클라우드 기반의 스마트팩토리 환경에서 안전한 통신을 위한 메시지 프로토콜 설계

김계창*
*(주)에이블정보기술
e-mail:kkc@ableit.co.kr

A Design Message Protocol for Secure Communication in Cloud Based Smart Factory Environment

Kye-Chang Kim*
*Ableit Co., Ltd

요 약

4차산업혁명이 도래하고 기존의 생산제조기술과 IT기술이 접목된 ICT융합기술에 대한 기술발전이 급속도로 향상되고 있다. 기존의 설비제조환경은 기존 폐쇄망인 운영환경에서 새로운 신기술을 적용한 스마트팩토리 환경으로 변화하여 사용자의 업무능력을 향상시키고 있으며, 스마트팩토리에서 생산된 물품은 수요자의 니즈를 충족하고 있다. 하지만 기존의 OT환경이 아닌 IT환경에서 발생하는 취약점 및 공격기법에 대해서는 보안성 강화에 대한 연구가 필요하고, 이를 대응하기 위한 안전한 네트워크 시스템이 제공되어야 한다. 그러므로 본 논문에서는 클라우드 기반의 스마트팩토리 환경에서 안전한 통신을 위한 메시지 통신프로토콜을 제안하였다. 또한, 제안한 메시지 프로토콜에 대해서 보안성 평가 및 기존의 공격기법에 대해서 안전성을 분석하였다.

1. 서론

스마트팩토리는 생산과정의 전 단계에 대해 자동화를 수행하며 ICT기술과 융합하여 지능적인 생산체계를 구축한 스마트 공장을 말한다[1][3]. 각 국가 별로 스마트팩토리에 대한 연구를 활발하게 수행하고 있으며, 제조공정에 따른 디지털화, 연결성 강화, 인공지능, 빅데이터 등 신기술과 접목하여 기능 적용에 대한 사항에 중점을 두고 있다. 개방적이며 신기술이 접목된 스마트팩토리에 대한 보안위협은 더욱 커질 것이며, 이에 따른 보안위협이 발전되어 스마트팩토리 운영환경을 위협할 것이다. 대표적인 보안위협 및 공격사례에 대한 내용을 살펴보면 국외에서도 경제적, 물질적인 타깃에 대한 다양한 사고가 발생하고 있으며, 인명 피해도 발생하고 있다[2].

본 논문에서는 클라우드 기반의 스마트팩토리 환경에서 위의 언급된 보안취약점 및 공격기법에 대해 안전하게 통신을 수행하기 위한 메시지 통신프로토콜을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 스마트팩토리 정의 및 특징, 스마트팩토리 보안위협 및 사고사례에 대한 관련 연구를 수행하였다. 3장에서는 사용자 등록, 인증 및 통신 메시지를 설계하여 안전한 메시지 프로토콜을 제안하였다. 4장에서는 보안성 평가를 수행하여 기존의 공격기법에 대해서 안전성을 분석하였다. 마지막 5장에서는 논문의 결론을 맺는다.

2. 관련연구

2.1 스마트팩토리 정의 및 특징

스마트팩토리는 팩토리 내 설비와 기계에 센서가 부착되어 데이터가 실시간으로 수집, 분석되어 스마트팩토리 내 시스템환경이 모니터링 되고, 이를 분석해 스스로 제어 및 통제가 되는 환경을 말한다[2][4].

국내·외에서 활발하게 스마트팩토리 기술에 대한 연구가 진행되고 있으며, 기존의 폐쇄적인 환경에서 4차산업의 신기술(IoT, Big Data, Ai 등)과 융합하여 신규 시스템 환경이 구축되어 이를 운영하는 사용자의 업무능력을 향상시키고 있다.

현재의 스마트팩토리의 인식 변화는, 발전소·공장시설 등의 운영기술(OT : Operational Technology) 영역의 경우 과거 폐쇄망에 대한 외부로부터의 접근이 엄격하게 통제되어 바이러스 등 악성코드 위협에 따른 보안위협에서 안전하다고 인식되어 왔지만, 사용자의 업무 효율성, 최신기술 적용에 대한 효율성 개선 추구를 위해 외부의 IT영역과 접점이 늘어남으로써 더 이상 해커의 공격 및 보안위협으로부터 안전하지

가 않다고 인식되어지고 있다[3].

2.2 스마트팩토리 보안위협 및 사고사례

스마트팩토리는 제품의 생산을 목적으로 하는 특성상 일반적인 네트워크 환경과 다른 환경을 가지고 있다. 기존 보안의 우선순위가 기밀성, 무결성, 가용성이면, 스마트팩토리의 우선순위는 가용성, 무결성, 기밀성이라고 할 수 있다. 이를 위해 스마트팩토리의 보안성은 가용성이 강화될 수 있도록 보안성이 향상되어야 한다. 스마트팩토리의 대표적인 보안위협은 다음과 같다[1-2].

첫 번째, 물리적으로 외부에 노출되어 있는 장치의 특성을 활용한 물리적 접근 공격이 있다. 두 번째, 자동화를 위해 장치 간 연계 형태를 이루는 제어시스템을 타깃으로 하는 공격이 있다. 세 번째, 가용성을 중심으로 한 다수의 공정 제어 네트워크를 공격하는 기법이 있다. 네 번째, 생성 모니터링 및 유지보수를 위해 설치된 연계망을 공격하는 기법이 있다. 다섯 번째, 설비 도입 및 유지보수를 위해 연계된 공급망을 대상으로 공격하는 기법이 있다. 여섯 번째, 노후된 설비를 공격하는 공격기법이 있으며, 마지막으로 외부 인터넷과 연결된 부분을 타깃으로 노리는 공격이 있다[4].

국외 사고사례에 대해서 살펴보면 우선 베네수엘라의 구리 댐(Guri Dam)에서 블랫아웃이 발생하여 교통 및 국가시설이 마비되었다. 이 사고에 대해 조사를 한 결과 해킹, 테러리스트의 소행 또는 방화라는 여러 가지 분석들이 있었다. 즉, 물질적인 접근에 대한 보안위협과 및 노후시설의 취약점을 이용하여 국가 손실에 대한 사고가 발생하였다. 두 번째, 인도 원자력 발전소는 백도어 악성코드를 활용한 해킹기법으로 원전 1기 네트워크가 가동이 중단되는 상황이 발생하였다. 세 번째, 미국 풍력·태양광 발전소의 사고사례는 스마트팩토리 내 운영하는 방화벽의 취약점을 이용하여 발전소 가동이 중단되었으며, 이에 따른 경제적, 물질적인 피해 파급효과를 유발하였다[5].

3. 제안한 메시지 통신프로토콜 설계

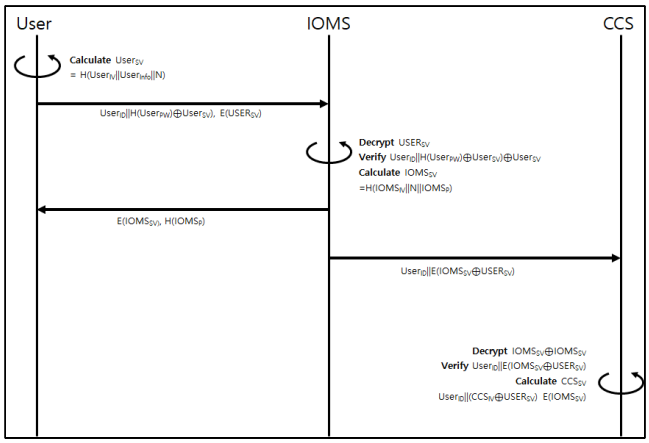
본 논문에서 제안한 메시지 통신프로토콜의 객체는 사용자, 내부운영 관리시스템 (IOMS : Internal Operations Management System), 클라우드 컴퓨팅 시스템 (CCS : Cloud Computing System)이며, 설계한 통신프로토콜의 파라미터는 [표 1]과 같다.

[표 1] 제안한 프로토콜의 설명

표기	서명
ID	신원값
PW	패스워드
SV	시그니처 값
IV	초기 값
N	난수값
P	파라미터
SV-U	시그니처의 사용자 인증값

3.1 사용자 등록

본 절에서는 클라우드 기반의 스마트팩토리 환경에서 안전한 통신을 수행하기 위해서 사용자 등록이 먼저 선행되어야 한다. 사용자는 내부운영 관리시스템을 통해 클라우드 컴퓨팅 시스템에 사용자 등록을 수행한다. 사용자 등록 프로토콜은 아래 [그림 1]과 같다.



[그림 1] 제안한 사용자 등록 프로토콜

Step 1) 사용자는 CCS에 사용자 등록을 수행하기 위해서 우선 $USER_{SV}$를 생성한다.

$$USER_{SV} = H(User_{SV}\|User_{info}\|N)$$

Step 2) 생성한 메시지를 암호화 수행 후 사용자에 대한 정보 및 파라미터를 기반으로 사용자 등록 메시지를 전송한다.

$$User_{ID}\|H(User_{PW}\oplus User_{SV}), E(User_{SV})$$

STEP 3) IOMS는 수신받은 파라미터 $USER_{SV}$를 복호화하고, 메시지를 검증한다. 이후 IOMS는 시그니처 파라미터를 생성한다.

$$IOMS_{SV} = H(IOMS_{IV}\|N\|IOMS_P)$$

STEP 4) IOMS는 생성한 메시지를 기반으로 사용자로부

터 응답메시지를 전송한다.

$$E(IOMS_{SV}, H(IOMS_P)$$

STEP 5) IOMS는 CCS로부터 사용자 등록에 관련한 메시지를 전송한다.

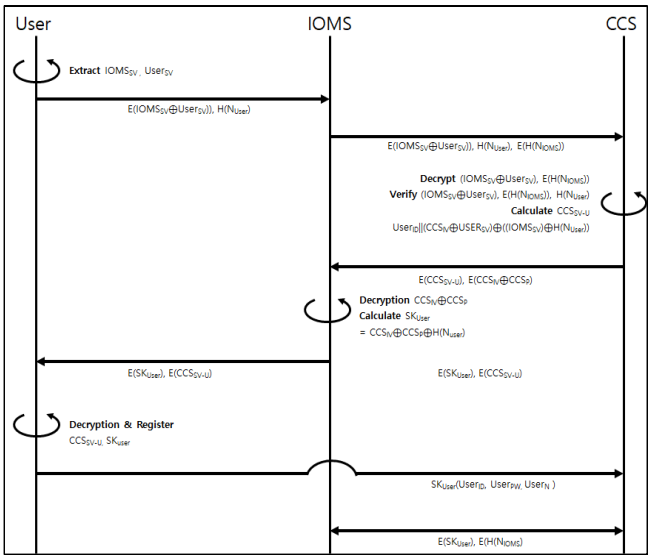
$$User_{ID} \| E(IOMS_{SV} \oplus User_{SV})$$

STEP 6) CCS는 IOMS를 통해 수신된 사용자 등록 메시지를 검증한다. 우선 $IOMS_{SV}$와 $USER_{SV}$를 복호화하며, 수신된 메시지를 검증한다. 마지막으로 CCS에서 수신된 메시지를 기반으로 사용자 등록을 수행하게 된다.

$$User_{ID} \| (CCS_{IV} \oplus User_{SV}), E(IOMS_{SV})$$

3.2 메시지 프로토콜 설계

본 절에서는 안전한 통신을 수행하기 위해서 메시지 통신 프로토콜을 설계한다. 우선 사용자는 내부운영 관리시스템을 통해 클라우드 컴퓨팅으로부터 사용자 인증을 수행 후 안전한 통신을 수행하도록 한다. 메시지 통신프로토콜은 아래 [그림 2]와 같다.



[그림 2] 통신 메시지 프로토콜 설계

Step 1) 사용자는 메시지를 전송하기 전 사용자 인증을 수행하기 위해서 $IOMS_{SV}$, $USER_{SV}$를 추출한다.

$$IOMS_{SV}, User_{SV}$$

Step 2) 추출한 메시지를 기반으로 IOMS로부터 사용자 인증 메시지를 전송한다.

$$E(IOMS_{SV} \oplus User_{SV})), H(N_{User})$$

Step 3) IOMS는 CCS로 사용자 인증 메시지를 전송한다.

$$E(IOMS_{SV} \oplus User_{SV})), H(N_{User}), E(H(N_{IOMS}))$$

Step 4) CCS는 수신된 메시지를 복호화 및 검증하고 CCS_{SV-U}를 생성한다.

$$E(IOMS_{SV} \oplus User_{SV})), H(N_{User}), E(H(N_{IOMS}))$$

$$CCS_{SV-U} = User_{ID} \| (CCS_{IV} \oplus User_{SV}) \oplus (IOMS_{SV}) \oplus H(N_{User}))$$

Step 5) CCS는 IOMS로부터 검증된 메시지를 기반으로 생성한 CCS_{SV-U}를 포함하여 IOMS로 사용자 인증완료 메시지를 전송한다.

$$E(CCS_{SV-U}), E(CCS_{IV} \oplus CCS_p)$$

Step 6) IOMS는 수신된 메시지의 CCS_{IV}, CCS_P를 복호화하고 세션키 SK_{User}를 생성한다.

$$SK_{User} = CCS_{IV} \oplus CCS_P \oplus H(N_{User})$$

Step 7) IOMS는 생성한 SK_{User}를 기반으로 사용자로부터 사용자 인증 완료 및 세션키를 생성한다.

$$E(SK_{User}), E(CCS_{SV-U})$$

Step 8) 사용자는 수신된 메시지를 복호화하고 등록한다.

Step 9) 사용자는 CCS의 시스템을 접속하기 위해 통신메시지를 세션키를 통해 암호화 후 전송한다.

$$SK_{User}(User_{ID}, User_{PW}, User_N)$$

Step 10) CCS는 수신된 메시지를 확인하기 위해서 IOMS와 메시지 송수신을 통해 수신된 메시지를 확인한다.

$$E(SK_{User}), E(H(N_{IOMS}))$$

4. 보안성 평가

본 절에서는 클라우드 기반의 스마트팩토리 환경에서 안전한 통신을 위한 메시지 프로토콜의 대한 보안성을 분석하기 위해서 데이터무결성, 중간자공격, 가용성에 대한 보안위협에 대해서 보안성에 대한 평가를 수행하였다.

데이터무결성의 위협 : 본 논문에서는 데이터 무결성에 대한 위협을 방지하기 위해 $IOMS_{SV}$, CCS_{SV}, $USER_{SV}$에 대한 데이터를 검증 후 이를 기반으로 생성한 파라미터 기반으로 메시지 통신을 수행하기 때문에 데이터 무결성에 대한 위협

은 기존 시스템 대비 안전하다.

중간자 공격에 대한 위협 : 기존 클라우드 시스템 기반에서 발생하는 중간자 위협에 대한 공격으로 데이터 위조, 데이터 탈취 등과 같은 위협이 발생하고 있다. 이러한 공격을 막기 위해서는 제안한 통신프로토콜에서 사용자의 인증을 수행한 후 SK_{User}를 통해 암호화를 수행하여 메시지를 전송한다.

가용성에 대한 위협 : 스마트팩토리 환경에서는 보안의 3요소인 가용성이 제일 우선시된다. 이러한 가용성에 대한 보안성을 높이기 위해서는 사용자 등록단계에서 내부운영관리시스템의 $IOMS_{SV}$를 생성하여 사용자를 등록하고, 이후 클라우드 컴퓨팅 시스템에서 CCS_{SV}를 생성 후 등록함으로써 스마트팩토리 환경의 보안성을 기존대비 향상시킬 수 있다.

[표 2] 기존시스템 대비 보안성 분석 결과

	기존 시스템	제안 프로토콜
데이터무결성의 위협	△	○
중간자 공격에 대한 위협	×	○
가용성에 대한 위협	-	○

5. 결론

본 논문에서는 클라우드 기반의 스마트팩토리 환경에서 안전한 통신을 수행하기 위해서 메시지 프로토콜을 설계하였다. 제안한 메시지 통신프로토콜을 설계하기 위해서 사용자 등록, 사용자 인증 및 메시지 통신프로토콜을 설계하여 스마트팩토리 환경에서 안전한 통신을 수행하도록 하였다.

보안성 평가를 수행하기 위해서 클라우드 융합환경에서 대표적으로 발생하는 보안위협, 공격기법에 대해서 보안성을 분석하였다.

스마트팩토리 환경은 기존의 폐쇄적인 환경에서 개방적인 환경으로 점차 확장되고 있으며, 신규 공격기법에 대한 연구를 꾸준히 수행해야 한다. 논문에서 제안한 통신프로토콜을 활용함으로써 클라우드 기반의 스마트팩토리 환경에서 보안성을 향상시킬 수 있으며, 안전한 메시지 통신이 더욱 활성화될 것으로 기대된다.

참고문헌

[1] 박형욱, “스마트 팩토리와 연관된 생산제조기술 동향”, 한국통신학회지(정보와통신) 33(1), 24-29, 2015.12

[2] 한은혜, “IT와 OT의 연계 증가에 따른 보안 취약점 개선 방안”, 정보보호학회지, 제 30권 5호, pp. 55-60, 1월, 2020. 10

[3] 우성희 외 1명, “스마트 팩토리의 주요기술과 도입사례”, 한국정보통신학회 2018년도 춘계학술대회, pp. 487-90, 2018년 5월

[4] ZDNet, “TSMC says variant of WannaCry virus brought down its plants,” 2018. 8. 6

[5] 테크월드뉴스, “[스마트팩토리 특집] 제조 기업, 스마트를 입다”, 2021. 4. 7.