https://doi.org/10.33778/kcsa.2022.22.4.099

스마트 홈 사물인터넷 기기(IoT)의 원격제어 시 사용자 권한 탈취 및 이상조작 방지를 위한 클라우드 보안인증 플랫폼 설계★

유 용 환*

요 약

최근 스마트 홈 가전 및 사물인터넷(IoT) 기기들의 사용량이 증가되고 있으나 모바일 서비스들을 통해 이를 이용하는 과정에서의 해킹, 신분도용, 정보유출, 개인 프라이버시의 심각한 침해 및 비정상 접속, 사용자의 오조작이 증가되고 있으며, 그 사실 여부를 확인하거나 입증할 방법이 매우 미흡한 상황이다. 특히, 스마트 홈에서 사용하는 IoT기기에서는 사양과 환경 등 많은 제약이 따르기 때문에 컴퓨터에서의 인터넷 보안 수준을 똑같이 제공하기 어렵다.

이러한 스마트 홈 IoT기기에서도 해킹 및 사용자 권한 탈취, 이상 조작으로 인한 사고예방, 기기조작에 대한 감사기록을 강화할 수 있도록 모바일 단말과 IoT기기 간에 보안인증의 관리기능을 가지는 클라우드 보안인증 플랫폼의 구축 방안을 제시하고자 한다.

Cloud security authentication platform design to prevent user authority theft and abnormal operation during remote control of smart home Internet of Things (IoT) devices

Yoo Young Hwan*

ABSTRACT

The use of smart home appliances and Internet of Things (IoT) devices is growing, enabling new interactions and automation in the home. This technology relies heavily on mobile services which leaves it vulnerable to the increasing threat of hacking, identity theft, information leakage, serious infringement of personal privacy, abnormal access, and erroneous operation. Confirming or proving such security breaches have occurred is also currently insufficient. Furthermore, due to the restricted nature of IoT devices, such as their specifications and operating environments, it is difficult to provide the same level of internet security as personal computers. Therefore, to increase the security on smart home IoT devices, attention is needed on (1) preventing hacking and user authority theft; (2) disabling abnormal manipulation; and (3) strengthening audit records for device operation. In response to this, we present a plan to build a cloud security authentication platform which features security authentication management functionality between mobile terminals and IoT devices.

Key words : IoT, Smart Home, Mobile, Security, Authentication, Blockchain

접수일(2022년 08월 30일), 수정일(2022년 09월 19일), 게재확정일(2022년 10월 25일)

★ 본 논문은 2021년도 남서울대학교 학술연구비 지원에 의해 연구되었음

* 남서울대학교 컴퓨터소프트웨어학과 조교수

1. 서 론

정보통신기술의 급속한 발전으로 사람, 사물, 공간, 데이터 등이 연결되는 초연결사회가 도래하게 되면서, IoT(사물인터넷)이 주요 이슈로 부각되었다. IoT 환경 중에서도, 최근 보급이 확산되고 있는 스마트 홈 분야는 가정 내 스마트 디바이스들을 유·무선 네트워크로 연결하여 자동화, 원격 제어, 에너지 관리 등을 통해 이용자에게 편의성을 제공하고 있다[1].

스테티스타(Statista)의 조사에 의하면 2021년 글로벌 스마트 홈 활용 가구 수는 2억 5,989만 가구로 추산되며, 2025년에는 4억 7,822만 가구로 증가할 것으로 예측되고 있다[2]. 스마트 홈에 거주하는 주민들은 스마트 홈 가전(TV, 냉장고, 보일러, 전등 등)과 IoT 기기 (CCTV, 창문 개폐기 등)의 조작을 원격에서 모바일로 편리하게 조작할 수 있고, 다양한 종류의 모바일 서비스들과 연동하는 스마트 홈의 영역이 급격하게 확대되고 있다.

2025년까지 전세계 IoT 연결기기 수도 309억대로 예측되지만, 통합주택제어판(월패드) 등 IoT기기 대상의 끊임없는 공격시도로 보안에 취약한 IoT기기로 인한 일상에서의 사이버위협이 증가할 것으로 전망된다. 이처럼 IoT 기기가 취약할 경우 사생활 정보유출, 디도스 공격 등 사이버 공격 수단으로 악용될 수 있어 IoT 기기에 대한 점검과 보안취약점 조치 강화가 필요하다[3]. 또한 실생활에서 일어날 수 있는 모바일 기기의 분실, 탈취로 인한 비정상적인 접속이나 사용자의 오조작 등으로 발생하는 사물인터넷의 사고 예방도 필요하다.

본 연구에서는 스마트 홈에서 사용하는 홈·가전 IoT기기의 수준별 특성과 보안취약점을 조사하고, 기존의 모바일, IoT 보안 수준을 강화할 수 있는 클라우드 보안인증 플랫폼의 보안 모델과 다중보안 프로세스를 설계하였다.

2. 스마트 홈 IoT 기기의 보안취약점

2.1 OWASP, IoT 기기의 10대 보안취약점

OWASP는 2021년 IoT 기기의 10대 보안 취약점을 <표 1>과 같이 제시하고 있다[4].

<표 1> IoT 기기의 10대 보안취약점

01. 접근 권한 취약점
02. 암호화 오류
03. 인젝션 (Injection)
04. 안전하지 않은 설계
05. 보안설정오류
06. 취약하고 오래된 요소
07. 식별 및 인증 오류
08. 소프트웨어 및 데이터 무결성 오류
09. 보안 로깅 및 모니터링 실패
10. 서버 측 요청 위조

2.2 홈·가전 IoT 제품 유형 및 보안요구사항

홈·가전제품 등 일상생활로 IoT 서비스가 확산되면서 PC 외에도 가정용 무선공유기를 비롯해 인터넷에 연결된 모든 홈· 가전 IoT 제품이 해킹 대상이 될 수 있다. 특히 IoT 제품은 일반 ICT 시스템과 달리 보안기술을 적용하기 어려워 상대적으로 보안에 취약하다는 문제점이 있다. <표 2>는 홈 · 가전 IoT 제품들의 유형별 주요보안위협에 대해 정리한 것이다[5].

<표 2> 홈·가전 IoT 제품 유형별 주요보안위협

유형	주요제품	주요보안위협	보안위협 원인
멀티미디어	스마트TV, 스마트 냉장고 등	- PC 환경에서의 모든 악용 행위 - 카메라/마이크 내장 시 사생활 침해	• 인증 메커니즘 부재 • 강도가 약한 비밀번호 • 펌웨어 업데이트 취약점 • 물리적 보안 취약점
생활가전	청소기, 인공지능 로봇 등	- 알려진 운영체제 취약점 및 인터넷 기반 해킹 위협 - 로봇청소기에 내장된 카메라를 통해 사용자 집 모니터링	• 인증 메커니즘 부재 • 펌웨어 업데이트 취약점 • 물리적 보안 취약점
네트워크	홈캠, 네트워크 카메라 등	- 사진/동영상을 공격자의 서버 및 이메일로 전송 - 네트워크에 연결된 홈캠 등을 원격으로 제어하여 임의 촬영 등 사생활 침해	• 접근통제 부재 • 전송데이터 보호부재 • 물리적 보안 취약점
제어	디지털 도어락, 가스밸브 등	- 제어기능 탈취로 도어락의 임의 개폐	• 인증 메커니즘 부재 • 강도가 약한 비밀번호 • 접근통제 부재 • 물리적 보안 취약점
	모바일 앱 (웹) 등	- 앱 소스코드 노출로 IoT 제품 제어기능 탈취	• 인증정보 평문 저장 • 전송데이터 보호 부재
센서	온/습도 센서 등	- 잘못된 또는 변조된 온·습도 정보 전송	• 전송데이터 보호 부재 • 데이터 무결성 부재 • 물리적 보안 취약점

2.3 홈·가전 IoT 보안항목별 보안요구사항

홈·가전 IoT 제품은 유형에 따라 세부 보안요구사항을 고려해야 한다. 센싱 제품은 기본적으로 제품 간 상호인증, 정보의 무결성을 요구하며, 제어 기능이 있는 제품의 경우 인증 및 무결성과 함께 제어정보에 대한 기밀성을 고려해야 한다. 구매 기능이 포함된 제품은 인증정보의 무결성 그리고 결제정보 등에 대한 기밀성 및 무결성을, 촬영기능이 제공되는 경우 개인정보보호 관점으로 촬영정보에 기밀성을 고려해야 한다. IoT 제품을 원격으로 운용하는 경우 사용자 인증을, 관리 기능이 있는 제품의 경우 설정 정보의 무결성 및 기밀성, 사용자에 대한 인증·인가 등 강한 보안성을 요구할 수 있다. <표 3>은 홈·가전 IoT 제품 유형별로 적용해야 하는 보안항목을 정리한 것이다[5].

<표 3> IoT 제품 유형별 적용해야 하는 보안항목

보안항목	보안요구사항	
인증	인증 및 접근통제	- 제품의 초기 인증정보 변경 - 사용자 인증 - 인증정보 보호 - 안전한 비밀번호 사용 - 접근통제
	IoT 제품간 상호인증	- 상호인증
암호화	안전한 암호 알고리즘 사용	
	안전한 암호키 관리	- 안전한 암호키 생성 - 안전한 암호키 전송 - 안전한 암호키 저장 - 안전한 암호키 파기
	안전한 난수 생성 알고리즘 사용	
데이터 보호	안전한 통신채널	- 안전한 통신채널 제공 - 안전한 세션관리
	저장 및 전송 데이터 보호	- 전송데이터 보호 - 저장데이터 보호 - 메모리 및 역공학 공격 대응 - 부채널 공격 대응
	개인정보 보호	
플랫폼 보안	설정값 및 실행코드 무결성 검증	- IoT 제품 주요 설정값 및 실행코드 무결성 검증
	안전한 업데이트	- 신뢰할 수 있는 업데이트 서버 - 업데이트 파일의 부인방지 및 무결성 보장 - 안전한 업데이트 기능 제공 - 펌웨어 분석 방지 기능 제공
	감사기록	- 감사기록 생성 - 감사기록 보호

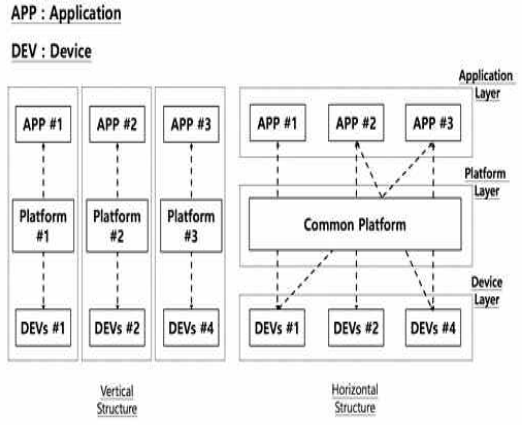
IoT의 서비스를 구성하고 있는 IoT관련 디바이스, 게이트웨이, 네트워크, 플랫폼, 서비스, 어플리케이션 중에서 특히, 디바이스에 대한 보안 위협이 가장 크다는 각종 관련 연구가 뒤따르고 있다.

저전력과 저사양 및 경량화라는 하드웨어적인 한계점, 펌웨어 패치의 어려움, 외부해킹, 기능 오작동 및 불능 등 기존 IT제품과 서비스에서 발생되거나 존재하였던 보안취약점과는 다른 보안 취약점을 내포하고 있는데, 이는 IoT디바이스의 환경적 요소의 한계점으로 인하여 발생 가능하기 때문이다[6].

또한, IoT서비스 영역에서는 애플리케이션 해킹, 비인가 사용자의 접속, 무차별 대입공격 등의 보안위협이 상존하고 있다[7].

2.4 홈·가전 IoT기기의 수직적 계열화에 따른 보안 취약점

현재까지 많은 IoT 플랫폼은 응용 서비스에 수직적인 구조를 가지고 서비스를 제공하였다. 따라서 플랫폼 자체가 응용 서비스에 종속적으로 구성되어 있어 응용 서비스 또는 디바이스들이 서로 상호운용을 할 수 없었다. (그림 1)의 IoT 플랫폼 수직 구조(Vertical Structure)와 수평 구조(Horizontal Structure)를 살펴보면 두 구조의 차이를 알 수 있다.



(그림 1) IoT 플랫폼 수직 구조와 수평 구조

수평 구조의 경우는 응용 서비스와 디바이스의 상호운용이 자유스러우나 수직 구조는 응용 서비스와 디바이스의 상호운용성에 대해서 경직되어 있다[8].

기존 스마트홈 IoT 통합서비스의 대다수는 플랫폼의 구조가 특정 가전그룹이나 홈넷사, 통신사, 건설사 중심으로 사일로 형태의 수직적 계열화 되어 있어 개방성과 확장성이 부족하며, 경쟁사 제품에 대한

서비스 지원이 불가한 경우가 많다. 또한 계열화에 속하지 않은 IoT기기의 경우는 응용서비스 뿐만 아니라 IoT의 보안 영역에서도 개별적인 모바일 앱을 사용해야 하는 폐쇄적인 구조를 가지고 있으며, IoT기기의 하드웨어가 저사양이거나 운영체제의 제약, 제조기업의 보안에 대한 투자여력 부족 등으로 다수의 스마트홈 IoT기기 들이 보안위협에 노출되어 있다.

상용화 제품 다수의 보안인증 수준도 누구나 설치하여 사용할 수 있는 개방된 앱에서의 단순한 접근절차(단지명&동호수 ID 또는 IP주소 및 패스워드 입력방식), 암호화가 되어 있지 않은 홈네트워크, 복합인증 체제의 부재 등 취약점이 상당수 노출되어 있다.

3. 스마트홈 IoT 기기의 클라우드 보안인증 플랫폼 설계

3.1 설계 개요

3.1.1 설계 목적

기존 스마트홈 IoT보안 플랫폼들의 대안으로 홈·가전 IoT 제품 유형별로 요구되는 보안항목들을 포괄적으로 적용하고, 경량화, 개방성, 확장성을 고려한 스마트홈 IoT기기의 클라우드 보안인증 플랫폼의 방안을 제시하고자 한다.

3.1.2 하이브리드 통합인증

스마트홈 IoT기기의 보안 취약점을 보완하기 위해 (그림 2)와 같이 ① 앱인증, ② 사용자인증, ③ 모바일 기기 인증, ④ IoT기기 권한인증 등이 복합적으로 적용되는 하이브리드 통합인증으로 구성하며, 발생하는 주요 이벤트들의 모니터링 및 로깅 기능을 가진다.

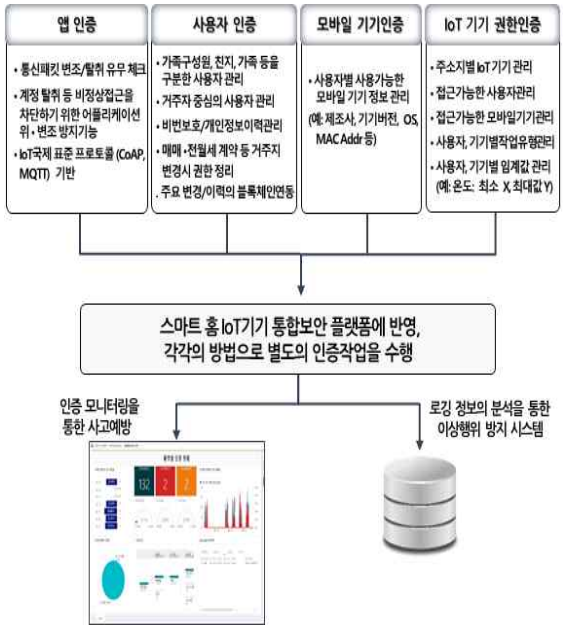
3.1.3 주요 고려사항

설계시의 주요 고려사항은 다음과 같다.

① 관련 앱과 모듈의 변조체크를 사용하여 보안키 및 물리코드 탈취 검증을 하는 해킹 탐지

② 카드나 USB를 사용하지 않고 단말 고유코드와 1회성 조합키를 사용

③ 해커에 의한 스니핑, 패킷조작 등을 방지하기 위한 통신 패킷의 변조 및 탈취유무를 체크



(그림 2) 스마트 홈 하이브리드인증 구성도

④ 모바일 단말의 IoT기기에 대한 인증프로세스

⑤ IoT기기의 무작위 핸들링을 방지

⑥ 사용자 단말을 마스터(Master) / 패밀리(Family)로 구분하여 마스터를 통한 IoT의 사용자 권한 등록을 주관하고, 해킹 또는 보안사고 시 사용자 상호간 인증절차를 통해 보안성을 강화

⑦ 등록/변경이력, 주요 제어정보 등의 감사기록을 블록체인과 연동하여 저장

3.2 시스템의 구성

시스템은 (그림 3)과 같이 서비스용 앱이 탑재된 모바일 단말, 스마트홈 IoT기기, 클라우드 보안인증 서버로 구성된다.

모바일 단말에서 스마트홈 IoT기기의 원격제어를 위한 사용자인증을 개시할 경우에 스마트홈 IoT기기에서는 앱인증, 사용자인증, 모바일기기 인증, IoT기기 제어범위 인증 등의 절차를 클라우드 보안인증 서버에 의뢰하고, 단말이나 사용자의 인증이 완료된 이후 스마트홈 IoT기기의 응용서비스를 개시하는 프로세스이다.

(그림 3) IoT 보안인증 시스템 구성도

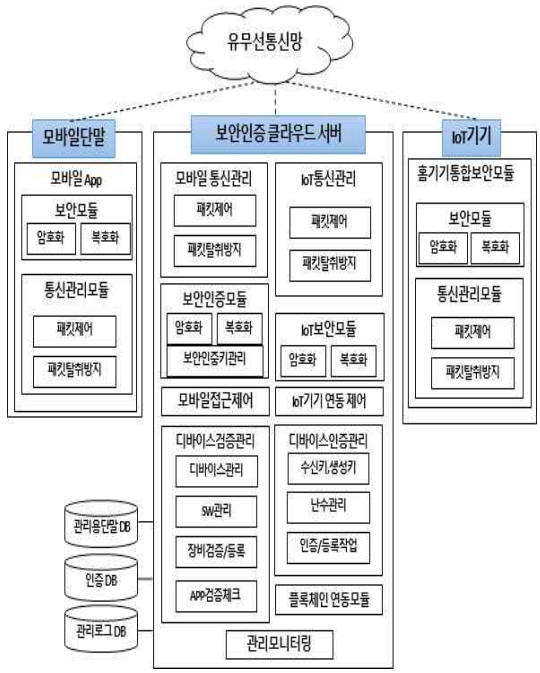
스마트홈 IoT기기는 이 과정에서 모바일 단말과 서버 간의 클라우드 보안인증 프로세스의 패킷을 중계하게 되며, IoT 특성별 주요 설정값의 변경이나 임계값을 넘어서는 제어가 시도될 경우 이를 보안인증 서버에 전달하여 수행 적정성 여부에 대한 검증을 요청한다.

보안인증서버는 IoT사용자의 단말정보, 사용자 등록 및 권한, 사용위치, IoT별 제어특성 등 IoT기기의 이상제어 방지를 위한 정보들을 보유하며, 중요한 등록/변경사항이나 제어이력에 대해서는 블록체인과 연동하여 로깅(Logging)을 한다.

모바일 단말에는 서비스를 위한 연동 모듈이 탑재되며, 이를 통해서 스마트홈 IoT기기에서의 직접적인 보안인증, 사고예방에 대한 시스템적인 부담을 경량화 시킨다..

3.3 시스템의 모듈별 기능

시스템은 IoT기기를 원격 제어하는 모바일 단말 부문, 보안인증을 담당하는 클라우드 서버 부문, 보안중계 및 서비스를 직접 담당하는 IoT기기 부문과 유무선통신망으로 구성되어 있으며, 주요 모듈의 구성도는 (그림 4)와 같다.



(그림 4) 시스템 모듈 구성도

3.3.1 모바일 단말의 모듈 구성

모바일 단말에서는 IoT기기의 등록 관리와 제어, 보안인증 서버와의 인증프로세스가 이루어진다.

단말의 해킹대비 모듈로는 소스코드 임의변조 체크 로직, 스니핑(sniffing) 및 패킷 탈취방지 로직, 패킷조작 방지 패리티(parity)체크 로직, 보안키 탈취, 물리코드 및 보안로직 변경방지 기능 등이 클라우드 보안인증서버와 연동하여 수행된다.

모바일 단말의 주요 모듈은 다음 기능이 포함된다.

① IoT기기의 관리 모듈
- IoT기기의 설정, 등록 및 관리
- IoT기기의 자동화 관리, 메시지 설정

② 보안 모듈
- 모바일 단말기기와 인증서버 간의 데이터의 암호 및 복호화 관리/운영 모듈 (ARIA, SEED 등)
- 모바일 단말의 하드웨어/네트워크 정보 수집
- 단말정보, 소스코드 해시(hash) 및 인증키 생성

③ 통신관리 모듈
- 통신패킷 및 보안프로토콜 관리/운영 모듈
- 통신패킷의 변조 및 탈취 유무 체크 기능

3.3.2 IoT기기의 모듈구성

IoT기기의 모듈은 ① 홈기기통합보안 모듈, ② 보안인증 모듈, ③ 통신패킷 관리모듈, ④ 패킷탈취 감시 모듈로 구성된다.

한국정보통신기술협회, “사물인터넷 정의 및 참조모델” 에 의하면 IoT는 응용 계층, 서비스 지원 및 응용지원 계층, 네트워크 계층, 디바이스 계층의 4개의 계층과 각 계층에 적용되는 관리 기능과 보안 기능으로 구성되어 있다[9].

보안인증 클라우드 서버와 모바일단말 간의 인증지원 모듈은 IoT 참조모델에서의 서비스 지원 및 응용지원 계층에 위치하게 되며, IoT기기의 특성 및 환경에 따라 모바일 단말과 보안인증 클라우드 서버와 인증을 위한 프로세스 상호연계 처리는 API(Application Programming Interface)와 연동 또는 인증프로세스 중계 로직으로 구현한다.

3.3.3 보안인증 클라우드 서버의 모듈구성

보안인증서버의 운영은 클라우드 서비스를 기본으로 하며, 주요 서브모듈로는 모바일 통신관리, IoT 통신관리, 보안인증모듈, IoT보안모듈, 모바일접근제어, IoT기기 연동제어, 디바이스 검증관리, 디바이스 인증관리, 블록체인 연동모듈, 관리 모니터링 모듈 등이 있다.

보안인증을 위해서는 패킷탈취방지, ID/PW 관리, 인증승인 관리, 보안키 등록/체크/삭제, DB암호화, 개인별 물리코드값 관리, 인증앱 관리, 모바일/서버 소스코드의 변조 체크 로직, 모바일 단말(Master/ Family) 관리/조회, IoT기기 관리/조회, 로그인 관리, 조회관리 앱, 블록체인로깅 모듈 등으로 구성된다.

단말 그룹간의 데이터 전송 및 통신에 대한 안전한 통신을 하기 위한 인증 데이타의 등록, 변경, 삭제 등에 대한 내용들은 로그관리DB를 통해서 관리한다. 단말 정보를 보관하는 단말DB와 장비별 인증 데이타를 관리하는 관리용 단말DB를 통해서 보안인증을 관리하며, 난수발생기를 이용해서 모바일 단말간의 인증승인, 보안인증 서버의 보안체크 등의 기능을 한다. 또한 인증 데이타는 관리용 단말DB의 라이센스 및 승인을 관리하는 기능을 갖는다. 또한 감사기록을 블록체인에 저장하고, 입증하는 기능을 수행한다.

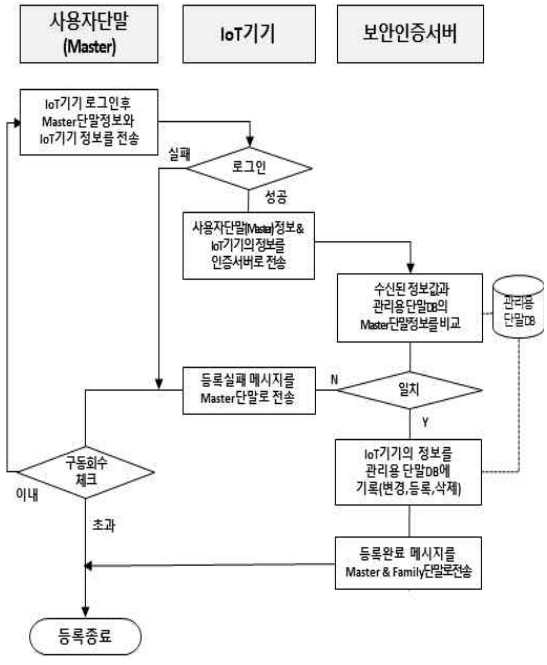
클라우드 보안인증서버에는 단말 간 인증, 장비변동, 사용자 등록/변경, 인증 오류 등이 발생 시 로그에 대한 이력DB 관리, 단말에 대한 정보관리DB 및 인증정보 DB가 생성된다.

관리용단말DB는 등록된 사용자의 단말 및 IoT기기에 대한 관리운영을 수행하고, 인증DB는 인증승인/거부 및 인증에러시의 결과값과 앱 프로그램 버전 정보, 사용자단말/IoT기기에서 수신된 보안인증 체크 값을 클라우드 보안인증서버에 제공하는 기능을 한다.

관리로그DB는 보안인증서버에서 실행하는 모든 작업의 로그를 기록하여 상태 조회, 통계 등의 정보자료 관리를 하는 기능을 수행하며, 향후 입증이 필요한 주요 사항의 등록/변경/조작 기록 등은 블록체인과 연동 저장한 후 감사자료로 활용한다. 그 밖에 사용자단말과 IoT기기에 대한 관리, 인증승인, 인증앱 관리, 인증서버 로그인 관리, ID / PW 관리 등의 기능을 한다.

3.4 사용자 등록 프로세스

IoT기기에 대한 초기 구입시 마스터(Master) 사용자 단말을 클라우드 보안인증 서버에 등록하며,



(그림 5) IoT 사용자 등록 프로세스

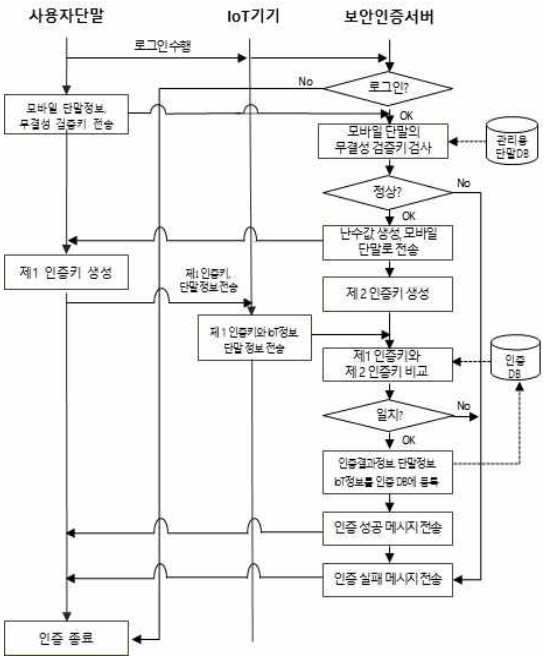
마스터 사용자의 인증하에 패밀리(Family) 사용자를 등록/변경할 수 있다. IoT 사용자의 등록 프로세스는 (그림 5)와 같다.

사용자 등록/관리에는 다음 기능들을 포함한다.

- 금융권 고객정보 보안수준의 개인인증
  (모바일기기정보, IP, 거주지, 접근권한 등)
- 비밀번호 보호기능(계정 취소, 복구 등)
- 비밀번호의 암호화 및 이력관리 기능
- 가구 구성원별 사용 모바일 기기의 정보관리
  (마스터/패밀리 등록, IoT기기별 사용권한 등)
- IoT기기 조작 시의 기준값과 임계값의 관리
- 개인정보의 변경이력 관리
- 사용자별 접근할 주소지와 IoT기기의 관리
- 매매, 전월세등 거주지 변경시 권한 정리
  (블록체인을 이용한 각종 계약서/신분증 관리)

3.5 사용자 인증 프로세스

(그림6)의 기기·사용자 인증 시퀀스 다이어그램(Sequence Diagram)은 사용자 단말의 IoT기기에 대한 인증프로세스로서 사용자단말 - IoT기기 간의 인증을 위해서 사용자단말, IoT기기와 보안인증서버 간의 인증작업 절차이다.



(그림 6) IoT기기·사용자 인증 시퀀스 다이어그램

사용자단말 및 IoT기기는 보안인증서버의 관리용 단말DB에 사용자 단말 및 IoT기기에 대한 정보가 등록 완료된 상태에서 인증프로세스 작업을 수행한다.

모바일단말의 인증절차는 모바일 단말에서 IoT기기에 로그인 요청 시 IoT기기는 인증절차를 보안인증서버 중심으로 수행하도록 통신패킷을 중계한다.

① 모바일단말에서 로그인 정보와 기본 단말 정보, 무결성 검증키를 전송한다

② 보안인증서버에서는 모바일 단말의 IoT 사용등록 여부와 무결성 검증키 검사 등을 수행한 후 1회용 난수값을 생성하여 전달한다.

③ 모바일 단말은 단말기의 고유정보(Mac address, 하드웨어 고유넘버, 앱의 버전, 소스코드의 해시값 등)와 난수값을 해시하여 제1인증키값을 생성하여 인증서버에 전달한다.

④ 보안인증서버는 DB에 등록된 모바일단말의 정보와 난수값을 해시하여 제2인증키값을 생성한 후 모바일단말에서 보내온 제1인증키값과 비교하여 일치여부를 체크한다.

인증 완료후 제어권은 IoT기기의 어플리케이션으로 넘어가며, 비정상 접속시도가 일정 횟수이상 발생하거나 IoT기기 제어시 기기별로 설정해 놓은 임계값을 초과하는 제어가 발생할 경우 IoT기기는 보안인증서버에 요청하여 마스터/패밀리 사용자의 2차 검증단계를 수행하고, 감사자료로 이력을 저장한다.

3.6 보안인증 플랫폼의 혁신성과 차별성

3.6.1 플랫폼의 핵심내용과 혁신성

스마트 홈 클라우드 보안인증 플랫폼의 핵심내용을 요약해 보면 <표 4>와 같다.

<표 4> 보안인증 플랫폼의 핵심내용

구분	핵심 내용	혁신성
모바일 인증 프로그램 (App)	- 모바일 단말에 대한 H/W 인증데이터 검증 및 앱의 변조방지 패리티 체크 - 단말의 보안인증 앱모듈과 클라우드서버 간의 상호인증을 통한 프로세스 제어	모바일 서버간 인증 프로세스
보안인증	- 보안인증 클라우드 시스템을 통한 IoT 보안 모듈의 경량화 및 보안성 강화	IoT기기 보안부담

클라우드 시스템	- 모바일단말 사용자 및 IoT기기의 등록/변경, 실거주 사용자 관리 - 단말인증시의 1회용 패스워드 사용 - 관리용단말DB, 인증DB, 관리로그DB 운용 - 주요정보 변경/이력의 블록체인 연동관리 - 비상시/오류발생시 등록 사용자간 상호인증	경감 및 글로벌 확장가능 클라우드 기반
소스코드 네트워크 보안	- 소스코드 임의 변조 체크 로직 - 스니핑/스푸핑 패킷탈취/조작 방지 로직 - 보안키 탈취, 물리코드/보안로직 변경방지 - 단말인증시의 1회용 패스워스 사용 등	복합 보안인증 프로세스

IoT기기와 사용자 단말 간의 보안 및 인증 프로세스에 보안인증 클라우드 시스템이 도입됨으로써 IoT 기기의 보안 서비스 개발 및 실행환경 구축에 대한 부담이 경감될 수 있고, 클라우드 기반으로 인해 글로벌 서비스로의 확장이 가능하다는 점과 소스코드 위변조 및 네트워크 취약점 등에 대한 복합 보안인증 프로세스, 등록된 사용자간의 상호 인증절차, 감사기록을 위한 주요 변경이력/사용이력의 블록체인 연동보관 등이 유기적으로 결합되어 있는 모델을 설계하였다.

3.6.2 기존 플랫폼과의 차별성

국내외 스마트홈 IoT보안 플랫폼들은 ① 네트워크 보안, ② 침입/악성코드 탐지, ③ 이상징후 탐지, ④ 바이러스 백신 설치 ⑤ 정보기술(IT)영역과 운영기술(OT)영역의 통합 모니터링, ⑥ 중요정보 보호, ⑦ 데이터베이스 접근통제 및 암호화, ⑧ 인증/권한 관리, ⑨ 매체 제어 등에서 1개 또는 일부 영역을 지원하고 있으나, 본 플랫폼은 앱 인증, 사용자 인증, 모바일 기기인증 및 스마트홈 IoT 기기별 제어범위 설정 등의 복합적인 하이브리드 인증을 통하여 비정상적 접근을 차단하며, 모바일 단말의 도난/분실이나 사용자의 오조작으로 인한 사고예방까지 가능하다.

4. 결 론

제시된 클라우드 보안인증 모델은 기기의 사양과 환경 등 많은 제약으로 인해 인터넷 상에서 컴퓨터와 같은 보안수준을 구현하기 어려운 IoT기기에서의 보안성을 강화하는데 더욱 유효할 것으로 기대된다. 특히, 대기업중심으로 계열화된 스마트홈 보안 플랫폼 관리 범위에서 벗어난 중소기업들이나 해외기업들도 용이하게 활용할 수 있을 것이다.

클라우드 인증서버와의 연결을 위해서는 IoT기기 소프트웨어 모듈 내에 관련 API의 추가 또는 제어로직의 간단한 변경 만으로 보안인증 기술을 적용하는 것이 가능할 수 있으며, 향후 스마트홈 IoT기기의 보안을 위한 글로벌 클라우드 서비스 모델로의 발전을 기대한다.

또한 스마트홈 분야 이외에도 IoT 기기를 사용하는 스마트 시티, 스마트 환경, 스마트 워터, 스마트 미터링, 스마트 리테일, 물류, 산업용 제어, 스마트 팜, e-헬스 등 다양한 분야의 보안성 강화에 확대 적용할 수 있을 것이다.

다만, 빅데이터 및 인공지능을 이용한 사용자행위 분석을 통해 보다 안전한 제어와 사고예방 기능이 강화된 스마트홈 IoT기기의 보안인증 플랫폼 모델로 향상시켜야 할 과제가 남아 있으며, 많은 IoT기기들이 용이하게 적용할 수 있기 위해서는 IoT기기의 운영체제별 오픈 API 및 SW개발도구(SDK: Software Development Kit)를 개발·보급하고, 이를 수용할 수 있는 규모의 클라우드 시스템의 운용이 필요하다.

참고문헌

[1] 한국인터넷진흥원, '사물인터넷 소형 스마트 홈가전 보안 가이드[기업용]', 2016.06.
[2] Statista, Number of Smart Homes forecast in the World from 2017 to 2025(in millions), (www.statista.com)
[3] 과기정통부, "'21년 사이버위협 분석 및 '22년 전망 분석(보도자료)", 2021.12.24
[4] OWASP,"the OWASP Top 10", 2021 (https://owasp.org/Top10/)
[5] 한국인터넷진흥원, '홈가전 IoT 보안가이드', 2017.07.
[6] 강병완, "사물인터넷(IoT)디바이스의 보안평가지표체계에 관한 연구",박사논문, pp2-3, 2016.12.
[7] 최성규, "IoT 장치의 취약점 분석절차 및 점검항목 도출", 박사논문, pp5-10, 2020.02.
[8] 권기덕, "사물인터넷 서비스 자율설정 미들웨어 플랫폼", 박사논문, p7, 2016.02

[9] 한국정보통신기술협회, “사물인터넷 정의 및 참조 모델” TTAK.KO-06.0346, 2013.12.

〔저자소개〕

유 용 환 (Young-hwan Yoo)

충남대학교 물리학과 이학사
숭실대학교 정보과학대학원 정보산업학과 공학석사
전) 미래에셋(대우증권) IT센터장
전) NH투자증권 신시스템구축센터장
전) 한국스탠다드차타드증권 Head of IT
전) KTB투자증권 IT본부장
전) 국제정보보안과학기술인협동조합 이사장
전) 피노텍 기술대표이사
전) 쉬프트정보통신 기술총괄사장
현) 한국스마트휴먼테크협회 스마트시티인증센터장
현) 남서울대학교 컴퓨터소프트웨어학과 조교수

email : yhyoo6@gmail.com