스마트 홈(Smart Home)의 기술 개발과 전망

지도교수 : 김 윤
연 구 자 : 박 준 석

< 목 차 >

요 약

스마트 홈은 4차 산업혁명 시대인 현대시대의 융합기술과 핵심기술이라고 할 수 있는 사물인터넷과 인공지능을 이용하고 스마트시대의 개념과 기술들을 주택 혹은 아파트 세대별로 적용시킨 기술로 지금도 기술적, 상품적으로 개발되고 있는 시대이다. 영화나 드라마 속에서만 보던 작은 기기 하나로 집 안의 가전제품들을 모니터링하고 제어시키는 것이 그리 멀지 않은 시대에 우리가 사용할 수 있는 미래가 오게 되었으며, 바쁜 일상을 살아가고 있고 앞으로 살아갈 현대인들에게 반드시 필요하다고 생각되는 기술이다.

주요 언어 : 스마트 홈, 사물인터넷, 인공지능, 보안

1. 서론

1.1 스마트 홈이란?

가정 자동화(Home Automation 또는 Domotics) 또는 스마트 하우스(Smart House)라고도 불리며, 가전제품(TV, 에어컨, 냉장고 등)을 비롯해 에너지 소비장치(수도, 전기, 냉난방 등), 보안기기(도어락, 감시카메라(CCTV)) 등 다양한 분야에서 모든 것을 통신망으로 연결해 모니터링 및 제어할 수 있는 기술을 말한다. 스마트 폰이나 인공지능 스피커가 사용자의 음성을 인식해 집 안의 모든 사물인터넷 기기를 연결하고 사용자의 특성에 따라 자동으로 작동하거나 원격으로 조종이 가능하다. 현재 스마트 홈은 원격제어에서 발전해 AI가 상황과 사용자의 취향을 학습하고, 이에 맞는 결과를 스스로 제공하는 방향으로 발전하고 있다.

1.2 스마트 홈과 관련 있는 기술

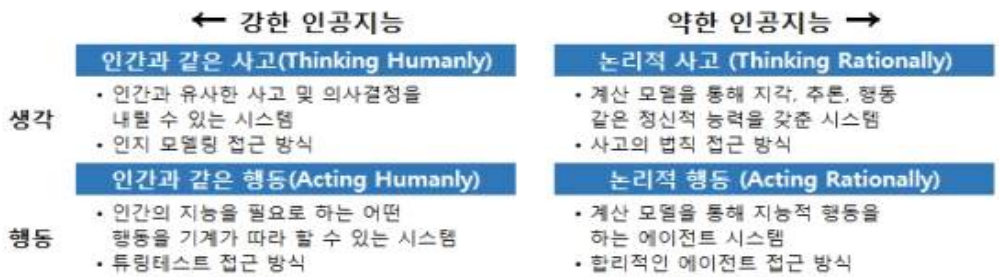
1.2.1 사물인터넷(IoT, Internet of Things)

4차 산업혁명의 핵심 기술 중 하나로, 네트워크 통신 기술을 이용하여 고유 ID와 센서, 통신기능을 탑재한 사물들을 연결하고, 이를 기반으로 다양한 서비스를 제공함으로 초 연결 사회를 가능하게 하는 기술로 제한된 네트워크 내에서만 구현되던 기존의 RFID 방식의 한계를 벗어나 인터넷이라는 무한한 공간을 갖는 네트워크로 확장하여 사물은 물론, 인간, 현실과 가상현실을 넘나들며, 상호작용하는 개념으로 발전했다.

이처럼 사물인터넷은 네트워크의 무한한 확장성이 담보되면서 헬스 케어·의료·복지, 교육, 건설, 스마트 홈 등 광범위로 사용된다. 사물인터넷에 연결되는 사물들은 자신을 구별할 수 있는 IP를 가지고 인터넷으로 연결되어야 한다는 특징이 있다.

1.2.2 인공지능(AI, Artificial Intelligence)

4차 산업혁명의 핵심 기술 중 하나로, 컴퓨터 프로그램을 이용해 인간의 학습능력, 추론능력, 지각능력, 자연어의 이해능력 등 모든 지능적인 행동들을 모방할 수 있고 인간처럼 학습하고 생각할 수 있는 컴퓨터 시스템을 의미한다.



[사진 1] 인공지능의 분류 조건

약 인공지능(Weak AI)은 미리 정의되어 있는 규칙 혹은 모델에 의해 인지능력을 필요로 하지 않는 정도의 논리적인 영역의 문제를 해결하는 시스템으로 대표적 사례에는 구글의 알파고(Alpha GO), 아마존의 알렉사(Alexa), 애플의 시리(Siri) 등이 있다.

강 인공지능(Strong AI)은 인간과 같은 사고와 행동을 할 줄 알며, 인간의 지능을 필요로 하는 행동을 기계가 따라하게 해줄 수 있는 시스템으로 모든 분야에서 인간과 동등하거나 우월한 능력을 가진 인공지능으로 대표적 예로는 영화 <터미네이터>에 등장하는 스카이넷과 공상과학 소설(SF)이나 영화 속에 자주 등장하는 인공지능 로봇들이 대표적이다.

초 인공지능(Super AI)은 모든 면에서 인간의 능력을 훨씬 초월하는 인공지능으로 인공지능이 강 인공지능 단계에 접어들면 지속적인 자체 지능 개선을 통해 초 인공지능 단계로 이행할 것으로 예측되는데, 초 인공지능의 능력의 한계는 현재 인간의 상상을 초월하는 범위로서, 인간은 초 인공지능에 대해 이해하기 어렵다고 한다.

초 인공지능이 구현될 경우, 인류는 초 인공지능의 도움으로 영생을 누리거나 아니면, 열등한 종으로 분류되어 멸종될 가능성도 있다고 한다.

1.2.3 사물인터넷, 인공지능과 스마트 홈의 관련성

사물인터넷과 스마트 홈의 관련성으로는 네트워크 통신 기술을 이용해 사물들을 하나의 통신망으로 제어하는 것이다. 인공지능과 스마트 홈의 관련성으로는 상황과 사용자의 취향을 학습해서 이에 맞는 결과를 제공하는 방향으로 발전하고 있기 때문에 학습을 한다는 점에서 인공지능의 학습능력과 관련성이 있다.

2. 본론

2.1 스마트 홈의 특징

첫 번째, 무궁무진한 발전성. 인공지능과 사물인터넷이 발전하면 이 2가지 기술의 융합이라고 볼 수 있는 스마트 홈의 발전성은 더 높아질 것이고, 스마트 홈을 지원하는 기기들이 지속적으로 늘어나고 있음에 따라 보안적, 생활적으로도 발전성이 높다고 본다.

두 번째, 주택 관리에서 발생하는 스트레스의 감소. 바쁜 일상을 살아가서 시간적 여유가 주말 뿐이고 주말에 주택 관리만 하다가 어느새 끝난 주말로 인해 주택 관리에 스트레스를 받는 현대인들이 있다. 이 때 스마트 홈을 이용하면 회사에서 업무를 보고 있더라도, 집 내에서 휴식을 취하고 있다고 하더라도 주택을 자동으로 모니터링하고 가전제품을 원격으로 조종시킬 수 있기 때문에 주택 관리로 인한 스트레스가 줄어들 수 있다.

세 번째, 자동 주택 관리로 인해 늘어난 여가시간. 이 특징은 두 번째 특징에 대한 추가점으로 주택을 자동으로 청소 및 관리를 해주기 때문에 스마트 홈이 현대인들의 여가시간을 제공해주기 때문에 자기관리와 취미 생활을 하는 여가시간이 늘어난다.

2.1.1 스마트 홈의 장점

스마트 홈의 가장 큰 장점을 꼽자면 편리함이다. 시간과 공간 제약 없이 인터넷으로 집 안의 사물들을 다룰 수 있는데, 이제는 사용자가 직접 하지 않더라도, 인공지능과 로봇이 집 안의 전자기기를 제어하고 바쁜 일상을 살아가는 현대인에게 시간은 금과 같은데 예를 들어 장을 보러가지 않더라도 인공지능이 탑재된 냉장고에서 식자재 파악 및 자동주문이 가능하다는 이유로 편리함을 꼽을 수 있다.

2.1.2 스마트 홈의 단점

첫 번째는 위조된 디바이스로 대부분의 스마트 홈 디바이스는 고유 ID나 인증서 형태로 디바이스 식별자를 가지게 되는데 이 고유 식별자를 암호화하여 보호해야 하는데 그렇지 못한다면 악의적 공격자가 이 식별자를 생성하는 프로세스를 알아냄으로써 이를 쉽게 복제할 수 있다. 고유 식별자를 허가 없이 복제할 수 있게 된다면 공격자가 복제된 디바이스를 통해 네트워크 내부로 쉽게 침투하게 되고 그로부터 후속 공격을 펼칠 수 있다.

두 번째는 데이터 가로채기로 스마트 홈 환경에 사용되는 대부분의 통신 인터페이스는 블루투스, 와이파이 같은 무선 기술을 기반으로 하는데 이런 대부분의 무선 기술은 특정한 형태의 보안 보호 메커니즘을 갖추고 있으나 활용 사례 자체의 제약 때문에 악의적 접근을 막아낼 정도로 견고하지 않다는 단점이 있다.

세 번째로 데이터 조작은 가로채기의 위험성뿐이 아닌 악의적 공격자가 중요 데이터를 조작 및 변경할 수 있는 위험성도 있어 데이터 무결성 보호가 스마트 홈 환경에서 또 다른 중요한 보안 과제이다. 요금 정보, 민감한 구성 데이터, 자원사용 같은 중요 데이터들이 조작된 값으로 통신되거나 저장되지 않도록 사용자가 검토해야 한다.

마지막 네 번째로 멀웨어 감염은 네트워크로 접근한 후 가장 흔하게 이루어지는 공격은 멀웨어를 설치하는 것으로 감염된 디바이스를 활용해 또 다른 공격을 할 수 있게 된다.

커넥티드 홈 디바이스가 공격을 받아서 멀웨어가 설치되면, 이러한 디바이스들을 봇넷으로 추가해 디도스(DDoS) 공격을 할 수 있다. 그 후, 컴퓨터뿐만이 아니라 다양한 스마트 홈 디바이스들이 디도스 공격을 전개하여 혼란이 가중 될 수 있다.

이러한 스마트홈 디바이스의 수는 네트워크에 연결된 컴퓨터 수보다도 훨씬 더 많기 때문에 봇넷 디도스 공격을 통한 피해 규모와 속도는 훨씬 더 심각할 것으로 예상된다.

2.2 스마트 홈 구성에 필요한 도구

2.2.1 첨단 ICT(Information & Comminication Technology)

ICT는 하나의 케이블 연결이나 링크 시스템을 통하여 오디오 수준의 전화망을 컴퓨터 네트워크와 결합하는 의미로 사람과 사람 사이를 연결하거나 인간과 사물, 사물과 사물끼리의 연결이 가능하다는 특징을 가지고 있다.

ICT가 스마트 폰의 예시로는 우리가 실생활에서 익숙하게 사용하는 스마트 폰이나 태블릿 PC를 예로 들 수 있다. ICT가 스마트 홈 구성에 필요한 도구인 이유는 스마트 홈이 스마트 폰이나 태블릿 PC와 가전제품들을 연결해서 모니터링이나 제어를 하기 때문에 인간과 사물을 연결 시켜주는 특징이 있기 때문이다.

2.2.2 스마트 센서

첫 번째, 움직임을 감지하는 모션센서로 모션센서를 창문과 문에 부착한다면 사람들이 집에서 언제 외출하는지 알 수 있고, 창문이나 문의 움직임으로 침입자를 감지하게 된다면, 무선 기술을 통해 ICT 기기로 알림을 받을 수 있고 모션센서를 CCTV에 연결한다면 센서가 녹화를 활성화시켜 침입 장면을 캡처 할 수 있다는 것과 사람이 없는 방에 조명이 켜져 있다면 그 방의 조명을 원격으로 끄는 식으로 에너지 절약에도 도움이 된다.

두 번째, 누출·습기 감지 센서는 물과 관련 있는 싱크대 세면대 등에 설치하여 겨울철 수도가 얼거나 아무도 없는 집에 수도꼭지를 제대로 잠그지 않아 물이 세는 경우 등을 사전에

방지할 수 있게 해줌으로써 수도요금 폭탄 방지도 가능하다.

세 번째, 온·습도 센서는 스마트 온도조절장치와 연결하여 사용하면 집 안과 밖에서 집의 습도와 온도를 파악함으로 집의 냉방과 난방을 제어 할 수 있으며, 이 뿐 아니라 집 안의 대기 품질에 대한 모니터링으로 미세먼지, 공기부패와 같은 오염 물질도 감시가 가능하다.

네 번째, 인터콤과 허브가 있는데 이 센서들의 역할은 여러 개의 센서를 집 내부에 설치했기 때문에 한 곳에서 모든 것을 관리하기 위해 사용하는 것으로 버튼 하나만으로 긴급 서비스나 수리 서비스를 요청할 수 있다.

구분	소재	설계	설비	양산	핵심	평균
미국	100	100	90	85	100	95
유럽	100	100	95	95	100	98
일본	100	95	90	100	100	97
한국	55.5	72.4	70.0	69.7	55.8	64.7

[표 1] 국가별 센서기술 수준 분석(자료 : CHO Alliance(2015))

스마트 센서 기술은 주로 유럽과 미국을 중심으로 개발되고 있다. 국내의 센서 핵심기술 수준은 55%, 미국 95%, 유럽 98%에 비해 매우 낮은 수준으로 국내 수요의 대부분을 수입에 의존하고 있는 상황이다. 그러나 국내 대기업들을 중심으로 빠르게 대응 중이지만, 중소기업의 자발적 움직임에 대해서는 아직 미흡하다고 볼 수 있다.

2.2.3 컨트롤러

스마트 센서에 의해 감지된 환경 변화나 사용자에 의해 입력된 명령 등의 각종 정보를 분석하여 필요한 조치를 확인하고, 특정한 기기가 적절하게 작동하도록 명령하고 관리하는 장치로서, 인공지능처럼 스스로 정보를 분석하고 판단해서 조치하는 인공지능 컨트롤러와, 스마트 폰이나 태블릿 PC 등 사용자가 직접적으로 명령을 입력하는 컨트롤 디바이스로 나눌 수 있다. 인공지능 컨트롤러의 경우 KT의 기가지니(GiGa Genie), SK텔레콤의 누구(NUGU), 아마존의 알렉사(Alexa) 등과 같은 인공지능 스피커 혹은 스마트 홈 허브와 같은 형태로 공급되고 있다.

2.2.4 유・무선 네트워크

센서에 의해 취득된 정보나 컨트롤러에 의해 실행되는 명령이 해당 기기에 실시간으로 전달되도록 기능하며, 모든 센서와 컨트롤러, 기기들 간 연결성을 확보하기 위한 하드웨어로서 실내 뿐 아니라 외부와의 연결도 가능하도록 다양한 표준의 네트워크가 필요하다.

가장 많이 사용될 네트워크인 Wi-Fi는 통신 속도가 빠르고 거리가 긴 반면 전력 사용량이 많다는 단점 때문에 크기가 크고 전력 공급량이 많은 가전제품에는 적합하지만 전구나 가스, 도어락 같은 크기의 작고 저 전력을 사용하는 기기들에는 적합하지 않다.

비콘(Beacon)*1이나 지그비(ZigBee)*2, Z-Wave 등과 같은 근거리, 소용량, 저전력 특성을 가진 무선 네트워크 프로토콜들은 실내 크기가 작고 전력 사용량이 적은 기기들 간 통신에 적합하다.

2.2.5 스마트 홈 기기(가전제품)

주어진 여건에 따라 적절하게 사용자에게 직접적인 편의(청소, 온도습도 조절, 도어 개폐 등)를 제공하는 기기들로서 컨트롤러에 의해 작동되거나 자체 인공지능에 의해 작동되기도 하는데 주택을 스마트 홈으로 신축하는 경우, 건설회사가 스마트 홈의 정보 인프라뿐 아니라 직접적인 편의를 제공하는 스마트 홈 기기들도 포함해서 제공하게 되며, 필요한 경우 사용자가 추가적으로 스마트 홈 기기를 구매해서 보완할 수도 있다.

반대로 기존 주택을 스마트 홈으로 발전시키는 경우에는, 사용자가 스마트 홈 정보 인프라를 구축하기 위해 정보통신 업체에 서비스를 요청하고 필요한 가전제품을 선별적으로 구매해서 사용해야 한다.

2.3 스마트 홈의 관련 사례

2.3.1 욕실의 경우

욕실에 스마트 홈을 적용시키는 예시 첫 번째로는 욕조의 수심 제어와 수온 제어이다. 수심 제어의 경우 반신욕이나 목욕을 하기 위해 욕실에 들어가기 전 물을 먼저 받아야 하는데 계속 보고 있자니 시간이 오래 걸리고 안보고 있자니 물이 얼마나 차는지 모르는 점이 있는데, 스마트 홈을 욕조에도 적용 시킨다면 물이 어느 정도 찼다면 자동으로 물이 꺼지고 알람음이 울린다면 물 낭비도 적어진다는 장점도 생겨난다.

수온 제어의 경우도 반신욕이나 목욕의 예시로 들 수 있는데, 물을 받다 보면 뜨겁거나 차가운 경우가 있는데 이때 에도 수온을 특정 온도로 맞춰두면 욕조에 들어갈 때 적정 온도라서 딱 좋게 있을 수 있다.

욕실에 스마트 홈을 적용 시키는 예시 두 번째로는 욕실의 조명 조절과 스피커이다. 예시를 들어보면 어느 날 바다에 있는 듯 한 기분을 내고 싶다고 한다면 조명을 하늘색으로 조절하고 기기를 스피커에 연결해 파도 소리를 튼다면 바다에 가 있는 기분을 낼 수 있다.

2.3.2 차고나 현관 대문의 경우

차고나 현관 대문에 스마트 홈을 적용시키는 예시 첫 번째, 차고의 경우로 센서를 이용해 사람이 차고 내부에 들어와서 차에 탑승하는 모션을 감지할 수 있는 모션 센서를 설치해서 차고의 문이 열리고 반대로 차고 내부에서는 차량의 번호판을 인식할 수 있는 센서를 설치해 차량이 센서에 감지되면 차고의 문이 열리는 방식으로 사용이 가능하다.

차고나 현관 대문에 스마트 홈을 적용시키는 예시 두 번째, 현관 대문의 경우로 해당 집의 거주자를 시스템에 등록해두고 등록자가 귀가한다면 문이 열리고 미등록자가 온다면 연동되어 있는 장치(스마트 폰, 태블릿PC)로 알림을 전송시켜서 수상한 사람이라면 경찰을 출동시키는 등의 방식으로 사용이 가능하다.

2.3.3 집 내부 공기 환기와 공기청정의 경우

집 내부의 공기 환기와 공기청정에도 스마트 홈을 적용할 수 있다. 이건 공기청정기의 역할이 중요하다고 할 수 있는데 집 안의 공기에 안 좋게 변화가 생긴다면 창문을 자동으로 열고, 반대로 창문이 열려있는데 미세먼지로 인해 집 안의 공기에 변화가 생긴다면 창문을 자동으로 닫는 식으로 사용이 가능하다.

2.4 스마트 홈 관련 보안활용 사례

스마트 홈의 관련된 보안활용 사례로는 인증, 보안통신, 저장 데이터 암호화 및 무결성 보호, 보안적 펌웨어 업데이트가 있다.

첫 번째, 인증. 네트워크상에서 사용자, 컴퓨터, 디바이스, 머신 등의 신원을 확인하고 허가된 사람과 조작되지 않은 디바이스만 액세스할 수 있도록 하는 것으로, 인증 용도로 하드웨어 기반 보안은 디바이스의 비밀 정보(암호화 키, 패스워드 등)를 보안적으로 저장할 수 있다.

두 번째, 보안 통신. 임베디드 시스템 아키텍처에서 디바이스와 시스템들은 다양한 표준 및 고유 프로토콜을 사용하는 이종 네트워크들을 통해서 연결되기에 가로채기나 메시지 위조 같은 위협으로부터 이들 시스템 사이의 통신을 보호해야 한다.

세 번째, 저장 데이터 암호화 및 무결성 보호. 많은 임베디드 디바이스가 민감한 사용자 데이터를 저장한다. 이 데이터를 암호화하거나 서명을 사용해 이 데이터의 무결성과 기밀성을 보호할 수 있다.

과제는 암호화키를 보안적으로 저장하는 것으로 공격자가 이 키를 알아낼 수 있으면 데이터를 손쉽게 해독할 수 있다.

마지막 네 번째, 보안적 펌웨어 업데이트. 임베디드 시스템으로 소프트웨어와 펌웨어를 주기적으로 업데이트해야 할 수 있다.

하지만 업데이트하려는 소프트웨어와 시스템을 보호하는 것은 쉬운 일이 아니다. 소프트웨어만으로 보호되는 업데이트는 위험할 수 있다. 소프트웨어는 읽히고 분석되고 조작될 수 있어서 업데이트나 시스템을 손상할 수 있기 때문이다. 소프트웨어에 보안적인 하드웨어를 결합함으로써 보안을 높일 수 있다.

2.5 스마트 홈의 보안 위협 요소와 대응방안

스마트 홈은 여러 디바이스가 IoT로 연결되어 다양한 애플리케이션을 통해 제어되기 때문에 언제든지 보안 취약점을 노출 할 수 있다. 스마트 홈의 보안을 위협하는 요소로는 인증서 복제 위협, 멀웨어 감염, 데이터 탈취와 조작이 있다.

첫 번째, 인증서 복제 위협. 대부분의 스마트 홈 디바이스는 고유 ID나 인증서 형태로 디바이스의 식별자를 가지는데 이 고유 식별자를 암호화 하지 않으면 공격자가 이를 쉽게 복제할 수 있고, 공격자는 복제된 디바이스를 통해 네트워크 내부로 쉽게 침투가 가능하고 이로 인해 사용자의 데이터 탈취나 홈 네트워크가 공격을 받을 수 있다.

두 번째, 멀웨어 감염. 공격자가 네트워크 접근 후 가장 흔하게 사용하는 공격으로 멀웨어를 사용하는 이유는 감염된 디바이스를 활용하면 또 다른 공격이 가능하기 때문에 멀웨어가 설치되면 공격자는 감염된 디바이스들을 봇넷으로 활용해 DDos 공격을 할 수 있다.

세 번째, 데이터 탈취와 조작. 대부분 블루투스나 와이파이 같은 무선 기술을 기반으로 하는 스마트 홈 환경은 보안에 취약하다는 단점이 있기 때문에 항상 주의해야 한다.

이에 따른 사용자의 대응방안으로는 디바이스 별로 식별자를 암호화 시키는 것, 스마트 홈 보안기기 혹은 스마트 홈 보안 서비스를 이용한다가 있다.

기업의 대응방안으로는 스마트 홈과 사물인터넷 기기의 보안 중요성을 인지하고 위협에 대비하기 위한 맞춤형 보안 서비스의 제공이 있다.

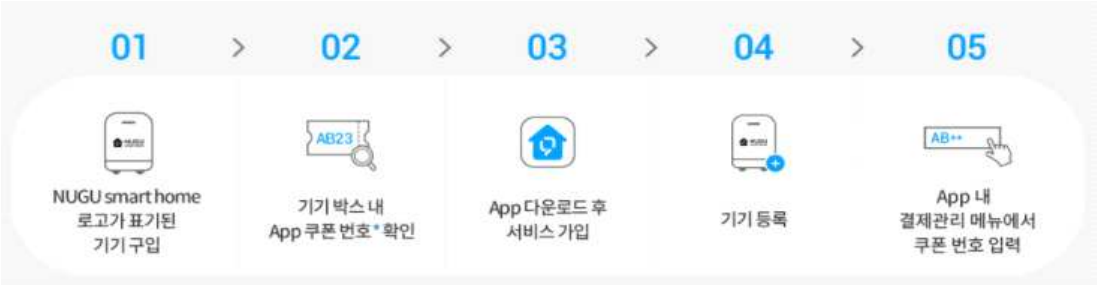
2.6 스마트 홈 관련 국내기업

스마트 홈 기술에 관련이 있는 국내의 기업으로는 삼성전자, LG, SKT 등이 있다.

삼성전자는 스마트 기기와 연동해 다양한 홈 케어를 수행할 수 있는 지능형 컴퍼니언 로봇 '볼리'를 공개했다. 가족을 위한 맞춤형 식단을 짜서 간편하게 요리를 할 수 있도록 레시피까지 추천해주는 사물인터넷(IoT) 냉장고 '패밀리허브'와 인공지능(AI) 보조 셰프인 '삼성봇 셰프'의 업그레이드 버전 등을 공개했다.

LG는 '어디서든 내 집처럼'을 주제로 집 안팎의 경계를 허물고 AI로 제품과 서비스를 서로 연결하는 'LG 씽큐존', 집 안팎을 구분 짓는 출입문의 역할을 넘어 IoT 공간 솔루션 가운데 하나로 구성한 것인 '스마트도어'를 구성했다. 이 외에도 실제로 옷을 입지 않아도 옷의 헐렁함과 같은 피팅감을 확인할 수 있는 '씽큐 핏'도 있다.

SKT는 2016년 9월 1일 스마트 스피커 NUGU가 출시되었는데, 아마존의 '에코'를 한국형으로 만든 것으로 기능은 Apple의 인공지능 Siri처럼 음성인식으로 대부분 동작하는데 다른 점이 있다면 빅 데이터를 이용한 인공지능으로 아직 오류가 있으며, 인공지능의 특성상 조금씩 수정되며 점차 나아질 전망으로 스마트폰과 연동하고 싶으면 NUGU 앱을 설치하고 연동해야 한다.



[사진 2] NUGU의 기기 연결 방법

NUGU를 이용해 스마트 홈 기기를 연동시키려면 먼저 NUGU smarthome 로고가 표기되어 있는 제품을 구입하고 기기 박스나 기기에 붙어있는 번호를 확인 후 다운을 받아 둔 애플리케이션에 앞에서 확인한 기기번호를 등록한다.

3. 결론

스마트 홈은 위 설명처럼 보안위협사례(인증서 복제 위협, 멀웨어 감염, 데이터 탈취와 조작)에 대한 확실하고 효과적인 대응방안이 출시되면 대응방안에 따라 보안체계를 구축함으로써 보안적으로도 확실한 발전이 보장되기 때문에 사용자의 개인정보 보호에도 도움이 되고, 인공지능과 사물인터넷이 발전함에 따라 무궁무진한 발전성을 가진 스마트 홈이 사용자의 편리함을 제공해주기 때문에 스마트 홈의 기술적, 보안적인 전망은 확실히 좋다고 생각하며, 우리가 생각하고 영화에서 보았던 작은 기기 하나로 집의 모든 것을 제어하는 편리함을 기반으로 한 시대가 멀지 않았다고 본다.

참고문헌

[1] 위키백과, 우리 모두의 백과사전

[2] https://brunch.co.kr/@kakao-it/311

[3] https://www.homify.co.kr/ideabooks/6125609

[4] https://m.blog.naver.com/skinfosec2000/221531360936

[5] http://elec4.co.kr/article/articleview.asp?idx=18832

[6] https://www.sktsmarthome.com

[7] https://crevate.com/project/future-smart-home-technologytend/

[8] https://brunch.co.kr/@iotstlabs/130