클라우드 컴퓨팅 기반 사물인터넷의 안전성 향상을 위한 보안요구사항 분석

김득훈*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail: dh_kim@sch.ac.kr

Analysis of Security Requirements for Improving Secure in IoT based on Cloud Computing

Deuk-Hun Kim*, Jin Kwak**
*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University.
**Department of Information Security Engineering, Soonchunhyang University.

요 약

정보통신기술(ICT)의 발전으로 사람 간의 통신에서 모든 사물들과 상호 통신으로 확장된 사물인터넷 환경이 이슈화되고 있다. 또한, 사물인터넷 환경은 기존의 데이터량보다 사용되는 데이터량이 크기 때문에 클라우드 컴퓨팅 기술을 기반으로 데이터를 처리 및 관리한다. 그러나 클라우드 기반 사물인터넷은 다양한 영역에서 여러 통신기술이 복합적으로 구성되므로 사용자의 정보가 노출될 위험이 높다. 따라서 클라우드 기반 사물인터넷 환경의 보안 위협을 분석하고 보안요구사항을 도출하여 안전성을 향상시키고자 한다.

1. 서론

최근 ICT(Internet Communication Technology)가 발전하면서 통신의 주체가 모든 사물로 확대되는 초연결사회로 변화하고 있다. 이에 따라 사용자는 시·공간 제약 없이 정보와 지식을 통하여 새로운 가치 창출을 할 수 있게 되었으며, 이를 실현하기 위한 기술로써 사물인터넷(IoT : Internet of Things)이 주목받고 있다[1]. 따라서 사물인터넷 서비스에 필요한 요소 기술로 단말과 센서, 네트워크, 서비스 플랫폼, 빅데이터 처리, 보안과 프라이버시 보호 기술 등 다양한 기술이 연구되고 있다[2]. 특히 사물인터넷은 모든 사물이 센서를 내장하고 있으며, 네트워크를 통해 센싱되는 데이터를 처리하는데 사용되는 데이터량이 크기 때문에 가상화된 자원을 이용하는 클라우드 컴퓨팅 기반의 데이터 관리 기법에 대한 연구가 필요하다. 그러나 사물인터넷은 사용자가 센서를 통해 단말과 정보를 상호 소통하므로 사용자의 정보가 노출되기 쉽다. 또한, 사물인터넷은 여러 기술들이 복합적으로 상호 연동되어 이루어짐에 따라 다양한 환경에서 사용자의 정보를 목표로 공격하는 보안 위협이 존재할 수 있다. 따라서 클라우드 컴퓨팅 기반의 사물인터넷을 이용하는 사용자의 정보를 보호하기 위해서 각 환경에서 발생할 수 있는 보안 위협을 분석하고, 이를 방지하기 위한 보안요구사항을 도출하여 안전성을 향상시켜야 한다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구를 통해 사물인터넷과 클라우드 컴퓨팅의 개념을 살펴보고, 3장에서 각 환경의 보안 위협을 분석한다. 4장에서는 보안요구사항을 도출하고, 5장에서 결론을 맺는다.

2. 관련 연구

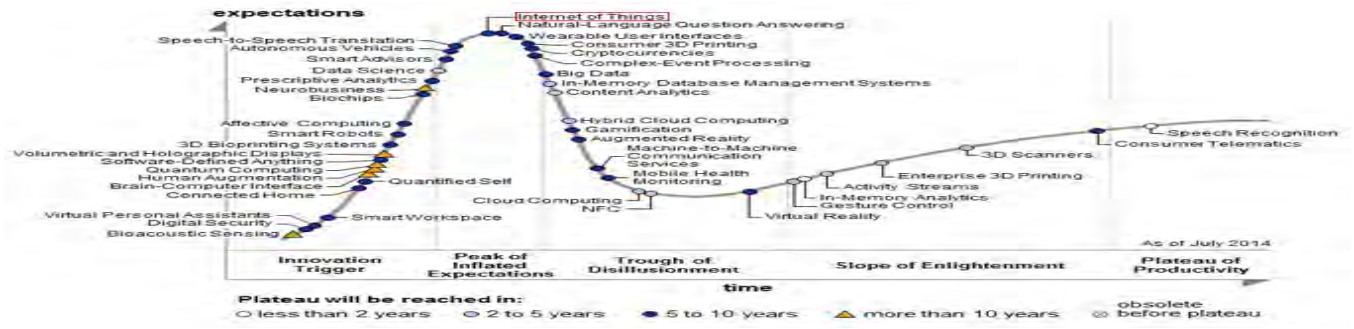
2.1 사물인터넷

사물인터넷은 ICT를 기반으로 모든 사물을 유·무선 네트워크로 연결하여 사람-사물, 사물-사물 간의 정보를 상호 소통하는 지능형 환경이다. 최근 미국에서 개최된 CES 2014[1]에서 사물인터넷과 관련된 제품이 주가 되어 전시되는 등 사물인터넷에 대한 관심이 높아지고 있다. 미국의 시장조사 전문기관 가트너(Gartner)는 현재 관심이 고조되어있는 기술의 최상위 분야로 사물인터넷을 선정하였다. (그림 1)은 가트너가 예측한 미래 전망을 나타내며 해당 서비스의 기술이 연구 및 발전하는데 5~10년 정도 걸릴 것으로 예측하였다[3].

사물인터넷은 큰 범주로 디바이스(단말/센서) 영역, 네트워크(유/무선) 영역, 서비스 인터페이스(플랫폼/애플리케이션) 영역으로 구분 가능하다. (그림 2)는 사물인터넷의

이 논문은 2014년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2012R1A2A2A01010886).

1) CES(Consumer Electronics Show) : 미국가전협회(CEA : Consumer Electronics Association)의 주관으로 개최되는 세계 최대 규모의 가전제품 박람회



(그림 1) Gartner Hype Cycle 2014

영역과 세부 구성 요소를 나타낸다. 각 영역별 역할은 다음과 같다[1].

(그림 2) 사물인터넷 영역 및 구성 요소

❑ 디바이스 영역

디바이스(단말/센서) 영역은 사물에 내장된 통신기능을 이용하여 특정 사물에서 수집 및 추출한 데이터를 다른 사물 또는 데이터 가공 및 처리기능을 담당하는 게이트웨이로 전송하는 역할을 수행한다.

❑ 네트워크 영역

네트워크(유/무선) 영역은 사람-사물, 사물-사물 간 전송되는 데이터를 송수신하는 유선 및 무선 통로의 역할을 수행한다. 사물인터넷 환경의 대용량 트래픽 처리와 통신의 효율성 및 네트워크 관리를 위한 기술들이 접목되어 있다.

❑ 서비스 인터페이스 영역

서비스 인터페이스(플랫폼/애플리케이션) 영역은 수집된 데이터를 가공·추출·처리하여 사용자가 인식하고 판단할 수 있도록 정보를 생성하며, 사물인터넷을 이용하는 다양한 디바이스를 제어 및 관리하는 역할을 수행한다.

2.2 클라우드 컴퓨팅

클라우드 컴퓨팅은 사용자에게 일정한 비용을 받고, 가상화 기술을 이용하여 ICT 디바이스 자원을 관리 및 제공하는 서비스로써 사용자는 자신의 정보를 언제, 어디서든 클라우드 서버에 저장하고 이용할 수 있다. 특히, 사물인터넷 서비스에서 사용되는 대용량의 정보를 저장 및 관리하는 기술에 유용하게 활용될 수 있다. 이에 따라 구글 및 애플 등의 다양한 기업들이 클라우드 컴퓨팅 기반의 사물인터넷 기술 개발을 진행하고 있다.

대표적으로 구글과 애플의 기술들은 다음과 같다[4][5].

❑ 구글 네스트

구글은 클라우드 기반의 네스트(Nest) 플랫폼을 이용하여 모바일·자동차·TV·웨어러블 디바이스 및 각종 센서의 연결을 지원하고 제어 및 관리하기 위하여 연구중이다. 또한, 네스트와 호환되는 다양한 센서 및 디바이스의 데이터를 클라우드 컴퓨팅을 이용하여 동기화하고 실시간으로 제공한다.

❑ 애플 홈킷

애플은 사물인터넷 환경의 스마트홈 구축을 위하여 홈킷(HomeKit)을 발표했다. 즉, 가정 내부의 다양한 전자기기를 아이폰·아이패드 등과 호환이 되도록 지원하고, 디바이스-디바이스 간의 연결을 제공한다. 또한, 애플 홈킷은 상호 연결되어있는 홈디바이스를 클라우드 기반으로 제어 및 관리한다.

3. 보안 위협

클라우드 컴퓨팅 기술에 기반하는 사물인터넷은 공격자가 다양한 영역에서 공격을 시도할 수 있으며, 이에 따라 영역별 보안 위협을 분석해야 한다. 사용자의 정보가 노출될 위협이 존재하는 영역은 크게 디바이스 영역, 네트워크 영역, 서비스 인터페이스 영역 및 클라우드 컴퓨팅 영역으로 분류할 수 있으며, 각 영역에서 발생할 수 있는 보안 위협은 [표 1]과 같다.

<표 1> 클라우드 기반 사물인터넷의 영역별 보안 위협

구 분	보안 위협
디바이스	데이터 위/변조, 정보유출, 악성코드 감염, 비인가 접근
네트워크	정보유출, 데이터 위/변조
서비스 인터페이스	데이터 위/변조, 정보유출, 악성코드 감염, 비인가 접근
클라우드 컴퓨팅	

❑ 데이터 위·변조

공격자는 클라우드 기반 사물인터넷의 모든 영역에서 사용자 정보에 대한 데이터 위/변조가 가능하다. 디바이스 영역에서는 운영체제의 취약점을 이용하여 데이터 접근권한을 획득한 후 저장·센싱 데이터를 위/변조할 수 있다. 또한, 네트워크 영역에서는 중간자 공격(Man-in-the-Middle attack)을 시도하여 각 영역에서 전송되는 데이터를 가로채고 위/변조된 데이터를 전송한다. 서비스 인터페이스와 클라우드 컴퓨팅 영역에서는 각 서비스의 API 취약점을 이용하여 사용자의 데이터가 저장된 데이터베이스에 불법접근 후 저장된 정보를 위/변조한다.

❑ 정보유출

사용자가 클라우드 기반 사물인터넷을 이용할 때 모든 영역에서 정보유출이 될 수 있다. 디바이스 영역에서 단말/센서를 이용하는 사용자 인증이 취약한 경우, 네트워크 영역에서 데이터를 암호화하지 않고 전송하는 경우, 서비스 인터페이스와 클라우드 컴퓨팅 영역에서는 각 영역의 플랫폼 또는 애플리케이션의 취약점을 이용하여 사용자의 정보가 외부로 유출된다. 이에 따라 사용자의 프라이버시 문제가 발생할 수 있다.

❑ 악성코드 감염

공격자는 디바이스 영역에서 운영체제의 취약점을 이용하고, 서비스 인터페이스와 클라우드 컴퓨팅 영역에서는 API 취약점을 이용하여 각 영역에 신·변종 악성코드를 삽입한다. 이를 통해서 공격자는 사물인터넷을 이용하는 사용자의 정보를 불법적으로 획득한다.

❑ 비인가 접근

공격자는 디바이스 영역에서 운영체제의 취약점을 통해 접근권한을 획득할 수 있다. 또한 서비스 인터페이스와 클라우드 컴퓨팅 영역에서 각 영역의 플랫폼 및 API 취약점을 통해 접근권한을 획득한다. 이에 따라 공격자는 인가되지 않았지만 불법적으로 사물인터넷에 접근하여 사용자의 정보를 획득한다.

4. 보안요구사항

❑ 기밀성

기밀성은 정보유출을 방지하기 위한 특성으로써 클라우드 기반 사물인터넷 환경에서 센서에 의해 센싱된 데이터 또는 디바이스의 데이터를 각 영역에 암호화하여 전송해야 한다. 또한 클라우드 컴퓨팅을 통해 데이터를 관리할 때 데이터를 암호화하여 저장해야 한다. 이때, 사물인터넷 환경의 기기 성능을 고려하여 안전성이 입증된 경량화 암호 알고리즘을 사용해야 한다.

❑ 무결성

무결성은 데이터 위/변조를 방지하기 위한 특성으로써 공격자가 악의적인 공격 기법 또는 취약점을 이용하여 데이터가 위/변조될 경우, 기존 사용자 정보의 해쉬함수 또는 MAC 코드를 이용하여 무결성 검증을 시도하고 이를 통해 사용자 정보를 보호한다.

❑ 익명성

익명성은 정보유출 시 2차 피해를 방지하기 위한 특성으로써 해당 사용자의 사물인터넷 통신 정보를 마스킹(*)하여 저장한다. 이에 따라 클라우드 기반 사물인터넷의 각 영역에서 발생하는 보안 위협으로 인해 정보가 유출될 경우 사용자의 익명성을 보장한다.

❑ 접근제어

접근제어는 비인가 접근을 방지하기 위한 특성으로써 역할 기반/상황 인식 접근제어 등의 기술을 클라우드 기반 사물인터넷에 적용하여 불법적인 접근을 차단한다.

❑ 사용자 인증

사용자 인증은 정보유출을 방지하기 위한 특성으로써 클라우드 기반 사물인터넷의 각 영역에서 정당한 사용자를 인증한다. 이때 사물인터넷 환경에 적합한 경량화 사용자 인증을 해야 한다.

❑ 운영체제 보안

운영체제 보안은 클라우드 기반 사물인터넷에서 이용되는 운영체제의 취약점을 통해 악성코드 및 접근권한 획득하고 사용자 정보를 유출하는 취약점을 방지하기 위한 특성으로써 항상 운영체제 보안 업데이트를 실시하여 사용자 정보를 보호한다.

5. 결론

사물인터넷 환경이 급속하게 발전하고 있다. 또한, 데이터량이 크기 때문에 클라우드에 기반한 사물인터넷 환경이 주목받고 있다. 특히 사용되는 정보는 사용자와 밀접한 관계가 있으므로 보안 기술을 이용하여 사용자 정보를 보호하는 것이 중요하다. 따라서 도출된 보안요구사항은 사물인터넷 보안 기술 개발에 도움이 될 것으로 기대된다.

참고문헌

[1] "2014 국가정보보호백서" 국가정보원, 미래창조과학부, 방송통신위원회, 안전행정부 저

[2] 김호원 "사물인터넷 서비스에서의 보안 이슈" 한국정보과학회 정보과학회지 제32권 제6호, 2014. 6, pp.37-41

[3] 가트너, http://www.gartner.com/

[4] 구글 네스트, https://nest.com/

[5] 애플, http://www.apple.com/