SUGISAKA MASANORI

Journal of Robotics, Networking and Artificial Life
Vol. 9(3); December (2022), pp. 240–244
ISSN (Online):2352-6386; ISSN (Print):2405-9021
https://alife-robotics.org/jrnal.html

Research Article

Cross-organizational Non-repudiation Industrial Control Log System Based on Blockchain

I-Hsien Liu[1], Yao-Chu Tsai[1], Chu-Fen Li[2], Jung-Shian Li[1]

[1]Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University, No.1, University Rd., East Dist., Tainan City 701401, Taiwan
[2]Department of Finance, National Formosa University, No. 64, Wenhua Rd, Huwei Town, Yunlin County 632301, Taiwan

ARTICLE INFO

Article History
Received 03 November, 2021
Accepted 11 September 2022

Keywords
ICS security
Data integrity
Blockchain
Log verification

ABSTRACT

Industrial control system (ICS) and critical infrastructure have become increasingly dependent on cyber-physical systems nowadays. Since ICS network is vulnerable to adversarial attacks, building secure operation mode is essential. In order to secure the integrity of data in ICS, this paper proposes a blockchain-based log system implemented on physical industrial equipment. Applying cross-organizational blockchain transaction mechanism in the specialized master-slave network model, industrial control transmission logs can be verified and non-repudiation

1. Introduction

With the development of automation and network communication in modern manufacturing technology, the concept of Industry 4.0 has been proposed in recent years, also known as the Fourth Industrial Revolution. The Industrial Internet of Things (IIoT) is one of the widely researched issues. The purpose is to innovate in the industrial economy, construct a smart-conscious industrial environment, and develop smart factories with adaptability, resource efficiency and human-machine collaborative engineering.

Critical infrastructure (CI) is related to Industrial Control System (ICS) which contains various kinds of IIoT. Security and reliability of ICS has become a concern of government as well as industry. In 2019, The Department of Homeland Security, United States published “A Guide to a Critical Infrastructure Security and Resilience” to regard CI security as national security [1]. ICS relies on secure data collection and transmission to avoid damage. As a subgroup of ICS, Supervisory Control and Data Acquisition (SCADA) system is composed of hardware and software to implement data storage, processing, and communication. For instance, Programmable logic controller (PLC) is one of operating component in SCADA, which transmits signal among manufacturing equipment and machines, serving as a fundamental part in cyber-physical system [2].

PLC is basically a terminal device that can online control low-level I/O devices, such as sensors or motors, and usually connects to the PC via Ethernet to embed program. As a kind of embedded system on the Industrial

Corresponding author’s E-mail: ihliu@cans.ee.ncku.edu.tw, yctsai@cans.ee.ncku.edu.tw, chufenli@gmail.com, jsli@mail.ncku.edu.tw
www.ncku.edu.tw, www.nfu.edu.tw

Internet, it is exactly at the risk of encountering network attacks. In 2021, a real incident happened in a water treatment plant in Florida. A hacker tried to remotely hack into the water purification control system with an attempt to fill a potentially harmful chemical [3].

In order to ensure the integrity of data delivery and information security, this paper designs a blockchain-based network architecture for operation logs verification in industrial control system.

2. Background

In this section, we mainly discuss a widely used ICS protocol and a type of electronic certificate for virtual assets in blockchain.

2.1. *Modbus TCP*

Modbus is one of the standard communication protocols among PLCs, and it is also commonly used in the current industrial field. Furthermore, Modbus TCP can transmit data through Ethernet TCP/IP. Because Modbus is a plaintext protocol belonging to the application layer, it is easy to be interpreted or tampered by hackers, able to conduct man-in-the-middle attack (MitM) and other malicious behaviors.

2.2. *Non-Fungible Token*

Non-Fungible Token (NFT) is a cryptocurrency based on blockchain that is often used in games and artworks Each NFT represents specific digital data with a unique code that can be stored in blockchain. Electronic files that can be easily copied in the past, such as pictures, audio files, videos, etc. They are difficult to identify whether are original files. Now digital data can be made into NFT form to get verification via blockchain transaction logs.

3. System Architecture

There is explanation of proposed method and overall framework in this section. Building a system to generate credential logs through blockchain transactions, the objective is to coordinate cross-organizational operations and leave common operation logs as evidence for auditing.

3.1. *Network Model*

The requirement on IIoT is strict due to transmission time and memory space. Most business owners tend to avoid changing or upgrading hardware because of cost and the possibility of production interruptions [4].

Modicon is a brand belonging to Schneider Electric. In 1979, Modicon announced a master-slave architecture to implement Modbus protocol. This paper refers to this framework concept and constructs a master-slave mechanism for message verification based on blockchain. For the purpose of implementing blockchain in ICS environment, we design a network architecture presented in Fig. 1. The framework is a master-slave network model imported in ICS [5].

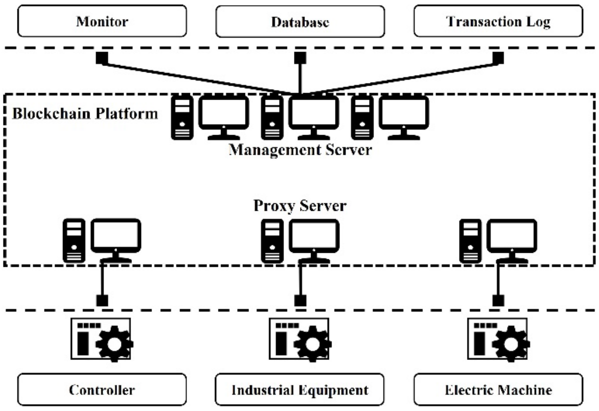

Fig. 1 Blockchain-based ICS network model

The network model explains the ICS devices, such as PLCs, industrial equipment, and electric machines, are clients of the proxy server. The proxy server connects to blockchain, so that it can communicate in a protected environment, transferring message to the ICS devices in the LAN. PC is usually used to be a proxy server, which is more suitable for fast executing blockchain programs in terms of performance. This paper makes use of the consensus certificate from a blockchain transaction to guarantee the data integrity when ICS devices transmits signals. In our architecture, the proxy server executes blockchain transactions for ICS devices.

We propose a method to wrap the Modbus contexts in a block when processing blockchain transactions. Block is a JSON file containing some transaction information, and there is an “extraData” field in it. Putting the message content of a Modbus packet in this field for the sake of transmission in blockchain, data sealed in blocks cannot be easily tampered from logs.

Combined with the immutability property of blockchain, we set a management server to efficiently protect all account information on the network and record the transaction process. With buffer storage, proxy servers regularly back up operation data read from ICS devices. And then the management server synchronizes the transaction logs stored in local proxy servers.

The master-slave architecture also makes blockchain verification mechanism compatible in ICS environment. With servers in the blockchain platform, ICS devices do not need imbedding extra software or changing setup for blockchain application.

3.2. *Blockchain-based Registration Process*

According to water resources organization structure in Taiwan, including reservoirs, dams, spillways, weirs, and clean pools, this paper plans blockchain-based registration and transaction process for cross-organizational operation.

The blockchain-based registration process we propose consists of three divisions, PLC, proxy server, and management server. The process is as follows.

- Step 1: PLC provides the Device ID to its proxy server. The objective is to ask for creating a new account in blockchain.
- Step 2: Proxy server sets up an account public key, and then requests the management server to become its peer.
- Step 3: Proxy server peers with management server and send the corresponding information to management server.
- Step 4: The management server synchronizes the account information of the proxy server.
- Step 5: The account pointing to the PLC is added in the blockchain by management server.
- Step 6: Management server returns a message to confirm the proxy server that the registration has been successful.

3.3. *Blockchain-based Transaction Process*

After finishing blockchain registration process, transactions can be launched among accounts. The blockchain-based transaction process we design mainly includes five elements, PLC A, proxy server A, PLC B, proxy server B, and management server. And the whole process can be divided into two phases.

Phase 1: Request from domain A to domain B

- Step 1: PLC A sends Modbus TCP packets to proxy server A to request authentication to access the resources of PLC B.
- Step 2: Proxy server A and proxy server B synchronizes the account information of each other.
- Step 3: Proxy server A initiates a transaction through the blockchain and transfers the Modbus TCP *message to proxy server B in the extraData field.*
- Step 4: Proxy server B accepts the transaction and signs the certificate by its private key.
- Step 5: Proxy server B takes out the Modbus TCP message in extraData field and sends it to PLC B.

Phase 2: Response from B to A

- Step 6: PLC B sends proxy server B a Modbus TCP packets to make a reply to PLC A.
- Step 7: Proxy server B initiates a transaction through the blockchain and transfers the Modbus TCP message to proxy server A in the extraData field.
- Step 8: Proxy server A accepts the transaction and signs the certificate by its private key.
- Step 9: Proxy server A takes out the Modbus TCP message in extraData field and sends it to PLC A.
- Step 10: Proxy server A and proxy server B synchronize their transaction information to the management server for transaction record backup.

4. Experiment

This paper applies blockchain to record the holding register status of a PLC using Modbus TCP query via Ethernet. Experiments are conduct in the blockchain platform based on Ethereum, generating transaction logs to be preserved in a standardized format called NFT. Containing information about ICS operation, these logs can serve as non-repudiation digital evidence. In addition, a database is created, providing transaction query to assist evidence investigation work. ICS field operation data can be collected from the management server system if it is necessary to clarify responsibilities.

The experimental environment setup is shown in Fig. 2. During online transactions among proxy servers, the

Modbus data is transferred with blockchain verification. At the end of each transaction, proxy servers peer with the corresponding management server, synchronizing their transaction logs. Making the logs into NFT for private data preservation is also applicable so that network administrator can examine all operation records. By adjusting the block generation period in genesis block, transmission time measurement can be implemented with various conditions, and the result is shown in Table 1. We found that the transmission time approximates the product of the block generation period and the number of block confirmation (B.C.).

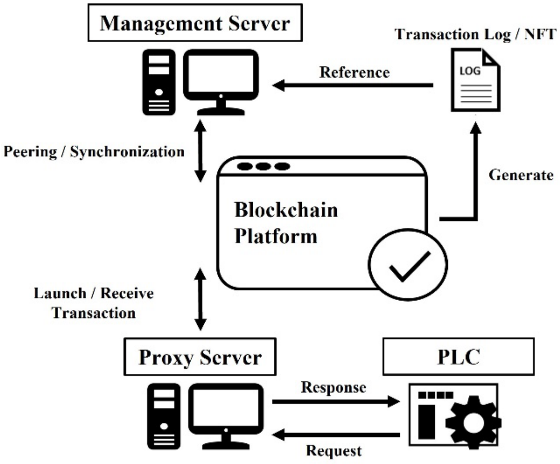

Fig. 1 Experiment environment setup

Table 1. Transmission time with different periods

Period (sec)	B. C.	Number of Transactions	Average Time (sec)	Standard Deviation (sec)
1	3	1000	3.0004	0.0524
3	2	1000	6.0008	0.0772
5	1	1000	5.0010	0.0513
10	1	1000	10.0019	0.0826
15	1	1000	15.0006	0.0561

5. Conclusion

ICS cyber security has been a research focus nowadays. For the purpose of ensuring the transmission integrity, this paper applies blockchain verification to industrial network. The designed master-slave network model would improve the adaptability of blockchain mechanism in ICS. We also plan the registration and transaction process in cross-organizational framework, conducting implementation on physical industrial equipment. The transaction logs as NFT form are eligible to become non-repudiation evidence since it is not easily tampered. Our blockchain server platform complies with the coordination of ICS devices and IT management system.

Acknowledgements

This work was supported by the Ministry of Science and Technology (MOST) in Taiwan under contract numbers MOST 110-2218-E-006-013-MBK and MOST 111-2218-E-006-010-MBK.

References

1. F. Enayaty-Ahangar, L. A. Albert, and E. DuBois, “A survey of optimization models and methods for cyberinfrastructure security,” *IISE Transactions*, vol. 53, no. 2, pp. 182-198, 2020.
2. A. Ghaleb, S. Zhioua, and A. Almulhem, “On PLC network security,” *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 62-69, 2018.
3. CNN, “Florida water treatment facility hack used a dormant remote access software, sheriff says,” [Online]. Available: https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html. [Accessed May. 26, 2021].
4. G. Bonney, H. Höfken, B. Paffen, and M. Schuba, “ICS/SCADA Security Analysis of a Beckhoff CX5020 PLC,” *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Feb. 9-11, 2015.
5. C. Wu, J. Lu, W. Li, H. Meng, and Y. Ren, “Master-slave Blockchain Based Cross-domain Trust Access Mechanism for UPIOT,” *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, May. 15-18, 2020.

Authors Introduction

Dr. I-Hsien Liu

He is a research fellow in the Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU) and Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his PhD in 2015 in Computer and Communication Engineering from the National Cheng Kung University. His interests are Cyber Security, Wireless Network, Group Communication and Reliable Transmission.

Mr. Yao-Chu Tsai

He was born in Pingtung, Taiwan in 1997. He received his B.S. degree from the Department of Systems and Naval Mechatronic Engineering, National Cheng Kung University, Taiwan in 2020. He is acquiring the master's degree in Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University in Taiwan.

Prof. Chu-Fen Li

She is an associate professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European Journal of Operational Research, Journal of System and Software, International Journal of Information and Management Sciences, Asia Journal of Management and Humanity Sciences, and others.

Dr. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include wired and wireless network protocol design, network security, and network management. He is currently involved in funded research projects dealing with optical network, VANET, Cloud security and resource allocation, and IP QoS architectures. He is the director of Taiwan Information Security Center @ National Cheng Kung University. He serves on the editorial boards of the International Journal of Communication Systems.