스마트홈 네트워크에서 댁내 인증서 기반의 IoT 디바이스 상호인증 방안

안희성*, 지은화*, 서창호**, 신용태*
*숭실대학교 컴퓨터학과
**공주대학교 응용수학과
{ralra876,ewjhee}@naver.com* chseo@kongju.ac.kr** shin@ssu.ac.kr*

Mutual Authentication based on Home-certificate among IoT Devices in the Smart Home Network

Hee-Sung Ahn*, Eun-Wha Jhee*, Chang-Ho Seo**, Yong-Tae Shin*
*Dept of Computer, Soong-Sil University
**Dept of Applied Mathematics, Kong-Ju University

요 약

IoT 디바이스의 범위와 서비스 시장의 확산과 함께, 스마트홈 환경에서 사용되는 디바이스의 종류도 점점 증가하고 있다. 이에 따라 IoT 디바이스의 제어 및 관리의 관점에서 사용자 도용, 불법적인 접근 같이 다양한 보안 위협도 고려해야 한다. 이러한 위협으로 인해 스마트홈 내 디바이스 간의 신뢰적인 인증이 필수적으로 갖춰야할 요구사항이 되었다. 즉, 스마트홈 내에서 유효한 권한을 가진 디바이스의 접근만을 허용하여 안전한 서비스를 제공해야 한다. 본 논문에서는 스마트홈 네트워크 환경에서 IoT 디바이스 간 신뢰적으로 통신할 수 있도록, 댁내 인증서 기반의 디바이스 등록 및 인증서 발급 절차와 디바이스 인증 및 서비스 제공 절차를 통한 IoT 디바이스 상호 인증 방안을 제안한다.

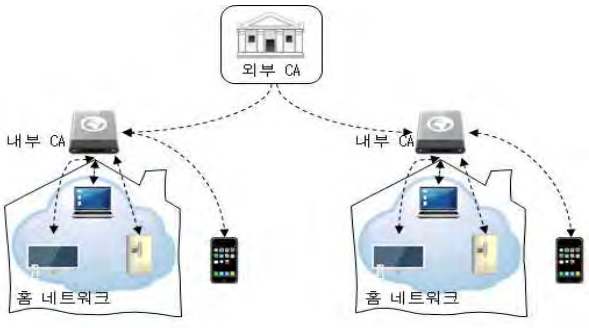
1. 서론

사물지능통신 기술인 사물인터넷(IoT, Internet of Things)이 사람과 사물, 사물과 사물 간에 정보를 교류하고 상호 소통하는 지능형 인프라를 가진 미래 인터넷 기술로 부각되고 있다. 특히, 생활 및 가전 관련 디바이스들이 네트워크로 연결되어 시간과 장소에 구애받지 않고 사람과 자연스러운 작용을 통해 생활의 편의를 극대화하는 스마트홈 환경이 사물인터넷의 주요 서비스 중 하나로 연구되고 있다. 따라서 스마트홈 네트워크에 접근하는 디바이스의 진위성 확인 및 인증이 중요한 보안 요소로 작용한다. 비(非)인가된 사용자 혹은 디바이스를 통해 스마트홈 서비스가 제공될 경우, 불법적인 접근을 통한 정보 유출, 정상 서비스 이용 방해 등의 형태로 서비스의 안정성에 직접적인 위협 및 피해를 유발할 수 있다[1]. 이에 본 논문에서는 스마트홈 네트워크 환경에서 디바이스 사용자 및 디바이스 등록을 바탕으로 IoT 디바이스 간 신뢰성을 확보하여 안전한 통신을 할 수 있는 댁내 인증서 기반의 상호인증 기법을 제안한다.

2. 관련연구

2.1 댁내 인증서 기반의 홈 디바이스 인증 체계

홈 네트워크에서의 댁내 인증서 기반의 홈 디바이스 인증 체계란 [그림1]과 같이 보안 홈 게이트웨이가 댁내의 모든 디바이스들에게 인증서를 발급하는 CA의 역할을 하는 것이다. 이때 보안 홈 게이트웨이는 end-entity 디바이스 인증서를 발급하기 위해서 self-sign 인증서를 발행하여야 하고, 또한 외부 CA로부터 자신의 인증서를 발급받아야 한다. 이 홈 게이트웨이 인증서는 홈 게이트웨이와 홈 네트워크 서비스 제공사업자 사이의 인증에 사용된다[2]. 디바이스를 위한 인증서는 x.509 인증서를 따른다.



(그림 1) 댁내 인증서 기반 홈 네트워크 인증 체계

2.2 지문 인증 시스템

홈 네트워크 사용에 있어 정당한 사용자임을 확인을 위하여 디바이스에 입력된 사용자의 입력 정보와 로컬 컴퓨

이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2012-0029927)

터 혹은 호스트 컴퓨터에 미리 등록되어 보관중인 사용자의 정보를 상호 비교하여 일치 혹은 불일치를 결정하는 것을 말한다[3]. 지문이 타인과 동일한 패턴을 가질 확률은 10억분의 1이다. 이러한 특징은 인증 체계에서 사용자 도용 등의 불법적인 접근으로 인한 피해를 막아 신뢰성과 안전성을 높이는 인증 방법이 될 수 있다.

3. 본론

본 논문에서는 선행기술인 댁내 인증서 기반의 홈 디바이스 인증 체계를 토대로, 스마트홈 네트워크 환경에서 사용할 IoT 디바이스에 대하여 (1) 디바이스 등록 및 인증서 발급 절차와 (2) 디바이스 인증 및 서비스 제공 절차로 구분하여 제안한다. 정당한 디바이스 사용자에 대한 사용자 인증을 위하여 HS(Home Server)에는 사용자의 지문 등록이 완료되어 있음을 전제로 한다. HS에 등록되어 있는 지문 정보는 스마트홈 내의 IoT 디바이스들을 제어 및 관리할 수 있는 메인 디바이스(MD)에 대하여 등록 및 인증을 시도할 때 사용한다.

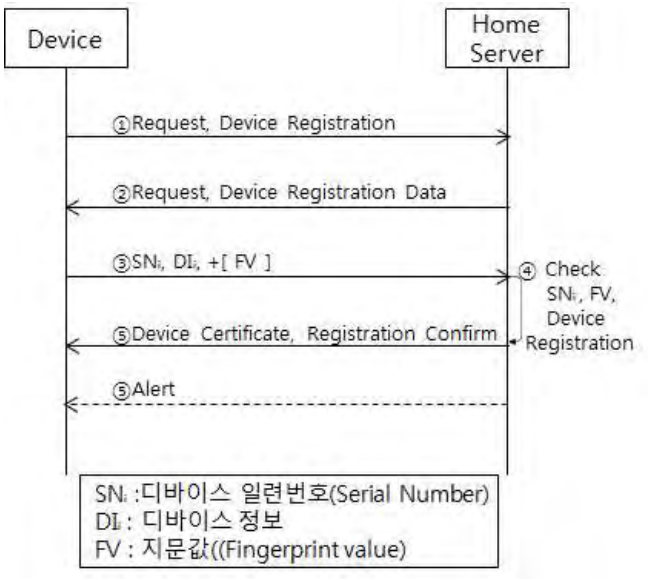
3.1 디바이스 등록 및 인증서 발급 절차

디바이스 등록 및 인증서 발급 절차는 사용자의 스마트홈 네트워크 내에 사용되는 모든 IoT 디바이스를 대상으로 한다. 이 과정에서 디바이스는 일련번호(SN, Serial Number)와 디바이스 정보(DI, Device Information)를 HS에 전송하고, MD로의 등록을 원하는 경우 사용자의 지문 정보를 추가로 전송한다. 디바이스가 HS에게 보낸 정보에 대하여, HS가 검증 후 해당 디바이스의 등록 여부를 결정한다. MD로 등록할 IoT 디바이스는 지문 인식 시스템이 탑재되어 있어야 한다.

① IoT 디바이스가 HS로 디바이스 등록 요청 메시지를 보낸다. ② 이 메시지를 받은 HS는 홈 네트워크용 IoT 디바이스임을 확인하기 위한 데이터를 디바이스에게 요청한다. ③ 이를 받은 IoT 디바이스는 디바이스 일련번호와 디바이스 정보를 전송하고, MD 등록 요청일 경우 탑재된 지문 인식 시스템을 통해서 추출한 지문값을 HS에 추가로 전송한다. ④ HS는 디바이스 일련번호의 적합성이 확인 되면 디바이스 등록을 한다. 지문값을 같이 전송받은 경우에는 디바이스 일련번호 확인 후, HS에 저장되어 있는 지문값과 동일한 지문인지 검증한다. 확인이 완료되면 사용자의 스마트홈 MD로 등록한다. 단, MD가 이미 등록되어 있는 경우에는 사용자는 MD의 변경을 선택할 수 있다. ⑤ 디바이스 등록을 성공한 경우, HS는 디바이스 인증서와 등록 완료 확인 메시지를 IoT 디바이스로 보낸다. 디바이스 등록 실패 시 IoT 디바이스로 경고 메시지를 보낸다.

3.2 디바이스 인증 및 서비스 제공 절차

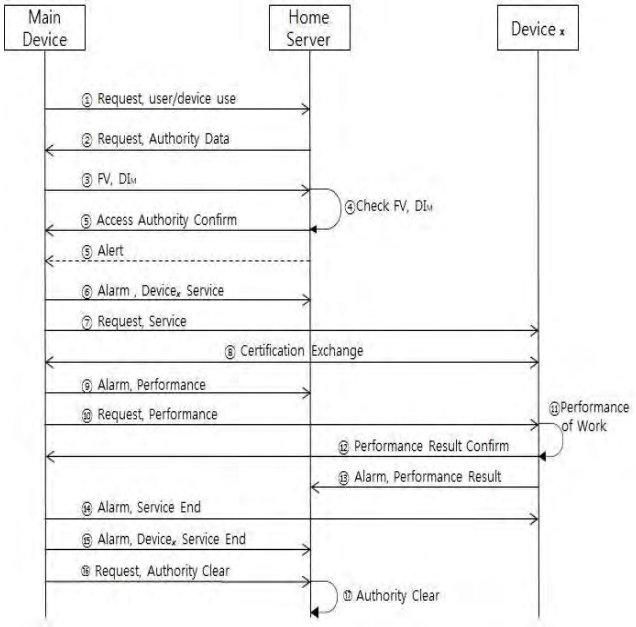
시간 및 공간에 관계없이 IoT 디바이스를 사용하기 위하여 홈 서버와 사용자 간의 인증, 사용자와 디바이스 간의 인증, 디바이스와 디바이스의 인증이 필요하다. MD를 통한 지문 인증을 사용하면 홈 서버와 사용자 간의 인증, 사용자와 디바이스간의 인증이 한 번의 절차로 처리된다.



(그림 2) 디바이스 등록 및 인증서 발급 절차

① MD는 HS로 서비스 사용을 위한 인증 요청 메시지를 보낸다. ② 이 메시지를 받은 HS는 정당한 사용자 및 디바이스 확인을 위한 데이터를 MD에게 요청한다. ③ 이를 받은 MD는 디바이스 정보와 지문을 추출하여 지문값을 HS로 전송한다. ④ HS는 이 지문값을 사전에 저장되어 있는 지문값과 동일한 값인지 비교 검증한다. 지문의 유효성이 검증되면 MD는 HS에 등록된 모든 디바이스에 대한 접근권한을 가지게 된다. ⑤ HS는 MD의 접근권한이 유효하면 권한 획득 확인 메시지를 MD에게 전송하고 지문 검증 실패 시 경고 메시지를 MD에게 전송한다. ⑥ MD는 Device1에게 서비스 요청을 시작하기에 앞서 HS에게 서비스 시작 알람 메시지를 보낸다. MD가 Device1 이외의 다른 디바이스에게 서비스를 취하려는 경우, 이 과정부터 다시 진행된다. ⑦ MD는 Device1에게 서비스 시작 요청 메시지를 보낸다. ⑧ Device1은 MD의 서비스 요청을 받아들이기 전 각자의 디바이스 인증서를 상호 교환하여 서로 정당한 홈디바이스 사용임을 확인한다. ⑨ MD는 Device1에게 작업 요청을 시작하기에 앞서 HS에게 작업 알람 메시지를 보낸다. ⑩ MD는 Device1에게 처리할 내용이 담긴 작업 요청 메시지를 보낸다. ⑪ Device1은 작업 메시지 확인 후, 작업을 실행한다. ⑫ Device1은 작업 종료 후 MD에게 작업 결과 확인 메시지를 전송한다. ⑬ Device1은 HS에게 작업 결과 알람 메시지를 전송한다. ⑭ MD는 Device1에서 더 이상 수행할 서비스가 없으면 Device1에게 서비스 종료 알람 메시지를 보낸다. ⑮ MD는 HS에게 Device1의 서비스 완료 알람 메시지를 보낸다.

⑯ MD는 다른 디바이스 사용 여부가 없으면, HS에게 접근권한 해제를 요청한다. ⑰ 이를 받은 HS는 MD에게 부여한 접근권한을 해제한다.



(그림 3) 디바이스 인증 및 서비스 제공 절차

4. 안전성 분석

제안하는 IoT 디바이스 상호 인증 방안은 다음과 같은 이점을 도출할 수 있다. 스마트홈 네트워크에서 시간 및 공간의 제약 없이 IoT 디바이스를 사용하기 위해서는 홈 서버와 사용자 간의 인증, 사용자와 디바이스 간의 인증, 디바이스와 디바이스의 인증이 필요하다. MD를 통한 지문 인증을 사용하면 홈 서버와 사용자 간의 인증, 사용자와 디바이스간의 인증이 한 번의 절차로 처리할 수 있어서 사용자에게 편리성을 제공한다. 사용자의 유일무이한 지문 정보를 통해 정당한 디바이스 사용자 이외의 불허가된 디바이스 사용자의 접근을 차단할 수 있다.

또한 인증서 기반 상호인증 체계 방안을 사용함으로서 스마트홈 네트워크에 접근하는 디바이스 간의 통신 체제에 안전성을 제공한다. HS로부터 각 디바이스에 부여된 인증서를 바탕으로 정당한 디바이스간의 전송된 메시지는 부인방지 및 메시지 위/변조 여부를 검증할 수 있다. 또한 MD와 스마트홈 네트워크를 사용하는 타 디바이스 간 직접 통신과 동시에 HS를 중심으로 인증 및 처리 메시지가 저장되므로 차후 디바이스에 대한 사이버 공격으로 부터의 분석이 용이하다.

5. 결론

다양한 IoT 디바이스의 확산으로 스마트홈 네트워크에서의 보안이 중요시 되고 있다. 특히, 디바이스 사용자 및 디바이스의 식별과 인증이 편리하고 안전하게 이루어지는 기술이 필수적으로 요구되어진다. 본 논문에서는 댁내 인증서 기반 기술을 응용하여, 디바이스 등록 및 인증서 발급 절차와 디바이스 인증 및 서비스 제공 절차를 통한 신뢰할 수 있는 IoT 디바이스 상호인증 방안을 제안하였다. 이러한 제안은 스마트홈 디바이스 인증 체계에 편의성과 보안성을 제공할 수 있다. 그러나 디바이스 인증 체계에서 보안에 대한 위협은 점점 더 발전하고 있으며, 특히 디바이스 간의 통신에 의한 정보 유출 피해가 증가하고 있다. 이에 대한 강력한 암호화 알고리즘 마련이 필요하며, 향후 이를 고려한 연구를 추가할 예정이다.

참고문헌

[1] 박정효. "ICT 기기인증 보안기술 현황", 한국통신학회지 (정보와통신), vol.31, no.5, pp.20-26, 2014.

[2] 이덕규, 김도우, 한종욱. "홈네트워크 보안 기술 및 표준화 동향", 전자통신동향분석, vol.23, no.4, pp.89-101, 2008.

[3] A. Jain, L. Hong, R. Bolle, "On-line fingerprint verification", IEEE Trans. Pattern Analysis and Machine Intell, vol.19, no.4, pp.302-314, 1997.

[4] 노태헌, 이윤석, 전하용, 정민수. "홈 네트워크에서의 디바이스 인증기법에 관한 연구", 한국멀티미디어학회 학술발표논문집, pp.559-562, 2008.

[5] 심성구, 박호진, 박준희. "스마트홈 표준화 현황 및 추진전략", 정보과학회지, vol.30, no.8, pp.19-25, 2012.

[6] 이덕규, 김도우, 한종욱. "홈네트워크 보안 기술 및 표준화 동향", 전자통신동향분석, vol.23, no.4, pp.89-101, 2008.

[7] 전종암, 김내수, 고정길, 박태준, 강호용, 표철식. "IoT 디바이스 제품 및 기술 동향", 한국통신학회지 (정보와통신), vol.3, no.4, pp.44-52, 2014.

[8] 박지예, 강남희. "안전한 WEB of Things 응용을 위한 개체 인증 기술", 한국통신학회논문지, vol.38, no.5, pp.394-400, 2013.