Journal of Convergence for Information Technology
Vol. 11. No. 7, pp. 21-30, 2021
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2021.11.07.021

클라우드 서비스 기반 스마트 홈 환경에서 안전한 데이터 통신을 위한 메시지 통신 프로토콜 설계

박중오
성결대학교 파이데이아학부 조교수

A Message Communication for Secure Data Communication in Smart Home Environment Based Cloud Service

Jung-Oh Park
Assistant Professor, Division of Paideia, Sungkyul University

요 약 사물인터넷 기술 발전으로 스마트 차, 스마트 헬스케어, 스마트 홈, 스마트 팜 등 다양한 클라우드 컴퓨팅 기반 서비스가 확대되고 있다. 새로운 환경의 등장함에 따라 개인정보 또는 기업 기밀 등 중요 정보에 대한 노출 가능성, 해킹으로 인한 금전적인 피해 사례, 악의적인 공격기법으로 인한 인명피해 등 다양한 문제가 지속하여 발생하고 있다. 본 논문에서는 스마트 홈 기반의 안전한 통신을 수행하고, 사용자 데이터 보호를 위한 메시지 통신프로토콜을 제안한다. 세부 과정으로 스마트 홈 환경에서 안전한 디바이스 등록, 메시지 인증 프로토콜, 갱신프로토콜을 새롭게 설계하였다. 스마트 홈 서비스 관련 보안 요구사항을 참고하여 대표 공격기법에 대한 안정성을 검증하고, 성능을 비교분석을 수행한 결과 통신 측면 약 50%, 서명검증 측면 약 25%의 효율성을 확인했다.

주제어 : 메시지 프로토콜, 사물인터넷, 스마트 홈, 디바이스 인증, 클라우드 서비스

Abstract With the development of IoT technology, various cloud computing-based services such as smart cars, smart healthcare, smart homes, and smart farms are expanding. With the advent of a new environment, various problems continue to occur, such as the possibility of exposure of important information such as personal information or company secrets, financial damage cases due to hacking, and human casualties due to malicious attack techniques. In this paper, we propose a message communication protocol for smart home-based secure communication and user data protection. As a detailed process, secure device registration, message authentication protocol, and renewal protocol were newly designed in the smart home environment. By referring to the security requirements related to the smart home service, the stability of the representative attack technique was verified, and as a result of performing a comparative analysis of the performance, the efficiency of about 50% in the communication aspect and 25% in the signature verification aspect was confirmed.

Key Words : Message Protocol, IoT, Smart Home, Device Authrntication, Cloud Service

1. 서론

사물인터넷 기술의 발달로 인해 다양한 융합서비스가 생겨나고 있으며, 이를 사용하는 사용자로부터 삶의 질은 향상되었다. 스마트 폰 및 사물인터넷 장비의 폭넓은 보급으로 인해 무선 네트워크 통신 기술이 발전되어 사용자마다 요구하는 사항의 서비스를 다양하게 제공받을 수 있다[1,2]. 그러나 빠르게 진화하는 스마트 홈 기술로 인해 다양한 공격기법으로 인해 금전적인 손실이 발생하고 있으며, 사용자 프라이버시 유출로 인한

*Corresponding Author : Jung-Oh Park(pjo21@naver.com)
Received May 31, 2021
Revised July 8, 2021
Accepted July 20, 2021
Published July 28, 2021

정신적인 피해도 입고 있다. 또한, 지속적인 공격 시도가 아닌 손쉽게 구할 수 있는 장비 및 해킹툴로 인해 스마트 홈서비스의 보안환경을 위협할 수 있다[1,3-5]. 그러므로 본 논문에서는 스마트 홈기반의 안전한 통신을 수행하고, 사용자 데이터 보호를 위한 메시지 통신 프로토콜을 제안한다. 클라우드 서비스 기반 스마트 홈 환경에서 디바이스 등록, 메시지 인증 프로토콜, 갱신프로토콜을 설계하여 안전한 통신을 수행하도록 한다.

본 논문의 구성은 다음과 같다. 2장은 스마트 홈 서비스 기반 보안 기능 및 보안 요구사항을 분석한다. 3장은 제안한 메시지 프로토콜을 설계하는 부분으로 디바이스 등록절차, 메시지 인증 및 통신 프로토콜 설계, 디바이스 및 사용자 갱신 관리 절차를 설계한다. 4장은 성능평가 항목으로 안전성 분석 및 성능 효율성에 관해서 서술한다. 5장은 결론을 맺는다.

2. 스마트 홈 서비스 기반 보안 기능 및 보안 요구사항

IoT 기반의 스마트 홈 서비스 시스템은 홈 서버, 홈 게이트웨이(무선 액세스 포인트), 스마트 장비로 구성되어 있으며, 무선 네트워크 기반에서 데이터를 송수신할 수 있다[1,6]. 스마트 홈 서비스는 인터넷 연결 기능을 통해 내부 혹은 외부에서 다양한 공격시도를 통해 취약점이 발생할 수 있다. 스마트 홈 환경에서 발생하는 공격사례를 살펴보면 악성코드 감염을 통한 스팸 메일 발송, 게이트웨이/디바이스의 취약점을 이용한 비인가 접근, 암호화 통신 미사용 및 미흡으로 인한 사용자 프라이버시 위협, 물리적 디바이스 탈취를 통한 장치 제어권 획득이 대표적이다[3].

그러므로 스마트 홈 시스템의 보안성을 강화하기 위해 보안 기능을 적용하고 이를 안전하게 운용해야한다. 첫 번째 관리하는 홈서버의 경우 디바이스 등록 및 삭제과정에 대한 관제기능이 적용되어야 하며, 이를 위한 안전한 보안정책 수립이 요구된다. 두 번째 홈 게이트웨이는 내부 데이터 통신 및 외부 인터넷 접속을 수행함으로써 인증, 접근제어, 데이터 암호화와 같은 보안 기능이 적용되어야 한다. 마지막 서비스 제공자 및 스마트 홈 디바이스 통신 구간에서 안전한 디바이스 관리를 위한 펌 웨어 관리, 데이터 복제방지, 안전한 데이터 수집 및 송신과정에 따른 상호 인증기능이 적용되어야 한다[7]. 그리고 스마트 홈 서비스 기반의 보안 위협사례에서는 무결성 훼손, 데이터 유출로 인한 사용자 프라이버시 위협과 같은 보안위협이 있으며 재전송 공격, 중간자 공격, 스푸핑, 스니핑과 같은 다양한 공격기법이 있다[3,8]. 무선 보안의 3대 요소인 기밀성 측면에서 데이터가 안전하게 전송할 수 있도록 안전한 암호 프로토콜을 통해 메시지가 전송되어야 한다. 또한, 디바이스 식별 정보 관리를 통해 비인가 및 허용하지 않은 사용자에 대한 접근제어를 설정해야 한다. 두 번째 무결성 측변에서는 중요 데이터는 안전하게 저장하기 위해 보안 모듈의 사용을 권장하고 있다. 마지막으로 가용성 측변에서는 소프트웨어 보안업데이트, 효율성 있는 보안 정책 수립을 통해 안전한 통신 환경에 제공되어야 한다. 다중 인증 또는 이중 인증은 여러 가지 인증 기법을 활용하여 사용자를 인증하는 방식이다. ID인증기법으로 1차 인증하고, 생체인증이나 OTP 등의 인증기법으로 2차 및 추가인증을 수행하는 방식이다[9,10].

최근 3년이내 사물인터넷 사용자를 위해 안전한 보안기능에 대한 연구는 활발히 진행하고 있다. 대표적으로 N사에서 서비스 트래픽에 대한 분산통신기법, 적재적소에 유연하게 적용 가능한 인프라 제공, 지속 모니터링을 통한 보안 관제 서비스가 있다.

3. 제안한 메시지 프로토콜 설계

본 장에서는 클라우드 서비스 기반 스마트 홈 환경에서 안전한 데이터 통신을 위한 메시지 프로토콜을 제안한다. 디바이스 등록절차, 사용자 인증 및 통신프로토콜 설계, 디바이스 및 사용자 갱신 프로토콜로 세 가지 절차에 관한 내용을 다룬다. 각 절에서 사용하는 쓰이는 약어는 다음 Table 1과 같다.

Table 1. Abbreviations for the proposed Message Protocol

Abbreviations	Explanation
Nonce	Random value
IV	Identification Value
HID	Home Iot Device
TIMESTAMP	Time stamp
S/N	Serial Number
INFO	Information Value

(Continued)

Table 1. Abbreviations for the proposed Message Protocol

Abbreviations	Explanation
P/W	Password
Cert	Authentication Value
MS	Administration Server
CCS	Cloud Computing Server
SQ	Order Identification
RV	Register Order Value
Key	Stream-based key value
Rotate	Rotation Operations
IMEI	Device Identification Number

3.1 디바이스 등록절차

본 절에서는 스마트 홈 환경에서 홈 IoT 장비의 등록절차에 관해서 서술한다. 홈 IoT 장비는 무선 액세스 포인트를 통해 관리서버와 클라우드 서버의 검증을 수행하여 등록한다. 등록과정에서 등록값(RV), 클라우드 컴퓨터상의 IoT 순번식별값(SQ-)을 생성하며 이를 기반으로 스트림기반 킷값을 생성한다. 디바이스 등록절차에 대한 설명은 Fig. 1과 같다.

(1) HOME IoT 장비는 무선 액세스 포인트로부터 등록요청 메시지를 전송한다.

(2) 이를 수신한 무선 액세스 포인트는 HOME IoT 장비로 식별값 요청 메시지를 전송한다.

(3) HOME IoT 장비는 난수를 생성 후 HOME IoT 장비의 식별값을 생성한 후 식별값 응답 메시지를 전송한다.

$$E_{K-HID}(IV_{HID}\|TIMESTAMP\| S/N_{HID})\, E_{K-HID}(Nonce) \quad (1)$$

(4) 무선 액세스 포인트는 수신한 값과 자신의 시리얼 넘버 및 정보를 암호화하여 관리서버에 전송한다.

$$E_{K-HID}(IV_{HID}\|TIMESTAMP\|S/N_{HID}),\ E_{K-HID}(Nonce),\ E_{K-WAP}(S/N_{WAP}\|INFO_{WAP}) \quad (2)$$

(5) 관리서버는 수신받은값의 무선 액세스 포인트의 시리얼넘버, 정보, 타임스탬프를 검증 후 식별값을 점검한다. 이후 계산과정을 거쳐서 장비의 등록값을 생성한다.

$$Device_{R-i} = Info_{MS-D-i}\, SHA-2(S/N_{HID}\| SHA-2(P/W_{HID}) \quad (3)$$

(6) 관리서버는 생성한 디바이스 등록값을 포함 후 인증서와 같이 클라우드 컴퓨팅 서버에 등록된 식별값 검증 요청메시지를 전송한다.

$$E_{K-MS}(INFO_{WAP}\|TIMESTAMP),\ E_{K-MS}(Device_{R-i}\oplus MS_{CERT}),\ E_{K-MS}(MS_{CERT}) \quad (4)$$

(7) 클라우드 서버는 수신받은 메시지를 복호화 후 무선 액세스 포인트의 정보, 타임스탬프, 관리서버의 인증서를 검증한다. 이후 클라우드 컴퓨팅 서버의 등록값(RV)와 순서 식별값(SQ-i)을 생성한다.

$$R_{W-i} = SHA-2(INFO_{WAP}\|MS_{CERT})\oplus SHA-2(TIMESTAMP), SQ-i_{CSS} \quad (5)$$

(8) 등록값과 식별값을 생성한 클라우드 컴퓨팅 서버는 생성한 값을 암호화하여 관리서버로 등록완료메시지를 전송한다.

$$E_{K-CSS}(RV_{W-i}, SQ-i_{CSS}) \quad (6)$$

(9) 관리서버는 수신한 값을 복호화 후 등록값과 순서식별값을 검증 후 등록값(RV)와 무선 액세스 포인트에서 생성한 난수값을 등록한다.

(10) 관리서버는 무선 액세스 포인트로 아래와 같은 값을 포함한 식별값 검증 완료 메시지를 전송한다.

$$E_{K-MS}(SQ-i\oplus S/N_{WAP}) \quad (7)$$

(11) 무선 액세스 포인트는 순서식별값 검증을 위해 계산과정을 거쳐서 순서식별값을 점검한다. 이후 점검한 식별값을 활용하여 스트림기반 키를 생성한다.

$$Key_{Steam}(W-i) = SQ-i \oplus SHA-2(TIMESTAMP) \| INFO(Rotate_{Half}) \quad (8)$$

(12) 무선 액세스 포인트는 스트림키값을 등록 후 HOME IoT 장비로 등록완료 메시지를 전송한다.

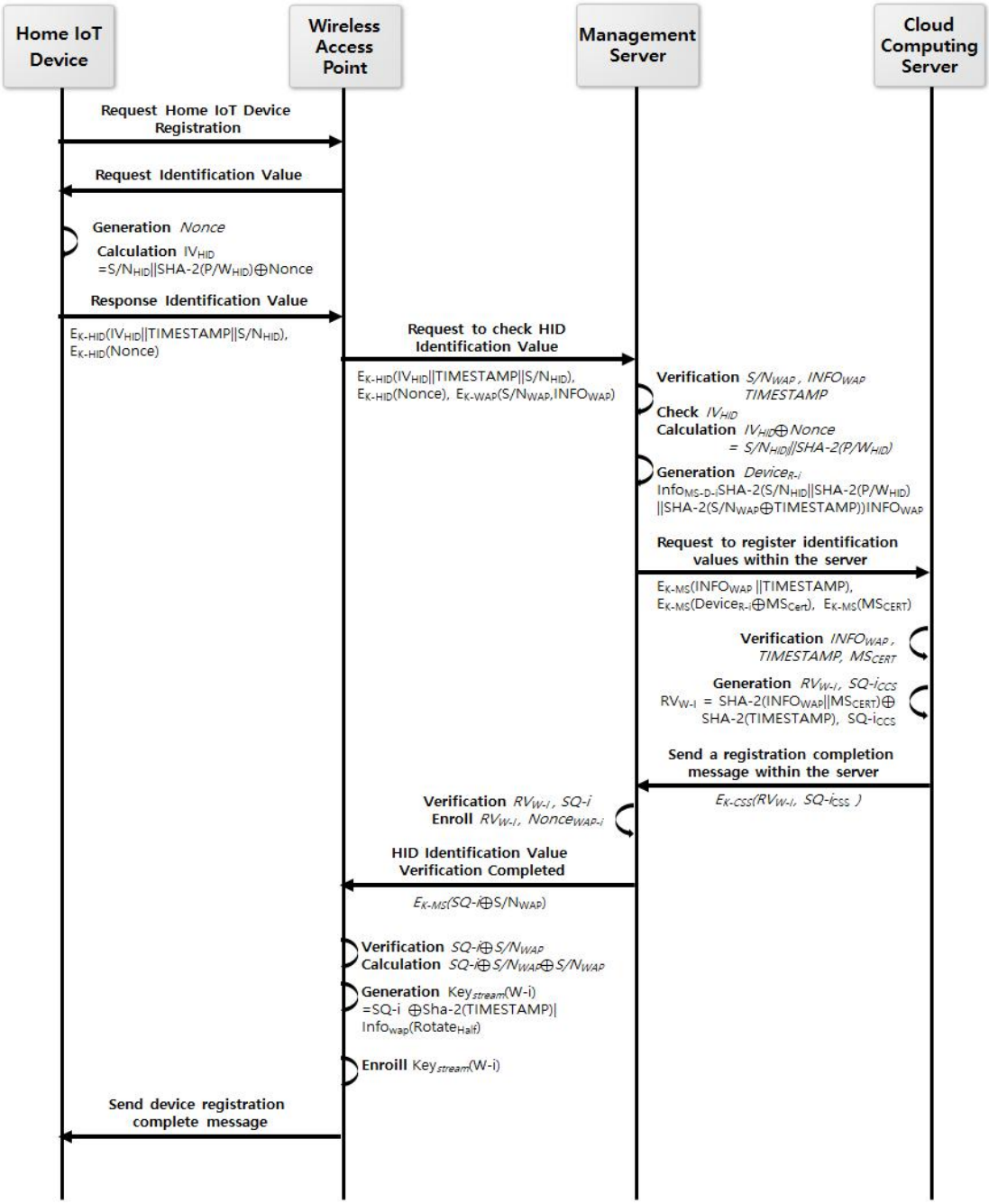

Fig. 1. Device Registration Procedure

3.2 메시지 인증 및 통신프로토콜 설계

본 절에서는 등록된 식별값을 기반으로 메시지 인증 및 통신 프로토콜에 관해 서술한다. 사용자는 무선 액세스 포인트를 통해 우선 HOME IoT 장비의 수집된 데이터를 요청한다. 무선 액세스 포인트는 관리서버와 클라우드 컴퓨팅 서버를 통해 사용자 및 HOME IoT장비의 검증 과정을 수행한다.

이후 스트림 기반의 키를 생성하여 사용자로부터 안전한 메시지를 전송하도록 한다. 메시지 인증 및 통신 프로토콜 설계절차는 Fig. 2와 같다.

(1) 사용자는 무선 액세스 포인트로부터 HOME IoT 장비로부터 수집된 데이터를 요청한다.

$$E_{K-U}(IMEI||User_{info} \oplus SHA-2(PW), \quad E_{K-U}(SHA-2(PW) \tag{9}$$

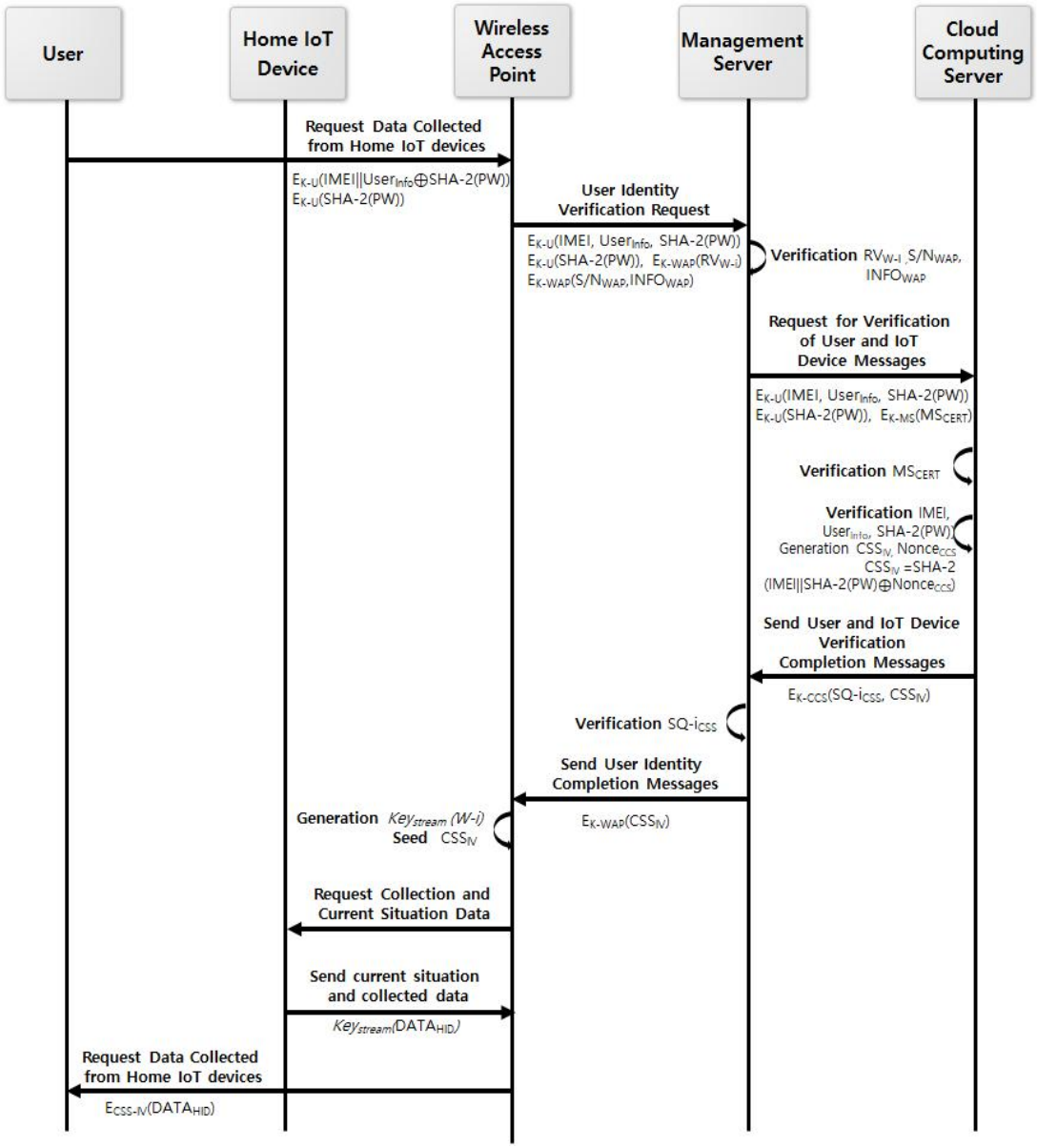

Fig. 2. Message authentication and communication protocol procedures

(2) 메시지를 수신한 무선 액세스 포인트는 관리서버로부터 사용자 신원검증 요청 메시지를 요청한다.

$$E_{K-U}(IMEI, User_{Info}, SHA-2(PW), \\ E_{K-U}(SHA-2(PW)), E_{K-WAP}(RV_{W-i}), \\ E_{K-WAP}(S/N_{WAP}, INFO_{WAP}) \quad (10)$$

(3) 관리서버는 수신받은 메시지 등록 식별값, 무선 액세스 포인트의 시리얼넘버, 정보를 검증 후 클라우드 컴퓨팅 서버로부터 사용자 및 HOME IoT 장비의 메시지 검증 요청 메시지를 전송한다.

$$E_{K-U}(IMEI, User_{Info}, SHA-2(PW)), \\ E_{K-U}(SHA-2(PW)), E_{K-MS}(MS_{CERT}) \quad (11)$$

(4) 클라우드 컴퓨팅 서버는 수신받은 메시지의 인증서, 사용자의 신원확인값 및 정보 등을 확인하고 클라우드 컴퓨팅 서버의 등록 식별값 및 난수를 생성한다.

$$CCS_{IV} = SHA-2 \\ (IMEI \| SHA-2(PW) \oplus Nonce_{CSS}) \quad (12)$$

(5) 클라우드 컴퓨팅 서버는 사용자와 HOME IoT 장비 검증 완료 메시지를 암호화하여 송신한다.

$$E_{K-CCS}(SQ-i_{CCS}, CCS_{IV}) \quad (13)$$

(6) 관리서버는 메시지를 수신 후 순서식별값을 검증 후 무선 액세스 포인트로부터 사용자 식별완료 메시지를 전송한다.

$$E_{E-WAP}(CSS_{IV}) \quad (14)$$

3.3 디바이스 및 사용자 갱신 관리

본 절에서는 등록된 타임스탬프 기반으로 디바이스 및 사용자 식별값에 대한 갱신 절차를 서술한다. 관리서버는 무선 액세스 포인트를 활용하여 HOME IoT장비 와 사용자의 식별값을 갱신한다. 이후 갱신한 값을 클라우드 컴퓨팅 서버로 재등록하여 향후 안전한 데이터 통신을 수행하도록 한다. 디바이스 및 사용자 갱신 관리 절차는 Fig. 3과 같다.

(1) 관리서버는 무선 액세스 포인트로 디바이스 완료 예정 메시지를 전송한다.

$$E_{K-MS}(SQ-i \| TIMESTAMP) \quad (15)$$

(2) 무선 액세스 포인트는 클라우드순서식별값과 타임스탬프를 검증 후 사용자로부터 디바이스 등록에 대한 유효기관 만료 메시지를 전송한다.

$$E_{K-WAP}(S/N_{WAP} \| TIMESTAMP), \\ E_{K-WAP}(SHA-2(PW), E_{KP-}(INFO_{WAP})) \quad (16)$$

(3) 사용자는 수신한 메시지의 무선 액세스 포인트의 식별값, 타임스탬프, 비밀번호를 검증 후 무선 액세스포인트로부터 디바이스 갱신 요청 메시지를 전송한다.

$$E_{K-U}(USER_{INFO} \oplus SHA(PW_{Renewal})), \\ E_{K-U}(SHA(PW_{Renewal})) \quad (17)$$

(4) 수신받은 무선 액세스 포인트는 관리서버로부터 사용자 신원 검증요청 메시지를 전송한다.

$$E_{K-U}(USER_{INFO} \oplus SHA(PW_{Renewal})), \\ E_{K-U}(SHA(PW_{Renewal})), \\ E_{K-WAP}(S/N_{WAP}, INFO_{WAP}) \quad (18)$$

(5) 관리서버는 수신받은 메시지의 식별값 정보를 검증 후 등록된 식별값을 추출한다. 이후 클라우드 컴퓨팅 서버로부터 디바이스 및 사용자 검증 요청 메시지를 전송한다.

$$E_{K-U}(USER_{INFO} \oplus SHA(PW_{Renewal})), \\ E_{K-U}(SHA(PW_{Renewal})) \quad (19)$$

(6) 클라우드 컴퓨팅 서버는 수신 받은 메시지의 사용자 정보, 갱신된 비밀번호를 검증 한다. 이후 등록된 식별값, 순서값을 생성한다.

$$RV_{W-i} = SHA-2(INFO_{WAP} \| MS_{CERT}), \\ \oplus SHA-2(TIMESTAMP_{i+1}), SQ-i_{CCS+i} \quad (20)$$

(7) 클라우드 컴퓨팅 서버는 관리서버로부터 사용자 및 디바이스 검증 완료 메시지를 전송한다.

$$E_{K-CSS}(RV_{W-i+1}.SQ-i_{CCS+i}) \quad (21)$$

(8) 관리서버는 무선엑세트포인트로 사용자 검증 완료 메시지를 암호화 후 전송한다.

$$E_{K-CSS}(RV_{W-i+1}.SQ-i_{CCS+i}) \quad (22)$$

(9) 무선 액세스 포인트는 HOME IoT 장비로부터

디바이스 식별값 요청 메시지를 전송한다. 이후 HOME IoT 장비는 난수값을 생성 후 암호화하여 무선 액세스 포인트로부터 디바이스 식별값 응답 메시지를 전송한다.

$$E_{K-HID}(Nonce_{HID-N}) \quad (23)$$

(10) 무선 액세스 포인트는 메시지를 수신 후 등록값을 기반으로 스트림기반 키를 생성한다. 이후 사용자로부터 디바이스 갱신완료 메시지를 전송한다.

4. 성능평가

4.1 안전성 분석

본 절에서는 클라우드 서비스 기반 스마트 홈 환경에서 발생하는 공격기법 및 취약점에 대한 안전성에 관한 내용을 다룬다. 대표적인 취약점인 데이터 조작 및 무결성 훼손 및 사용자 프라이버시 위협과 재전송 공격, 중간자 공격에 대해 분석한다.

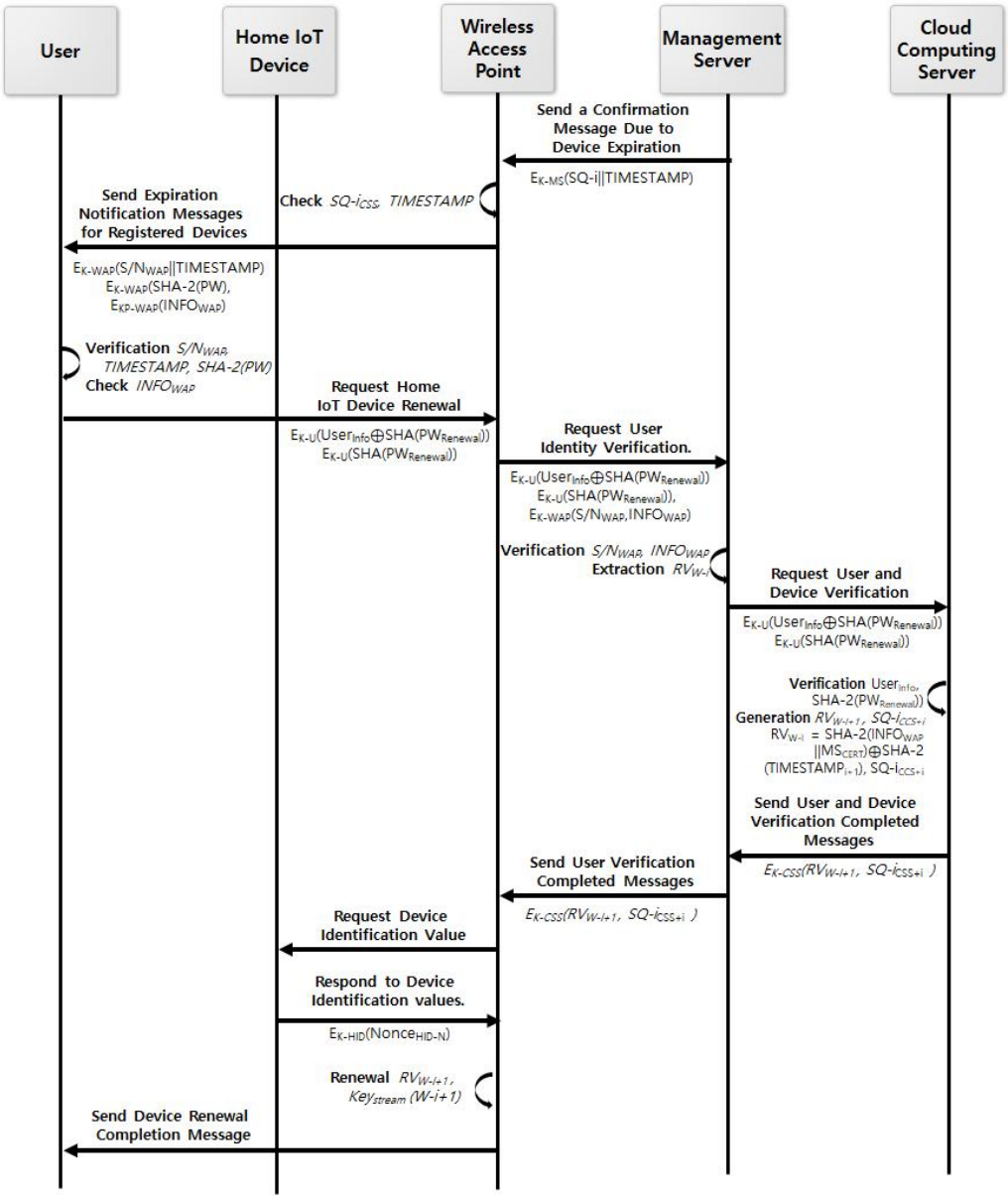

Fig. 3. Device and User Renewal Management Procedures

4.1.1 신체적 건강 데이터 조작 및 무결성 훼손

스마트 홈 서비스 기반 무선 네트워크 환경에서는 생성한 데이터를 안전하게 전송하고 무결성을 보장하기 위해서는 안전한 통신 프로토콜을 설계해야 한다. 본 논문에서는 메시지 전송에 대한 안전성을 보완하기 위해 메시지 통신 과정에서 클라우드 컴퓨팅 서버에서 생성한 CCS_{IV}를 시드값으로 스트림키 값을 생성하였다. 이를 기반으로 사용자로부터 안전하게 메시지를 전송하도록 프로토콜을 설계하였다.

4.1.2 사용자 프라이버시 위협

스마트 홈 서비스를 사용하는 많은 사용자가 프라이버시 침해와 정보유출에 대해서 안전할 수 없으며, 이에 대한 금전 및 정신적인 피해를 보고 있다. 본 논문에서는 더 안전한 서비스를 수행하고 사용자 프라이버시 보안성을 높이기 위해 수집된 데이터 전송과 사용자 데이터 전송에 대한 킷값을 다르게 생성하여 메시지 프로토콜을 설계하였다. 그리고 물리적인 장비탈취에 따른 데이터 유출을 방지하기 위해서 사용자와 HOME IoT 장비의 검증을 관리서버와 클라우드 컴퓨팅 서버에서 이중인증을 수행한다.

4.1.3 재전송 공격

재전송 공격은 스마트 홈 환경에서 대표적인 공격이며 재전송 공격을 받은 네트워크 인프라(관리서버, 클라우드 컴퓨팅 서비스)는 정상적인 서비스를 수행하지 못하게 한다. 이를 방지하기 위해 등록 절차에서 생성된 스트리밍 킷값, 사용자로부터 수집된 데이터를 전송할 수 있는 스트림기반 킷값을 다르게 생성하여 데이터를 안전하게 전송할 수 있다. 그리고 유효기간을 체크하여 등록된 타임스탬프를 기반으로 사용자 및 디바이스를 안전하게 관리할 수 있다.

4.1.4 중간자 공격

중간자 공격은 스마트 홈 환경뿐만 아니라 무선네트워크 환경에서 빈번히 발생하는 공격기법 중의 하나이다. 스마트 홈 환경의 HOME IOT 장비는 무선 네트워크를 활용하여 데이터를 전송함으로써 기존 공격기법을 응용한 변종의 중간자 공격에 대해서 안전할 수 없다. 그러므로 이에 대한 피해를 방지하기 위해 HOME IoT와 사용자의 신원값을 관리서버에서 인증을 수행한다. 그리고 클라우드 컴퓨팅에서 생성한 $RV, SQ-i$검증값을 관리함으로써 중간자 공격기법은 실패하게 된다.

4.2 보안성 비교평가

보안성 비교평가를 수행하기 위해 기존 무선 네트워크 환경에서 활용하는 SSL/TLS 및 WPA, WPA2 및 AES와 비교분석을 수행하였다. 앞 절의 공격기법 및 취약점을 기반으로 안전성을 분석하였으며, 이에 따른 분석한 내용은 다음 Table 2와 같다.

Table 2. Analyze security of existing algorithms and proposed protocols

	SSL/TLS & WPA	WPA2 & AES	Proposed communication protocol
Encryption and Decryption Process	4E+4D+2V	4E+4D+2V	3E+3D+2H
Signature and Verification Procedures	Perform authentication through third parties	Certificate and Symmetric Base	Self-authentication and hashtree-based validation
Retransmission Attack	Enable	Disable	Disable
Intermediate Attack	Enable	Enable	Disable
Mutual authentication	Disable	Disable	Enable
Data Modulation	Enable	Enable	Disable
Certificate Renewal Management Aspects	Management required	Effective	Very effective

암/복호화 과정에서 기존 SSL/TLS 및 WPA, WPA2 및 AES에서는 4번의 암복호화와 2번의 제3자 검증을 수행하는 반해, 제안한 통신프로토콜을 3번의 암복호화와 2번의 자가인증기반 해시 검증을 통해 메시지를 검증한다. SSL/TLS 및 WPA는 RC4 기반 암호를 사용하여 통신함으로써 재생공격에 취약하나, WPA2 및 AES와 제안한 통신프로토콜에서는 재전송 공격에 대응하기 위해 신원값 검증 및 $RV, SQ-i$ 검증값을 체계적으로 관리하고, 상호인증값을 수행함으로써 중간자 공격에 안전하다. 데이터 변조를 막기 위해 기존의 SSL/TLS 및 WPA, WPA2 및 AES와 달리 HOME IoT와 클라우드 컴퓨팅 서버에서 이중인증을 수행하였다. 마지막으로 인증서 관리 측면에서는 갱신프로토콜

에서 제안한 타임스탬프 및 스트림기반의 키 관리를 통해 효율적으로 사용자의 인증서를 관리할 수 있다.

위에서 언급한 SSL/TLS 및 WPA, WPA2 및 AES와 제안한 통신프토콜에 대해 효율성을 비교하기 위해 Intel(r) Core(TM) i5-8565U CPU @ 1.60GHz 1.80GHz, Windows 10 Professional 운영체제 환경에서 Java(jdk 1.8.0_31)기반, Mariadb-10.6.0, Eclipse Software를 사용하였다.

메시지 통신프로토콜과정에서는 기존 PKI기법 대비 약 50%의 효율성과 서명검증 속도에서는 약 25%의 효율적인 측면을 확인할 수 있었다.

그리고 PKI는 중간자 공격에 대한 취약점이 있으며, 인증서 갱신 관리측면, 데이터 변조에 대한 미흡사항이 있다. 제안한 통신 프로토콜은 안전성분석에 대한 공격기법 및 취약점에 대해서 보완하였으며, 상호인증과 데이터 변조기법을 방지하기 위해 안전성을 강화하였다.

WPA 및 SSl/TLS, WPA2 및 AES와 제안한 통신프로토콜의 메시지 통신 프로토콜과 서명검증의 결과는 Fig. 4와 같다. 메시지 통신 프로토콜과정에서는 WPA 및 SSl/TLS 대비 약 30%, WPA2 및 AES기법 대비 약 18%의 메시지 통신에 대한 효율성을, 서명검증 속도에서는 약 33%, 16%의 효율적인 측면을 확인할 수 있었다. 제안한 프로토콜에서는 서명 및 검증 방법에서 자가인증을 통한 해시 트리 기반의 검증을 수행함으로써 기존의 인증방식인 신뢰 된 제 3자가 검증하는 대비 높을 효율성을 가졌다. 마지막으로 인증 갱신 측면에서는 자가인증을 통해 암복호화에 대한 절차를 간소화하여 더욱 효과적으로 속도가 감소하는 것을 확인하였다.

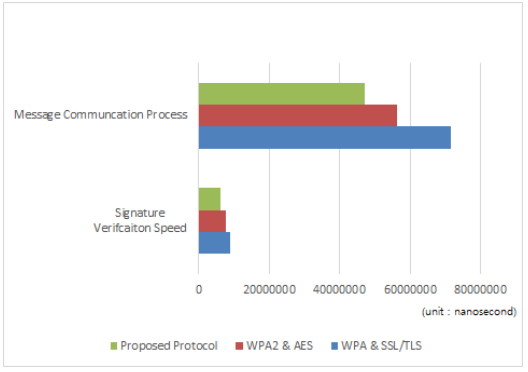

Fig. 4. Efficiency Comparison Analysis Chart

5. 결론

본 논문에서는 클라우드 서비스 기반 스마트 홈 환경에서 안전한 데이터 통신을 위한 메시지 프로토콜을 제안하였다. 디바이스 등록 절차, 사용자 인증 및 통신 프로토콜, 갱신프로토콜을 설계하여 사용자가 HOME IoT 장비로부터 안전하게 데이터를 통신하도록 하였다. 스마트 홈 환경에서 발생하는 재생공격, 중간자공격, 무결성 훼손, 인증서 공격기법 및 효과적인 관리측면에 대해 안전성을 분석하였다. 추가로 무선 네트워크 환경에서 사용하는 암호화 및 인증기법인 WPA2 및 AES 기법과 효율성 분석을 통해 통신 절차에서 약 18%, 서명값 검증의 속도 부분에서 약 16%의 높은 효율성을 확인할 수 있었다.

향후 제안한 메시지 프로토콜을 활용하기 위해서 소형장비에서도 활용할 수 있도록 본 논문에서 연구된 인증프로토콜이 적용되어야 한다. 그리고 사용자 운영환경의 보안성을 강화하기 위해 보안정책을 수립하여야 한다. 마지막으로 무선네트워크 환경에서 시도되고 있는 변종 및 신규공격기법에 대한 위험성을 분석하여 이를 사전 예방할 대응방안을 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. W. Jin, J. O. Park & M. S. 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] 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

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

[7] 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

[8] 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.

[9] B. R. Zebari, A. Abdulazeez, D. Zeebaree, D. Zebari & J. Saeed. (2020). A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction. *Journal of Applied Science and Technology Trends, 1(2),* 56-70.
DOI : 10.38094/jastt1224.

[10] H. J. Mun. (2018). Biometric information and OTP based on Authentication Mechanism using Blockchain. *Journal of convergence for Information Technology, 8(3),* 85-90.
DOI : 10.22156/CS4SMB.2018.8.3.085

박 중 오(Jung-Oh Park) [정회원]

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