Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.553

스마트 홈에서 안전한 디바이스 제어 명령을 위한 토큰 기반 사용자 동적 접근제어 기법

유 혜 선,[1†] 서 민 혜[2‡]
[1,2]덕성여자대학교 (학생, 교수)

Token-Based User Dynamic Access Control for Secure Device Commands in Smart Home

Hyeseon Yu,[1†] Minhye Seo[2‡]
[1,2]Duksung Women's University (Student, Professor)

요 약

사물인터넷 기술의 빠른 발전과 코로나19 팬데믹 이후 가정 내 활동의 증가로 인해 사용자들의 스마트 홈에 대한 수요가 크게 증가하였다. 스마트 홈 시장의 규모가 매해 빠르게 증가하고 사용자의 수가 늘어남에 따라 개인정보보호 및 각종 보안 문제에 대한 중요성도 함께 커지고 있다. 현재는 필요에 따라 한시적으로 다른 사용자들에게 스마트 홈 소유자 권한을 부여하고 시스템에 접근하도록 한다. 그러나 부여된 권한에 대한 관리가 제대로 이뤄지지 않을 경우 쉽게 악의적인 공격자의 접근을 허용할 수 있다. 또한, 스마트 홈 디바이스 및 센서를 통해 수집된 개인정보를 이용한 2차 피해의 발생 가능성에 대한 예방도 필요하다. 따라서 본 논문에서는 사용자의 편의성을 감소시키지 않으면서 스마트 홈 시스템에 대한 무분별한 접근을 방지하기 위해 접근 권한을 스마트 홈 디바이스의 기능 및 종류에 따라 세분화하여 설계하고 사용자 개인 디바이스를 활용한 토큰 기반 사용자 접근제어 기법을 제안한다.

ABSTRACT

Due to the rapid development of IoT technology and the increase in home activities after the COVID-19 pandemic, users' demand for smart homes has increased significantly. As the size of the smart home market increases every year and the number of users increases, the importance of personal information protection and various security issues is also growing. It often grants temporary users smart home owner rights and gives them access to the system. However, this can easily allow access to third parties because the authorities granted are not properly managed. In addition, it is necessary to prevent the possibility of secondary damage using personal information collected through smart home devices and sensors. Therefore, in this paper, to prevent indiscriminate access to smart home systems without reducing user convenience, access rights are subdivided and designed according to the functions and types of smart home devices, and a token-based user access control technique using personal devices is proposed.

Keywords: smart home, fine-grained access control, token-based device control

I. 서 론

우리 사회는 4차 산업 혁명의 등장 이후 IoT (Internet of Things), AI(Artificial Intelligence), 로봇 등 빠르게 성장하는 기술로 인해 초연결 사회로 나아가고 있다. 단순히 컴퓨터뿐만이 아니

Received(02. 27. 2024), Modified(1st: 04. 29. 2024, 2nd: 06. 24. 2024), Accepted(06. 24. 2024)

† 주저자, 20200876@duksung.ac.kr
‡ 교신저자, mhseo@duksung.ac.kr(Corresponding author)

라 사람과 사물까지도 연결되는 사물인터넷 시대에 접어들며 자연스레 주거 환경의 변화도 이루어졌다. 가전제품들을 연결한 IoT 시스템을 구축하고 이에 각종 센서까지 연결함으로써 우리의 주거 환경은 이제 컴퓨터가 홈과 인간을 관리하는 형태로 점차 변화하고 있다. 또한, 세계 최대 규모의 IT 가전 전시회인 CES 2023에서 초연결, 초지속 등의 키워드가 강조되며 기존의 기술과 각종 기기 간의 연결에 주목했다. 이에 따라 기존의 IoT 기술과 가전제품들이 연결된 스마트 홈 시장에 관한 관심도 더욱더 높아지고 있는 추세이다.

스마트 홈이란 IoT 기술을 기반으로 집 안의 가전, 냉난방, 보안 등 가정 내에 있는 다양한 장치들을 유·무선 네트워크로 연결하여 집안에서 수집되는 모든 정보를 모니터링 및 제어할 수 있는 기술을 의미한다. 스마트 홈 기술의 발전을 통해 가정에서의 삶의 질과 편의성을 높이고, 연결된 다양한 원격 제어 디바이스를 통해 에너지 효율을 높일 수 있었으나 정보보안 측면의 문제는 여전히 중요하게 논의되고 있다. 권한이 없는 방문자가 집안의 기기에 임의로 접근하여 정보를 조회하거나 기기를 제어하는 프라이버시 및 보안 문제는 스마트 홈에 있어 해결해야 할 중요한 문제 중 하나이다[1]. 스마트 홈은 한정된 사람이 한정된 단말만을 만지는 환경으로 사용자의 변동이 매우 적다[2]. 하나의 예로 냉난방 시스템에 문제가 발생한 경우 엔지니어에게 스마트 홈 시스템 접근 권한을 부여해야 하는 상황을 생각해 볼 수 있다. 역할 또는 개인별 상황에 따라 차등적으로 부여된 시스템 접근 권한이 부여되지 않은 경우 엔지니어와 같은 한시적 방문객에게 스마트 홈 전체 제어가 가능한 Home Owner의 권한을 부여할 수밖에 없다. 그러나 이는 불필요한 홈 제어 장치 또는 디바이스로의 접근을 허용하게 되며 권한 부여 및 철회에 대한 관리 부주의로 타인에게 스마트 홈 내의 개인정보가 불필요하게 노출될 수 있다. 또한, 공격자가 이를 통해 Home Owner 권한 계정 탈취 공격에 성공할 경우 스마트 홈 시스템 해킹, 프라이버시 침해와 같은 보안 문제가 발생할 수 있다.

따라서 본 논문에서는 스마트 홈 환경에서 사용자의 무분별한 시스템 접근 방지를 위해 토큰을 사용한 사용자 접근제어 기법을 제안한다. 제안 기법은 토큰링 기술을 차용한 토큰을 통해 사용자 인증 및 스마트 홈 디바이스 제어를 한 번에 처리함으로써 명령 전달을 위한 새로운 세션 연결이 불필요하며, 시스템 서버 접근 시 이중인증 방식을 사용함으로써 안전성을 높이고 있다. 제안 기법에서는 스마트 홈 사용자들의 접근 권한을 스마트 홈 디바이스의 종류에 따라 세분화하여 설계하고 있어 다양한 역할 및 상황에 따라 불필요한 시스템 접근을 막기 위한 최소한의 권한만을 부여할 수 있다. 접근 권한 설정의 경우 스마트 홈 소유자의 관여 없이도 권한 설정 시스템상에서 자동으로 수행되므로 소유자의 시스템 관리의 편리성을 높일 수 있다. 또한, 모든 스마트 홈 기기들과 사용자가 각각 인증을 수행하지 않고, 시스템 서버를 통해 사용자와의 인증을 수행하므로 낮은 컴퓨팅 파워와 배터리 등의 문제 해결을 기대할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 현재 스마트 홈 연동 표준으로 주목받고 있는 매터(Matter) 프로토콜과 스마트 홈 환경에서 토큰을 활용한 인증 및 제어를 수행하는 기존 연구들을 분석한다. 3장에서는 스마트 홈에서 안전한 접근제어 프로토콜이 만족해야 하는 안전성 모델이 무엇인지 설명한다. 4장에서는 제안하는 사용자의 무분별한 시스템 접근 방지를 위한 토큰 제어 기법에 대하여 설명한다. 5장에서는 제안 기법의 기능성을 설명하고 6장에서는 안전성을 분석한다. 마지막으로 7장에서 결론을 맺는다.

II. 관련 연구

2.1 Matter Protocol

최근 매터 표준이 등장함에 따라 디바이스 제조사에 상관없이 모든 플랫폼에 제품 연동이 가능해졌다. 매터는 개방형 스마트 홈 연동 표준으로 가정 내에서 이용하는 모든 스마트 디바이스 간의 연결성을 개선하기 위해 개발된 누구나 사용 가능한 IoT 프로토콜이다.

IP 프로토콜을 기반으로 동작하기 때문에 IP만 지원된다면 통신 프로토콜과 관계없이 모든 디바이스에 적용할 수 있다는 장점이 있다. 매터 표준에서는 스레드, 와이파이, 이더넷, 블루투스 등을 지원한다. 특히 스레드 프로토콜에서는 전용 허브 없이 이를 지원하는 모든 스마트 홈 기기를 연결하여 사용할 수 있으며 데이터를 안전하게 암호화하고 안정적인 사용이 가능하다.

모든 매터 지원 디바이스는 고유한 인식자(identifier)를 가지고 동작한다. 그리고 디바이스

유형 및 제조사 브랜드를 확인하는 인증서를 이용해서 동작한다. 인증서 관리를 위해 PKI 혹은 공개키 인프라에 의존하고 인증서 데이터는 enclave인 별도의 칩에 안전하게 저장된다. 그 외에 세션 연결(대칭키 암호 사용)을 통해 통신을 수행한다.

매터 표준은 역할기반 접근 제어(role-based access control) 방식을 사용하여 사용자에게 특정 역할을 부여하고, 그 역할에 따라 각각의 장치에 대한 접근 권한을 제한할 수 있다. 그러나 스마트 홈과 같이 사용자의 상황이나 환경이 빈번하게 변하는 환경에서 역할기반 접근제어 기법만으로는 상황적 조건을 충분히 반영하기 어렵다. 또한, 역할을 설정하고 관리하는 과정이 복잡해질 수 있으며, 환경이 변화하거나 새로운 장치 또는 사용자가 추가될 때마다 역할과 권한 설정을 업데이트해야 하므로 부담이 될 수 있다. 그 외에도 매터 표준은 다양한 플랫폼 간의 상호 운용성을 촉진하기 위해 제안되었지만, 다양한 디바이스들의 모든 기능을 지원하지 않는다. 따라서 특정 기능을 사용해야 하는 경우 별도의 플랫폼을 사용해야 할 수 있다. 또한, 매터 표준을 준수하는 스마트 홈 디바이스들은 지원되는 기능에 따라 다양성이 제한될 수 있다. 매터 표준은 다양한 이기종 디바이스 간의 상호 운용성을 개선하는 데 있어 중요한 역할을 하지만, 모든 기능을 완벽하게 지원하는 것은 아니므로 여전히 사용자는 특정 브랜드나 모델을 선택해야 한다는 한계를 가진다.

이와 달리 본 연구에서는 상황인식 기반 접근제어(context-aware access control) 기법과 역할기반 접근제어 기법을 결합하여 사용자 동적 접근제어가 가능하도록 설계되어 있어 상황 정보에 따라 일반 사용자의 역할과 접근 범위가 자동으로 설정된다. 이에 따라 Home Owner의 수동적인 관리가 불필요하고, 공격자가 일반 사용자의 계정을 취득하였을 때 접근 권한의 임의 변경이 불가하다. 그리고 상황 정보에 따라 접근 가능 시간이 설정되므로 일정 시간 이후에는 스마트 홈 시스템에 접근이 불가하다는 장점이 있다. 또한, 토큰의 데이터 필드에 개별적으로 명령을 전달함으로써 다양한 스마트 홈 디바이스들이 지원하는 기능들을 제한하지 않고 사용할 수 있다. 이는 매터 표준의 한계를 보완하고 사용자에게 더 나은 선택의 폭을 제공할 수 있다. 따라서 본 연구를 통해 스마트 홈 환경의 다양성과 유동성을 더 잘 반영하고, 더욱 세밀하고 유연한 접근제어 정책이 구현 가능할 것이며 사용자 경험을 개선하는 데 중요한 역할을 할 것으로 기대된다.

2.2 토큰 기반 접근제어

토큰을 기반으로 인증을 수행한 기존 논문들의 경우 주로 짧은 액세스 토큰을 통해 특정 사용자의 인증을 수행한다. 액세스 토큰 발급을 위해서 우선으로는 사용자 인증이 수행되어야 하고, 발급받은 액세스 토큰의 인증 이후에 디바이스 제어 명령 등의 시스템 접근 및 제어가 가능하다.

T.A. Khoa et al.은 Firebase, Google 가상 서버 등과 같은 서비스 대신 개인 서버 시스템을 구축하여 사용한다. 사용자 인증이 완료되면 개별 인증 토큰이 부여되고 JSON 패킷에 사용자 ID, 인증 토큰, 스마트 홈 디바이스, 제어 명령 메시지를 담아 통신한다. 해당 연구에서 주장한 바와 같이 서버 리소스를 다른 사용자와 공유할 필요가 없고, 개인의 필요에 따라 시스템을 설정할 수 있다는 점 등의 다양한 장점이 있으나 일반 사용자들이 직접 자택 내 서버 게이트웨이를 구축하여 사용하는 것에는 한계가 있다[3].

K. Yang et al.은 사용자의 신뢰도를 기반으로 실시간으로 액세스 토큰과 액세스 권한이 변경되는 동적 접근제어 메커니즘을 설계하였다. 이를 통해 기존 연구들보다 정교하고 안전한 동적 액세스 제어 조정이 가능함을 보여줬으나 단기 토큰의 유효성 판단에 대한 고려는 이뤄지지 않았다는 한계가 있다. 따라서 해당 연구에서 사용자의 신뢰 동적 평가를 기반으로 블록체인 스마트 계약을 사용하여 액세스 단기 토큰의 유효성을 자동으로 결정하는 프로세스를 만드는 것을 향후 목표로 한다[4].

S. Ameer et al.은 역할기반 방식과 속성기반 접근제어 방식을 결합하여 하이브리드 액세스 제어 모델을 제안한다. 또한, 짧은 액세스 토큰을 사용하여 사용자 인증을 수행하도록 하였다. 해당 연구에서는 접근제어 기법에 관한 연구만 진행되어 디바이스 명령 제어에 대한 부분은 고려되지 않았다[5].

이외에도 데이터 자체에 대한 보안과 더불어 개인정보 침해 및 데이터 변조에 대한 보안을 위하여 IoT 환경에 블록체인을 통합한 기술이 연구되고 있다. 블록체인이 통합되면 분산 원장 기술이 적용되고 이를 통해 토큰 기반의 접근제어 수행이 가능하다.

N. Tapas et al.은 기존의 IoT-Cloud 솔루션에 대한 개선을 위해 리소스 액세스 권한 부여 및 위

임 의무 메커니즘을 블록체인에서 수행하도록 하고 사용자의 신뢰 판단을 배포된 스마트 컨트랙트로 이동한 분산형 설계 형태를 제안하였다. 그러나 본 연구에서는 개인정보보호에 대한 부분은 고려하지 않았다는 한계가 있다[6].

Y. Liu et al.은 컨소시엄 블록체인 네트워크와 분산 식별자를 활용하여 각각의 사용자가 다양한 ID 관계에 대한 DID와 액세스 권한 부여를 위한 자격 증명을 관리할 수 있도록 설계하였다. 그러나 본 연구는 각각의 스마트 홈 디바이스 및 센서의 자격 증명에 액세스하고 확인하는 과정이 필요하며 프로토타입을 제안한 것으로 실생활의 서비스에 적용하기에는 확장성이 떨어진다는 한계가 있다[7].

A. Mukherjee et al.은 공통 IoT Hub와 블록체인의 스마트 컨트랙트를 사용하여 경량화되고 분산화된 보안과 개인정보보호를 제공한다. 해당 연구에서는 허브의 메모리에 액세스 토큰을 모두 캐싱하여 인증된 장치에 대한 중복 인증을 방지한다. 그러나 캐싱된 토큰을 안전하게 저장하는 방식에 대한 고려가 이뤄지지 않았다는 한계가 있다[8].

앞선 기존의 연구들과 달리 본 연구에서는 토큰을 명령을 전달하기 위한 캐리어의 역할과 더불어 권한 정보를 담아 특정 사용자의 인증과 접근제어를 다루는 용도로 사용한다. 토큰 상에 제어 명령을 담아 통신을 하게 되면 사용자 인증 이후 스마트 홈 디바이스 명령 전달을 위한 또 다른 세션을 생성하지 않아도 되므로 보다 효율적이다. 또한, 블록체인 기반의 플랫폼에서의 모든 거래에는 수수료가 부과되며 거래가 블록체인에서 승인되는 데에는 시간이 소요되므로 처리 시간에 영향을 미치는 점 등 실제 실생활에 적용되는데 제한되는 기술적 특징들이 있다. 따라서 본 연구에서는 블록체인 기술을 사용하지 않으면서 토큰 상에 스마트 홈 디바이스 제어 명령을 담아 통신을 수행하는 방식을 제안한다.

III. 안전성 모델

본 장에서는 스마트 홈에서 안전한 접근제어 프로토콜이 만족해야 하는 보안 목표와 공격자 유형별 공격자에게 허용된 공격의 행위를 중심으로 설명한다.

3.1 보안 목표

본 연구에서 제안하는 프로토콜은 다음과 같은 보안 목표를 가진다.

- **비인가된 인증 방지**
  시스템은 비인가된 인증 시도를 자동으로 감지하고 차단하여, 외부 및 내부 공격자로부터의 위협으로부터 보호한다.
- **접근 권한 및 등급의 변경 통제**
  사용자의 접근 권한 및 등급 변경을 통제하여, 무분별한 권한 변경이나 상승을 방지한다.
- **프라이버시 보호**
  데이터 암호화, 접근제어 등의 데이터 처리 방식을 통해 스마트 홈 서비스를 이용하는 모든 사용자의 개인정보 및 민감 정보를 보호한다.
- **추적 불가능성**
  스마트 홈 디바이스 및 센서 제어 시 세션 키, RC(Revision Counter) 값 등의 매개변수를 사용함으로써 공격자가 사용자의 통신을 추적할 수 없도록 보호한다.

3.2 공격자의 행위

공격을 수행하는 공격자는 외부 공격자 또는 내부자(Home Owner 이외의 사용자)로 구분된다. 먼저, 외부 공격자는 스마트 홈 시스템이나 네트워크에 직접적으로 속하지 않은 사람들을 말하며, 이들은 주로 개인정보의 도난, 재산 침해, 또는 불법 침입 등의 비인가 접근과 제어를 목표로 한다. 내부 공격자는 스마트 홈 시스템이나 네트워크에 이미 접근 권한을 가지고 있는 사람들을 말한다. 이들은 일반적으로 가정 구성원, 친구, 또는 시스템에 접속할 수 있는 기타 인물이 될 수 있으며 악의적으로 시스템의 설정을 변경하여 보안 취약점을 만들거나 시스템의 정상적인 기능을 방해할 수 있다.

- **재생 공격(replay attack)**

재생 공격은 공격자가 네트워크 통신에서 이미 전송된 메시지 또는 데이터를 재전송하여 공격을 수행하는 것을 말한다. 공격자는 해당 공격을 통해 사용자의 개인정보를 탈취하거나 시스템 제어를 목표로 한다.

외부 공격자는 공격 표적의 스마트 홈 네트워크를 감시하고 유효한 통신 세션에서 데이터 패킷을 가로채 데이터를 변조하거나 그대로 재전송하여 공격자가

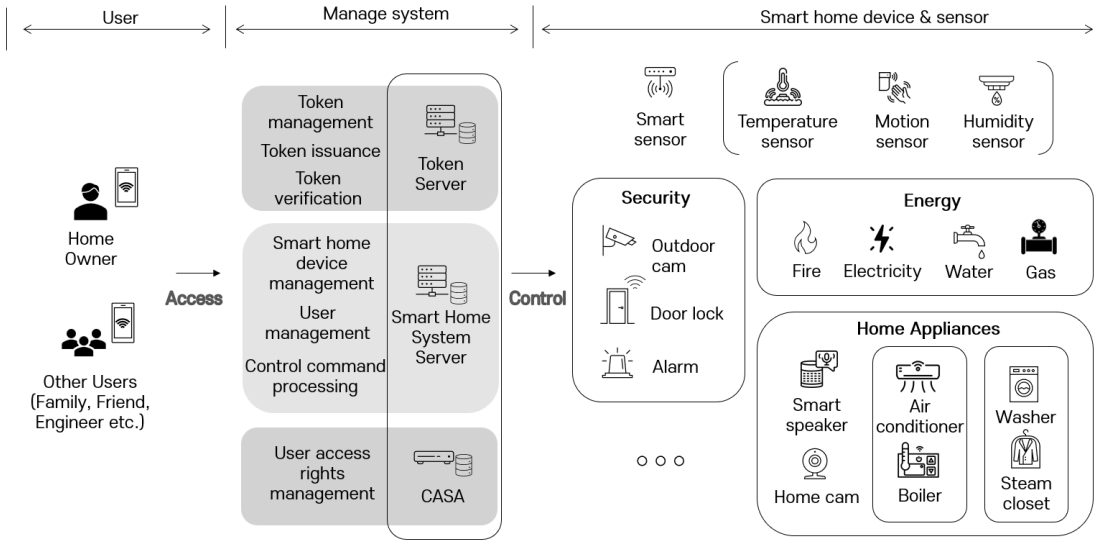

Fig. 1. System Architecture

원하는 동작을 수행하도록 할 수 있다. 예를 들어, 공격자가 스마트 잠금장치의 열쇠 신호를 가로채고 재전송하여 성공하면 무단으로 집에 침입할 수 있다.

▪ 액세스 권한 변경

액세스 권한 변경 공격은 공격자가 스마트 홈 시스템 내에서 사용자의 권한을 변경하여 부정한 액세스를 얻거나 시스템을 제어하는 것을 말한다. 공격자는 해당 공격을 통해 사용자의 개인정보 유출, 시스템 무단 액세스를 통한 물리적 위협 등이 가능하다.

외부 공격자가 특정 사용자의 토큰을 탈취했다 가정하자. 이때 공격자는 모든 스마트 홈 디바이스 및 센서에 접근할 수 있도록 접근 권한을 변경하거나 해당 사용자가 더는 시스템에 액세스할 수 없도록 접근 권한을 조작할 수 있다. 내부 공격자는 CASA(Context-Aware Service Agent)에 의해 스마트 홈 시스템 내에서 사용자 자신에게 부여된 접근 권한을 모든 스마트 홈 디바이스 및 센서에 접근할 수 있도록 변경할 수 있다. 예를 들어, 스마트 홈 시스템에 접속하여 내부 혹은 외부 공격자가 사용자의 권한을 상승시키면, 스마트 홈 내의 모든 디바이스를 제어할 수 있게 된다. 이를 통해 공격자는 보안 카메라를 조작하여 사용자의 사생활을 침해할 수 있다. 반대로 스마트 홈 소유자와 같이 특정 사용자의 권한을 감소시키면, 스마트 홈 디바이스에 접근 불가능하고 공격자는 보안 시스템의 비활성화 명령을 전송하여 시스템을 무력화시키거나 사용자의 편의를 저해시킬 수 있다.

▪ 수정 공격(manipulation attack)

수정 공격은 공격자가 스마트 홈 시스템의 데이터를 조작하거나 변경하여 원하지 않는 동작을 유발하는 공격을 말한다. 공격자는 해당 공격을 통해 시스템의 데이터 무결성을 침해하고, 사용자의 편의성을 저하하는 것을 목표로 한다.

외부 공격자가 사용자의 토큰을 탈취하였다면, 토큰의 데이터 필드에는 명령 값에 대한 암호화 처리가 되어 있지 않으므로 원하는 명령으로 이를 수정하여 공격자가 원하는 동작을 수행하도록 유도할 수 있다. 이를 통해 조작된 명령 또는 데이터로 인한 시스템 오류가 유발될 수 있고, 원하지 않은 동작을 수행하도록 할 수 있다. 예를 들어, 만약 공격이 성공한다면 가짜 보안 경고를 생성하여 사용자를 속일 수 있고, 잘못된 명령을 전달함으로써 디바이스의 동작을 변경할 수 있다.

▪ 중간자 공격(man-in-the-middle attack)

중간자 공격은 공격자가 통신하는 두 사이의 중간에 위치하여 데이터를 가로채고 조작하는 공격을 말한다. 공격자는 해당 공격을 통해 개인정보 유출, 금전적 손실 등을 목표로 한다.

외부 공격자는 통신하는 두 개체 사이에 위치하고 네트워크 트래픽을 가로채 사용자의 중요한 정보를 추출하고 조작하여 원래의 목적과 다른 동작을 유도할 수 있다. 공격이 성공적으로 수행되었다면 조명, 난방 등 스마트 홈 디바이스 또는 센서 등의 제어를 위조하여 사용자의 편의를 저하하거나 시스템을 방해할 수 있다.

- **위장 공격(spoofing attack)**

위장 공격은 공격자가 자신의 신원을 가장하여 시스템에 접근하거나 통신하는 것을 말한다. 공격자는 해당 공격을 통해 부정한 액세스를 획득하는 것을 목표로 한다.

외부 공격자는 토큰 값을 직접 생성하여 부정한 액세스를 획득할 수 있다. 정상적으로 토큰을 생성하였다면 공격자는 해당 토큰을 통해 스마트 홈 시스템에 접근 가능하며 이를 통해 개인정보를 탈취하고 보안 시스템을 무력화시켜 2차 범죄를 일으킬 가능성 또한 배제할 수 없다. 이외에도 내부 공격자는 본인에게 인가된 접근 권한을 이용하여 스마트 홈 시스템 내에서 접근 가능한 디바이스 혹은 센서의 설정을 악의적으로 변경할 수 있으며, 개인정보 또는 사용 패턴 등과 같은 민감한 정보를 외부로 유출할 수 있다.

IV. 제안 기법

본 논문에서는 일반 사용자의 각 단말은 기존에 발급받은 토큰을 사용함으로써 반복적인 인증 단계 및 접근제어 단계를 최소화할 수 있다. 제안하는 프로토콜의 설명에 앞서 사용자는 스마트 홈 구축에 필요한 애플리케이션을 사용하기 위해 스마트폰과 같은 개인 단말을 소유하고 있고, 스마트 홈 시스템 서버에 인증에 필요한 ID/PW 및 생체정보 등의 등록과정을 사전에 진행하였음을 가정한다.

Fig. 1.은 제안 시스템 구성도이다. 각 단계의 프로토콜 절차 설명은 Table 1.을 따른다.

Table 1. Description

Notation	Description
U_i	The i-th user
O	Home Owner
TS	Token Server
SS	Smart Home System Server
CASA	Context-Aware Service Agent
SD_j	The j-th Smart Home Device
PID_i	Pseudo identity of U_i
AI	Access information (Guest, Friend, Engineer etc.)
pi	Permission Information
RC	Initial Revision Counter value
r_i	Random number(Revision Counter Increasing value)
N_i	Nonce of Token Server per U_i
d(·)	Bio-information comparison algorithm
τ	Maximum allowable error rate
Bio	Bio-information(face information)
B_i	Facial feature values
E(·)	Symmetric encryption algorithm
D(·)	Signature verification algorithm
Sig(·)	Signature algorithm
pk	Public key
sk	Private key
HMAC(·)	Hash message authentication code algorithm
K	Hash key
H(·)	Hash algorithm
SK_i	The session key between U_i and SS
SK_j	The session key between SD_j and SS
$SK_{ts-(entity)}$	The session key between TS and entity(CASA, SS, U_i)

4.1 디바이스 등록 단계

일반 사용자들이 스마트 홈 시스템에 접근하기 위해서는 사용하고자 하는 개인 단말 등록이 필요하다. 일반 사용자는 스마트 홈 시스템 서버에 사용자 등록 과정을 사전에 진행한다. 사용자 등록은 SSL/TLS와 같이 안전한 채널을 통해 진행되며 이 과정에서 클라이언트와 서버 간의 공유키(세션 키)를 공유하

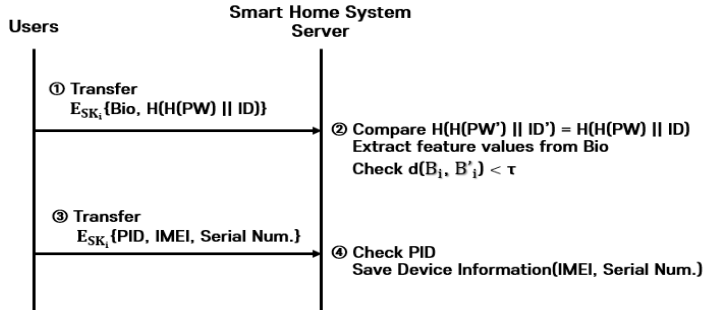

Fig. 2. Device Registration

고, 일반 사용자는 스마트 홈 시스템 서버로부터 통신에 사용할 사용자 가상 식별 정보인 PID를 발급받는다. 이후 단계별 통신은 하나의 세션이 종료될 때마다 새롭게 생성된 공유키(세션 키)를 이용하여 암호화된 상태로 진행된다. 디바이스 등록 단계는 Fig. 2.와 같이 4단계로 동작한다.

① 일반 사용자는 사용자 등록 시 사용했던 ID/PW와 생체 정보(Bio)를 입력하여 스마트 홈 시스템 서버에 접근한다.

$$U_i \rightarrow \text{SS: } E_{SK_i}(Bio, H(H(PW) \| ID))$$

② 사용자로부터 식별 정보를 전달받은 스마트 홈 시스템 서버는 사용자 DB에 저장된 정보와 비교한다. 사용자 DB에는 ID/PW는 각각 ID, H(PW) 형태로 저장되어 있고 생체정보로부터 추출된 특징값은 B_i로 저장되어 있다.

사용자 인증은 ID/PW 값을 먼저 비교하고 이의 결과에 따라 생체정보를 이용하여 마지막 인증을 진행하게 된다. 생체정보로는 지문, 홍채, 얼굴 등이 있지만 본 논문에서는 얼굴 정보를 활용한다. 사용자 등록과정에서 저장했던 얼굴 정보는 [11]에서 제안한 Face recognition 알고리즘을 사용하여 얼굴 정보에 대한 특징값을 사용자 DB에 저장한다. 사용자의 로그인 요청이 들어오는 경우 새롭게 입력받은 얼굴 정보에 대한 특징값을 추출하고 이를 사용자 DB에 저장된 특징값과 비교하여 정상적인 사용자인지 판단한다.

$$\text{SS: } H(H(PW') \| ID') \stackrel{?}{=} H(H(PW) \| ID)$$
$$\text{Extract feature values from Bio}$$
$$d(B_i, B'_i) < \tau$$

③ 일반 사용자는 사용할 개인 단말 정보를 스마트 홈 시스템 서버에게 전달한다. 개인 단말 정보는 총 2가지로 스마트폰과 같은 이동성을 가진 스마트 단말에 부여되는 IMEI(International Mobile Equipment Identity)와 단말 고유 번호인 시리얼 번호(serial number)를 사용한다. 이때 사용자 등록과정에서 스마트 홈 시스템 서버로부터 전달받은 사용자 가상 식별 정보인 PID를 함께 전송한다.

$$U_i \rightarrow \text{SS: } E_{SK_i}(PID, IMEI, Serial Num.)$$

④ 스마트 홈 시스템 서버는 먼저 PID를 확인한다. 사용자 DB에 해당 PID의 정보가 존재하는 경우, 전달받은 디바이스 정보(IMEI, Serial Num.)를 사용자 DB에 저장하며 개인 단말 정보를 등록한다.

4.2 토큰 발급 단계

4.2.1 액세스 권한 설정

토큰 발급을 위해서는 해당 사용자의 액세스 권한 선정이 필요하다. 본 논문에서 사용할 접근제어 기술은 [1]을 따른다. 이 기법에서는 스마트 홈 소유자의 관여 없이 스마트 홈 내/외의 다양한 센서와 디바이스를 통해 수집된 사용자의 상황 정보에 따라 실시간으로 사용자의 역할을 자동으로 설정한다. 상황인식 기반 접근제어 기법과 역할기반 접근제어 기법을 결합한 것으로 사용자 동적 접근제어가 가능하도록 설계되었다.

일반 사용자가 스마트 홈 시스템에 접근하고자 하는 경우 CASA는 해당 사용자의 수집된 상황 정보

를 판별하게 된다. 그 후 사용자의 권한 정보와 세부적인 서비스 접근 범위는 사전에 정의된 정책에 따라 설정된다. 이때 세부적인 서비스 접근 범위는 일반적인 역할기반 접근제어 방식처럼 생활 가전, 주방 가전, 보안, 에너지, 헬스, 자녀안심 등 스마트 홈 디바이스의 그룹에 따라 사전에 정해져 있는 것이 아닌 접근 요청하는 사용자의 상황 정보에 따라 동적으로 역할이 설정된다[1]. 일반 사용자의 스마트 홈 시스템 접근 권한과 세부적인 서비스 접근 범위는 CASA에 의해 결정되나 스마트 홈 소유자에 의해 수정되거나 추가 또는 삭제될 수 있다.

사용자의 동적 접근제어를 위해 사용자 정보, 역할 정보, 스마트 홈 서비스 접근을 요청하는 사용자의 현재 위치 정보, 스마트 홈 정보 접근 시간 정보, 스마트 홈 서비스 접근 빈도수의 총 5가지 정보를 확인한다.

우선 첫 번째로 사용자의 신원 확인을 위해 로그인 단계를 거치며 ID/PW 정보를 확인한다. 그 후 스마트 홈 접근 범위를 제한하기 위해 서비스 요청을 보낸 사용자 개인 디바이스의 현재 위치 정보를 확인한다. 세 번째 항목인 Role Group은 사용자의 접근 권한을 판별하기 위해 미리 역할 그룹을 정의해둔 것으로 기본적으로는 Home Owner, Friend, Engineer 등이 있다. Home Owner는 스마트 홈 시스템의 모든 제어가 가능하며, Friend는 부분 제어가 가능하고, Engineer는 점검 또는 수리가 필요한 디바이스, 센서의 그룹만 제어할 수 있다. 이외에도 세분화된 역할 그룹을 추가할 수 있으며, 접근 권한에 따라 서비스 접근 범위와 시스템 접근 허용 시간에 차이가 있다. 허가된 사용자의 액세스 시간과 액세스 빈도수는 세 번째 항목인 Role Group의 판단 근거가 된다. 사용자의 역할 판별을 위해 이를 수식화하여 표현하면 다음과 같다.

$$Familiar = \text{if}(\text{Pr}evious\ Role\ of\ Access\ User = Home\ Owner \parallel Friend \parallel Enginner \parallel Other) + Access\ Count\ of\ Access\ User(case : access\ count \geq 5)$$

$$User\ Role : Case\ User\ Familiar, \text{if}\ Access\ Device\ Location = In\ Smart\_Home\ then\ Assign\ Upper\ Role\ Calss\ else\ Access\ Device\ Location = In\ Out\ Smart\_Home\ then\ Assign\ \text{Pr}evious\ Role$$

$$User\ Accessible\ Time = Access\ Device\ Location[In\ Smart\_Home \parallel Out\ Smart\_Home](weight)* Access\ Time(immediate\ value) + Access\ Count$$

이처럼 [1]에서 제안한 접근제어 기법을 통해 사용자별 스마트 홈 시스템 접근 권한을 설정할 수 있다. 그러나 본 논문에서 제안하는 토큰에 시스템 접근 권한을 명시하기 위해 이를 bit string 형태의 접근 등급으로 변환하여 사용하고자 한다. 접근 권한 AI(Access Information)의 접근 등급 pi(Permission Information)의 변환 과정은 다음과 같다.

다양한 스마트 홈 디바이스 및 센서가 n개의 그룹으로 나뉜다고 할 때, pi의 길이가 m-bit라고 하자. 그룹 수 n의 크기가 커지기 위해서는 매우 세분화된 그룹화가 필요하며, 세분될수록 하나의 그룹에 속하는 디바이스 및 센서의 수는 1에 가까워진다. 그러나 세분화된 정도가 지나칠수록 그룹이라는 의미가 사라지고 개별 디바이스 및 센서가 되므로 n의 범위는 $0 < n \leq 20$로 제한한다.

$n < m$라 가정할 때, 하나의 그룹의 접근 권한 표기를 위해 사용되는 bit 수는 (m/n)이다. 이때, (m/n)의 값이 정수가 아닌 경우에는 나머지를 제외한 몫의 값에 해당하는 수로 사용하며 접근 권한 표기 후 남은 bit가 발생하는 경우 0으로 채워 m-bit를 만족하도록 구성한다. 권한이 부여된 그룹의 (m/n)개의 bit는 랜덤으로 생성되며, 권한이 없는 그룹인 경우에만 모두 0으로 표기된다.

일반 사용자 A와 B의 AI가 같을 때, pi가 같을 확률을 계산해보자. n = 5, m = 256일 때, 두 사용자가 모든 그룹에 접근 권한이 있다고 가정하자. 하나의 그룹이 가지는 비트 수를 계산해보면 $m/n = \frac{256}{5} = 51.2$이므로 각각의 스마트 홈 디바이스 및 센서 그룹은 51 bits의 길이를 가진다. 그룹별 51-bit는 랜덤한 비트열로 생성되며 총 256-bit에서 (51×5)-bit를 제외한 값인 1bit는 0으로 채워 pi를 결정하게 된다.

두 사용자의 pi가 같을 확률을 계산해보면 다음과 같다. 각 그룹은 51-bit를 랜덤하게 가지므로 하나의 그룹이 같을 확률은 $\frac{1}{2^{51}}$이다. pi가 같을 확률은 $\frac{(pi\text{가 같은 경우의 수})}{(\text{전체 경우의 수})} = \frac{1}{(2^{(m/n\text{의몫})})^n}$로 값을

대입하여 계산하면 $\frac{1}{(2^{51})^5} = \frac{1}{2^{255}}$이다. 이를 통해 n의 범위가 $0 < n \leq 20$일 때, m의 값이 충분히 크다면 두 사용자의 pi가 같을 확률은 0에 수렴함을 알 수 있다. 따라서 일반 사용자 A와 B의 AI가 동일한 경우 pi가 같을 확률은 현저히 낮다.

4.2.2 토큰 발급

본 논문에서 제안하는 토큰은 [2]에서 제안한 토큰을 기반으로 설계하였다. 두 토큰의 차이점은 인증 필드에 사용자의 스마트 홈 시스템에 접근할 수 있는 접근 권한 등급과 토큰의 유효기간을 명시하였다는 것이다. 또한, 제안하는 토큰의 경우 토큰 서버를 통해 발급되는 반면 [2]에서 제안한 토큰은 사용자의 개인 디바이스에서 직접 토큰을 생성하여 사용한다. 본 논문에서는 스마트 홈 소유자가 일반 사용자들의 시스템 접근 권한과 토큰을 통합 관리할 수 있도록 토큰의 구조를 변경하였다.

토큰은 인증 필드와 데이터 필드로 구성되어 있다. 인증 필드(auth field)는 정당한 사용자의 토큰인지 검증하기 위한 정보를 담은 필드이고, 데이터 필드(data field)는 스마트 홈 디바이스 제어 명령 또는 그에 따른 결과를 담은 필드이다. 토큰의 인증 필드의 구조는 Table 2.와 같다. 토큰은 토큰 서버를 통해 발급 및 관리되며, 일반 사용자의 개인 단말은 발급된 토큰을 통해 스마트 홈 시스템 제어가 가능하다.

Table 2. Token Auth Field structure

Filed	Description
TokenNumber	Unique serial number of the token
PID	Pseudo identity of Ui
HMAC(K, IMEI⊕Serial Num.)	Hash message authentication code with IMEI and serial number
RC	Revision Counter value
H(pi⊕N_i)	Hash values for XOR operations of pi and N_i
Expiry Date	The validity period of the token

일반 사용자가 스마트 홈 시스템에 접근하려고 할 때 토큰을 발급받은 적이 없거나 혹은 기존에 발급받았던 토큰의 사용 가능 기한이 만료되었을 경우 토큰을 발급받게 된다. 토큰 발급은 Fig. 3.과 같이 4단계로 동작한다.

① 일반 사용자는 토큰 발급 요청을 보낸다. 해당 패킷은 사용자 가상 식별 정보(PID)와 RC 값의 증가량을 나타내는 난수 r_i를 세션 키 SK_i로 암호화하여 전송한다. 토큰 서버는 스마트 홈 시스템 서버에게 PID의 유무를 확인하고 결과(exist 또는 non-exist)를 확인한다. 만약 결괏값이 exist인 경우, 토큰 서버는 사용자에게 해시 키 K를 발급한다. 해시 키 K는 데이터의 무결성과

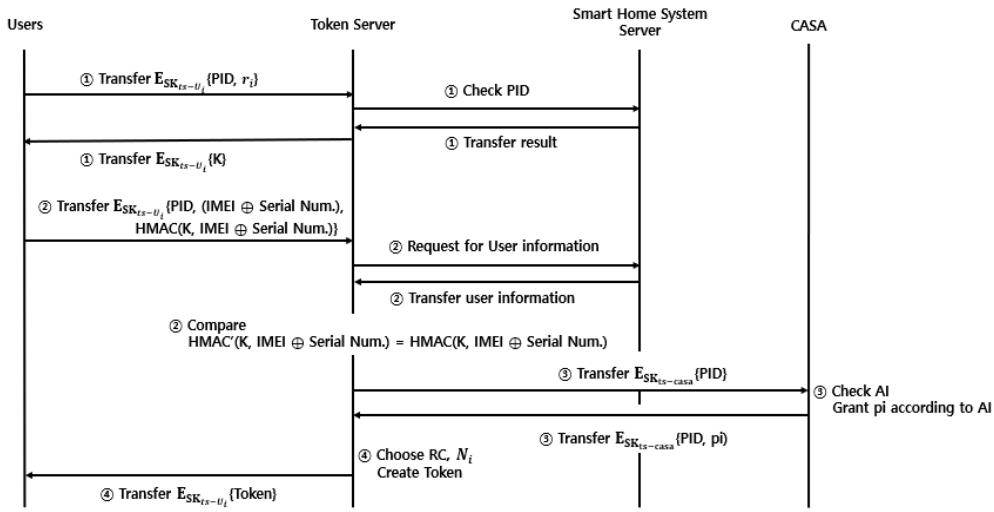

Fig. 3. Issuing token

통신의 주체인 사용자가 인증된 개체임을 알리는 목적으로 사용한다.

$U_i \rightarrow$ TS: $E_{SK_{ts-U_i}}(PID, r_i)$
TS $\leftrightarrow$ SS: Check PID
TS $\rightarrow U_i$: $E_{SK_{ts-U_i}}(K)$

② 사용자는 자신의 단말 정보를 XOR 연산한 후 해시 키 K를 사용하여 HMAC(Hash Message Authentication Code) 값을 생성한다. HAMC 값과 단말 정보, PID값을 세션 키 SK_i로 암호화하여 토큰 서버에게 전송한다. 사용자로부터 토큰 발급 요청을 받은 토큰 서버는 스마트 홈 시스템 서버의 사용자 데이터베이스에서 PID에 해당하는 단말 정보(IMEI, SerialNum.)를 받아 HMAC 값을 비교한다.

$U_i \rightarrow$ TS:
$E_{SK_{ts-U_i}}(PID, (IMEI \oplus SerialNum.),$
$HMAC(K, IMEI \oplus SerialNum.))$
TS:
$HMAC'(K, IMEI \oplus SerialNum.)$
$\quad ? = HMAC(K, IMEI \oplus SerialNum.)$

③ 사용자의 단말 정보가 일치하는 경우 토큰 서버는 토큰 생성에 필요한 값인 사용자의 권한 등급(pi)을 얻기 위해 상황인식 서비스 에이전트(CASA)에게 PID를 세션 키 $SK_{ts-casa}$로 암호화하여 보낸다. CASA에서는 PID에 해당하는 사용자 역할에 따른 권한 정보(AI)를 판단하고 이에 따른 권한 등급(pi)으로 변환하여 자신의 데이터베이스에 저장한 후 토큰 서버에게 PID와 pi를 전송한다.

TS $\leftrightarrow$ CASA: $E_{SK_{ts-casa}}(PID)$
$E_{SK_{ts-casa}}(PID, pi)$

④ 이를 확인한 토큰 서버는 초기 Revision Counter 값으로 사용할 랜덤한 RC 값과 공격자가 사용자의 pi를 확인하여 악용할 수 없도록 안전성을 높이기 위해 연산에 사용될 난수 N_i를 선택한다. 토큰 서버는 Table 2.의 모든 값을 채워 토큰을 생성한 후 사용자에게 전송한다.

TS $\rightarrow U_i$: $E_{SK_{ts-U_i}}(Token)$

4.3 디바이스 제어 단계

4.3.1 토큰 검증

토큰 관련 정보는 모두 토큰 서버가 관리하는 데이터베이스에 저장되어 있다. 그러므로 토큰 검증을 위해서는 스마트 홈 시스템 서버와 토큰 서버의 통신이 이루어져야 한다. 토큰 검증은 Fig. 4.와 같이 5

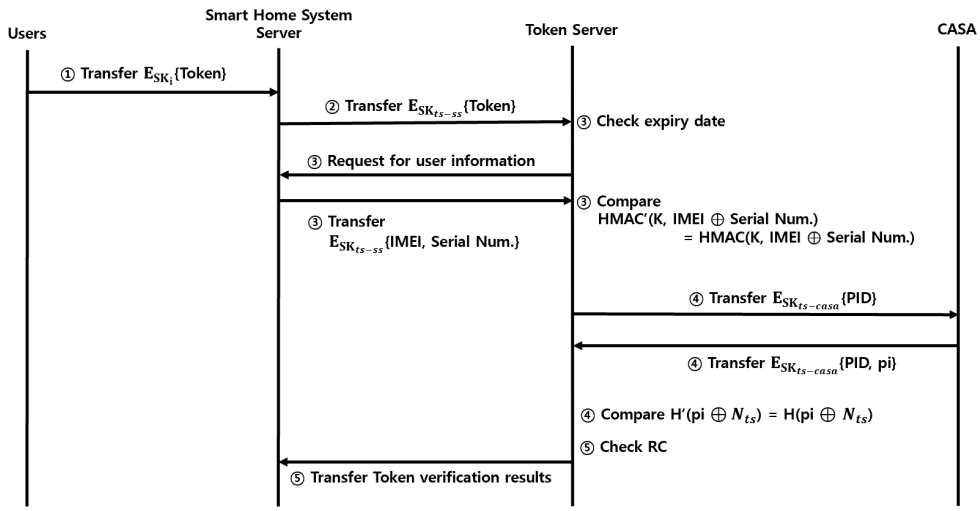

Fig. 4. Token Validation

단계로 동작한다.

① 일반 사용자는 토큰의 데이터 필드에 명령을 담아 스마트 홈 시스템 서버에게 디바이스 제어 요청을 보낸다. 요청 패킷에는 토큰 담아 전송한다.

$U_i \rightarrow$ SS: $E_{SK_i}(Token)$

② 요청을 받은 스마트 홈 시스템 서버는 토큰의 인증 필드에 있는 값 중 PID가 자신의 사용자 데이터베이스에 있는지와 해당 사용자에게 발급한 토큰 번호가 맞는지 확인한다. 일치하는 경우 사용자의 PID와 토큰을 토큰 서버에게 전달하고 그렇지 않으면 세션을 종료한다.

SS $\rightarrow$ TS: $E_{SK_{ts-ss}}(Token)$

③ 토큰 서버는 우선 토큰의 인증 필드에 있는 만료기한을 먼저 확인하여 아직 유효한 토큰인지 폐기해야 할 토큰인지 판별한다. 유효한 토큰이면 토큰 서버는 스마트 홈 시스템 서버에게 사용자 정보를 요청하고, 아닌 경우 Deny 메시지를 보낸다.

TS: Check Expiry Date
TS $\leftrightarrow$ SS: Request for IMEI, SerialNum.
$E_{SK_{ts-ss}}(IMEI, Serial Num.)$

스마트 홈 시스템 서버는 사용자 DB에서 PID의 단말 정보를 전달하고 토큰 서버는 이를 비교하는 과정을 수행한다. 값이 일치하는 경우 다음 과정으로 넘어가고 아닌 경우 스마트 홈 시스템 서버에게 Deny 메시지를 전달한다.

TS:
$HMAC'(K, IMEI \oplus Serial Num.)$
$\quad ? = HMAC(K, IMEI \oplus Serial Num.)$

④ 상황인식 서비스 에이전트(CASA)에게 사용자 PID를 공유키(세션 키)로 암호화하여 전송하면 같은 키로 CASA는 이를 복호화하여 자신의 데이터베이스에 해당 PID가 존재하는지 먼저 확인한다. 해당 값이 존재하면 그에 해당하는 접근 권한 등급(pi)을 토큰 서버에게 전송한다.

TS $\leftrightarrow$ CASA: $E_{SK_{ts-casa}}(PID)$
$E_{SK_{ts-casa}}(PID, pi)$

토큰 서버는 상황인식 서비스 에이전트(CASA)에게 전달받은 pi 값과 자신의 데이터베이스에 저장되어 있던 난수 N_i를 통해 토큰의 인증 필드에 있는 값과 비교한다.

TS: $H'(pi \oplus N_i) ? = H(pi \oplus N_i)$

⑤ 이전 제어 요청 시 확인했던 토큰의 RC 값에 정확히 r_i만큼 변화하였는지 확인하여 통과한 경우 토큰 검증이 완료된다.

TS: $RC' ? = RC + r_i$

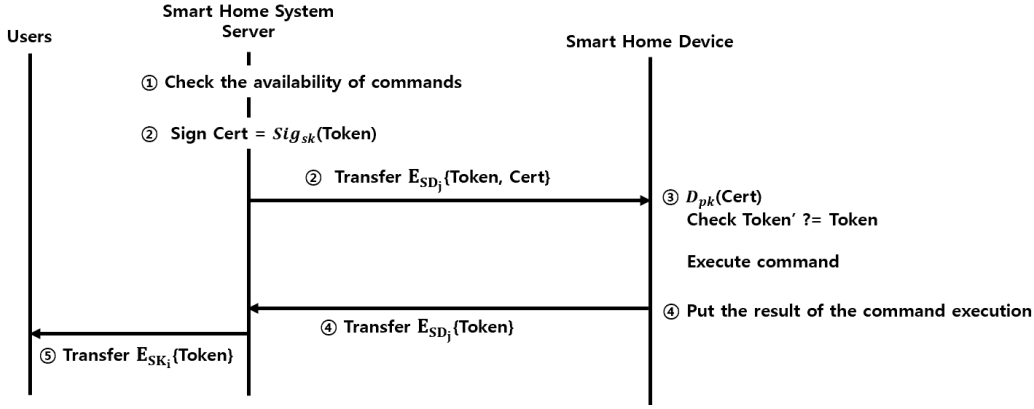

Fig. 5. Smart home device control

4.3.2 디바이스 제어

앞서 토큰 검증이 성공적으로 완료된 경우 디바이스 제어과정을 수행하게 된다. 디바이스 제어는 Fig. 5.와 같이 5단계로 동작한다.

① 사용자의 접근 권한 등급에 따라 서비스 접근 범위 내에 있는 명령인지 확인한다.

② 스마트 홈 시스템 서버는 자신의 개인 키인 sk로 토큰에 서명한 후 스마트 홈 디바이스에게 전달한다.

SS: $Cert = Sig_{sk}(Token)$
SS → SD_j: $E_{SK_j}(Token, Cert)$

③ 토큰과 서명 값을 전달받은 스마트 홈 디바이스는 스마트 홈 시스템 서버의 공개키로 서명 값을 복호화하여 토큰 값과 일치하는지 확인하는 서명 검증 절차를 우선 수행한다. 검증에 성공한 경우에는 데이터 필드에 담긴 명령을 실행한다.

SD: $D_{pk}(Cert)$
Token' ?= Token

④ 명령 수행을 마치면 데이터 필드에 명령 수행 결과를 담아 스마트 홈 시스템 서버에게 전달한다.

SD_j → SS: $E_{SK_j}(Token)$

⑤ 스마트 홈 시스템 서버는 공유키(세션 키) SK_j를 통해 암호문을 복호화하고, 토큰의 데이터 필드를 확인한다. 이때, 데이터 필드에 명령 수행 결과에 대한 데이터가 담겨있지 않고, 비어있거나 명령 요청 데이터가 그대로 담겨있는 경우 ③번 과정으로 돌아간다. 스마트 홈 시스템 서버는 사용자에게 명령 수행 결과를 담은 토큰을 전송하며 디바이스 제어과정을 마친다. 이때, 암호화하여 전달하는 메시지는 동일하나 ④번 과정에서 사용하는 키와 해당 과정에서 사용하는 키는 다르므로 재생 공격이 어렵다.

SS → U_i: $E_{SK_i}(Token)$

V. 기능성 분석

5.1 자동화된 접근제어

자동화된 접근제어는 Home Owner의 개입 없이 CASA가 자동으로 일반 사용자의 접근 권한을 설정하는 것을 의미한다. 시스템상에서 자동으로 접근 권한 설정이 이루어지므로 스마트 홈 시스템 서버는 방문한 적이 있는 사용자이더라도 매번 새롭게 등록해야 하는 번거로움을 방지할 수 있다. 또한, 관리자는 자택에 방문객이 있을 때마다 수동적으로 사용자 역할 설정을 수행하지 않아도 되므로 편리하게 시스템 관리가 가능하다.

[4]에서는 사용자의 신뢰도를 평가하여 스마트 홈 시스템 접근 허용 여부에 대해 시스템상에서 자동으로 판단한다. 그러나 [5]에서는 역할기반 접근제어 방식과 속성기반 접근제어 방식을 중심으로 두 가지의 하이브리드 모델을 제시하였으나 동적 속성과 정적 속성 판단 시 스마트 홈 소유자의 개입이 필요하다. 또한, [6], [7]에서는 제어 권한이 있는 사용자가 다른 사용자에게 접근 권한을 위임해주는 방식이므로 자동화된 접근 권한 설정을 만족하지 않는다.

5.2 세분화된 권한 설정

세분화된 권한 설정이란 스마트 홈 디바이스 및 각종 센서 등에 제어 명령을 내릴 수 있는 권한을 특징에 따라 분류된 그룹별로 설정할 수 있는 것을 의미한다. 본 연구에서는 이를 통해 시스템 서버가 모든 사용자에게 제한 없이 서비스를 제공하는 것을 막고, 타인의 불필요한 정보의 접근을 방지할 수 있다.

[4]에서는 어떤 스마트 홈 디바이스 또는 센서를 사용할 수 있는지, 어떤 기능을 사용할 수 있는지는 판단하지 않았으므로 세분화된 권한 설정을 만족하지 않는다. 만약 [4]에서 세분화된 권한 설정을 만족하기 위해서 신뢰 등급의 개수를 늘린다고 가정해보자. 사용자의 행동 데이터셋에 대한 비정상 여부를 판단하는 라벨 또한 더 세분되어야 정확한 신뢰 등급의 분류 및 선정이 가능하다. 그러나 신뢰 등급이 세분되어 개수가 증가할 때마다 딥러닝 모델에 입력되는 데이터셋의 비정상 여부를 재분류하는 것은 시스템에 과부하를 일으킬 수 있고, 개별 사용자의 스마트 홈에서 이러한 복잡한 딥러닝 모델을 사용하는 것은 매우 어려울 것으로 예상된다. 따라서 [4]에서 세분화

Table 3. Comparison table

	[2]	[3]	[4]	[5]	[6]	[7]	[8]	Our
2-factor authentication	X	X	X	-	X	-	X	O
Anonymity	O	O	O	-	X	X	X	O
Non-traceability	O	O	O	-	X	X	X	O
Automated access control	-	-	O	X	X	X	X	O
Fine-grained access control	-	-	X	X	X	X	X	O

된 권한 설정 기능을 추가하기 위해 신뢰 등급을 세분화하고 이러한 변동 과정을 유동적으로 가능하게 하는 것은 매우 어렵다. [5], [6], [7], [8]에서는 각각의 스마트 홈 디바이스 및 센서에 접근할 수 있는 권한을 부여하므로 본 연구에서 의미하는 세분화된 권한 설정과 다르다.

VI. 안전성 분석

6.1 비인가된 인증 방지

비인가된 인증 방지란 스마트 홈 시스템이 비인가된 인증 시도를 자동으로 감지하고 차단하여 공격자의 위협으로부터 시스템을 보호하는 것을 의미한다.

제안하는 프로토콜이 비인가된 인증 방지에 대한 안전성을 만족하기 위해서는 수정 공격, 중간자 공격, 위장 공격에 안전해야 한다. 본 연구에서는 스마트 홈 시스템 사용자의 계정 로그인 시 ID/PW뿐만이 아니라 개인기기(ex. 스마트폰)를 활용한 생체인증을 사용함으로써 ID/PW 단일 인증 방식의 취약성을 보완하고, 계정 탈취 위험성을 낮춘다. 또한, 사용자 단말기와 같은 물리적 요소가 요구되고 HMAC 방식을 사용하므로 사용자의 개인 단말을 물리적으로 탈취하지 않는 이상 단말 정보를 알기 어렵고, 통신에 사용되는 세션 키, 변화하는 RC 값, 난수 등 다양한 파라미터 값을 동시에 유추하기는 어려우므로 위장 공격에 안전하다. 더불어 추가적인 인증 단계를 제공함으로써 공격자가 모든 요소를 동시에 탈취하는 것을 어렵게 하므로 중간자 공격에 안전하다. 그 외에도 공격자가 토큰의 데이터 필드에 있는 사용자의 명령을 수정할 수 없도록 통신 주체별, 매 세션마다 모두 다른 키를 사용한다. 다시 말해, SSL/TLS 통신의 안전성에 기반하여 통신을 수행하므로 수정 공격에 안전하다. 따라서 본 연구에서는 접근 권한 및 등급의 변경 통제의 보안 목표를 만족하며 이중인증을 사용하여 보안성을 높였다.

[2]에서는 토큰 자체의 안전성을 향상시키기 위한 RC 값 사용과 같은 보안 조치가 되어 있으나 사용자가 직접 생성하는 토큰만을 사용한 인증을 수행하며, [3]에서는 ID/PW로만 단일 인증한다. [4]에서는 개인 식별 정보와 기기 정보만을 수집하여 사용하며, [6]에서는 초기 사용자 인증은 ID/PW로 진행하고 이후 인증은 인증 토큰을 사용한다. [8]에서는 개별 장치 ID 및 스마트 홈 허브에서 발급한 공유 비밀번호를 통해 인증(등록)한다. 사용자들은 여러 사이트에 동일한 ID/PW를 사용하는 경우가 많고 서비스 제공자들은 다중인증을 제공하지 않는 서비스가 존재하며 특히 중소기업의 경우 대기업 대비 정보보호 역량이 제한되어 있다는 문제가 있어[9] 단일 인증 방식만을 사용하는 것이 아닌 추가적인 보안 조치를 취해 사용자의 신원을 안전하게 보호하지 않았으므로 효과적인 비인가된 인증 방지가 어렵다는 한계가 있다.

6.2 접근 권한 및 등급의 변경 통제

사용자의 스마트 홈 시스템 접근 권한 및 등급 변경을 통제하여 무분별한 권한 변경이나 상승을 방지해야 한다.

제안하는 프로토콜이 접근 권한 및 등급의 변경 통제에 대한 안전성을 만족하기 위해서는 재생 공격과 액세스 권한 변경 공격에 안전해야 한다. 사용자들이 스마트 홈 디바이스 및 센서에 명령을 전달할 때 메신저의 역할과 더불어 인증의 용도로도 사용되는 Token은 CASA에 의해 사용자의 역할과 접근 범위가 자동으로 설정되므로 특정 개인이 임의로 변

경하는 것은 불가하다. 또한, Token이 생성되면서 유효 시간이 설정되어 일정 시간 후에는 유효하지 않은 Token이 되며, 변화하는 RC 값에 따라 달라지는 Token 값에 의해 공격자가 재생 공격 및 액세스 권한 변경 공격 수행 시 스마트 홈 시스템에서는 이를 비인가된 인증 시도로 감지하고 차단한다. 따라서 본 연구는 접근 권한 및 등급의 변경 통제의 보안 목표를 만족하며 토큰을 통한 스마트 홈 디바이스 및 센서 제어를 수행함으로써 보안성을 높였다.

〔4〕에서는 시스템이 사용자의 신뢰도를 평가하여 접근 가능한 범위를 자동으로 판단하므로 접근 권한을 무분별하게 변경하는 것은 어렵다. 〔5〕, 〔6〕, 〔7〕, 〔8〕에서는 각각의 스마트 홈 디바이스 및 센서에 접근할 수 있는 권한을 부여하나 〔5〕와 달리 〔6〕, 〔7〕, 〔8〕의 경우 블록체인 기술을 사용하여 거래자의 신원을 투명하게 명시하는 것을 원칙으로 하므로 비인가된 사용자인 공격자가 접근 권한을 임의로 변경하는 것은 어렵다.

6.3 프라이버시 보호

스마트 홈 시스템은 개인정보를 모니터링하고 제어하는 데 사용되므로 개인정보보호가 중요하다. 또한, 사용자들의 정보보안에 대한 인식이 높아지면서 개인정보보호에 대한 우려도 증가하고 있다. 이러한 이유로, 사용자들은 스마트 홈 시스템을 통해 자신의 개인정보나 생활 방식이 무단으로 공개되거나 악용되지 않을 것을 기대한다. 따라서 본 연구에서는 데이터 암호화, 접근제어 등의 데이터 처리 방식을 통해 스마트 홈 서비스를 이용하는 모든 사용자의 개인정보 및 민감 정보를 보호한다.

프라이버시 보호에 대한 안전성을 만족하기 위해서는 3장의 안전성 모델에서 언급된 5가지의 공격이 불가해야 한다. 본 연구에서는 모든 통신은 SSL/TLS 통신의 안전성에 의하여 통신 과정에서 사용자의 기밀정보들이 공격자에게 노출될 가능성이 매우 낮으며 사용자 식별 정보로 스마트 홈 시스템 서버가 생성한 가상 식별 정보인 PID를 사용한다. 이때, PID는 스마트 홈 시스템 서버가 랜덤하게 생성하여 각각의 사용자에게 부여한 것으로 공격자가 스마트 홈 시스템 서버의 관리자 계정 탈취에 성공하거나 사용자의 개인정보가 저장돼있는 데이터베이스를 직접 확인하지 않는 이상 통신 과정에서 탈취한 정보를 통해 사용자의 신원을 특정할 수 없다. 이와 함께 단말 정보를 안전하게 Token에서 사용하기 위해 HMAC에서의 대칭키 암호의 안전성에 의하여 접근 등급(pi)이 보호되고 CASA에 의해 자동으로 사용자의 역할과 접근 범위가 설정되므로 중간자 공격 및 수정 공격, 액세스 권한 변경 공격에 안전하다. 그 외에도 매 세션별 다른 키를 사용하고 동일한 메시지가 2번 이상 반복되지 않아 재생 공격에 강하며, 토큰 서버가 사용자별로 다른 난수를 사용하며 해시함수를 통해 접근 등급(pi)을 보호하고 변하는 RC 값에 따라 Token 값이 달라지므로 위장 공격에 안전하다. 제안하는 프로토콜은 이와 같은 공격들에 안전하므로 보안 목표 중 프라이버시 보호를 만족한다.

〔2〕에서는 개인 식별 정보를 디바이스 정보로 대신 사용하며 이를 해시함수로 암호화하여 통신한다. 〔3〕에서는 ID/PW는 SHA 256으로 암호화하여 통신하며, 〔4〕에서 또한 ID를 해시함수로 암호화하나 〔2〕와 달리 난수를 결합한다는 차이점이 있다. 또한, 〔2〕, 〔3〕, 〔4〕에서는 본 연구와 같이 해시키, 난수, 세션 키 등 파라미터 값을 필요로 하므로 프라이버시 보호를 만족한다. 그러나 〔6〕, 〔7〕, 〔8〕의 경우 블록체인 기술에서는 거래자의 신원을 투명하게 명시하는 것을 원칙으로 하므로 익명성과 프라이버시 보호를 만족하지 않는다.

6.4 추적 불가능성

추적 불가능성이란 공격자가 사용자의 신원을 알고 있더라도 통신 메시지 상에 포함되는 암호 키 등 다른 매개변수의 값들을 알지 못하므로 사용자의 통신을 추적할 수 없다는 것을 의미한다〔10〕.

공격자가 특정 사용자의 신원 및 통신에 사용되는 PID 값을 알고 있다고 가정한다. 제안하는 프로토콜이 추적 불가능성을 만족하기 위해서는 재생 공격과 위장 공격을 막아야 한다. 본 연구에서는 사용자의 통신이 추적되지 않도록 매 세션마다 다른 키를 사용하고 같은 메시지를 반복적으로 사용하지 않음으로써 재생 공격에 안전하다. 또한, 공격자가 특정 사용자인 척 행동하여 사용자 정보를 도용하거나 통신을 추적할 수 없도록 단말 정보(IMEI, Serial Num.), 해시함수, 난수, RC 등의 값을 이용하여 보안 메커니즘을 강화하였다. 정상적인 사용자가 스마트 홈 디바이스 및 센서에게 명령을 전달하는 등의 과정에서 RC 값의 변화에 따라 토큰값 또한 변하므

로 공격자가 올바른 토큰을 생성하는 것은 어려우므로 위장 공격에 안전하다. 이처럼 세션 키와 RC 값 등의 매개변수를 적절히 사용하며 각 통신 세션이 고유하고 안전하게 유지함으로써 공격자가 특정 사용자의 신원과 PID 값을 알고 있더라도 사용자의 통신 내용과 패턴을 추적할 수 없도록 보호한다. 따라서 본 연구는 추적 불가능성을 만족한다.

〔2〕에서는 본 연구와 마찬가지로 공격자는 세션 키, 해시키, RC 값 등을 알아내야 한다. 〔3〕에서는 SHA 256 암호 키, 〔4〕에서는 해시키, 난수 값 등을 알아야 하므로 추적 불가능성을 만족한다. 그러나 〔6〕, 〔7〕, 〔8〕의 경우 블록체인 기술에서는 모든 거래를 투명하게 공개하는 것을 원칙으로 하므로 추적 불가능성을 만족하지 않는다.

VII. 결 론

최근 우리는 개인 수집 데이터에 기반한 일상 속에 살아가고 있다. 특정 역할만 수행하는 단순한 기계에 불과했던 가전제품들이 이제는 사용자의 생활 정보를 수집하고, 이를 토대로 서비스 데이터를 생성하여 제공하는 등 다양한 부가가치를 창출하면서 가전 시장에서 데이터 기반의 기기들의 점유율이 높아지고 있다. 그러나 스마트 홈 시장에서는 다양한 스마트 가전 기기들과의 연결성에 주목하고 보안에 대한 부분은 시장의 성장세에 비해 뒤따라가지 못하고 있다.

스마트 홈에서는 스마트 디바이스를 통해 홈 내외에서 자유롭게 스마트 홈 디바이스에 접근 및 제어가 가능해지고, 스마트 홈 내에서 수집되는 모든 정보에 대한 조회가 가능하다. 따라서 스마트 홈의 개인정보 보호에 대한 보안 조치가 필수적이며, 보안성을 높이면서 스마트 홈 시스템 사용자의 편의성을 저하시키지 않도록 하는 것이 중요하다.

본 논문에서는 스마트 홈 환경에서 안전한 디바이스 제어 명령을 위한 토큰 기반 사용자 동적 접근제어 기법을 제안하였다. 제안 기법은 사용자가 스마트 홈 서비스에 접근하였을 때 CASA에 의해 접근 권한은 스마트 홈 디바이스의 기능 및 종류에 따라 세분화하여 자동으로 설정되며, 사용자 개인 디바이스를 활용한 토큰 기반 기법을 제안한다. 이는 기존의 스마트 홈 서비스가 수동적으로 사용자의 스마트 홈 내의 디바이스 접근 권한을 설정하지 않도록 하고, 한시적 사용자에게도 일률적으로 스마트 홈 소유자의 권한을 부여하여 서비스를 이용하도록 하는 것을 방지한다. 또한, 토큰 내 Revision Counter 값을 추가함으로써 제3자에 의해 변조되거나 조작된 토큰 사용을 막을 수 있다.

본 논문에서는 세분화된 권한 설정 방식에 대한 아이디어만 제시하였으므로 향후 안전성 향상을 위한 연구가 요구된다. 또한, SmartThings, LG ThinQ 등 다양한 스마트 홈 플랫폼에서의 활용 연구를 진행할 예정이다.

References

〔1〕 Do-eun Cho and Si-jung Kim, “User Dynamic Access Control for Privacy Protection in Smart Home,” Journal of Platform Technology, 6(3), pp. 17-22, Sep. 2018

〔2〕 Nam-gon Lee, “Enhance authentication and security used tokens in a smart home environment: enhanced authentication with tokens,” Konkuk University Postgraduate master’s thesis, Feb. 2018

〔3〕 T.A. Khoa, L.M.B. Nhu, H.H. Son et al. “Designing Efficient Smart Home Management with IoT Smart Lighting: A Case Study,” Wireless Communications and Mobile Computing, vol. 2020, Nov. 2020.

〔4〕 K. Yang, L. Zhao, X. Yu and K. Cheng, J. Ma, “Research on Dynamic Access Control Mechanism Based on Short-term Token and User Trust,” 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), pp. 60-63, Jul. 2022.

〔5〕 S. Ameer, J. Benson and R. Sandhu, “Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT,” IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 5, pp. 4032-4051, Oct. 2023.

〔6〕 N. Tapas, F. Longo, G. Merlino and A. Puliafito, "Experimenting with smart contracts for access control and delegation in IoT," Future Generation Computer Systems, vol. 111, pp. 324-338, Oct. 2020.
〔7〕 Y. Liu, Q. Lu, S. Chen, Q. Qu, H. O'Connor, K.K.R. Choo and H. Zhang, "Capability-based IoT access control using blockchain," Digital Communications and Networks, vol. 7, no. 4, pp. 463-469, Nov. 2021.
〔8〕 A. Mukherjee, M. Balachandra, C. Pujari, S. Tiwari, A. Nayar, and S. R. Payyavula, "Unified smart home resource access along with authentication using blockchain technology," Global Transitions Proceedings, vol. 2, no. 1, pp. 29-34, Jun. 2021.
〔9〕 Hyun-jung Kwon, Hong-ju Jung and Kyeong-seok Han, "A Study on the Necessity of Applying Multi-factor Authentication for User Authentication," Journal of The Korea Society of Information Technology Policy & Management (ITPM), 12(4), pp. 1899-1903, Aug. 2020
〔10〕 A. Goel, J. Patel and C. Patel, "BLS based authentication and token-based authorization for Smart Home," 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1-7, Oct. 2022.
〔11〕 Dai-hwan Lim, "Personal Authentication System Using Multimodal Biometric Algorithm," The Journal of Korean Institute of Information Technology, 15(12), pp. 147-156, Dec. 2017

〈저자소개〉

유 혜 선 (Hyeseon Yu) 학생회원
2020년 3월~현재: 덕성여자대학교 사이버보안 학사과정
〈관심분야〉 정보보호, IoT 보안

서 민 혜 (Minhye Seo) 종신회원
2012년 2월: 고려대학교 수학과 졸업
2020년 2월: 고려대학교 정보보호대학원 정보보호학과 박사
2020년 3월~2020년 8월: 고려대학교 정보보호연구원 연구교수
2020년 9월~현재: 덕성여자대학교 사이버보안전공 조교수
〈관심분야〉 암호, 인증, 프라이버시