Development of an Integrity Monitoring System for Reactor Protection System using Blockchain Technologies

Moon Kyoung Choi [a], Chan Yeob Yeun[b], Poong Hyun Seong [a*]
[a]*Department of Nuclear and Quantum Engineering, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon 34141, Korea*
[b]*Center for Cyber-Physical Systems, Electrical and Computer Engineering Department, Khalifa University, PO BOX 127788, Abu Dhabi, UAE*
[*]*Corresponding author: phseong1@kaist.ac.kr*

1. Introduction

The Instrument & Control (I&C) systems of Nuclear Power Plants (NPPs) are physically isolated from external networks and have a different operational environment from the conventional IT systems. As a result, NPPs were regarded safe from external cyber attacks. However, it was determined that the isolated networks are not safe from cyber attacks. [1]. Especially, attacks on Programmable Logic Controllers (PLCs) deployed in the safety protection system of NPPs would be critical. Cyber threats on the PLCs can cause problems related to the safety [2]. Korea Institute of Nuclear Nonproliferation and Control (KINAC), which is in charge of the NPP cyber security regulation in Korea, requests a utility to comply with cyber security controls and to perform a cybersecurity risk management based on the regulatory guide RS-015 [3].

However, there is currently no system capable of detecting malicious modification of data on PLCs in real-time. Besides, the safety systems such as a safety pump & valve do not operate in normal condition, so it is difficult to detect whether their integrity of control logic data is attacked in normal condition. Thus, it is necessary to monitor the integrity of PLC and to protect them from cyber threats such as modification of deployed logics or set points in PLCs.

In this study, cryptographic algorithm and blockchain technology are used for monitoring the tamper of PLCs. A system that monitors integrity of Reactor Protection System (RPS) using the blockchain network was developed in this study. It is the first time to apply blockchain technology to monitoring PLC integrity for plant safety.

2. Development of a private blockchain network for monitoring the data integrity of PLCs

In this section, some of the techniques used to model the detector channel are described.

2.1 Blockchain Technologies

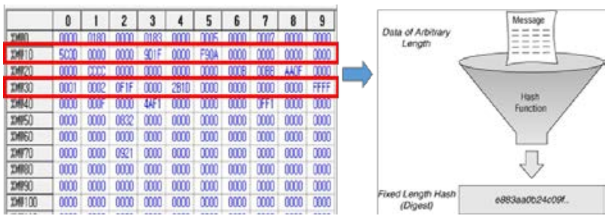
Blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable, and updateable only via consensus or agreement among peers [4]. Blockchain is a technology that is implemented by combining technologies rather than a single technology in order to prevent manipulation of data. All stored information in the distributed blockchain network is cryptographically linked block by block using Secure Hash Algorithms (SHA), which are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (a hash function) which is designed to also be a one-way function [5].

There are two types of blockchain. Public blockchain are open to the public and anyone can participate as a node in the decision-making process. Private blockchain is private and open only to a consortium or group of individuals or organizations that has decided to share the ledger among themselves. Considering NPPs network characteristics, it is more appropriate to apply a private blockchain network.

2.2 Encryption of PLC data using Secure Hash Algorithm (SHA)

In the current blockchain used in Bitcoin, it is considered that the amount of bitcoin and its transaction information should be protected and secured. In NPP cybersecurity perspective, data in PLC should be protected and secured like the bitcoin. After reading the registered data in the PLC memory, it is converted to a bit string of a fixed size through the secure hash algorithm (SHA-256) as shown in Fig 1. The hash value always has the same value if an input data is constant. If a different hash value is obtained compared to an existing hash value, it means that the data in PLCs has been modified.

The labview program was used to implement the function to read the data in PLC memory in real time.



	0	1	2	3	4	5	6	7	8	9
%MW0	0000	0180	0000	0183	0000	0005	0000	0007	0000	0000
%MW10	5C00	0000	0000	901F	0000	F90A	0000	0000	0000	0000
%MW20	0000	CCCC	0000	0000	0000	0000	0008	00BB	AA0F	0000
%MW30	0001	0002	0F1F	0000	2810	0000	0000	0000	0000	FFFF
%MW40	0000	000F	0000	4AF1	0000	0000	0000	0FF1	0000	0000
%MW50	0000	0000	0832	0000	0000	0000	0000	0000	0000	0000
%MW60	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
%MW70	0000	0000	0921	0000	0000	0000	0000	0000	0000	0000
%MW80	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
%MW90	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000
%MW100	0000	0000	0000	0000	0000	0000	0000	0000	0000	0000

Fig 1. Converting data in each memory address of PLC to hash value

2.3 Checking the modification of PLCs data using Merkle tree

A Merkle tree is a tree in which every leaf node is labelled with a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Merkle trees allow efficient and secure verification of the contents of large data structures [6]. Merkle tree method can be used to quickly check the integrity of various data. Data in each leaf node would be logic codes in PLC memory, and all the hashed data are finally combined to the one constant hash value called "Merkle root". Merkle root value could be the representative hash value about the integrity of the whole data. Although a tiny part of data is manipulated, merkle root becomes completely different. It is also possible to detect which PLC data is tempered as shown in Fig 2.

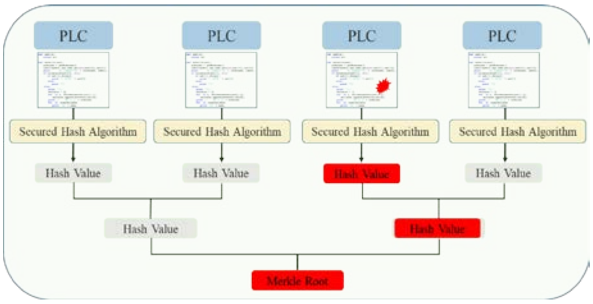


Fig 2. PLC code integrity check using merkle tree

2.4 Block structure and data of the private blockchain

Table I shows the configuration of the private blockchain. The blockchain for monitoring the data integrity of PLCs was developed in JavaScript. It consists of five nodes, and a new block is mined in every 5000ms. As consensus of the blockchain network, Proof-of-Authority was chosen. There is no need to use a proof-of-work method that is unnecessary and consumes electricity in the private blockchain network. In PoA-based networks, transactions and blocks are validated by approved nodes, known as validators. However, if the attacker identifies a validator node, data tampering is possible. Thus, the validator node is randomly selected among the total nodes in the blockchain network. Therefore, it is possible to detect which PLCs and which control logics are manipulated by cyber attack through real-time integrity check using this private blockchain, as shown in Fig 3. Data stored in the block is shown in Table II.

Table I: Configuration of the private blockchain

Program Language	Node.js (JavaScript)
# of nodes in the network	5
Transaction & Mining period	5000ms
Cryptographic algorithm	SHA-256
Consensus Algorithm	Proof-of-Authority (PoA)
Communication in network	Web API

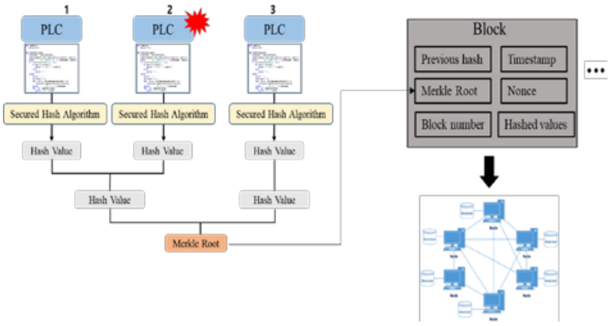


Fig 3. Private blockchain network for monitoring the data integrity of PLCs

Table II: Data stored in the block

Items	Meaning
Block number	The sequent number of the current bock, which is used as the title of the block
Previous hash result	The hash result of the previous block
Data (Transaction data)	Hash value of several PLC control logic data and log data
Merkle root	The compressed hash of all the hashed transaction data, which is the representative value for overall data integrity
Nonce	The solution of the puzzle problem for the current block
Timestamp	The time the current block was appended to the block chain
Current hash result	The hash result of the current block

3. Development of integrity monitoring system for Reactor Protection System (RPS) using the proposed blockchain network

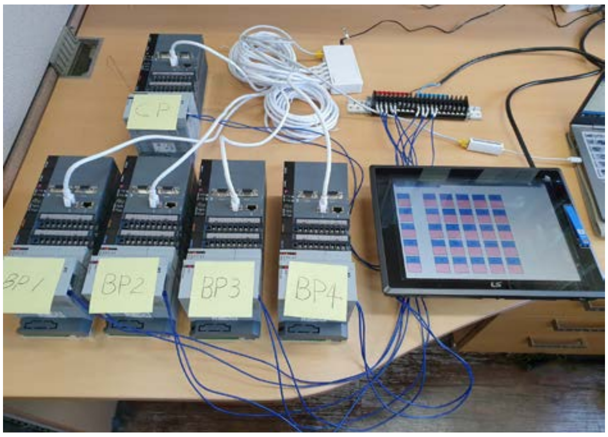


Fig 4. Prototype of integrity monitoring system for RPS using the blockchain

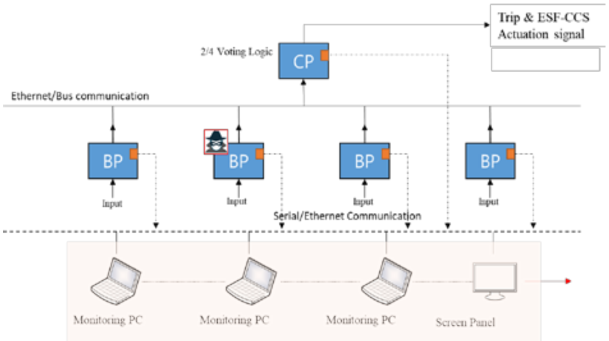


Fig 5. Detecting data modification in RPS using the blokchain network

RPS prototype consisting of four Bistable processors and one Coincidence processor as shown in Fig 4. Each PLC communicates with each other using the Modbus Ethernet protocol. Data stored in each process's memory is read in real time and stored in the proposed private blockchain network as shown in Fig 5. If an attack modulates data from a particular processor, the blockchain will store different data than before. In addition, the integrity of the PLCs can be monitored in real time through the HMI, and an alert alarm appears to allow the system manager to recognize an attack when data tampering is detected.

There is a limitation. It is impossible to develop the prototype system using POSAFE-Q PLC used in the current NPPs in Korea. Alternatively, the prototype was developed using other PLCs made by LSIS that are widely used in industrial control systems.

4. Conclusion

The existing blockchain is mainly used in the field related to cryptocurrency. The data about transaction of cryptocurrency were hashed and stored. In this study, the data of the PLC code, not that of cryptocurrency, was hashed, and stored in the block. . In this study, data in PLC memory were converted to hash values through SHA-256, and those are abbreviated to merkle root hash. The converted hash values are stored into blocks with timestamp, previous hash, etc. The blockchain network shared the recorded data about PLC code integrity, so it is hard not only to delete the data but also to temper the data.

In this study, a prototype system that monitors the integrity of the reactor protection system was developed using the proposed blockchain network,

One of the main features of this paper is that it is first try to explore blockchain technology to the cyber security of I&C system of NPP. It can detect cyber attacks such as false code injection attacks to PLC, and monitor which PLC's integrity has been compromised.

Acknowledgement

This research was supported by the KU-KAIST institute, Korea, under 2019 R&D program supervised by KAIST

REFERENCES

[1] Kesler, B. (2011). "The vuln2016erability of nuclear facilities to cyber attack." Strategic Insights 10(1): 15-25.
[2] Analysis report of cyber attack trend for critical infrastructure, AhnLab, 2016.
[3] RS-015, “원자력시설등의 컴퓨터 및 정보시스템 보안”, KINAC, 2014.
[4] M. Pilkington, “Blockchain Technology: Principles and Applications,” Res. Handb. Digit. Transform., pp. 1–39, 2015.
[5]Shai Halevi and Hugo Krawczyk, Randomized Hashing and Digital Signatures.
[6] Merkle, R. C. (1988). "A Digital Signature Based on a Conventional Encryption Function". Advances in Cryptology — CRYPTO '87. Lecture Notes in Computer Science. 293. p. 369. Doi:10.1007/3-540-48184-2_32. ISBN 978-3-540-18796-7.