IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 8, 2020, accepted June 19, 2020, date of publication June 26, 2020, date of current version July 8, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3005134

A Novel Monitoring System for the Data Integrity of Reactor Protection System Using Blockchain Technology

MOON KYOUNG CHOI[1], CHAN YEOB YEUN[2], (Senior Member, IEEE), AND POONG HYUN SEONG[1]

[1]Department of Nuclear and Quantum Engineering, Korean Advanced Institute of Science and Technology (KAIST), Daejeon 34141, South Korea
[2]Center for Cyber-Physical Systems, EECS Department, Khalifa University, Abu Dhabi, United Arab Emirates

Corresponding author: Poong Hyun Seong (pheong@kaist.ac.kr)

This work was supported in part by the Khalifa University–Korean Advanced Institute of Science and Technology Institute through the 2019 Research and Development Program supervised by the Korean Advanced Institute of Science and Technology (Development of Blockchain Based Cyber Security Technology for Nuclear Power Plants), South Korea, under Grant N11190054, in part by the Center for Cyber-Physical Systems, Khalifa University, under Grant 8474000137-RC1-C2PS-T3, and in part by the National Research and Development Program through the National Research Foundation of Korea (NRF) funded by the Korean Government (Ministry of Science, ICT and Future Planning) under Grant NRF-2016R1A5A1013919.

ABSTRACT Nuclear Power Plants (NPPs) are physically isolated from external networks and have different operational environments than conventional information technology (IT) systems. Accordingly, NPPs were regarded as safe from external cyber-attacks. However, it was later determined that isolated networks are not safe from cyber-attacks. Malicious data injection attacks on Programmable Logic Controllers (PLCs) deployed in the safety system of NPPs are critical to nuclear facilities, as they were in the Stuxnet attack. It is necessary to monitor the integrity of PLC data and protect the PLCs from cyber threats such as modification of deployed logic or setpoints. To address this problem, this paper proposes a novel system for monitoring data integrity of PLCs using blockchain technologies. Considering the NPP environment, we developed a private blockchain system to monitor the data integrity of PLCs. The new concept that is Proof of Monitoring (PoM) for data integrity of PLCs was proposed to overcome the limitation for applying the private blockchain to the cybersecurity of NPPs. Additionally, we developed an integrity monitoring system for the Reactor Protection System (RPS)—a safety system in NPPs—using the developed blockchain. It can detect cyber-attacks (such as false code injection attacks on PLCs) and monitor which PLC integrity has been compromised in real-time. A validation experiment using a false data injection attack on PLCs was performed on the developed system, and the results confirmed that the developed system successfully monitored the modification of data in the PLCs.

INDEX TERMS Blockchain, cybersecurity, data integrity, detection, monitoring system, programmable logic controller (PLC), reactor protection system (RPS).

I. INTRODUCTION

The Instrument & Control (I&C) systems of Nuclear Power Plants (NPPs) are physically isolated from external networks and have different operational environments than conventional information technology (IT) systems. Accordingly, NPPs were regarded as safe from external cyber-attacks. However, it was determined later that isolated networks are not safe from cyber-attacks [1]. In 2010, Stuxnet destroyed approximately 1000 centrifuges at Iran's uranium enrichment facility in Natanz. The Stuxnet attack against the Iranian nuclear program demonstrates the critical impact that a sophisticated adversary with a detailed knowledge of I&C systems can have on safety-related infrastructures [2], [3]. Attacks on Programmable Logic Controllers (PLCs) deployed in the safety protection system of NPPs would be especially critical because cyber threats on PLCs can cause problems related to safety [4].

Korea Institute of Nuclear Nonproliferation and Control (KINAC), which oversees the NPP cybersecurity regulations

The associate editor coordinating the review of this manuscript and approving it for publication was Ana Lucila Sandoval Orozco.

in Korea, requests that utilities comply with cybersecurity controls and perform cybersecurity risk management based on regulatory guide RS-015. KINAC/RS-015 recommends implementing security controls to ensure the integrity of critical systems and monitor cyber-attacks against them [5]. However, there is currently no system capable of detecting malicious modification of data on PLCs in real-time. Furthermore, it is difficult to detect whether the integrity of control logic data has been attacked under normal conditions because safety systems (e.g., safety pumps and valves) do not operate under normal conditions. There is no security control for monitoring the data integrity of safety controllers. It is necessary to monitor the integrity of PLCs and protect them from cyber threats such as the modification of deployed logic or setpoints in PLCs. Blockchain technologies (hereafter referred to as simply ''blockchain'') may be an effective solution to the problem. Blockchain combines multiple technologies such as cryptographic and distributed systems, rather than using a single technology, to prevent data manipulation [6], [7]. In an existing system, if an attacker compromises system integrity and eliminates evidence of the attack, the attack is difficult to detect [8]. However, if blockchain is used, the recorded data becomes impossible to alter, thus eliminating evidence of the attack and overcoming the limitations of a single point of failure. Blockchain also satisfies the security requirements in the cybersecurity regulatory guidelines of KINAC/RS015 presented in Table 1.

TABLE 1. Security requirements in KINAC/RS015 [5].

Satisfaction	Requirements of security controls
✓(satisfied)	Detection of unauthorized manipulation of information
✓	Prevention of illegal data manipulation
✓	Protection of records from malicious changes and deletions
✓	Perform monitoring and cyber-attack detection
✓	Prevention of stored logs from being tampered

In the preliminary study [9], we proposed a conceptual framework of NPP cybersecurity using blockchain. This paper is a follow-up study. In this research, we have implemented the concept from the preliminary study and developed data integrity monitoring system of nuclear safety system using blockchain. Considering the context of the NPP environment, we develop blockchain for monitoring the falsification of data in PLCs in real-time. In contrast to blockchains for cryptocurrency, the developed blockchain in this study store integrity about data such as control logic and setpoints. We also develop a system that monitors the integrity of a Reactor Protection System (RPS) using the developed blockchain. The validity of the developed system is demonstrated through an experiment that injects false data into PLCs.

In this study, we propose a novel system for monitoring the data integrity of RPS using a private blockchain. Our main contributions are summarized as follows:

1) We develop a private blockchain considering the context of the NPP environment and propose a novel system that monitors the data integrity of PLCs using this blockchain. It is possible to monitor the integrity of PLCs in real-time (every 5000-6000ms) against cyber threats.

2) We apply the developed blockchain system to RPS, which is the safety system in an NPP for monitoring system integrity. A real RPS prototype is used to develop the monitoring system, and its validity is demonstrated experimentally.

3) This is a pioneering study as the first to exploit blockchain with PLCs for security monitoring. The proposed system is not limited to only a few systems—its usability can be extended to monitor the data integrity of other control systems in real-time.

The remainder of this paper is organized as follows. Section II describes the preliminaries about blockchain including general characteristics. Section III describes the private blockchain for monitoring the data integrity of PLCs. Section IV describes the RPS data integrity monitoring system using the private blockchain developed in Section 3. Section V concludes this paper.

II. PRELIMINARIES: BLOCKCHAIN

This section describes the preliminaries about blockchain, including the general characteristics, types, and consensus.

A. GENERAL CHARACTERISTICS

Blockchain is a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updatable only via consensus or agreement among peers [10]. For an organization that cannot afford a single point of failure, the blockchain makes it practically impossible for cybercriminals to compromise sensitive information. Blockchain is managed not only managed by trusted administrators or developers; it is well-managed by anyone who can be either trusted or from a known or unknown party. Blockchain is a series of blocks connected by a hash. Each block is divided into two parts: the block header and the block body. All transactions involved in a block constitute the block body. The block header consists of a hash of the last block header defined as previous hash, a timestamp, and a Merkle root of the transaction data. These blocks connect individually and form a chain. The hash of the last block header contains all of the information about the last block, which ensures the integrity of the block data. If transactions in the previous block are maliciously altered, the Merkle root of all transactions involved in that block is also changed, which results in a change of the hash of its block header [11]. This change iteratively spreads to the subsequent blocks and forms a fork. However, this new chain is not a consensus that all of the consortium nodes agree on. Because of this ingenious structure, blockchain is inherently resistant to data-tampering. Unlike the current centralized system, blockchain

is a distributed system. To successfully attack the data stored in the blockchain, the attacker must attack the data of other nodes simultaneously in a short period even if the attacker succeeds in tampering with the data of one node in the network. These features overcome the limitations of existing centralized security controls.

B. TYPE OF BLOCKCHAIN

In general, there are two types of blockchain: public and private. A public blockchain is open to the public—anyone can participate as a node in the decision-making process. Users may or may not be rewarded for their participation. These ledgers are not owned by anyone. The public blockchain can also be called permissionless ledgers. The blockchain is secured by crypto-economics, which are economic incentives and cryptographic verification such as Bitcoin. Because of the large number of nodes participating in the network, transaction speed is low but security is high.

A private blockchain is private and open only to a consortium or group of individuals or organizations who have decided to share the ledger only between themselves. In the blockchain, the write permissions belong to one organization or with a specific group of individuals. Read permissions are public or restricted to a large set of users. Transactions in this type of blockchain are verified by very few nodes in the system. Transaction speed is high because of the small number of nodes participating in the network but security is lower than that of a public blockchain.

C. CONSENSUS IN BLOCKCHAIN

Consensus is a method for nodes in a blockchain network to decide whether to write specific data in a block. Several different consensus algorithms exist depending on the blockchain type, the blockchain purpose, and the environment in which the blockchain will be applied, but this study discusses representative consensus.

Proof-of-Work (PoW), used in Bitcoin, relies on proof that sufficient computational resources have been spent before proposing a value for acceptance by the network. PoW requires defining an expensive computer calculation, also called mining. A reward is given to the first miner who solves each block's problem. Network miners compete to be the first to find a solution for the mathematical problem. The advantage of PoW is that anyone can join a PoW network, and this is well-established as a functional consensus mechanism. The primary downsides of PoW networks are low speeds and financial costs: running the computers to do these computations is very expensive [12].

Proof-of-Stake (PoS) has the same objectives as PoW—to secure the network against attack and allow consensus to occur in an open network. Unlike PoW, where the algorithm rewards miners who solve mathematical problems to validate transactions and creating new blocks, with PoS the creator of a new block is chosen a deterministically, depending on wealth, also defined as his or her stake [12].

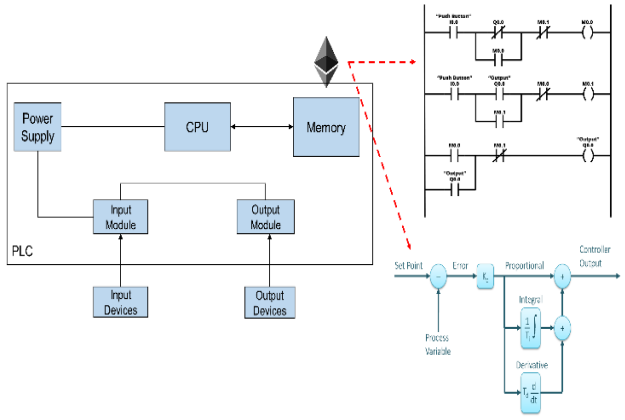


FIGURE 1. Security target for NPP cybersecurity.

Proof-of-Authority (PoA) networks are used only when all blockchain participants are known. In PoA, each participant is known and registered with the blockchain. Such a blockchain is called a permissioned chain, as only computers that are part of this approved list of authorities can forge blocks. Unlike PoW or PoS, there is no mining mechanism involved in PoA. PoA is primarily used in private blockchain environments that do not require excessive computational competition. However, since authority nodes are more important than other general nodes, it is necessary to manage them properly and protect them from attack. To prevent the authority nodes from being compromised, there are ways to apply additional security controls to authority nodes or to prevent attackers from identifying the authority nodes. The model proposed in [13] provides a solution to prevent cases in which the blockchain network is compromised due to attacks on multiple nodes.

III. PRIVATE BLOCKCHAIN FOR MONITORING DATA INTEGRITY OF PLC

This section describes considerations when applying blockchain technology to NPP cybersecurity. Considering the NPP environment, it describes the development of a private blockchain that monitors PLC data integrity. We also describe a communicating function that we developed to read PLC data to be stored in the blockchain in real-time using LabVIEW software.

A. CONSIDERATIONS IN NPP CYBERSECURITY PERSPECTIVE

In the current blockchain used in cryptocurrency, the amount of cryptocurrency and its transaction information should be protected and secured. Regarding what types of data should be protected for NPP cybersecurity, PLC data directly related to nuclear safety (e.g., control system setpoints, safety system control logic, etc.) might be the answer, as illustrated in Fig 1. Such data should not be modulated by anyone. In this study, PLC data related to safety is considered equivalent to cryptocurrency data.

The type of blockchain suitable for the environment of NPPs was discussed. There is a limitation in applying a public blockchain to NPP networks. Since NPP networks are isolated from the outside, only pre-approved insider identities should be able to access the network. If the data of controllers is open to unauthorized individuals, the data can also provide sensitive system information to external individuals or potential attackers. Using a public blockchain with features of the zero-knowledge proof mechanism provides the advantage of data anonymity, but this anonymity impedes detailed analysis of the data. In this study, use of a private blockchain is suitable because the data should not be anonymized in order to check whether the data of the PLC has been tampered with or not. This is because it is difficult to specifically analyze data of a specific PLC stored in a block if all transaction data is anonymized. Therefore, applying a public blockchain is not appropriate in the NPP environment. Considering the context of an NPP network, it is more suitable to apply a private blockchain.

We considered a consensus algorithm suitable for private blockchain to be applied to the NPP environment. Blockchain consensus algorithms such as PoW used in existing cryptocurrency are computationally expensive and inefficient [14]. When applied to NPP cybersecurity, compensation for the mining of blocks is also unnecessary. Consequently, private blockchain networks generally use PoA as a consensus algorithm. Although using PoA in the private blockchain environment has advantages in performance and efficiency, from the attacker's point of view, if he or she knows which node is the validator node, the block data can be tampered with. To solve this problem, it is desirable to select a miner randomly every time among the nodes constituting the network. Therefore, we applied random rotation-based PoA consensus, in which the miner node is randomly-selected to prevent attackers from identifying the miner node every time from among the validated nodes. Even if some of the authority nodes are compromised or abnormal, it is possible to distinguish the abnormal node by comparing with blocks verified by other normal nodes. For example, let's suppose that one of the 10 nodes is compromised. In the round where 9 normal nodes were selected as the validator nodes, the verification result was A, while in the round where the compromised node was selected as the validator node, the verification result was B. Then, we can infer that there is a problem in the node indicating the verification result as B. Therefore, if a specific authority node is selected to verify the block and the values stored in the blockchain are different from other blocks, it can be inferred that the authority node has a problem. This is Proof of Monitoring (PoM) for data integrity of PLCs, and it is a newly-proposed concept in this paper to overcome the limitation for applying private blockchains to cybersecurity of NPPs. This is Proof of Monitoring (PoM) for data integrity of PLCs, and it is a newly proposed concept in this paper to overcome the limitation for applying private blockchains to cybersecurity of NPPs.

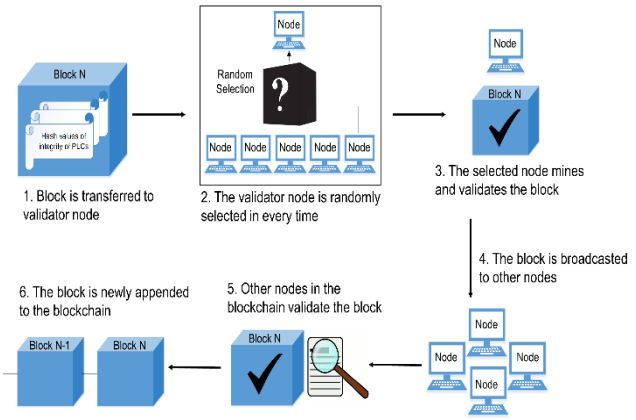


FIGURE 2. Process of Proof-of-Monitoring (PoM) for data integrity of PLCs.

Figure 2 shows the Proof-of-Monitoring (PoM) process to ensure the data integrity of PLCs. In the PoM process, first, a new block containing data on the integrity of PLCs is transferred to the validator node. At this time, the validator node is randomly selected at every time point among nodes in the blockchain network. The selected node mines and validates the block. After this step, the block is broadcasted to other nodes. Other nodes in the blockchain validate whether the block is well mined or the block was transferred by an authorized node in the blockchain. After this validation process, the block is newly appended to the blockchain. Due to the random selection rule for a validator node, potential attackers cannot determine which node validates the newly generated block. This iteration of the generating block is repeated in random intervals between 5000–6000 ms such as in the frequency hopping method that is used to switch transmitting radio signals among several frequency channels to prevent signal interceptions. It is very difficult for attackers to compromise or attack the new block in a very short time. The frequently changed and irregular intervals of generating blocks could prevent attackers from planning attacks that exploit regular detection intervals. In the PoA method, a limitation exists in that validator nodes are already defined in the network, but PoM for data integrity of PLCs with the rule of randomly selecting validator nodes can minimize these limitations.

B. COMMUNICATION PROGRAM WITH PLCs

Existing blockchain systems have stored data on cryptocurrencies traded between users. The aim of this paper, as discussed in Section III. A, is to store data contained in PLC memory in the blockchain. Therefore, it is necessary to develop a program that reads PLC data and stores it in real time. We developed a program that implements the function to read data by communicating with PLCs using LabVIEW software, as shown in Fig. 3.

This function reads data stored in PLC memory in real time using Ethernet TCP / IP communication protocol. Each PLC datum is read and saved in a text file in real time.

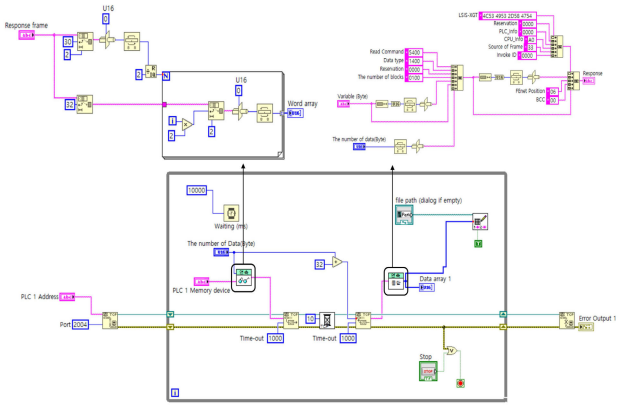


FIGURE 3. Code for communicating with PLCs to read memory data using LabVIEW software.

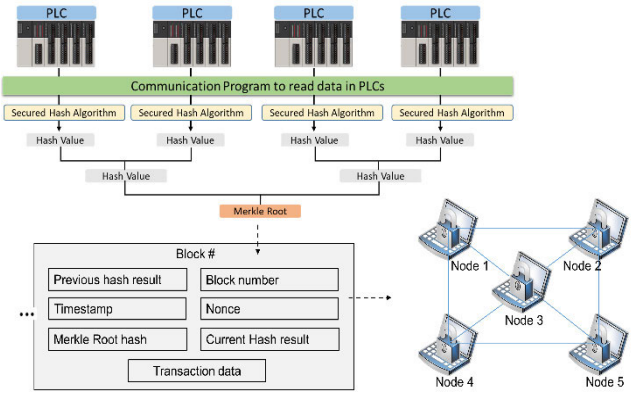


FIGURE 4. The architecture of the PLC data integrity monitoring system using the blockchain.

To implement this function, it is necessary to set an IP address, memory area to read, communication port, and message frame format according to the communication protocol. The communication program with the developed PLC saves the data stored in the PLC specific memory in text format. There may be concerns that the attack surface is likely to increase due to the new function using Ethernet TCP/IP communication. However, it is expected that various existing attacks can be prevented through the new function. In addition, when applied to the nuclear control systems, a one-way communication function between PLCs and the blockchain must be implemented due to the nuclear cyber security regulatory guidelines. This one-way communication function can prevent data integrity attacks against PLCs. It is expected that the attack surface due to the new function will be reduced further. The data of PLC obtained through the communication is stored in the blockchain proposed in the next section.

C. PRIVATE BLOCKCHAIN FOR MONITORING DATA INTEGRITY OF PLC

In this section, we introduce a private blockchain for monitoring the data integrity of a PLC. We also describe the architecture of the PLC data integrity monitoring system using the blockchain network, the configuration of the system, and the structure of data in the blockchain.

Fig. 4 illustrates the architecture of the PLC data integrity monitoring system using the blockchain network. Each PLC's data are considered transaction data in the blockchain of the existing cryptocurrency. PLC data are encrypted by the Secure Hash Algorithm (SHA)-256 algorithm every 5000-6000ms, as in real-time, and recorded in the block. The randomly selected validator node verifies the recorded data and distributes it to other nodes in the private blockchain network. After being written to the blockchain network, the data is virtually immutable.

Table 2 presents the configuration of the blockchain, which was developed based on JavaScript. It consists of five nodes,

TABLE 2. Configuration of the private blockchain.

Configuration	Element
The number of nodes in the blockchain	5
Transaction and mining period	Random time intervals between 5000–6000 ms
Cryptographic algorithm	SHA-256
Consensus algorithm	Proof of Monitoring (Random rotation)

and a new block is generated in iterations with random intervals between 5000–6000ms by a validator node. SHA-256 was used as a cryptographic algorithm; it is a cryptographic hash function that takes an input of a random size and produces an output of a fixed size. Hash functions are powerful because they are ''one-way.'' Random rotation-based PoA was selected to generate consensus in the blockchain network. If the attacker identifies a mining node, data tampering is possible. Thus, the mining node was randomly selected among the total nodes in the blockchain network.

The data stored in the developed blockchain is presented in Table 3. The block number, previous hash result, transaction data, Merkle root, nonce, timestamp, and current hash result are written in the block. The block number is the number of blocks created. The previous hash result is the hash value of the previous block. Unlike the data stored in the blockchain of cryptocurrencies, the blockchain proposed in this study stores PLC data (e.g., control system logic, setpoint data, etc). Verifying data integrity is inefficient if the quantity of PLCs is significantly increased. Considering this limitation, the Merkle root was used to easily verify the integrity of all data and could be the representative hash value about the integrity of several PLCs [15]. Data in each leaf node are PLC data obtained by the communication program proposed in Section III.B, and all the hashed data are combined into a single constant hash value called ''Merkle root''. The timestamp is the time when the current block is generated. When monitoring the data integrity of the PLC, the timestamp represents when the data changed. Nonce is a solution of

TABLE 3. Block structure.

Items	Meaning
Block number	The sequence number of the current bock, which is used as the title of the block
Previous hash result	The hash result of the previous block
Transaction Data	Hash values of data stored in PLCs (data of ladder logic, setpoint of components, configuration of PLCs)
Merkle root hash	The compressed hash of all the hashed transaction data, which is the representative value for overall data integrity of PLCs
Timestamp	The time the current block was appended to the blockchain
Nonce	The solution of the puzzle problem for the current block
Current hash result	The hash result of the current block

the work required to connect the previous block with the current block. The current hash result is the hash value of the current block, which is also included in the next block to be generated.

IV. RPS INTEGRITY MONITORING USING THE DEVELOPED BLOCKCHAIN

This section describes the RPS data integrity monitoring system using the private blockchain developed in Section.3. This section describes the introduction of RPS, the development of an RPS integrity monitoring system using the developed blockchain, and its experimental validation.

A. PROTOTYPE OF REACTOR PROTECTION SYSTEM (RPS)

The RPS being developed in Korea is designed with a 2-out-of-4 redundant architecture, and every channel is implemented with the same architecture. A single RPS channel consists of a redundant Bi-stable Processor (BP), a redundant Coincidence Processor (CP), an Automatic Test & Interface Process (ATIP), and a Cabinet Operator Module (COM). The BP module generates a logic-level trip signal by continuously comparing the sensor inputs with the predefined trip setpoints. The logic-level trip signals generated in the BP module of any channel are transferred to the CP modules of all the channels. The CP module monitors the logic-level trip signals transferred from the four BP modules. When two or more logic-level trip signals from the BP channels are activated, the CP modules activate the output signal for the reactor trip [15].

We developed RPS prototype using PLCs from LSIS that are widely used in industrial control systems as shown in Fig 5. Instead of implementing the full scope of RPS, we simplified RPS by using four BPs and one CP. Four BPs are designed to send a signal to the CP when they exceed the setpoint value by comparing the input value with the setpoint value. The CP is designed to generate a trip signal when it receives a signal from two or more BPs out of four BPs. Each PLC communicates using the Ethernet protocol.

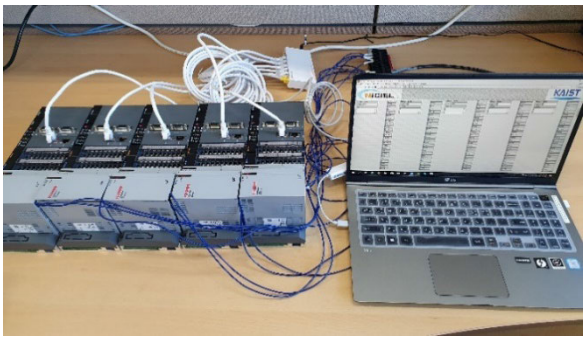


FIGURE 5. Prototype of reactor protection system.

B. MONITORING RPS DATA INTEGRITY

In the previous section, we proposed a private blockchain that reads and stores the data integrity of PLC. The RPS prototype was also developed.

Fig. 6 illustrates the system for monitoring the data integrity of RPS using the developed blockchain. Data from a specific memory area of each PLC is read through the communicating function programmed in LabVIEW from Section III. B, and this data is stored in a private blockchain network. This system acts as a Closed Circuit Television (CCTV) that continuously monitors the security of the RPS. If the attackers illegally change the data of a specific PLC, it is immediately stored in the blockchain, and it is apparent that the integrity value of that PLC has changed. Even if a small part of the large data set stored in the PLC is changed, the hash value is completely changed. This system does not affect the safety of PLCs at all because it only reads data stored in PLC memory (logic, set point, etc.). The unavailability of the system has a problem with only the function of integrity monitoring, but does not affect the safety. Since it is impossible to attack the hash function and attack the majority of nodes in the blockchain system, which is a strong encryption technology, in a short time, it is difficult for the proposed system to become unavailable due to the attacks. Even if the system becomes unavailable, the security managers can figure out the abnormality of the system because new blocks are not created in the blockchain anymore. Thus, the mangers can infer the incident and inspect the status of the safety system that is the security target.

Fig.7 depicts the block data representing RPS integrity. It indicates the 11th block in the blockchain (including the block index, timestamp, transaction data, etc.). Hash values indicate each PLC's integrity in the transaction. Hash values representing data integrity for BP1, BP2, BP3, BP4, and CP1 are stored in the block. Since BP1, BP2, BP3, and BP4 all have the same data, the data integrity values of the four PLCs are displayed equivalently. The data from CP1, however, differs from that of the BPs because of different hash values. A block is created every 5000-6000ms, and for an attacker to modify this data, all previous block data must be forged before the next block is created.

Fig. 8 depicts the human-machine interface (HMI) screen of the developed RPS integrity monitoring system.

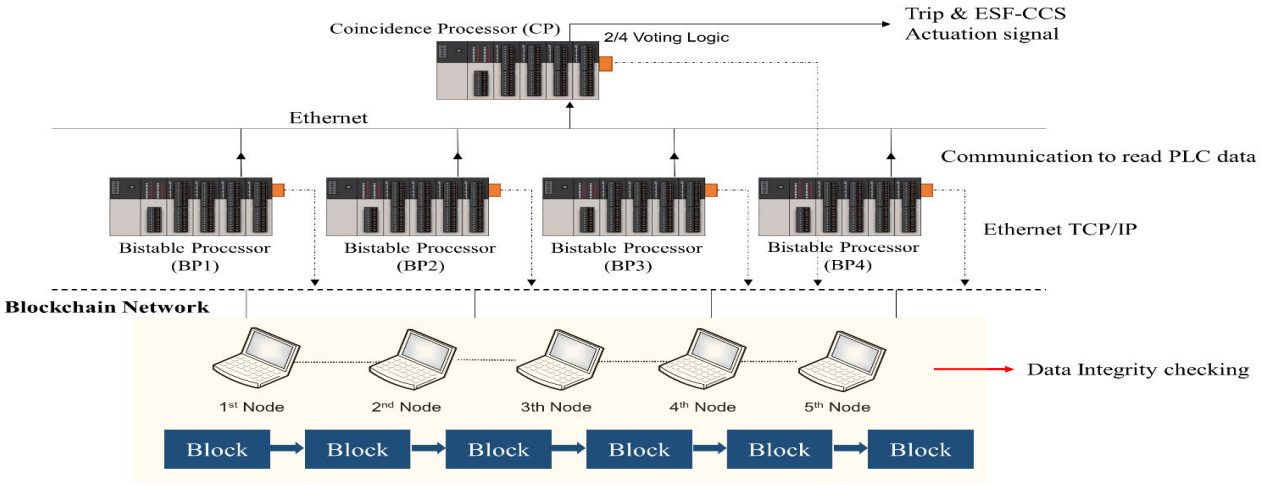


FIGURE 6. A system for monitoring the data integrity of RPS using the proposed blockchain.


```
{
    "index": 11,
    "timestamp": 1571743251959,
  ▼ "transactions": [
    ▶ { ··· }, // 1 item
    ▼ {
          "Data_BP1": "0062e167766561c4bfd1c9405bed8b3ee2bad80cd80a3b7832ade5bfe677f17e",
          "Data_BP2": "0062e167766561c4bfd1c9405bed8b3ee2bad80cd80a3b7832ade5bfe677f17e",
          "Data_BP3": "0062e167766561c4bfd1c9405bed8b3ee2bad80cd80a3b7832ade5bfe677f17e",
          "Data_BP4": "0062e167766561c4bfd1c9405bed8b3ee2bad80cd80a3b7832ade5bfe677f17e",
          "Data_CP1": "1104fa130a80eb69003f6e2781cb66ce776b32c769a4d092861b21f4da3fe555"
      }
    ],
    "nonce": 264427,
    "hash": "0000afbced7baec3bfb3caf038b702d7d489a4b00402e2fcca4cca971e2487ff",
    "merkleRoot": "253f1be88cf079f61daee941597809121267b296352fef394e0b6c91abfa734c",
    "previousBlockHash": "0000cf22d224133d219b28bb966266adbc5da050f7aa439d73f96f17945cc194"
},
```


FIGURE 7. Data from the RPS integrity monitoring system using the developed blockchain network.

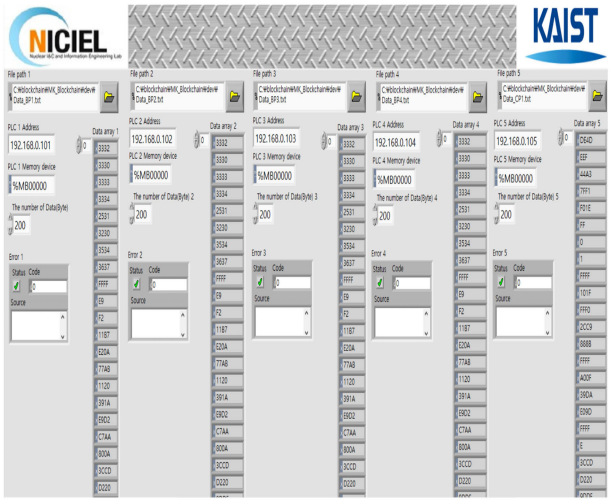


FIGURE 8. HMI screen of the developed RPS integrity monitoring system.

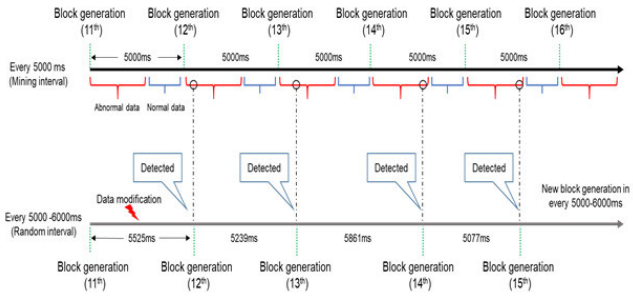


FIGURE 9. Detection mechanism of the developed monitoring system.

The security manager of the NPP configures the PLCs that should be monitored, and the PLC data is automatically stored in the developed blockchain network. It is necessary to assign the PLC's IP address to be monitored and input the memory area of the PLC. If the user enters the quantity of data to be loaded from the input memory address, the program saves the data stored in the memory as text data.

C. VALIDATION EXPERIMENT

Experiments were conducted to validate whether the developed monitoring system can detect illegal PLC data changes. We performed a test featuring a false data injection attack on a specific PLC for validation. As a representative cyber-attack, the false data injection attack manipulates system data to mislead the control center. Many studies have demonstrated the impacts of the attack on modern power systems [16]–[21].

The developed monitoring system has a detection mechanism as shown in Figure 9. In the detection mechanism, a new block is created at random intervals of 5000–6000 ms, and the hash values of PLC data at the time of creation are stored in the block. If blocks are generated in iterations with regular intervals, such as every 5000 ms, the attacker could exploit the blocks by using attacks with intervals faster than 5000 ms,

as shown at the top of Figure 9. However, because new blocks are generated at random intervals between 5000–6000 ms, the attacker fails to predict the detecting time. Consequently, it could be possible to detect changes in PLC data regardless of the attack timing, as shown in the bottom of Figure 9.

False data has been injected to the Coincidence Processor 1 while the monitoring system was operating. Before the 11th block was created and the 12th block was generated, as shown in Figure 9, the CP1 data was changed from the 'FFFF' value to the '0000' value. The hash values were changed immediately due to the data modification, and the changes could be detected in the 12th block, as shown in Figure 10.

FIGURE 10. Detection of the false data injection to data of CP1.

Figure 10 illustrates the 11th and 12th blocks. In the 11th block, data regarding the data integrity of PLCs is recorded, and the Merkle root value, which indicates the integrity of the entire system, is also recorded. The data integrity of PLCs of the 1st to 11th blocks have the same value, but the data integrity value of the CP in the 12th block changes. This implies that the data of the CP was changed due to a false data injection attack. Nodes in the blockchain are immediately synchronized to these changes in hash value. Even if the storage of the data change recorded is delayed due to synchronization between the blockchain nodes, change is detected in the block after the 13th that is the next following block. Accordingly, the security manager can then detect that the data of CP1 had been modified among the five PLCs. It is possible to verify which PLC data item has been modified with a specific, known timestamp. In current systems, detecting whether a PLC's data has been tampered with is difficult if an attack modifies the PLC's data and eliminates evidence of the attack. However, by applying this system to monitor integrity, modification of data can be easily detected. The attacker will not attack the target system because he or she cannot eliminate evidence of the attack. We also plan to add a function that generates an alarm signal if the hash value of the PLC stored in the blockchain changes.

The range of intervals for generating new blocks would be determined according to the system's performance and configuration. We expect to generate blocks faster than 5000–6000 ms through system optimization to ensure better real-time performance using servers with the high computational performance.

V. CONCLUSION

We confirmed the necessity of monitoring PLC data integrity to protect against cyber threats. In this paper, we proposed a novel system for monitoring PLC data integrity using a blockchain. We developed a private blockchain considering the context of the NPP environment. In the development process, a new concept of Proof-of-Monitoring (PoM) for data integrity of PLCs was proposed. We also exploited the developed blockchain system for monitoring the data integrity of RPS which is a safety system in NPP. A RPS prototype was built and used to develop the monitoring system, and its validity was demonstrated experimentally. This is a pioneering study in that it is the first to exploit blockchain with PLCs for security monitoring. The proposed system is not limited to a specific system, and the proposed blockchain system can be extended to integrity monitoring of other control systems. The system can detect cyber-attacks, such as false code injection attacks to PLC logic, and monitor which PLC's data integrity has been compromised. In conclusion, we newly presented the blockchain-based system as a solution for detecting cyber attack such as Stuxnet that causes malfunction of control systems by modifying data of PLCs. The security level of NPPs is expected to be improved because the attacker's stealth is not guaranteed due to the immutability of monitored data in real-time (every 5000-6000ms) on the blockchain. In order for the developed system to be applied to a real power plant system, it is necessary to verify and evaluate whether it does not affect the performance of the safety system. Further work is needed on this point.

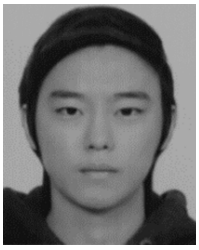
APPENDIX

Video clip about the system is available on https://youtu.be/9Xz7F5qVCus. Source codes of the system can be publicly available after this paper is accepted.

REFERENCES

[1] D.-Y. Kim, "Cyber security issues imposed on nuclear power plants," *Ann. Nucl. Energy*, vol. 65, pp. 141–143, Mar. 2014.
[2] N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet dossier," *Symantec-Secur. Response*, vol. 1, no. 2, pp. 1–69, 2011.
[3] B. Kesler, "The vulnerability of nuclear facilities to cyber attack," *Strateg. Insights*, vol. 10, no. 1, pp. 15–25, 2011.
[4] J.-G. Song, J.-W. Lee, G.-Y. Park, K.-C. Kwon, D.-Y. Lee, and C.-K. Lee, "An analysis of technical security control requirements for digital I&C systems in nuclear power plants," *Nucl. Eng. Technol.*, vol. 45, no. 5, pp. 637–652, 2013.
[5] *KINAC/RS-015, Regulatory Standard on Cyber Security for Computer and Information System of Nuclear Facilities*, South Korea, 2015.
[6] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview–national Institute of standards and technology internal report 8202," NIST Interagency/Internal Rep., 2018, pp. 1–57.
[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, Oct. 2008," Tech. Rep., 2019, p. 53. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] J.-G. Song, J.-W. Lee, C.-K. Lee, K.-C. Kwon, and D.-Y. Lee, "A cyber security risk assessment for the design of I&C systems in nuclear power plants," *Nucl. Eng. Technol.*, vol. 44, no. 8, pp. 919–928, 2012.
[9] M. K. Choi, P. H. Seong, and C. Y. Yeun, "Developing blockchain-based cyber security techniques in nuclear power plants," in *Proc. 13th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2018, pp. 164–167.
[10] I. Bashir, *Mastering Blockchain Distributed*. Birmingham, U.K.: Packt Publishing Ltd., 2017.
[11] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.
[12] B. Hill, P. Valencourt, and S. Chopra, *Blockchain Quick Reference*, 1st ed. Birmingham, U.K.: Packt Publishing, 2018.
[13] S.-K. Kim, C. Y. Yeun, E. Damiani, Y. Al-Hammadi, and N.-W. Lo, "New blockchain adoptation for automotive security by using systematic innovation," in *Proc. IEEE Transp. Electrific. Conf. Expo, Asia–Pacific (ITEC Asia-Pacific)*, May 2019, pp. 1–4.
[14] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart., 2018.
[15] M. S. Niaz and G. Saake, "Merkle hash tree based techniques for data integrity of outsourced data," in *Proc. CEUR Workshop*, vol. 1366, 2015, pp. 66–71.
[16] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
[17] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
[18] J. Chen, G. Liang, Z. Cai, C. Hu, Y. Xu, F. Luo, and J. Zhao, "Impact analysis of false data injection attacks on power system static security assessment," *J. Mod. Power Syst. Clean Energy*, vol. 4, no. 3, pp. 496–505, Jul. 2016.
[19] A. Robles-Durazno, N. Moradpoor, J. McWhinnie, G. Russell, and I. Maneru-Marin, "PLC memory attack detection and response in a clean water supply system," *Int. J. Crit. Infrastruct. Prot.*, vol. 26, Sep. 2019, Art. no. 100300.
[20] T. H. Morris and W. Gao, "Industrial control system cyber attacks," in *Proc. 1st Int. Symp. ICS SCADA Cyber Secur. Res.*, 2013, pp. 22–29.
[21] B. Lim, D. Chen, Y. An, Z. Kalbarczyk, and R. Iyer, "Attack induced common-mode failures on PLC-based safety system in a nuclear power plant: Practical experience report," in *Proc. IEEE 22nd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Jan. 2017, pp. 205–210.



MOON KYOUNG CHOI received the B.S. and M.S. degrees in nuclear and quantum engineering from the Korea Advanced Institute of Science and Technology (KAIST), South Korea, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree. He was a Research and Teaching Assistant with KAIST. He has studied the areas, such as security, safety of nuclear power plants, human factors engineering, and I&C systems in nuclear power plants. He has numerous conference and journal publications. His current research interests include cyber security of nuclear power plants, block chain, and ICT technologies.

CHAN YEOB YEUN (Senior Member, IEEE) received the M.Sc. degree from Royal Holloway, in 1996, and the Ph.D. degree in information security from the University of London, in 2000. He joined Toshiba TRL, Bristol, U.K. He was the Vice President of the Mobile Handset Research and Development Center, LG Electronics, Seoul, South Korea, in 2005. He was responsible for developing the Mobile TV technologies and its security. He left LG Electronics, in 2007. He has been with ICU (KAIST), South Korea, since August 2008, and has been with Khalifa University Science and Technology, since September 2008. He is currently an Associate Professor with the Electrical Engineering and Computer Science Department and an Active Member with the Center for Cyber-Physical Systems (C2PS). He is also a Lecturer in information security and engineering courses with Khalifa University. He has published more than 130 journal and conference papers and nine book chapters. He holds ten international patent applications. His current research interests include cyber security, the IoT/USN security, cyber physical system security, cloud/fog security, and cryptographic techniques. He serves several steering committee members of the international conferences and the editorial board members of the International Journals.

POONG HYUN SEONG received the B.S. degree in nuclear engineering from Seoul National University, Seoul, in 1977, and the M.S. and Ph.D. degrees in nuclear engineering from the Massachusetts Institute of Technology, Cambridge, in 1984 and 1987, respectively. He was with the Korean Nuclear Safety Commission, from September 2006 to August 2009. He was a Commissioner with the Korea Atomic Energy Promotion Council, from November 2016 to November 2019. He is currently a Professor of nuclear and quantum engineering with the Korea Advanced Institute of Science and Technology, Daejeon, South Korea. He has published numerous articles on nuclear power plant human–machine interface and instrumentation and control system development and validation. His research interests include research and development on human factor engineering/human reliability assessment, digital instrumentation and control systems reliability, cyber security of nuclear power plants, and so on. He was the President and the Executive Vice President of the Korean Nuclear Society, from September 2014 to August 2016. He was the Chair of the Human Factors Division, American Nuclear Society (ANS), from June 2006 to June 2007. He served as an Editor-in-Chief for the International Journal *Nuclear Engineering and Technology (NET)*, from September 2003 to August 2008. He serves as an Editorial Board Member for *Journal Reliability Engineering and System Safety (RESS)*.