Development of a Monitoring System for Data integrity of PLC code 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

As the main systems for managing the operation, control, monitoring, measurement, and safety function in an emergency, instrumentation and control systems (I&C) in nuclear power plants (NPPs) have been digitalized gradually for the precise operation and its convenience [1]. The I&C systems of 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 [1]. However, it was determined that the isolated networks are not safe from cyber attacks. 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. The representative event is Stuxnet attack that destroyed about 1000 centrifuges at Iran's nuclear facility [2]. Thus, It is necessary to monitor the integrity of PLC logic 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. Blockchain is a digital ledger or distributed database that records transactions of value using a cryptographic hash function that is inherently resistant to modification. A block contains a set of transactions, a hash of the previous block, timestamp (indicating when the block was created), block number, and so on [3]. The deployed codes in PLC memory are hashed through hash algorithm, and they are recorded into the blockchain.

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 is expected that cyber security level would be enhanced through monitoring the integrity of PLCs.

2. Development of A Monitoring technique for data integrity of PLC code using blockchain technology

In this section, how a monitoring technique for the integrity of PLC logic using blockchain technology has been developed is described.

2.1 Conversion of PLC logic code to hash value using Secure Hash Algorithm (SHA)

The Secure Hash Algorithms (SHA) 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 hash of a fixed size. It's designed to be a one-way function, infeasible to invert [4].

The cryptographic algorithm is applied to valid the PLC code integrity. The users of PLCs use the logic builder program to set the input and output data, designs the logic, and downloads it to the PLC. In the implementation of downloading logic to PLC, functional block diagram codes are converted to C languages, and they are compiled to machine instruction codes, which are loaded into the PLC memory area. In this study, the integrity of PLC code is monitored using hash algorithm. PLC logic codes based on c language or machine language are converted to hash value through the secure hash algorithm. 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 logic code in PLCs has been modified.

In order to check the temper of PLC code, logic based on C language and machine code in PLC are converted to cryptographic value through secure hash algorithm as shown in Fig 1. The obtained hash value representing the integrity of PLC code will be recorded into a block, as the record of bitcoin transaction is stored in blockchain.

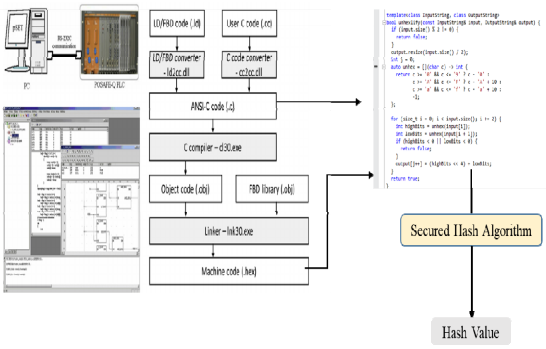

Fig 1. Conversion of PLC code to hash value

2.2 Checking the modification of PLCs logic 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 [5]. 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 hash value becomes completely different. It is also possible to detect which PLC code is tempered as shown in Fig 2.

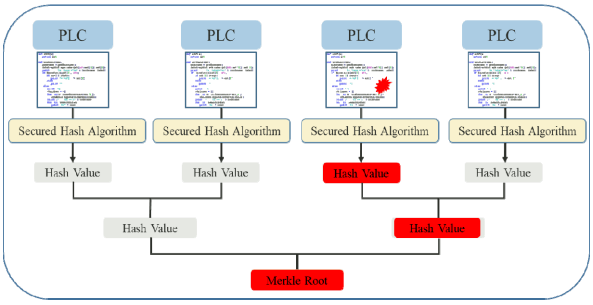

Fig 2. PLC code integrity check using merkle tree

2.3 Monitoring data integrity of PLCs using blockchain

If such a record of code integrity can be manipulated easily, and stored only on one system, then it becomes meaningless. So blockchain technology to store the data including the previous hash value, timestamp, and merkle root hash value in a block is used, and all the nodes in the blockchain network manage this ledger. The technique developed in this study uses the digital signature technique to ensure the confidentiality of the data. In addition, since it is a private blockchain, only pre-defined nodes can participate in the network. Even if the attack transmits the manipulated data using a device that is not pre-defined in the blockchain, repudiation can be prevented by using the private key and the public key as shown in Fig 3.

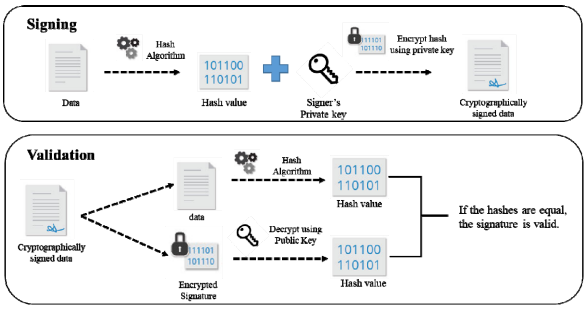

Fig 3. Data transportation using digital signature in blockchain

If a record of downloading the logic to the PLC is recorded in the Blockchain, it is impossible to manipulate the data in the recorded block. If an attacker wants to delete the record of changes to the PLC logic at a specific time, he must also manipulate the data in other blocks connected to the block. This is virtually impossible. This is one of the key features of Blockchain. In addition to ensuring the integrity of the data recorded in the block, auditability can also be guaranteed due to the merkle tree property.

Even if the data recorded in the Blockchain is forged, more than half of the ledgers constituting the Blockchain network should be also manipulated as shown in Fig 4. If an attack deletes the data record of a particular node, it takes a record of the other nodes and updates it.

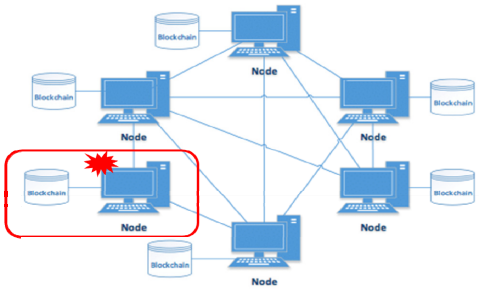

Fig 4. Distributed ledger in blockchain network

2.4 Experiment

An experiment was conducted as a feasibility study of the proposed system in lab-scale. This Blockchain was programmed using Javascript. Three PLCs were simulated in this experiment. The PLC logic codes were not real data from real PLC devices. Those were written using C language. First, the blockchain network called a c language-based logic file in a specific directory, and the code was converted into a hash value, and stored and managed in the blockchain. The hash values of each code were stored in the blockchain every 10 seconds.

In this experiment, the second PLC's code among three PLC logic codes in total was tempered, and then data stored on the blockchain was be monitored as shown in Fig 5.

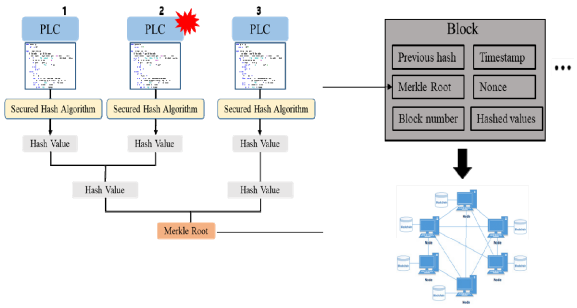

Fig 5. Experiment for monitoring modification of PLC codes using blockchain

Fig. 6 shows the record stored in blockchain when second PLC code is tempered. Because of modification that “if (x==1)” is modified to “if (x==1000)”, the hash value about second PLC code was completely changed, and the Merkle root value was changed as shown in Fig 6. If system managers check this event, they could figure out that certain PLC logic is tempered by someone or malicious code attack.

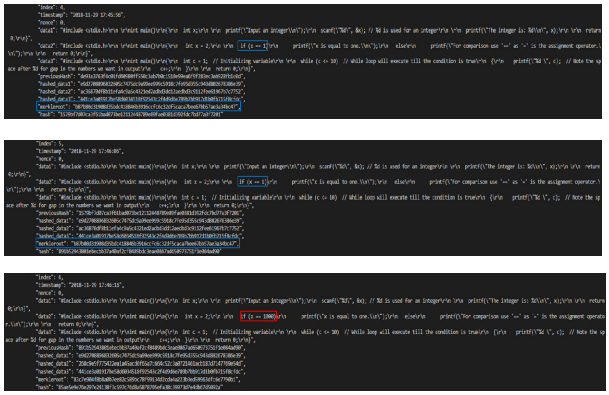

Fig 6. Data in blockchain when logic code is tempered

3. Conclusions

A cyber threat to a nuclear facility can lead to physical destruction that can affect plant safety. Especially, PLCs deployed in the safety system of NPPs would be critical. Thus, a monitoring technique for modification of PLC logic code using blockchain is proposed in this paper. Logic codes in each PLC are converted to hash value through cryptographic algorithm, and those are united to merkle root hash value for efficient and secure verification. Data representing the integrity of PLC logic codes is stored in blockchain, and the data could be monitored whether all logic codes of PLCs are tempered. The feasibility of the proposed system was confirmed through experiment.

As a further work, a test-bed of the reactor protection system (RPS) is going to be designed using real PLC devices, and proof of concept will be conducted using the test-bed.

It is expected that it can detect cyber attacks such as false code injection attacks to PLC logic, and monitor which PLC's code integrity has been compromised. The security level of NPPs is expected to be improved because the attacker's stealth is not guaranteed and the integrity of systems is continuously monitored.

Acknowledgement

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

REFERENCES

[1] Do Yeon Kim, “Cyber security issues imposed on nuclear power plants”, Annals of Nuclear Energy, Vol 65, pp.141-143, 2014.

[2] Brent Kesler, “The Vulnerability of Nuclear Facilities to Cyber Attack”, Strategic Insights, Vol 10, pp.15-25, 2011,

[3] Imran Bashir, “Mastering Blockchain”, Packt, Birmingham, UK.

[4] Shai Halevi and Hugo Krawczyk, Randomized Hashing and Digital Signatures.

[5] 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.