스마트홈 IoT 기술 및 프라이버시 최신 연구 동향*

신유원 [O1] 이현수 [2] 최우혁 [3] 김희평 [4] 정 용 [5] 이의진 [1]

[1] 한국과학기술원 전산학부, [2] 한국과학기술원 지식서비스공학대학원

[3] 한국과학기술원 정보전자연구소

[4] 한국과학기술원 헬스사이언스연구소, [5] 한국과학기술원 바이오및뇌공학과

youwon.shin@kaist.ac.kr, hslee90@kaist.ac.kr, woohyeok.choi@kaist.ac.kr, heepkim@kaist.ac.kr, yong@kaist.ac.kr, uclee@kaist.ac.kr

Smart Home IoT Technology and Privacy Research Trends

Youwon Shin[O1] Hyunsoo Lee[2] Woohyeok Choi[3] Heepyung Kim[4] Yong Jeong[4,5] Uichin Lee[1]

[1] School of Computing, KAIST, [2] Graduate School of Knowledge Service Engineering, KAIST

[3] Information & Electronics Research Institute, KAIST

[4] KI for Health Science and Technology, KAIST, [5] Department of Bio and BrainEngineering, KAIST

요 약

스마트홈이란 주거 환경 내에서 사물 인터넷 기술 활용을 통해 다양한 서비스 및 정보를 제공하여 거주자의 생활의 질을 높여주는 시스템을 의미한다. 최근 코로나 19 대유행 및 비대면 서비스의 증가로 인해 스마트홈 서비스 및 관련 분야의 지속적인 성장이 예측된다. 본 논문에서는 스마트홈 응용 서비스와 스마트홈 사용자 보안 및 프라이버시에 관련된 스마트홈 플랫폼 기반 연구 동향을 보고한다. 최근 10년간 수행된 선행연구 사례 조사를 통해 데이터 수집, 지능형 추론, 제어/상호작용 기술에 대한 분류와 보안 및 프라이버시 주요 염려사항을 분류하였고, 이를 통해 데이터 기반 미래 스마트홈 플랫폼의 연구 방향을 제시하고자 한다.

1. 서 론

스마트홈은 주거 환경내에 사물 인터넷(IoT)과 인공지능(AI) 기능이 탑재된 가전 제품 및 가정 설비를 통해 거주자에게 다양한 서비스 및 정보를 제공하여 생활의 질을 높여주는 시스템을 의미한다. IoT 기기의 상용화 및 보급 확대로 인해 가정 내의 가전 등을 네트워크를 통해 연결하고 스마트폰, 스마트 스피커, 월 패드 등으로 제어하는 스마트홈이 통신 서비스/기기 회사 주도로 보급되고 있다. 국내 스마트홈 시장은 전년도 대비 2020년에 약 10.4% 성장한 것으로 추정되며, 2025년까지 연평균 8.4%의 성장세가 예상된다[1].

한편, 최근 코로나 19 인해 가정에 있는 시간이 증가함에 따라 비대면 서비스에 대한 관심이 증대되었으며, 사무실로써의 가정 (재택 근무), 학교/학원으로써의 가정 (원격 수업, 홈스쿨링), 건강 증진을 위한 가정 (원격 의료, 예방 의료) 등으로 가정의 역할이 확대되고 있다. 따라서, 미래 스마트홈은 기존의 단순 주거 환경 모니터링 및 원격 가전 제어를 넘어, 원격 교육, 건강 관리, 가사 노동 저감, 재택 근무 등 미래 가정의 다양한 가능성을 반영할 수 있는 스마트홈 플랫폼으로써 설계될 필요가 크다.[1]

미래 스마트홈 플랫폼의 방향을 제시하고자 과거 선행연구 사례를 조사하였다. 센서 네트워크 및 사물 인터넷을 활용하여 다차원 데이터를 수집/분석하고 사용자에게 다양한 모달리티로 서비스를 제공할 수 있는 플랫폼 기반 논의하고자 스마트홈의 구성 요소, 관련 기술 및 응용 서비스들에 대한 선행연구를 분석했다. 또한, 스마트홈 환경에서 개인 정보 생성 및 공유 과정을 통해 발생할 수 있는 보안/프라이버시 쟁점 탐색을 하였다.

* 이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원(2020R1A4A1018774)과 KAIST-KU 공동연구센터, KAIST 미래 스마트홈 연구센터의 지원을 받아 수행된 연구임.

2. 스마트홈 응용 서비스 사례 및 요소 기술

주요 키워드(smart home, sensing, application)를 활용하여 최근 10년간 출판된 대표 논문 20편을 선별한 뒤 스마트홈 분야 응용 서비스 종류 및 관련 기술을 파악하였다. 응용 서비스를 구조적으로 분석하기 위해 (1) IoT/센서 및 기기를 활용한 센싱, (2) 취득 정보 분석 및 의사 결정을 위한 인텔리전스, (3) 기기 조작 및 서비스 전달을 위한 제어/상호 작용으로 그림 1과 같이 분류하였다.

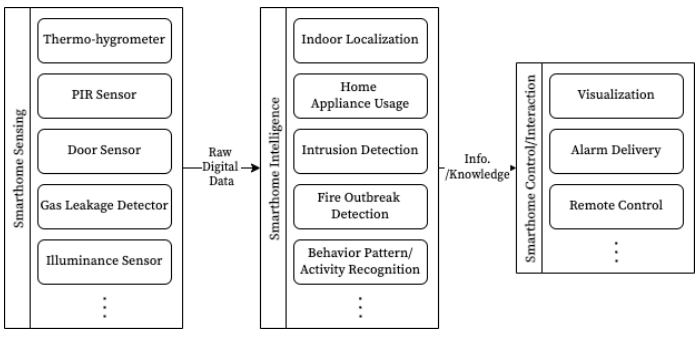

그림 1. 스마트홈 응용 서비스의 기능적 구성

기존 스마트홈 관련 연구에서 주로 연구된 지능형 서비스는 크게 (1) 스마트홈 환경 관리 및 (2) 거주자 행동 인식으로 나눌 수 있다.

스마트홈 환경 관리는 가정 내 에너지 관리와 안전 및 위험 감지 관련 연구로 이루어진다. 에너지 관리 분야는 주로 가정 내 전기 사용량과 가스 사용량을 주기적으로 점검하고 거주자에게 알림을 제공하는 서비스와, 가전 기기의 효율적인 사용을 위해 특정 상태에 따른 가전 기기 제어의 자동화 서비스로 구성된다[2]. 안전 및 위험 감지 분야는 집 안에서 발생 가능한 화재나 가스 누출과 같은 위험 요인을 감지하고 거주자에게 알림을 주는 서비스로 구성되어 있다[3].

행동 인식 관련 서비스에 대해서는 가정 내 방범/보안과 이상 행동 패턴 감지(예: 낙상 등) 연구가 수행되었다. 방범 및 보안 분야는 출입문 또는 창문 근처의 이상 접근 또는 행동을 감지하고 내부 침입 시도에 대해 거주자에게 알림을 주는 서비스를 제공한다[4]. 이상 행동 패턴 감지 분야에서는 거주자의 실내 위치 및 움직임과 가전 기기 사용 여부를 알아내고 평소와 다른 행동 패턴 감지를 통해 거주자의 건강 상태를 파악하고 도움이 필요한 경우 외부기관 또는 간병인에게 알려주는 서비스가 주로 활용된다[5].

2.1 스마트홈 센싱 기술

앞서 제시된 응용 서비스 분야들에서 활용된 센서는 전술한 바와 같이 가정 내 환경 요인을 측정하는 센서와 거주자의 행동 및 위치를 추정하는 센서로 나눌 수 있다. 표 1에 최근 연구에서 대표적으로 사용된 센서들을, 활용한 응용 서비스 분야에 따라 정리한 결과를 나타내었다.

표 1. 스마트홈 응용 서비스 연구에서 활용된 주요 센서

활용 센서	서비스 분야			
	에너지 관리	안전 및 위험감지	방범 및 보안	이상행동 감지
온도계	O	O		
습도계		O		
광량계	O			
전력량계	O			
수량계	O	O		
가스 누출 탐지기		O		
가스 실린더 로드셀	O			
문 개폐 감지기			O	O
근적외선 센서			O	O
초음파 센서			O	O
감압 저항계			O	O
IP 카메라				O
웨어러블 센서				O

2.2 스마트홈 인텔리전스 기술

스마트홈 내에서 IoT 센서/기기로부터 취득한 가정 내 환경 및 거주자에 대한 데이터를 분석하여 의미 있는 정보를 생성하기 위해, 단일 센서 데이터 또는 복합적인 이종 센서 데이터가 활용되고 있다. 온도, 습도, 전력량 등의 환경 요인에 대한 데이터는 별도의 가공 없이 그대로 사용되고 있다. 반면, 화재 및 가스 누출 가능성, 외부 침입 시도 여부 및 침입에 취약한 상황, 거주자의 실내 위치, 가전 기기의 사용 여부 및 사용 패턴과 거주자의 일상 및 비일상 행동을 파악하는 데에는 여러 개의 센서 데이터의 복합적인 분석을 통해 정보를 도출하고자 하고 있다.

2.3 스마트홈 제어 및 상호 작용 기술

스마트홈 응용 서비스의 마지막 요소는, 센싱 및 인텔리전스를 통해 얻어진 정보를 활용하여 스마트홈의 상태를 변경하거나 거주자와 상호 작용하는 것이다. 조사된 연구들에서는 대표적으로 데이터 가시화, 알림 전달, 가전 원격 제어의 방식을 통해 응용 서비스가 제공되었다. 데이터를 웹, 모바일 앱, 홈 패널 등에 시각화 하거나, 특정 상황 발생 시 가전 기기의 상태를 자동으로 변화시키고, 경보기 또는 문자 및 전화 등을 통해 거주자와 간병인 및 외부 기관에 알림을 전달하는 형태가 주로 활용되고 있다.

3. 스마트홈 사용자 보안/프라이버시 이슈

스마트홈에서는 집안에 다양한 IoT/스마트홈 센서/기기가 홈네트워크로 연결되어 있다. 이로 인한 생활의 편의 증대 등 많은 이점이 있는 반면 홈 네트워크에 연결된 기기가 증가함에 따라 사용자의 데이터 보안 및 프라이버시 측면에서 취약점이 증가하고 있는 실정이다.

기존 스마트홈 보안 관련 연구는 주로 스마트홈 내에 발생할 수 있는 물리적 보안 및 프라이버시 위협 사항(예. 가택 침입)에 대한 탐색과 이를 조치하기 위한 개발자/연구자 중심의 보안/프라이버시 시스템 제언에 중점을 두고 있다. 스마트홈 사용자 보안 및 프라이버시 이슈를 알아보기 위하여 본 연구에서는 관련 주요 키워드 (user, privacy, smarthome)를 활용하여 최근 10년간 인간-컴퓨터 상호작용 분야 학술지에서 출판된 대표 연구 30편을 선별하여 사용자 중심 스마트홈 연구에서 도출된 사용자 보안 및 프라이버시 염려사항에 대하여 다음과 같이 정리하였다.

사생활 감시 사용자들로부터 자주 언급된 염려사항 중 하나는 스마트홈 기기를 매개로 한 불법 촬영 혹은 도청을 통한 사용자의 생활 모습 감시였다. 사용자들은 스마트 카메라/디스플레이에 내장된 카메라가 본인을 실시간으로 찍고 있다는 생각에 불쾌감을 표현했으며, 스마트홈 내 특정 장소 (예. 침실, 욕실 등)에 카메라를 비치하는 것에 우려를 표시했다. 또한 스마트 스피커의 경우 사용자의 사적인 대화 내역 도청을 통한 개인 사생활 유추 등에 대한 염려사항도 자주 언급이 되는 것으로 나타났다[6].

개인정보 유출 개인정보에 대한 원치 않는 접근 및 공유로 인한 개인정보 유출 역시 염려사항으로 보고되었다. 최근 한 연구에서 구글 홈 미니 사용자는 비밀번호 해킹을 통한 연동

기기 정보 및 본인의 사생활이 담긴 영상이 유출되는 것에 대해 불쾌감을 표하며, 스마트홈 기기 설치 자체가 꺼려진다고 응답했다. 특히 홈 어시스턴트와 같은 스마트홈 기기 비밀번호 설정의 경우 최초 설정 시 사용의 용이성을 위해 스마트홈 환경 내 다른 기기 및 다양한 소셜 네트워크 등과 연동이 되는 경우가 많고, 데이터 수집 철회가 어렵기 때문에 개인정보 유출이 용이하다는 사용자들의 우려사항이 보고되었다. 사용자들은 앞서 언급된 이유 등으로 인하여 사용자가 기기 개인정보 관련 재설정에 귀찮음을 느끼고, 기존의 설정을 유지하게 됨으로 인해 궁극적으로 스마트홈 기기 사용을 비롯한 전반적인 홈 시스템 보안의 취약성을 가져오게 된다는 사용자 응답이 보고된 바 있다[7].

개인정보 제3자 공유 개인정보가 공유되는 제3자의 주체에 따라서도 사용자들의 스마트홈 프라이버시 및 보안의 염려사항 및 정도가 달라지는 것으로 나타났다. 스마트홈 데이터가 공유되는 제3자는 크게 제조사, 광고 관계자, 인터넷 서비스 제공자, 정부 등이 있다. 사용자들은 대체적으로 제조사가 개인의 스마트 기기에 갖는 접근 권한에 대해 불편함을 느끼지 않았으며, 상품 및 제공 서비스 발전을 위한 연구로 본인들의 기기 사용 데이터가 익명으로 활용된다는 전제 하에 우호적인 반응을 보였다. 그러나 본인의 데이터의 활용처에 대한 명확한 고지 없이 광고에 활용되는 것에 거부감을 보였으며, 인터넷 서비스 제공자나 정부가 본인들의 스마트홈 데이터에 접근 권한을 갖는 것에 대해서는 사용자의 생활 감시 등의 이유로 불쾌감을 느꼈다[8].

스마트홈 구성원 간 사생활 침해 갈등 다양한 구성원이 함께 거주하는 다중 사용자 기반 스마트홈 환경의 경우 스마트 기기 공동 사용으로 인해 발생하는 사생활 침해 관련 이슈가 하나의 염려사항으로 언급되었다. 그 예로 부모와 자녀가 함께 스마트홈 기기를 공유하는 경우, 자녀의 사용 기록에 대한 부모의 접근 시도 및 감시 등이 사생활 침해 이슈로 제시되었다. 그 외에도 스마트홈을 비롯하여 스마트 기기에 대한 배경지식이 상대적으로 많은 사용자가 스마트홈 기기에 대한 주도권을 가지면서 발생하는 사용자간 갈등 등 관계의 역학에서 발생하는 사생활 침해 문제가 하나의 염려사항으로 보고되었다[9].

4. 시사점 및 향후 전망

본 논문에서는 사물인터넷(IoT) 기반 스마트홈 최근 기술 동향 및 프라이버시 이슈에 대하여 알아보았다. 기존 응용 서비스 연구에서는 주로 스마트홈 환경 요인 또는 거주자의 물리적인 행동에 대한 데이터를 기반으로 1차원적인 분석 및 이해를 통해 단순한 정보 전달 또는 원격 제어 및 자동화와 같은 단방향의 제어 및 상호작용 방식만 고려되어 있음을 확인했다. 따라서, 미래 스마트홈 플랫폼에는 스마트홈 환경 내 센서뿐만 아니라 개인 스마트 기기로부터 생성되는 다양한 디지털 데이터의 통합적인 수집과 거주자 및 관련 맥락을 모두 아우르는 분석이 필요하며, 이러한 과정에서 스마트홈과 거주자 간의 동적인 관계 변화도 고려할 수 있을 것으로 보인다. 또한 스마트홈과 거주자 간의 상호작용이 발생하는 조건 및 상황의 다양성에 대해서도 고려되어야 한다. 사용자 보안 및 프라이버시의 경우 기존의 단일 기기에 집중된 사용자 보안/프라이버시 연구에서 벗어나 다양한 IoT 기기 및 스마트홈 센서에 따른 사용자들의 데이터 수집 및 공유 민감도 등에 대한 다각적인 연구가 수행될 필요가 있다.

선행연구 사례 분석을 통해서 미래 스마트홈은 수많은 데이터가 생성 및 공유되는 데이터 집중적인 스마트홈 플랫폼(Data Intensive Smarthome Platform)이 진화할 것으로 기대된다. 다중 센서 및 사물 인터넷(IoT)을 활용하여 다차원 데이터를 수집 및 분석하고 이를 바탕으로 스마트홈과 거주자 간의 양방향 상호작용을 고려하는 서비스가 활성화될 것이다. 스마트 가전, 인공지능 비서 및 로봇 등을 활용해 사용자에게 선제적인 서비스를 다양한 모달리티로 제공할 수 있는 서비스 연구에 대한 논의가 활발해 질것으로 예상된다. 또한, 기존의 플랫폼 제공자 주도의 보안 및 프라이버시 관리에서 사용자와 협업하여 보안과 프라이버시를 관리하는 사용자 친화적 보안 및 프라이버시 위주의 패러다임 전환이 필요하다.

참 고 문 헌

[1] 한국스마트홈산업협회, 국내 스마트홈 산업 동향조사 보고서, 한국스마트홈산업협회, 2021

[2] Singh, Himanshu, et al. "IoT based smart home automation system using sensor node." 4th International Conference on Recent Advances in Information Technology (RAIT). IEEE, pp. 1-5. 2018.

[3] Ransing, Rasika S., and Manita Rajput. "Smart home for elderly care, based on Wireless Sensor Network." International Conference on Nascent Technologies in the Engineering Field (ICNTE). IEEE, pp.1-5. 2015.

[4] Jose, Arun Cyril, and Reza Malekian. "Improving smart home security: Integrating logical sensing into smart home." IEEE Sensors Journal 17(13), pp. 4269-4286. 2017.

[5] Basu, Debraj, et al. "Wireless sensor network based smart home: Sensor selection, deployment and monitoring." IEEE Sensors Applications Symposium Proceedings. 2013.

[6] Abdi, Noura, et al. "Privacy norms for smart home personal assistants." ACM CHI conference on human factors in computing systems. 2021.

[7] Bahirat, Paritoshet al. "Overlooking Context: How do Defaults and Framing Reduce Deliberation in Smart Home Privacy Decision-Making?." ACM CHI conference on human factors in computing systems. 2021.

[8] Zheng, Serena, et al. "User perceptions of smart home IoT privacy." Proceedings of the ACM on human-computer interaction 2.CSCW, pp. 1-20. 2018.

[9] Cobb, Camille, et al. ""I would have to evaluate their objections": Privacy tensions between smart home device owners and incidental users." Proceedings on Privacy Enhancing Technologies, 4, pp. 54-75. 2021.