Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.579

스마트 컨트랙트 기반의 산업제어시스템 접근 제어 메커니즘*

조 민 정,† 이 창 훈‡
서울과학기술대학교 컴퓨터공학과

Access Control Mechanism for Industrial Control System Based Smart Contract*

Minjeong Cho,† Changhoon Lee‡
Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

산업제어시스템은 센서, 액추에이터 등의 다양한 물리적인 장치들로 구성된다. 과거에 미국에서 발생했던 상수도 시설 원격 접속 사고, 전력 제어시스템 감염 등 대규모 피해를 가져온 보안 사고는 산업제어시스템 접근 제어의 취약점으로 인해 발생했다. 물리적 장치에 대한 접근제어는 신뢰할 수 있는 시스템을 통해 이뤄져야한다. 그러나 폐쇄망으로 구성된 산업제어시스템 내부에 단일 접근 제어 시스템을 구축하는 것은 신뢰성을 보장받을 수 없다. 또 단일 접근 제어 시스템은 장애나 사고 발생시 접근 제어 시스템이 작동 불가능해지므로 다른 접근 제어 방법이나 시스템이 필요하다. 본 논문에서는 신뢰성과 안정적인 운영을 제공하기 위해 운영 계층에 블록체인을 이용하고, 스마트 컨트랙트 배포를 통한 접근제어 메커니즘을 제안한다. 또한, 무결성, 기밀성보다 가용성이 우선시 되는 산업제어시스템을 고려하여 각 산업 환경에 맞게 소모할 컴퓨팅 자원을 설정할 수 있도록 신뢰 점수를 이용했다. 본 논문에서 제안하는 시스템은 기 제안된 블록체인 기반의 접근제어 시스템과 달리 현재 운영중인 산업제어시스템의 특성에 맞게 구성했다.

ABSTRACT

Industrial control systems consist of various physical devices such as sensors, actuators. Security Infringement such as waterworks facilities Remote Access Infringement and power control systems Infection have been occured by vulnerability of Access Control. Access control to physical devices must be fulfilled with a reliable system. However, Having a single access control system inside company can not guarantee reliability. In addition, when single access control is struggled with error or infringement, access control system is totally unavailable. so system requires a additional access control method or system. In this paper, we proposed access control mechanism for reliable and stable operation using blockchain and smart contract. Proposed Mechanism using trust score to consider resources to be consumed depending on each industrial environment in consideration of the industrial control system where availability is more important than integrity and confidentiality. Unlike other blockchain-based access control system, proposed system is designed for the currently operating industrial control system.

Keywords: Blockchain, Smart Contract, Industrial Control System(ICS), Access Control, Availability

Received(02. 12. 2019), Modified(05. 20. 2019), Accepted(05. 21. 2019)

* 본 논문은 2018년도 한국정보보호학회 동계학술대회에 발표한 우수논문을 개선 및 확장한 것임

* 본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (원전 비안전등급 제어기기(DCS) 사이버침해 예방 및 탐지 기술 개발, No. 20161510101810)

† 주저자, chomj@seoultech.ac.kr

‡ 교신저자, chlee@seoultech.ac.kr(Corresponding author)

I. 서 론

캘리포니아 운하 운영 마비 사고, 부셰르 원전 공격, 미국 상수도 시설 펌프 작동 시스템 파괴, 우크라이나 정전 상태 등 산업제어시스템을 대상으로 하는 공격이 지속되고 있다[1][2]. 2017년 카스퍼스키랩의 산업 사이버보안 비즈니스 어드밴티지 현황 보고서[3]에 따르면 표본으로 선택된 회사 가운데 54%에서 산업용 제어시스템과 관련된 보안 사고가 발생하였으며, 2018년 상반기 산업용 제어시스템 컴퓨터 보안위협 현황에 따르면 카스퍼스키랩 제품을 설치한 ICS 컴퓨터 중 41.2 %가 한번 이상 공격을 받았고 지난해 상반기부터 지속적으로 증가하는 추세이다[4].

특히, 미국 LA 교통시스템 마비, 호주 퀸즈랜드 하수 유출 사고 등은 접근제어 실패로 인해 발생한 보안사고이다. NCCIC(National Cybersecurity and Communications Integration Center)의 2014년~2017년간의 보고서[5]에 따르면 인적 자원 관리 실패 및 접근 제어 실패는 최상위 6개 취약점에 지속적으로 포함되었다. 또, Fireeye의 ICS 보고서[6]에 따르면 산업제어시스템의 주요 취약점에 취약한 사용자 인증이 포함되었다.

산업제어시스템은 물리적 요소들을 제어하는 시스템으로 물리적 요소를 제어함에 있어 신뢰할 수 있는 접근제어를 필요로 한다. 산업제어시스템은 일반적으로 폐쇄망으로 구성되어 내부에 신뢰할 수 있는 접근제어 시스템을 구축할 필요가 있다. 그러나 폐쇄망 내에 단일 인증 시스템을 구축하는 것은 신뢰성을 보장받을 수 없다. 또한, 단일 인증 시스템이 침해 사고 및 장애 발생으로 사용할 수 없는 경우 전체 시스템이 가동이 중단되거나 인증 시스템을 사용하지 않고 운영되어야 하는 단일장애점(POF, Point of Failure)이 된다.

본 논문에서는 산업제어시스템에서 제어계층의 접근제어를 위해 스마트 컨트랙트 기반의 접근 제어 메커니즘을 제안했다. 본 논문에서 제안하는 메커니즘에서는 인사 관리 시스템과 연계하여 접근제어시에 사람의 개인키로 명령을 서명하여 인증 받도록 했다. 또한, 산업제어시스템이 가용성 및 기밀성보다 무결성이 우선시 됨을 고려하여 신뢰 점수 시스템을 도입했다. 명령어에 요구되는 신뢰 점수에 따라 인증 받아야하는 노드의 개수를 정할 수 있으며 가용성에 문제가 없는 제어명령의 경우 신뢰 점수를 0으로 부여하여 인증을 받지 않을 수도 있다.

II. 산업제어시스템

산업제어시스템은 SCADA(Supervisory Control And Data Acquistition) 시스템, DCS(Distributed Control System), PLC(Progammable Logic Controllers) 등으로 구성된 시스템으로 전기, 수도, 폐수, 천연 가스, 운송 등 분산된 자산(asset)을 제어하는데 사용된다[7]. 산업제어시스템은 교체주기가 15~20년으로 일반적인 IT 시스템의 교체 주기가 3~5년인 것에 비해 긴 편이다. 또한 사고 발생 시 업무 불편 및 지연 뿐만 아니라 산업현장 운영 중단으로 인해 인명 피해 및 대규모 물리적, 경제적 피해를 입을 수 있다[8].

산업제어시스템은 운영 계층, 제어 계층, 현장장치 계층으로 구분할 수 있다[8]. 운영계층은 HMI(Human Machine Interface), EWS(Engineering Workstation) 등으로 이뤄지며 시스템의 상태를 모니터링하거나 제어 명령을 전송하는 역할을 한다. 제어 계층은 현장장치에서 계측, 수집한 데이터를 운영계층으로 전달하거나 운영계층에서 전송한 제어 명령을 받아 현장장치를 제어하는 역할을 수행한다. 제어계층은 PLC, DCS, RTU(Remote Terminal Unit)등으로 구성된다. 현장장치계층은 Sensor, Actuator 등 상태 데이터를 계측, 수집하거나 제어하는 장치로 구성된다.

산업제어시스템은 폐쇄망으로 운영되기를 권고되며 회사의 네트워크와 최소한 논리적으로 분리되어있어야한다. 또한 회사 네트워크 및 외부 네트워크의 연결이 필요한 경우 두 개의 네트워크 사이에 최소한 방화벽이 설치된 DMZ(Demilitarized Zone)가 존재해야 한다[7].

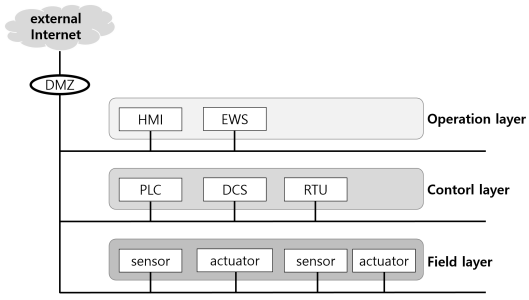

Fig. 1. Configuration of Industrial Control System

III. 스마트 컨트랙트

3.1 블록체인

블록체인[9]은 2008년 Satoshi Nakamoto가 제안한 암호 화폐 비트코인(bitcoin)에서 사용된 개념으로 P2P 거래를 안전하게 하기 위하여 데이터의 무결성을 보장해주는 데이터 분산 저장 방법이다.

블록체인의 개념은 Fig. 2와 같다. 블록체인은 데이터를 트랜잭션 단위로 나눠서 블록(block)에 저장한다. 트랜잭션은 트랜잭션 생성자의 개인키로 서명이 된 데이터 집합을 의미한다[9][10]. 비트코인에서 암호 화폐 소유 내역과 수신자의 공개키를 해쉬하여 송신자의 개인키로 서명한 것을 트랜잭션이라 한다. 이더리움은 송신금액, 스마트 컨트랙트를 위한 추가적인 데이터, 코드 실행을 위한 수수료, 송신자의 서명 등으로 이루어진 데이터 집합을 트랜잭션이라 한다.

블록에는 트랜잭션 외에 시간정보(timestamp), 블록 식별자(block id), 이전 블록의 해쉬값 등 부가적인 정보도 포함된다. 이전 블록의 해쉬값은 블록체인의 무결성을 보장하는 요소 중 하나이다. 여기서 사용된 해쉬값이란 일방향 함수인 해쉬함수를 통해 가변길이의 데이터를 고정 길이의 값으로 출력한 결과 값으로 입력에 따라 출력이 다르며, 출력을 보고 입력을 유추하기 힘들다. 또한 같은 출력을 내는 서로 다른 입력을 찾기 힘들다[11].

블록체인에서 이전의 블록을 해쉬하는 규칙을 합의 규칙(consensus protocol)이라 칭한다. 합의 규칙은 노드들 간에 무결성과 신뢰성을 제공하는 블록을 생성하기 위해 필요하다[12]. PoW(Proof of Work), PoS(Proof of Stake). PBFT, Ripple 등이 있다[13]. 이때 블록체인의 합의 과정에 참여하는 객체를 노드라고 한다.

블록체인은 모든 사람이 모든 블록을 갖고 있음을 전제로 하기 때문에 악의적인 사용자가 블록체인의 내용을 조작하기 위해서는 다수의 컴퓨터를 조작할 수 있어야한다. 다수의 컴퓨터에 저장된 블록체인을 조작하지 않고 블록체인을 조작하기 위해서는 현재 가진 해쉬값과 동일한 해쉬값을 만들 수 있는 입력을 찾아야하므로 공격이 어렵다.

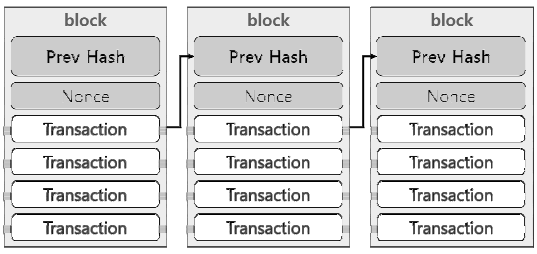

Fig. 2. Concept of Blockchain

3.2 블록체인의 유형

블록체인은 크게 Public blockchain, Consortium blockchain, Private blockchain로 구분할 수 있다[14].

Public blockchain이란 모든 노드가 합의 결정과정에 참여할 수 있고 블록체인을 열람할 수 있는 완전히 탈중화된 시스템이다.

Consortium blockchain이란 허가된 노드만 합의 결정과정에 참여할 수 있다. 블록체인의 열람 권한은 운영 방침에 따라 공개되거나 제한될 수 있다. 허가된 노드만 합의 결정과정에 참여할 수 있다는 점에서 부분적으로 중앙화되어 있다.

Private blockchain이란 한 기업에 의해 운영되는 것으로 완전히 중앙화된 시스템이다. 운영기업은 합의 결정과정에 참여 가능한 노드, 블록체인의 열람 권한등 블록체인에 관련된 모든 권한을 결정할 수 있다.

3.3 스마트 컨트랙트

스마트 컨트랙트는 1996년 Nick Szabo에 의해 제안된 개념이다[10][15]. 처음 제안된 스마트 컨트랙트는 디지털 형식으로 제시된 일련의 모든 규약을 의미하는 것으로 원초적인 예시로 자동 판매기가 있다. 비트코인은 거래를 위하여 스크립트를 통해 거래를 보장한 것으로 스마트 컨트랙트적 요소가 존재하지만 튜링 불완전 언어로 스크립트 형식의 코드 데이터를 배포할 수 없었다[10]. 그러나 튜링 완전 언어를 포함한 이더리움과 같은 블록체인들이 제안되며 블록체인에 스마트 컨트랙트를 배포하는 기술이 활성화 되었다.

IV. 사전연구

이찬영, 정만현, 민병길은 2017년 시간 동기화 방식 OTP를 이용하여 산업제어시스템에서 제어명령

무결성을 유지하는 방안을 제안했다. 해당 논문에서는 운영계층과 제어계층에 Add-on 장치를 추가적으로 설치하여 Add-on 장치에서 OTP 값을 생성, 검증하여 제어명령의 무결성을 검증했다. 운영계층에서는 제어명령과 생성된 OTP 값을 제어계층에 전달하며, 제어계층에서는 전달받은 OTP 값과 제어계층의 Add-on 장치에서 생성한 OTP 값을 비교하여 제어명령을 실행하거나 거부한다[16].

Yuanyu Zhang, Shoji Kasahara, Yulong Shen, Xiaohong Jiang, Jianxion Wan은 2018년 IoT(Internet Of Thing)에서 사용가능한 스마트 컨트랙트 기반의 접근 제어를 제안했다[17]. 제안하는 시스템은 ACC(Access control contract), JC(Judge contract), RC(Register contract)로 이뤄져있다. ACC는 하나의 주체가 하나의 객체에 접근 할 수 있는 권한을 저장하고 있으며 ACC는 여러 개가 배포될 수 있다. JC는 ACC에서 잘못된 접근을 하는 경우 부과될 패널티를 리턴한다. RC는 ACC와 RC가 배포되고 업데이트 되는 과정을 기록하고 관리한다.

Otto Julio Ahlert Pinno, Andre Ricardo Abed Gregio, Luis C. E. De Bona는 2017년 IoT에서 사용가능한 접근제어 아키텍처를 제안했다[18]. 제안하는 아키텍처에서는 Context Blockchain, Relationships Blockchain, Rules Blockchain, Accountability Blockchain으로 이뤄져 있다. Context Blockchain에서는 인가 결정시 필요한 조건들을 저장한다. Accountability Blckchain은 책임 추적성을 위해 모든 인가되고 거부된 접근을 기록한다. Rule Blockchain에서는 인가 규칙들을 저장한다. Relationships Blockchain에서는 User Block, Group Block, Device블록으로 나누어 블록들간의 관계와 공개 크리덴셜을 저장한다. 접근제어는 각 blockchain 내의 정보들을 이용하여 이뤄진다.

Aafaf Ouaddah, Anas Abou Elkalam 그리고 Abdellah Ait Ouahman은 블록체인 기반의 IoT 접근 제어 프레임 워크를 제안했다[19]. 해당 논문에서 제안하는 시스템은 비트코인의 UTXO(Unspanted Transaction Ouput)에서 착안하여 접근 권한을 transaction을 통해 인가하며 이를 UTXO 형식으로 관리하는 시스템이다. 접근 인가는 IoT 소유자만이 할 수 있으며 IoT 소유자는 접근 정책을 생성가능하며 UTXO 형식으로 접근 인가 트랜잭션을 발생시킬 수 있다. 해당 시스템에서는 접근의 인가, 접근을 위한 권한 토큰의 사용, 접근 권한 폐기 등의 기능이 있다.

V. 스마트 컨트랙트 기반의 접근제어시스템

본 논문에서 제안하는 메커니즘은 일반적으로 폐쇄망으로 구성되는 산업제어시스템의 제어계층과 운영계층에서 사용되는 시스템이다. 따라서 본 논문에서 제안하는 메커니즘을 프라이빗 블록체인으로 구성하여 현재 운영되는 시스템에 변경 없이 사용할 수 있도록 한다. 텍스트기반의 비밀번호 방식은 공유하기 쉬우며 제 3의 소프트웨어가 사용하거나 외부 회사의 직원 방문시에도 같은 비밀번호를 공유하여 사내 직원과 같은 권한을 주어야한다. 그러나 각 직원별 개인키를 발급함으로써 공유를 어렵게하며 타 회사 직원 방문시에도 게스트 사용자로 등록하여 별도의 개인키와 필요한 권한만을 발급해줄 수 있으며 폐기 또한 쉽다. 또한 등록되는 모든 공개키는 블록체인 형식으로 여러 운영계층의 기기에 저장되어 공격자가 다수의 운영계층을 조작하지 않으면 공격이 불가능하다.

본 논문에서 제안하는 메커니즘은 인적 자원 관리 시스템과 연계하여 접근 제어를 하는 것으로 5.1에서는 인적 자원 관리를 위한 스마트 컨트랙트에 대하여 설명으로 하고, 5.2에서는 각 인적 자원이 시스템을 운용하고 운용 내역을 저장하는 스마트 컨트랙트를 설명하며 5.3에서는 운용 요청을 검증하고 운용 결과를 기록하는 스마트 컨트랙트를 설명한다.

5.1 인적 자원 관리 스마트 컨트랙트

NCCIC에 따르면 2015~2017년 취약점 Top six에 임직원 식별 및 인증과 계정관리가 지속적으로 포함되었다. 임직원 식별 및 인증이란 직원이 회사를 떠날 때 계정 확보가 어려워지며, 관리자 액세스 권한이 있는 사용자의 경우 매우 민감함을 의미한다[5].

본 논문에서 제안하는 시스템의 인적 자원 관리 스마트 컨트랙트는 직원의 정보 관리와 블록체인을 연계하여 직원의 권한이 상승 및 하락하는 경우 즉각적으로 반영될 수 있도록 하며 직원이 이직이나 퇴직으로 인해 회사에서 권한이 사라질 때 또한 관리할 수 있다.

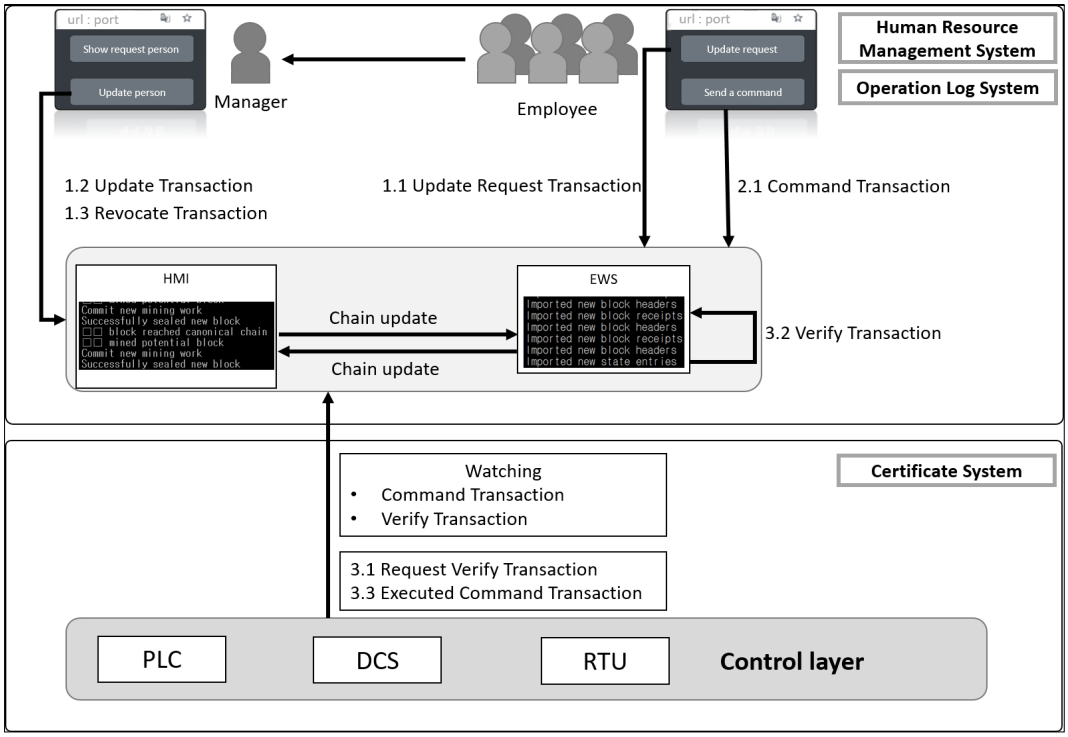

Fig. 3. Proposed System

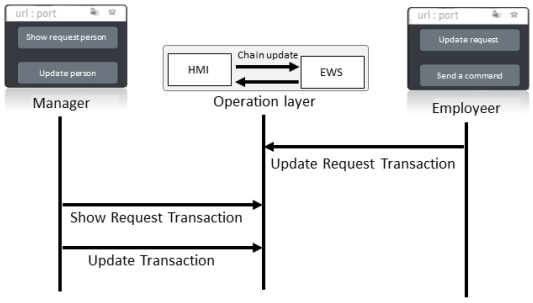

Fig. 4. Sequence Diagram of Human Resource System

5.1.1 갱신 요청 트랜잭션(Update Request Transaction)

직원의 개인키는 직원 본인만이 갖고 있어야 하며 관리자도 알 수 없어야한다. 따라서 신규 직원은 공개키, 개인키 쌍을 생성하고 공개키와 직원 식별번호를 파라미터로 하여 갱신 요청 트랜잭션을 발생시킨다. 발생된 트랜잭션은 모든 운영계층의 기기에 블록체인으로 저장되어 모든 노드가 볼 수 있다. 트랜잭션이 발생하면 인적 자원 관리 스마트 컨트랙트 내에는 요청한 갱신 내용이 직원 식별번호로 구분되어 저장된다.

5.1.2 갱신 트랜잭션(Update Transaction)

인사 관리자는 발생된 Update Request Transaction을 확인하고 해당 transaction에 들어 있는 직원의 식별번호를 확인하여 권한을 부여한다. 직원의 권한 부여는 갱신 트랜잭션을 통해 이루어진다. 기존 직원의 권한을 상승 또는 하락 시키는 경우에도 갱신 트랜잭션을 이용한다.

갱신 트랜잭션은 관리자 권한을 가진 계정만 발생시킬 수 있으며, 트랜잭션 발생시에 직원의 식별번호, 직원의 권한을 입력으로 한다.

5.1.3 폐기 트랜잭션(Revocate Transaction)

직원이 이직하거나 퇴직하는 경우 해당 계정은 계정 폐기 목록에 등록되어 관리된다. 폐기 트랜잭션은 인사 직원만 발생시킬 수 있으며, 입력으로 직원의 식별번호만 받는다. 직원이 퇴직하거나 은퇴하는 경우 모든 권한은 박탈된다. 휴직은 이에 해당하지 않

Table 1. Grade Access Algorithm

```
Input: S is the array that mapping command and need score
 1:  T_OC := Operation Command Transaction
 2:  T_VR := Verify Request Transaction
 3:  T_V := Verify Transaction
 4:  T_EC := Executed Command Transaction
 5:  N := need score
 6:  sum = 0
 7:  if T_OC upload to blockchain
 8:          sender, command, signature ← T_OC
 9:          T_VR (sender , command, signature)
10:          N ← S[command]
11:          while sum == N
12:                  if T_V upload to blockchain
13:                          result ← T_V
14:                  if result != 0
15:                          sum ← sum+ result
16:                  else
17:                          return alarm;
18l                  end if
19:          end while
20:          command executed
21:          T_EC(sender, command)
22:  end if
```

는다. 퇴직했던 직원이 복귀하는 경우에는 직원 식별 번호를 새로 부여받은 후 갱신 요청 트랜잭션을 통해 새로운 직원으로 등록을 하여야 한다.

5.2 운용 로그 스마트 컨트랙트

행위의 부인은 산업제어시스템의 보안 위협중 하나이다. 운영 계층 구성 요소를 통해 처리된 행위의 책임 추적성을 확보하지 못하는 경우 사고발생시 원인 파악에 많은 시간과 노력이 소요하게 되며 무결성에 영향을 미칠 수 있다[20]. 블록체인을 통해 운영 계층 구성 요소를 통해 처리된 행위를 기록함으로써 행위의 부인을 막을 수 있으며, 기록의 무결성 또한 보장할 수 있다.

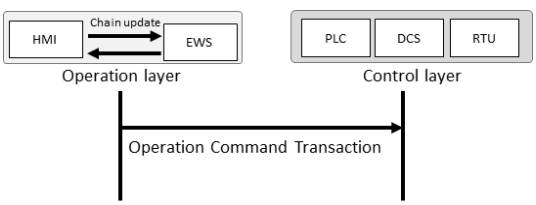

Fig. 5. Sequence Diagram of operation log system

5.2.1 명령 트랜잭션(Command Transaction)

본 시스템에서 운영 계층에서 제어 계층으로 명령을 내리는 것은 운용 로그 스마트 컨트랙트을 통해 실행된다. 직원이 제어 명령을 통해 제어 계층의 요소를 제어하고자 하는 경우 운용 로그 스마트 컨트랙트를 이용하여 명령 트랜잭션을 발생시킨다. 명령 트랜잭션은 제어 명령, 직원의 개인키를 이용한 제어명령에 대한 서명, 직원의 식별 번호를 입력으로 받는다. 제어 계층은 발생된 명령 트랜잭션을 확인하고 인증서 검증 스마트 컨트랙트를 실행한다.

5.3 검증 스마트 컨트랙트

운영 계층에서 제어 계층으로 제어 명령 및 업데이트 명령은 명령 트랜잭션을 통해 이뤄진다. 제어계층에서는 트랜잭션을 확인해 사용자, 사용자의 서명, 제어 명령을 확인할 수 있다. 제어계층은 해당 내용을 토대로 운영계층에게 검증을 요청한다. 이때 가용

성을 위하여 검증에 요구 점수를 지정할 수 있다. 요구 점수를 통한 접근제어 알고리즘은 Algorithm Grade Access와 같다.

운영 계층의 각 구성 요소는 신뢰 점수를 가지고 있다. 신뢰 점수는 관리자가 정할 수 있으며, 시스템에 물리적인 접근이 어렵거나 시스템에 접근 권한이 적을수록 높은 신뢰 점수를 받을 수 있다. 제어계층은 운영계층이 전달한 결과를 합산하여 요구 점수를 만족하는지 확인한다. 예를 들어 일반EWS의 신뢰 점수는 1, 관리자 EWS의 신뢰 점수가 3일 때 업데이트 명령의 요구 신뢰 점수가 5라면 일반 EWS 2대의 검증과 관리자 EWS 1대에서 발생한 검증 트랜잭션을 통해 업데이트 명령이 실행될 수 있다.

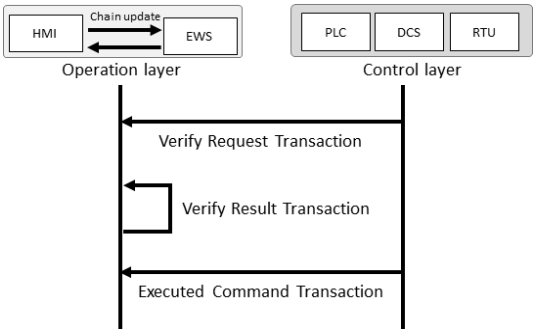

Fig. 6. Sequence Diagram of verify system

5.3.1 검증 요청 트랜잭션(Verify Request Transaction)

명령 트랜잭션을 확인한 제어 계층 요소는 운영 계층 요소에게 검증을 요청할 수 있다. 검증 요청 트랜잭션을 통해 검증을 원하는 명령과 서명을 랜덤으로 여러 운영 계층 요소에 전달하여 검증을 요청한다.

5.3.2 검증 트랜잭션(Verify Transaction)

검증 요청 트랜잭션을 받은 운영 계층 요소는 전달받은 값을 통해 서명을 검증하며, 이 결과를 운영 계층 요소의 개인키로 서명하여 전달한다. 제어 계층 요소는 검증 트랜잭션을 통해 반환된 결과와 신뢰 점수를 확인한다. 결과의 합이 요구되는 신뢰 점수를 만족하면 해당 명령을 실행한다. 가용성을 위해 빈번하게 일어나는 명령이나 해당 명령이 제어계층 요소에 변화를 가져오지 않는 경우에 요구 신뢰 점수를 0으로 설정하여 검증을 하지 않고 실행할 수 있다.

5.3.3 실행 결과 트랜잭션(Executed Command Transaction)

실행결과 트랜잭션은 제어계층이 명령을 실행시킨 뒤 발생시키는 트랜잭션으로, 받은 명령을 오류 없이 실행한 경우 트랜잭션을 발생시키고 장애나 중단으로 실행을 하지 못한 경우 트랜잭션을 오류 내용과 발생시킨다. 해당 트랜잭션은 실행된 명령의 신뢰 점수에 따라 일정 점수를 초과하는 경우에만 발생된다.

VI. 분 석

본 장에서는 [17], [18], [19]과 제안한 시스템을 비교했다. 비교는 Target, Blockchain type, Realtime-timeliness, Accountablility goal, Miner, Flexibility 의 부분으로 나눠서 한다.

Table 2. Comparison with other systems

	[17]	[18]	[19]	proposed
Target	IoT	IoT	IoT	ICS
Blockchain type	public	public	public	private
Realtime-timeliness	-	-	-	O
Accountability goal	giving penalty	posterior analysis	-	make system available quickly
Miner	based platform miner	IoT device	-	operation layer device
Flexibility	-	-	-	O

- : 논문에서 별도의 언급이 없음을 의미함.

6.1 Target & Blockchain Type

[17], [18], [19]에서 제안하는 시스템은 IoT를 위한 시스템으로 퍼블릭한 환경에서 구성되어 IoT 기기 혹은 서버의 소유주가 블록체인에 참가한다. 반면, 본 논문에서 제안하는 시스템은 폐쇄망 내에서 사용하는 프라이빗 블록체인으로 블록체인의 노드 구성에 참여는 한 회사의 자원으로 구성된다. 프라이빗 블록체인은 인가된 사용자만이 접근한다고 가정하므로 마이닝 과정을 생략할 수 있고, 마이닝 과정의 생

략은 컴퓨팅 자원을 절약할 수 있다.

6.2 Realtime-timeliness

산업제어시스템에는 실시간성이 요구된다. 그러나 [17]은 이더리움 기반으로 구성한 시스템으로 이더리움의 마이닝 시간에 영향을 받는다. 접근을 요구하고 접근 허가를 받으려면 관련 트랜잭션들이 블록에 올라가야하고 이는 기반 플랫폼의 마이닝 시간에 의존한다. [18]은 블록의 생성속도가 인가의 속도에 영향을 줌을 언급했다. 제안하는 시스템에서는 타 시스템의 플랫폼을 사용하지 않고 프라이빗으로 구성되는 시스템을 사용하며 마이닝 과정을 생략하여 접근을 요청하는 트랜잭션이 바로 처리된다.

6.3 Accountability goal

책임 추적성은 산업제어시스템에서 필수이다. 접근 허가 및 거부 여부는 블록체인내의 기록 추적을 통해 알 수 있다. 그러나 실제실행 여부는 알 수 없다. [18]은 기록 허가 및 거부 내역을 기록하여 수행된 기록에 대해 사후 분석을 할 수 있다고 하였으며, [17]은 [18]과 같이 인가된 기록 혹은 거부된 기록 이외에 패널티를 부과하고 부과한 내역을 기록하도록 했다. 그러나 산업제어시스템은 잘못된 접근 발생시 패널티가 필요하지 않으며 즉시 잘못된 접근에 대한 사유를 파악하여야 한다. 제안하는 시스템의 잘못된 접근 추적 목표는 빠른 원인 파악 및 정상 시스템 재가동으로 접근이 실제 실행된 후에도 트랜잭션을 발생시켜 접근인가 후 해당 명령이 실행되었는지 확인 가능하도록 구성했다.

6.4 Miner

블록체인의 중요한 구성요소 중 하나는 마이너이다. 합의과정에 참여하는 마이너는 트랜잭션의 검증 및 해쉬값 생성을 위해 계산 능력이 필요하다. 또한 마이너의 역할 및 능력은 블록체인의 블록 생성 속도에 영향을 준다. [17]의 마이너는 [17]에서 제안한 시스템이 기반으로 하는 이더리움 플랫폼의 마이너이다. 이는 마이너의 성능 및 참여자를 필요에 따라 변경할 수 없음을 의미한다. [18]의 마이너는 IoT 기기이다. 따라서 IoT 기기가 일정 수준의 메모리와 계산 능력을 갖춰야 한다. 그러나 산업제어시스템에서 IoT 기기와 비슷한 계층이라 볼 수 있는 센서, 계측기 등은 일반적으로 메모리와 계산 능력을 갖추고 있지 않으며 시스템 도입을 위해 해당 능력을 갖추도록 하는 것은 비현실적이다. 따라서 제안하는 시스템에서는 산업제어시스템에서 계산능력이 있는 운영 계층을 마이너로 선정하여 제안하는 메커니즘의 성능 및 접근 제어 역할에 지연이 없도록 했다.

6.5 Flexibility

산업제어시스템에서 가용성은 무결성 및 기밀성보다 우선시 되는 경우가 있다. 그러나 다른 종류의 접근 및 권한 요청에 동일한 수준의 접근 제어가 적용될 경우, 가용성을 만족하지 못할 수 있다. 따라서 빈번히 일어나는 접근에 대해서는 접근 제어를 위한 비용이 작아야하며, 자주 일어나지 않으나 시스템의 가용성에 큰 문제를 가져올 수 있는 업데이트 명령 같은 경우 접근 제어의 비용이 커야한다. [17], [18], [19]에서 제안된 시스템은 모든 접근 권한 요청에 동일한 수준의 검증을 수행한다. 그러나 본 논문에서 제안하는 시스템에서는 요구하는 권한의 수준에 따라 검증의 수준을 설정할 수 있다.

VII. 결 론

블록체인에 기반한 접근제어 시스템은 주로 데이터 혹은 IoT를 대상으로 하여 일반적인 컴퓨터 시스템처럼 가용성보다 무결성 혹은 기밀성이 우선시된다. 그러나 산업제어시스템에서 사용할 접근제어는 무결성 기밀성보다 가용성이 우선시되어야한다. 본 논문에서는 산업제어시스템에서 적용 가능한 스마트 컨트랙트 기반의 접근 제어 방식을 제안했다.

산업제어시스템은 시동 후 장기간 장비의 교체가 이루어지지 않으며, 업그레이드 또한 쉽지 않다. 따라서 본 시스템에서는 비교적 장비의 업그레이드가 쉬운 운영 계층의 요소를 이용하여 접근 제어를 제공할 수 있도록 하였으며 인사 관리 시스템을 동시에 운영할 수 있도록 했다.

본 논문에서 제안하는 시스템을 기존에 제안된 [17], [18], [19]과 비교를 했다. 기존에 제안된 시스템은 IoT를 위한 접근제어 시스템으로 가용성보다 무결성이 우선시 되었다. 그러나 본 논문에서 제안하는 시스템은 산업제어시스템의 폐쇄망내에서 작동하는 마이닝과정이 생략되는 프라이빗 블록체인을 통해

블록체인 유지 부하를 감소시켰으며, 가용성을 고려하여 제어 명령의 종류에 따라 접근제어에 차등을 두는 방안을 마련했다. 또한 블록체인의 특성상 일부 운영 계층 요소의 장애 혹은 침해사고로 인증 시스템을 사용 할 수 없는 경우에도 다른 운영 계층 요소를 통해 산업제어시스템을 중단 없이 운영할 수 있다.

References

[1] Jae Hoon Nah and Jung Chan Nah, "Standardization Trend of Industrial Control System Security", Review of KIISC, 26(4), pp.28-35, Aug., 2016

[2] Jun Hyoung Oh, Young in You and Kyungho Lee, "Infrastructure Incident and Control System Standard Trend", Review of KIISC, 27(2), pp.5-11, Apr., 2017

[3] IT World, "infrasturcture Hacking Damage Security Incident", 'The most important "facts", numerical value and statistics related to security in 2018', http://www.itworld.co.kr/news/111098, 2019.02.11.

[4] Kaspersky Lab, "The State of Industiral Cybersecurity 2017", 2017

[5] "Security Requirements for Industrial Control System - Part 1: Concepts and Reference Model", TTAK.KO-12.0307-Part1, June, 2017

[6] NCCIC, "ICS-CERT Monitor November-December 2017 US-CERT ", 2017

[7] Fireeye, "2016 ICS Vulnerability Trend Report". 2016

[8] ZDNet Korea, "industirl control system security", http://www.zdnet.co.kr/view/?no=20171124160854, 2019.02.08

[9] Stouffer, K., Falco, J., and Scarfone, K. "Guide to industrial control systems (ICS) security". NIST special publication, 800(82), 2011.

[10] Nakamoto, S. "Bitcoin: A peer-to-peer electronic cash system.", Oct. 2008.

[11] Wood, G. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum project yellow paper, 2014.

[12] Stallings, William. Cryptography and network security: principles and practice. Practice (6th Edition), Pearson, 2008.

[13] Sungbum Lee, Boohyung Lee, Sein Myung and Jong-Hyouk Lee, "Security Analysis of Blockchain Systems: Case Study of Cryptocurrencies." Journal of The Korea Institute of Information Security & Cryptology, 28(1), pp5-14, Feb, 2018.

[14] Daehwa Rayer Lee and Hyoungshick Kim, "Block Chain Research Trend Analysis: focusing on the consensus algorithm." Review of KIISC, 28(3), pp5-10, 2018

[15] Zheng, Z., Xie, S., Dai, H. N., Chen, X., and Wang, H. "Blockchain challenges and opportunities: A survey." International Journal of Web and Grid Services, 14(4), pp352-375, 2018.

[16] Szabo, Nick. "Smart contracts: building blocks for digital markets." EXTROPY: The Journal of Transhumanist Thought, 1996.

[17] Chanyoung Lee, Manhyun Chung and Byung-gil Min, "Industrial control system control command integrity protection scheme using OTP(One-Time Password)", Review of KIISC, 27(2), pp.34-40, Apr., 2017.

[18] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., and Wan, J. "Smart Contract-Based Access Control for the Internet of Things.",6(2), pp1594-1605, Apri., 2019

[19] Pinno, O. J. A., Grégio, A. R. A., & De Bona, L. C. "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT." In: GLOBECOM 2017-2017 IEEE Globa

l Communications Conference. IEEE, pp. 1-6, 2017.
〔20〕 Ouaddah, A., Abou Elkalam, A., & A it Ouahman, A. , "FairAccess: a new Blockchain based access control fram ework for the Internet of Things.", Se curity and Communication Networks, 9(18), pp5943-5964 , Feb., 2017.
〔21〕 "Security Requirements for Industrial Control System - Part 3: Control Lay er", TTAK.KO-12.0307-Part3, Jun., 20 17

〈저자소개〉

조 민 정 (Minjeong Cho) 학생회원
2014년~2018년 2월: 서울과학기술대학교 컴퓨터공학과 학사
2018년 3월~현재: 서울과학기술대학교 일반대학원 컴퓨터공학과 석사과정
〈관심분야〉 정보보호(Personal Information), 암호학(Cryptography), 블록체인 (Blockchain) 등

이 창 훈 (Changhoon Lee) 종신회원
2001년: 한양대학교 자연과학부 수학전공 학사
2003년: 고려대학교 정보보호대학원 석사
2008년: 고려대학교 정보경영전문대학원 정보보호전공 박사
2008년 4월~2008년 12월: 고려대학교 정보보호연구원 연구교수
2009년 3월~2012년 2월: 한신대학교 컴퓨터공학부 조교수
2012년 3월~2015년 3월: 서울과학기술대학교 컴퓨터공학과 조교수
2015년 4월~현재 : 서울과학기술대학교 컴퓨터공학과 부교수
〈관심분야〉 정보보호(Personal Information), 암호학(Cryptography), IoT(Inter-net of Things), 디지털포렌식(Digital Forensics) 등