산업융합연구 제22권 제4호 pp. 1-9, 2024
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2024.22.4.001

스마트 팩토리 환경에서 안전한 통신을 위한 인증 메커니즘 설계

박중오*
성결대학교 파이데이아학부 조교수

A Design of Authentication Mechanism for Secure Communication in Smart Factory Environments

Joong-oh Park*
Assistant Professor, Division of Paideia, Sungkyul University

요 약 스마트 팩토리는 최신 정보통신기술과 제조공정이 결합된 생산시설로, 급속한 발전과 글로벌 제조업의 변화를 반영하고 있다. 로보틱스 및 자동화, 사물인터넷의 통합, 인공지능 융합기술을 활용하여 다양한 제조환경의 생산 효율성을 극대하고 있다. 하지만 스마트 팩토리 환경에서 다양한 공격기법으로 인해 보안위협 및 취약점이 발생하고 있다. 스마트 팩토리 환경에서 보안위협이 발생하면 금전적인 손해, 기업이미지하락, 인명피해가 발생하여 이에 따른 보안대응이 필요하다. 따라서 본 논문에서는 스마트 팩토리 환경에서 안전한 통신을 수행하기 위한 보안 인증 메커니즘을 제안하였다. 제안한 인증 메커니즘에 대한 구성요소에서는 스마트 디바이스, 내부 운영관리 시스템, 인증 시스템, 클라우드 스토리지 서버가 있다. 스마트 기기 등록과정, 인증 절차. 이상징후 및 갱신절차를 세부적으로 설계하였다. 그리고 제안한 인증 메커니즘의 안전성을 분석하였고, 기존 인증 메커니즘과의 성능분석을 통해 대략 8%의 효율성을 확인하였다. 그리고 제안한 기술을 적용하기 위한 경량화 프로토콜 및 보안정책에 대한 연구방향을 제시하여 보안성 향상에 도움을 주고자 한다.

키워드 : 산업보안, 스마트 팩토리, 인증, 네트워크 보안, 융합기술

Abstract Smart factories represent production facilities where cutting-edge information and communication technologies are fused with manufacturing processes, reflecting rapid advancements and changes in the global manufacturing sector. They capitalize on the integration of robotics and automation, the Internet of Things (IoT), and the convergence of artificial intelligence technologies to maximize production efficiency in various manufacturing environments. However, the smart factory environment is prone to security threats and vulnerabilities due to various attack techniques. When security threats occur in smart factories, they can lead to financial losses, damage to corporate reputation, and even human casualties, necessitating an appropriate security response. Therefore, this paper proposes a security authentication mechanism for safe communication in the smart factory environment. The components of the proposed authentication mechanism include smart devices, an internal operation management system, an authentication system, and a cloud storage server. The smart device registration process, authentication procedure, and the detailed design of anomaly detection and update procedures were meticulously developed. And the safety of the proposed authentication mechanism was analyzed, and through performance analysis with existing authentication mechanisms, we confirmed an efficiency improvement of approximately 8%. Additionally, this paper presents directions for future research on lightweight protocols and security strategies for the application of the proposed technology, aiming to enhance security.

Key Words : Industrial security, Smart factory, Certification, Network security, Convergence technology

*Corresponding Author : Joong-oh Park(pjo21@naver.com)
Received January 15, 2024
Revised February 26, 2024
Accepted April 20, 2024
Published April 28, 2024

1. 서론

스마트 팩토리는 첨단 정보통신기술과 제조공정이 결합된 생산시설을 의미한다[1][13]. 산업4.0의 중심 요소로 디지털 기술을 활용하여 생산과정을 더욱 효율적으로 만들기 위해 스마트 팩토리 네트워크 기술이 활용되고 있다[2][14]. 그러나 스마트 팩토리 환경에서는 다양한 보안 위협이 존재하고 있다[3-4]. 이러한 공격으로 생산라인에 따른 금전적인 손해, 데이터 유출에 따른 기업이미지 하락, 물리적 장비의 조작으로 인명피해가 발생할 수 있다[4][5-6].

본 논문에서는 스마트 팩토리 환경에서 안전하게 통신을 수행하기 위한 인증 메커니즘을 설계하도록 한다. 본 논문은 다음과 같이 구성되어 있다. 2장 관련연구에서는 스마트 팩토리 정의 및 기술동향, 보안위협 및 요구사항에 대해서 서술하였다. 3장은 제안부로 스마트 팩토리 환경에서 안전한 통신 프로토콜 및 보안 메커니즘을 제안하였다. 4장 성능평가에서는 2장에서 언급된 보안위협에 대해서 안전성 분석 및 성능평가를 수행하였다. 5장에서는 결론을 마치며 향후 연구방향에 대해서 제시한다.

2. 관련연구

2.1 스마트 팩토리 정의 및 기술동향

스마트 팩토리는 고도로 디지털화된 첨단 정보통신 기술이 융합된 제조 기술 환경이라 말할 수 있다. 이러한 시설은 자동화 실시간 분석, 데이터 통신 및 교환을 통해 제조 환경에 따른 생산 효율성을 극대화하고 유연성을 향상시킨다[5][6][13-14].

스마트 팩토리의 기술 동향을 살펴보면 사물인터넷(IoT)활용, 빅데이터 및 분석, 로보틱스 및 자동화, 클라우드 컴퓨팅 활용 사이버 보안, 블록체인 등을 활용한다. 이러한 기술은 꾸준히 발전하고 있으며, 제조업 미래를 형성하는 큰 영향을 끼친다. 또한 ICT융합기술을 활용하여 디지털 변환 가속화가 이루어지고 있다[6][15].

2.2 스마트 팩토리 환경에서 보안위협 및 보안요구사항

스마트 팩토리 네트워크 환경에서 발생하는 공격기법 및 보안위협은 다양하다[7]. 대표적으로 사이버 물리 시스템 공격, 네트워크 공격(MITM), 내부 위협, 데이터 유출 등이 있다[8]. 우선 사이버 물리 시스템 공격은 스마트 팩토리 환경에서 사이버 물리시스템에 크게 의존하여, 해킹 및 공격이 발생하면 생산 라인의 물리적 장비를 조작하여 기기를 손상시킬 수 있다. 그다음 네트워크 공격(MITM)은 스마트 팩토리 환경이 다양한 네트워크가 연결되어 있다는 것을 활용하여 DDoS공격 또는 중간자 공격에 취약할 수 있다[9]. 그리고 내부 위협은 스마트 팩토리 환경에서 내부자에 의한 공격 또는 실수로 운영 중인 시스템을 크게 손상시킬 수 있으며, 외부에서 공격하는 것보다 치명적일 수 있다. 그리고 데이터 유출에 경우는 스마트 팩토리는 대량의 민감한 데이터를 처리하여 이 데이터가 유출되면 기업의 관리적인 측면, 대외적인 측면에서 크게 이미지가 하락할 수 있다[10][14]. 그리고 스마트 팩토리 환경에서 대표적인 보안위협은 아래 [Table 1]과 같다.

Table 1. Security threats in smart factory environments

Threat Type	Description	Example
Network Attack	Unauthorized access to a smart factory network environment to steal data or damage the system	DDoS attacks, phishing, sniffing
Malware	An attack using malicious software to infect the information systems of a smart factory or damage data.	ransomware, spyware
Insider Threat	Acts by employees within an organization who maliciously or accidentally threaten security.	abuse of access rights
Physical Threat	Physical damage to smart factory devices caused by hardware damage, power supply issues, or natural disasters.	Hardware damage, fire, flood

위와 같은 공격기법 및 보안 위협에 대응하기 위해서는 다음과 같은 보안 요구사항이 필요하다[11-13]. 우선 네트워크 보안으로 운영 중인 정보시스템의 보안성을 강화하기 위해서 방화벽, 침입탐지방지시스템, 암호화 등이 필요하다. 그리고 물리적 보안에서는 접근 통제, 감시 카메라 등이 필요하다[12]. 그다음 사용자 인증 및 접근제어를 설계하여 스마트 팩토리 환경에서 작동 중인 기기의 다단계 인증, 역할 기반 접근제어, 로그 관리가 수행되어야 한다. 마지막으로 이를 운영 및 관리하는 내부 직원의 사이버 정보통신 보안 교육 및 인식 제고가 필요하다[8][13-15].

3. 스마트 팩토리 환경에서 안전한 통신을 위한 인증 메커니즘 설계

본 장에서는 스마트 팩토리 환경에서 안전한 통신을 위한 인증 메커니즘을 제안한다. 우선 사용자는 스마트 기기 및 사용자 등록 절차를 거쳐서 상호 인증 메시지 통신을 수행한다. 그리고 등록된 디바이스 관리를 위해 이상징후 탐지 및 등록 절차를 제안한다. 본 논문에서 제안한 논문의 구성도는 아래 Fig. 1과 같다. 그리고 3장 1절에서 3절까지의 제안한 메커니즘에 나오는 약어는 아래 Table 2와 같다.

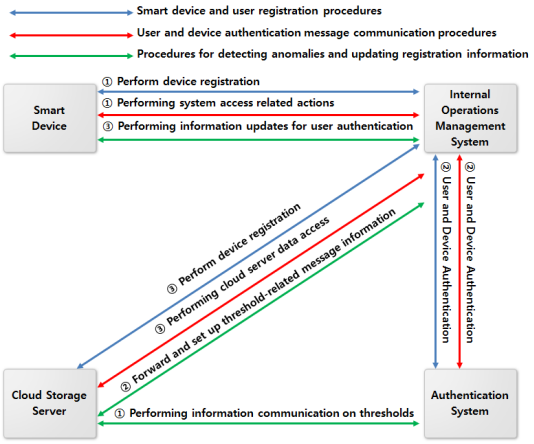

Fig. 1. Configuration diagram of communication protocol in the proposed smart factory environment

Table 2. Abbreviation and description

Abbreviation	Description
E_k	Encryption
H( )	Hash function
SD	Smart Devices
SDL	Smart device location value
SN	Serial number
CV	Authentication value
Cert	Certificate
AS	Authentication Server
IV	Initial settings value
IOMS	Internal Operations Management System
D_K	Decryption
LV	Permission value
LV-i	i-th permission value
TV	Threshold
TV-i	i-th permission value

3.1 스마트 기기 및 사용자 등록 절차

본 절에서는 사용자가 스마트 기기를 활용하여 스마트 팩토리 환경에서 스마트 기기 및 사용자 등록을 수행한다. 제안한 프로토콜은 아래 Fig. 2와 같다.

1) 사용자는 스마트 기기를 활용하여 내부 운영관리 시스템에게 등록 요청 메시지를 전송한다.
$E_K(H(SD_{SN}), SDL_{Info})$

2) 내부 운영 관리 시스템은 수신된 메시지를 확인 후 사용자에게 기기 및 사용자 정보 요청 메시지를 전송한다.

3) 수신된 메시지를 확인 후 기기에 대한 정보 추출 및 사용자 정보를 입력한다. 이후 내부 운영관리시스템에게 사용자 정보 및 기기 정보에 따른 응답 메시지를 전송한다.
$SD_{IV} = H(SD_{SN}) \oplus SD_{CV})$
$E_K(H(User_{PW}), SD_{IV} \oplus H(Time\,stamp_{User}), H(User_{cert})$

4) 내부 운영 관리 시스템에서는 인증 시스템에게 사용자 및 기기 정보 검증 요청메시지를 전송한다.
$E_K(H(SD_{sn}), (SDL_{Info}), H(User_{Cert}))$

5) 인증 시스템에서는 수신된 메시지를 복호화 후 사용자 및 기기에 대한 검증을 수행한다.
$AS_{IV} = AS_{Cert} \oplus H(Time\,stamp_{AS})$

6) 인증시스템에서는 수신 받은 메시지에 대한 검증을 수행 후 내부운영관리시스템에게 사용자 및 기기 정보 검증 응답메시지를 전송한다.
$E_K((AS_{IV}), H(Time\,stamp_{AS}))$

7) 내부운영관리시스템에서는 수신 받은 메시지를 복호화 후 사용자 및 기기정보에 대한 등록 작업을 수행한다.
$AS_{IV} \oplus H(Time\,stamp)$
Registering $AS_{Cert}, H(User_{cert})$

8) 내부운영관리시스템에서는 기기 및 사용자 등록 완료메시지를 사용자에게 전송한다. 이후 클라우드 스토리지 서버에 스마트 기기 등록 요청 메시지를 전송한다.
$E_K((AS_{IV}), H(SD_{sn}), SDL_{Info})$

9) 클라우드 스토리지 서버는 전송된 메시지에 대해서 스마트 기기에 대한 등록 작업을 수행한다.

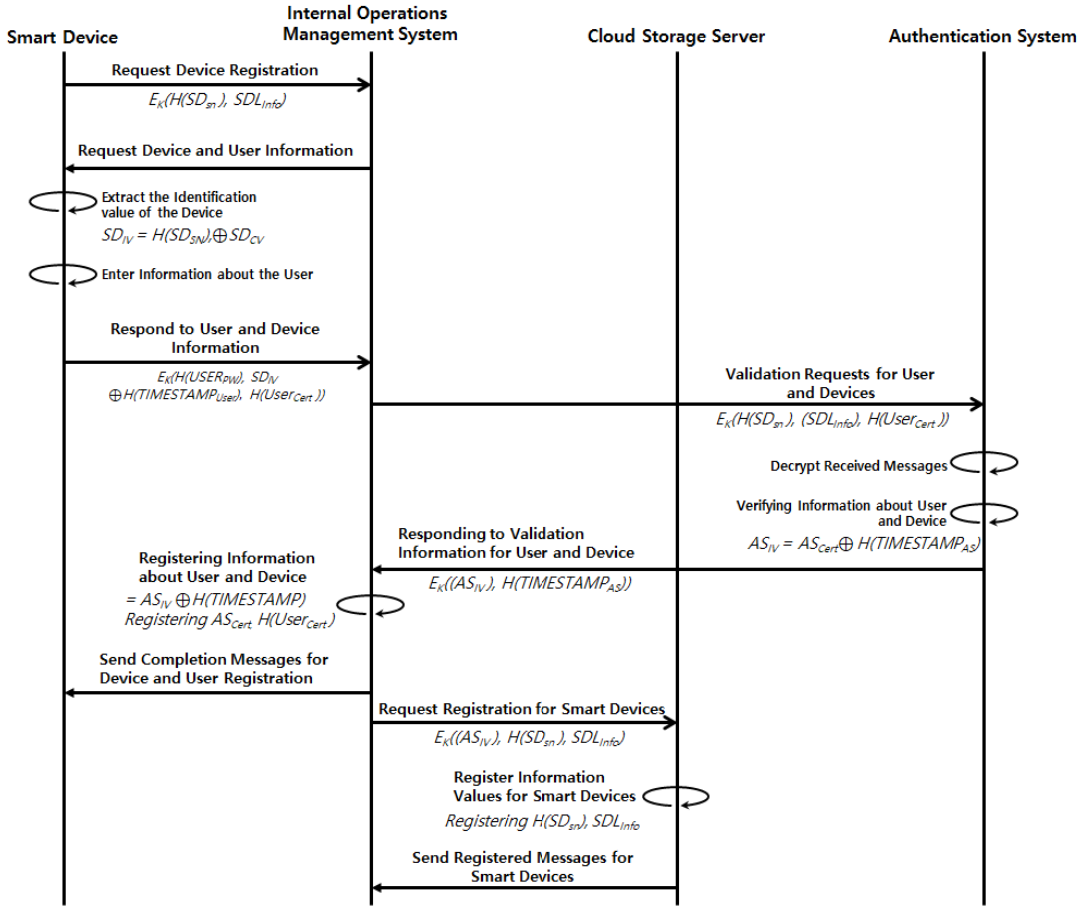

Fig. 2. Proposed smart device and user registration protocol

Registering $H(SD_{SN}), SDL_{info})$

10) 클라우드 스토리지 서버는 등록 작업을 완료 후 내부운영관리시스템으로부터 스마트 기기에 대한 등록 완료 메시지를 전송한다.

3.2 사용자 및 기기 인증 메시지 통신 절차

본 절에서는 사용자 및 기기 인증과정을 수행 후 메시지를 안전하게 통신하는 절차에 대해서 서술한다. 제안한 인증 및 통신 메시지 프로토콜 절차는 아래 Fig. 3과 같다.

1) 사용자는 기기를 활용하여 내부운영관리시스템 접근 요청을 수행한다.
$E_K((SD_{IV}), H(User_{Cert}))$

2) 내부운영관리시스템에서는 수신된 메시지를 확인 후 인증 시스템으로부터 기기 및 사용자에 대한 인증 요청 메시지를 전송한다.
$E_K(SD_{IV}), H(User_{cert}), SDL_{Info})$

3) 인증시스템에서는 수신된 메시지를 복호화 후 기기 및 사용자 인증 정보에 따른 검증작업을 수행한다.
$SD_{IV}, H(User_{Cert}), SDL_{info}$

4) 인증시스템에서는 내부운영관리시스템으로부터 기기 및 사용자 인증관련 정보에 따른 메시지를 회신한다.
$E_K(AS_{IV} \oplus Time\,stamp_{AS})$

5) 내부운영관리시스템에서는 인증정보를 검증 후 사용자로부터 기기 및 사용자 인증 완료 메시지를 회신한다.
$E_K(H(IOMS_{Cert}), (User_{LV}))$

6) 사용자는 수신된 메시지를 확인 후 내부운영관리시스템으로부터 클라우드 스토리지의 저장된 데이터

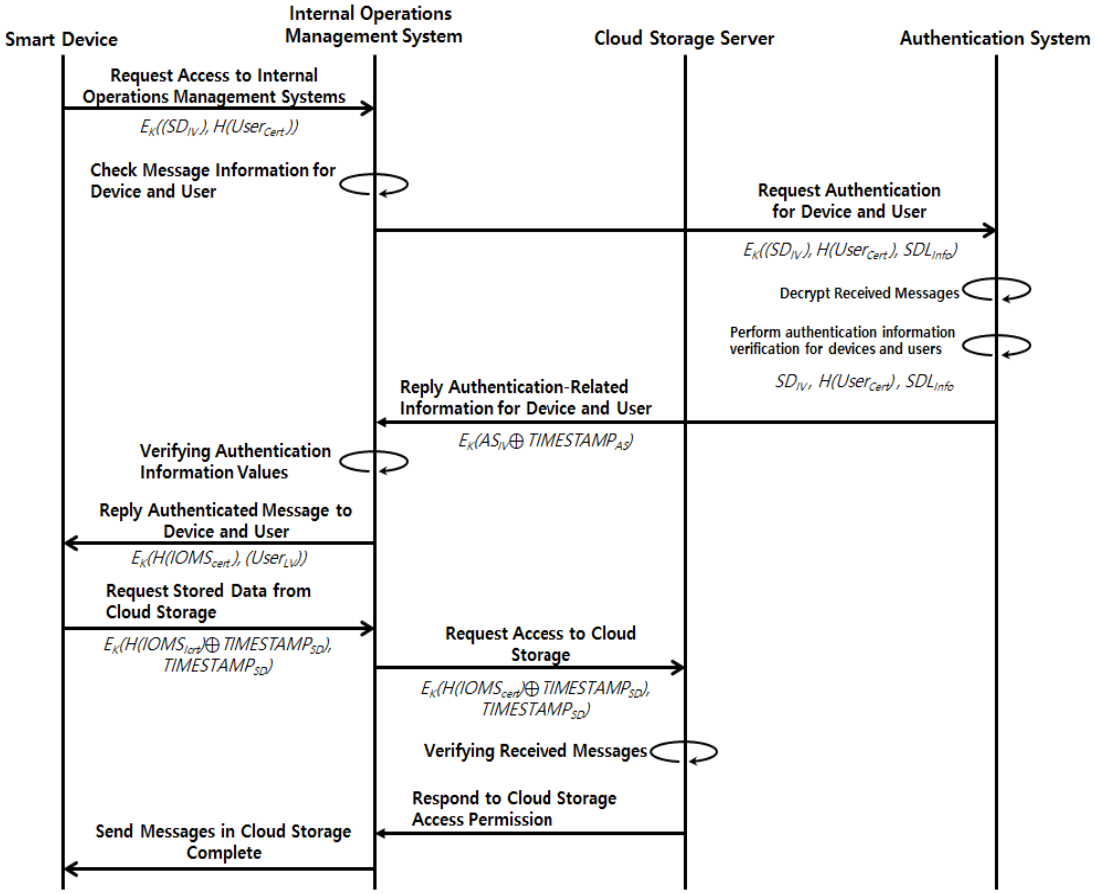

Fig. 3. Proposed smart device and user registration protocol

를 요청한다.

$E_K(H(IOMS_{Cert}) \oplus Time\ Stamp_{SD}), Time\ stamp_{SD})$

7) 내부운영관리시스템에서는 클라우드 스토리지 서버로부터 인증된 사용자에 대한 접근 요청 메시지를 전송한다.

$E_K(H(IOMS_{cert}) \oplus Time\ stamp_{SD}), Time\ stamp_{SD})$

8) 클라우드 스토리지 서버에서는 수신된 메시지를 검증 후 내부운영관리시스템으로부터 사용자 접근 가능한 응답메시지를 전송한다.

9) 내부운영관리시스템에서는 사용자에게 클라우드 스토리지 완료 메시지를 전송한다.

3.3 이상 징후 탐지 또는 등록정보 갱신 절차

본 절에서는 이상 징후 탐지에 대한 등록정보 갱신 절차에 대해서 서술한다. 제안한 이상 징후 탐지에 대한 등록정보 프로토콜 절차는 아래 Fig. 4와 같다.

1) 인증시스템과 클라우드 스토리지 서버는 항시 임계치 기준정보 및 현황에 대한 메시지를 수행한다.

2) 클라우드 스토리지 서버와 내부운영관리시스템에게 설정한 임계치 기준 값에 대한 만료 메시지를 전송한다.

$E_K((SD_{IV}), H(User_{Cert}), SDL_{Info})$

3) 내부운영관리시스템은 수신된 메시지를 복호화 후 인계치 기준 값 정보 및 현황을 확인한다.

$D_K((SD_{IV}), H(User_{Cert}), SDL_{Info})$

4) 내부운영관리시스템은 수신된 메시지를 확인 후 사용자로부터 인증정보 만료에 따른 갱신요청 메시지를 전송한다.

$E_K((SD_{TV}), SDL_{Info}), User_{LV})$

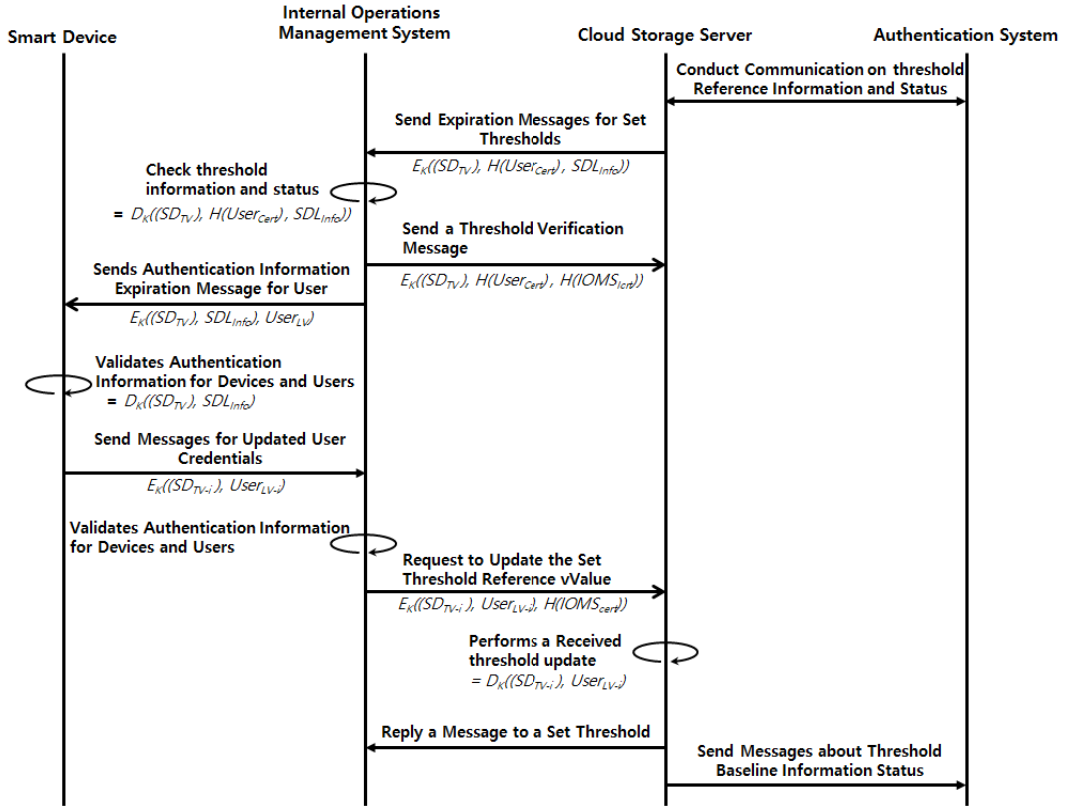

Fig. 4. Proposed smart device and user registration protocol

5) 사용자는 수신된 인증관련 메시지에 따른 정보현황을 확인한다.
$D_K((SD_{TV}), SDL_{Info}))$

6) 사용자는 내부운영관리시스템에게 기기 및 사용자에 대한 인증관련 갱신 메시지를 전송한다.
$E_K((SD_{TV-i}), User_{LV-i})$

7) 내부운영관리시스템에서는 수신된 메시지를 복호화 후 기기 및 사용자에 대한 갱신된 인증관련 정보를 수행한다.

8) 내부운영관리시스템에서는 이후 클라우드 스토리지 서버에게 설정한 임계치 기준 값 대한 갱신 요청 메시지를 전송한다.
$E_K((SD_{TV-i}), User_{LV-i}), H(IOMS_{cert}))$

9) 클라우드 스토리지 서버는 기기 및 사용자 임계치 기준 값 대한 갱신작업을 수행한다.
$D_K((SD_{TV-i}), User_{LV-i}))$

10) 클라우드 스토리지 서버는 갱신작업을 완료한 다음 내부운영관리시스템에게 설정한 임계치 기준 값에 대한 메시지를 회신한다. 이후 인증 시스템에게 인계치 기준정보 및 현황 메시지에 따른 통신을 유지한다.

4. 안전성 분석 및 성능평가

4.1 안전성 분석

본 절에서는 2장의 관련연구의 스마트 팩토리에서 대표적으로 발생하는 취약점 및 보안위협을 기반으로 안전성을 분석하고자 한다.

- 네트워크 보안 취약성 : 스마트 팩토리 환경에서는 다양한 장치와 시스템이 네트워크로 연결되어 있어 네트워크 침입, 데이터 유출에 따른 보안 취약성이 존재한다. 이에 따른 보안위협을 대응하기 위해 스마트 기기 및 사용자 등록과정에서 AS_{IV}를 생성하여 AS_{CERT}, $H(User_{Cert})$를 검증 및 등록하는 과정에서 등록된 사용자만 접근을 허용할 수 있다.

- 내부 위협 : 스마트 팩토리 운영하고 있는 환경에서 내부 직원 또는 관리자의 실수, 부주의, 혹은 악의적인 행위로 인해 데이터 유출, 시스템 손상과 같은 피해를 입을 수 있다. 이를 방지하기 위해서 이상 징후 탐지 또는 등록정보 갱신 절차에서 $E_K((SD_{TV-i}), User_{LV-i})$, $H(IOMS_{CERT})$를 활용하여 사용자에 대한 갱신 값을 관리할 수 있으며, 또한 임계치 기준정보에 따른 현황을 관리함으로써 내부운영관리에 따른 보안성을 강화 할 수 있다.
- 물리적 탈취에 따른 보안위협 : 장비나 서버실에 운영되고 있는 서버를 물리적으로 탈취하는 공격이 빈번하게 발생한다. 이러한 공격에 따른 보안위협을 강화하기 위해서 $E_K(H(SD_{SN}), (SDL_{Info}), H(User_{Cert}))$에 따른 정보를 검증하고, 이후 인증 시스템에서는 AS_{IV} 생성 후 검증, $H(SD_{SN})$, SDL_{Info})에 따른 기기정보를 등록 및 관리함으로써 취약점을 대응할 수 있다.
- 중간자 공격 : 스마트 팩토리 환경 뿐만 아니라, 기존 네트워크 환경에서 발생하는 중간자 공격 대표적인 보안위협이다. 이러한 공격에 대응하기 위해서 제안한 프로토콜에서는 네트워크 세분화 즉 내부운영관리시스템, 인증시스템에서 사용자 및 기기에 대한 인증에 대한 값(AS_{IV}, $User_{Cert}$) 대해 검증한다. 그리고 네트워크 환경에서 주기적인 모니터링 및 이상 징후 탐지를 수행하기 위해서 (SD_{TV-i}), $User_{LV-i}$)를 활용하여 중간자 공격(Man-in-the-Middle, MitM)이 실패로 끝난다.

4.2 보안성 평가

본 절에서는 제안한 통신 프로토콜의 보안성을 평가하기 위해서 기존의 암호 메커니즘을 활용한 통신 시스템과 비교 분석을 수행하였다. 관련연구 2장에서 서술된 보안위협, 앞 절에서 언급된 공격기법 등에 대해 보안성을 평가하였다. 분석한 내용은 Table 3와 같다.

제안한 보안 메커니즘은 기존 보안 메커니즘과 달리 상호 인증 및 이상 징후 탐지에 따른 서명 값 검증을 수행한다. 세션 하이재킹, SSL 스트리핑과 같은 공격기법 측면에서도 공격을 무마할 수 있다. 내부 직원에 따른 보안위협과 물리적 탈취측면에서는 3장에서 제안한 통신 프로토콜 및 이상 징후 탐지 프로토콜을 통해 보다 안전하게 통신을 수행할 수 있다. 또한 기밀성에 대한 갱신측면에서도 꾸준한 모니터링을 통해 갱신 값(인증서, 식별 값, 임계치에 따른 기준 값)을 안전하게 관리한다. 전체적인 서명 검증 과정과 메시지 통신 속도를 비교 분석하였다.

Table 3. Comparative analysis of existing and proposed security mechanisms

	Existing security mechanism (based on WPA2)	Existing security mechanism (based on SSL/TLS)	Proposed security mechanism
Signature and Verification Procedures	Conduct communication after verifying the signature value through a third party	Communi-cation via 4-way handshake process	Communicate with mutual authentication and detection of anomalies
Session Hijacking	Enable	Enable	Disable
SSL Stripping	Enable	Disable	Disable
Internal staff security threats	-	Disable	Disable
Security Threats from Physical Takeover	Enable	Enable	Disable
Aspects of managing updates to confidential values	Confidential value requires security	Confidential value requires security	Confidential value high security

제안한 보안 메커니즘의 성능을 분석하기 위해 기존 보안메커니즘(WPA2 기반, SSL/TLS 기반)과 비교 분석을 수행하였다. 제안한 보안 메커니즘은 기존의 보안메커니즘과 달리 동적으로 이상 징후 탐지 및 등록 정보에 대한 절차를 수행하고 있으며, 사용자 등록 및 기기 인증 과정에서 생성된 해쉬값을 기반으로 안전한 메시지를 수행하였다. 즉 인증서에 대한 사용자 인증을 1회만 수행함으로써 다수의 인증과정을 최소화하였다. Fig 5는 비교 분석을 수행한 결과 값으로 평균 시간(ms)을 나타냈으며, Fig. 6은 노드에 따른 성능분석 결과 값으로 평균시간(ms)을 나타낸다. 전체적으로 서명값 및 통신부분에서 SSL/TLS 대비 우수한 성능을 확인하였다. 즉 노드대비에서는 노드가 많아질수록 WPA 대비 높은 효율성을 확인하였다. 기존 WPA에서 발급하는 인증서 방식인 EAP-TLS를 사용하지 않고 해쉬함수 기반의 인증 값을 통해 메시지 통신을 수행함으로서 8% 향상된 메시지 통신 수행 값을 확인하였다.

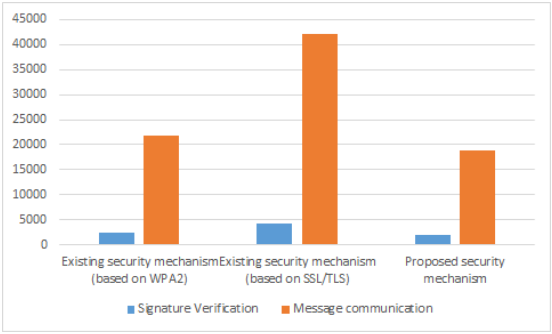

Fig. 5. Proposed smart device and user registration protocol

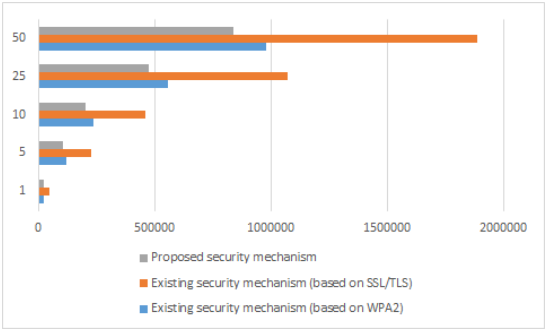

Fig. 6. Performance analysis results according to nodes

5. 결론

본 논문에서는 스마트 팩토리 환경에서 안전한 메시지 통신을 위한 인증 메커니즘을 설계하였다. 제안한 보안 메커니즘에서는 스마트 기기 및 사용자 등록 절차, 스마트 기기 및 사용자 인증 후 안전한 통신 프로토콜, 이상 징후 탐지를 위한 갱신관리 프로토콜을 제안하였다.

제안한 통신 프로토콜을 비교 분석하기 위해서 2장 관련연구에서 언급된 스마트 팩토리 환경의 공격기법, 보안 위협에 대해 안전성을 분석하였다. 그리고 기존 암호 프로토콜 대비 통신 노드가 향상할수록 높은 효율성을 확인할 수 있다.

향후 제안한 프로토콜을 사용하기 위해서는 중형이상의 장비가 한정되면 소형장비를 위한 경량 화된 통신 프로토콜에 대한 연구가 적용되어야 한며 내부위협 및 신규 변종공격에 따른 위협사항을 대비하기 위해서 안정적인 보안정책을 설계하고 연구해야 한다.

REFERENCES

[1] J. H. Han. (2016). Security Requirements for a Smart Home Service, TTAK.KO-10.0963. TTA.

[2] D. H. Kim & J. Kwak. (2015). Design of Improved Authentication Protocol for Sensor Networks in IoT Environment. Journal of the Korea Institute of Information Security & Cryptology, 25(2), 467-478,

[3] V. Sivaraman et al. (2015, October). Network-level security and privacy control for smart-home IoT devices. In 2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob) (pp. 163-167). IEEE.
DOI : 10.1109/WiMOB.2015.7347956

[4] B. Jin, D.Jung, S. Cha & M. Jun. (2016). Design and Estimation of a Session Key based Access Control Scheme for Secure Communications in IoT Environments. Journal of the Korea Society of Digital Industry and Information Management, 12(1), 35-41.
DOI : 10.17662/ksdim.2016.12.1.035

[5] N. Komninos, E. Philippou & A. Pitsillides. (2014). Survey in smart grid and smart home security: Issues, challenges and counter-measures. IEEE Communications Surveys & Tutorials, 16(4), 1933-1954.
DOI : 10.1109/COMST.2014.2320093

[6] C. C. Wu, W. B. Lee & W. J. Tsaur. (2008). A secure authentication scheme with anonymity for wireless communications. IEEE Communications Letters, 12(10), 722-723.
DOI : 10.1109/LCOMM.2008.080283

[7] Z. N. Rashid, S. R. Zeebaree & A. Shengul, (2019). Design and analysis of proposed remote controlling distributed parallel computing system over the cloud. In 2019 International Conference on Advanced Science and Engineering (ICOASE) (pp. 118-123). IEEE.

[8] S, J. Oh. (2015). A Study on Organizations Adopting Convergence-based Smart Work for Overcoming Constraints and Achieving Performance. Journal of Digital Convergence, 13(6), 113-124. DOI : 10.14400/JDC.2015.13.6.113

[9] Y. J, Park. (2015). Development of a ICT Convergence Business Model based on Smart Phone. Journal of Digital Convergence, 13(6), 81-89. DOI : 10.14400/JDC.2015.13.6.81

[10] Y. S. Jung. (2019). An IoT Information Security Model for Securing Bigdata Information for IoT Users. Journal of Convergence for Information Technology, 9(11), 8-14.
DOI : 10.22156/CS4SMB.2019.9.11.008

[11] D. J. Choi. (2019. 9. 18). Next Generation IoT Security in the 5G Era. ITFIND, pp1-15.

[12] I. K. Park & J. Kwak. (2018). Permission Management System for Secure IoT Devices in Android-Based IoT Environment. KIPS Transactions on Computer and Communication Systems, 7(2), 59-66.
DOI : 10.3745/KTCCS.2018.7.2.59

[13] NIST, “Framework for Improving Critical Infrastruct ure Cybersecurity Version 1.1,” 2018. 4

[14] Homeland Security, “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,” 2016. 9.

[15] NIST, “NIST SPECIAL PUBLICATION 800-82 REVISION 2- GUIDE TO INDUSTRIAL CONTROL SYSTEMS(ICS) SECURITY,” 2015. 5.

박 중 오(Park, Joong Oh) [정회원]

• 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
• 2003년 3월 : 명지대학교 전자계산교육 석사
• 2011년 8월 : 숭실대학교 컴퓨터공학 박사
• 2016년 3월~현재 : 성결대학교 조교수
• 관심분야 : Network security, PKI, Cryptography
• E-Mail : pjo21@naver.com