," IEEE Trans. Ind. Inform., vol. 14, no. 8, pp. 3690 - 3700, Aug. 2018.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congr. Big Data, Honolulu, HI, USA, Jun. 2017, pp. 557 - 564.

[4] W. Chen, M. Ma, Y. Ye, Z. Zheng, and Y. Zhou, "IoT service based on jointcloud blockchain: The case study of smart traveling," in Proc. IEEE Symp. Service-Oriented Syst. Eng., Bamberg, Germany, Mar. 2018, pp. 216 - 221.

[5] H. Liu, Y. Zhang, and T. Yang, "Blockchain enabled security in electric vehicles cloud and edge computing," IEEE Netw. Mag., vol. 32, no. 3, pp. 78 - 83, May/Jun. 2018.

[6] K. K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: Research challenges and opportunities," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3567 - 3569, Aug. 2018.

[7] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm," in Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage., 2015, pp. 697 - 701.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bit- coin.pdf

[9] Fernández-Caramés TM, Fraga-Lamas P. "A Review on the Use of Blockchain for the Internet of Things." in IEEE Access. 2018 May 31;6:32979-3001.