Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Study on the Internet of Things Security Outlook and Response Technology

Dong-hyuk Kim[*1], **Ki-Chul Shin**[2]

[1]*Division of Industrial Management Engineering, Hanbat National University*
[2]*Jeonbuk Regional Office, Small Business Corporation*

ABSTRACT

Internet of Things (Internet of Things: IoT) is developed for a wide range of products and services by integrating the concept of people and things. IoT service is different from the existing services because of various technological characteristics and it`s composed of complex technology elements. IoT has the strong possibility of new security vulnerabilities due to the configuration of specific services connected to the network security vulnerabilities of each element of the information processing technology itself. Therefore various security mechanisms, such as authentication / authorization mechanism and access control / authority control techniques, ID management techniques, management and key distribution scheme are required. In this paper, we looked at each security technologies for the IoT technology service configuration element to provide a safe and reliable IoT services that systematically present a security strategy for ensuring the safety of the IoT services environment.

KEYWORDS: IoT(internet of things services), Social network service, Post smartphone, ZigBee, USN (ubiquitous sensor network), PKI (public key infrastructure), SIM (subscriber identification module), M2M

ARTICLE INFO: Received 13 September 2016, Revised 7 October 2016, Accepted 7 October 2016.

[*]Corresponding author is with the Department of industrial Management Engineering, Hanbat University, 305-719, Dongseo daro-125 , Yuseong-gu Daejeon KOREA.

E-mail address: dhkim3s@hanbat.ac.kr

1. 서 론

사물인터넷(IoT)은 전등, 가전, 자동차, 헬스케어, 교량, 스마트 그리드, 지능형교통, 인간에 이르기까지 모든 것이 상호 연결될 수 있는 통신환경을 말하는 것으로, 현재 이들 장치가 사람들의 생활을 편리하게 만들어 주고 있다. 그러나 이러한 사물인터넷 환경은 해커들에게 새로운 공격 경로를 제공하고 있는 것도 사실이다.[1,2,3].

만약 사물인터넷 디바이스 수가 지속적이고 기하급수적으로 증가하여 일상생활에 더 많이 보급되고, 한편으로 가장 민감한 개인 데이터 및 주민번호와 은행정보로 접근이 가능할 경우 데이터의 기밀성 및 무결성 침해, 정보유출 등 보안 문제가 심각하게 대두될 수도 있다.[4,7].

본 논문의 구성은 다음과 같다. 2장에서 사물인터넷의 개념 및 서비스 실태에 대해서 기술하고, 3장에서는 사물인터넷의 보안 기술을 살펴본다. 4장에서는 사물인터넷 보안 전략을 제시하고, 5장에서 결론을 제시하였다.

2. 사물인터넷의 정의 및 서비스실태

2.1 사물인터넷 정의

유선 및 무선으로 언제 어디서나 연결이 가능한 스마트기기와 모든 사물들이 네트워크에 확장되어 연결됨에 따라 단시일 안에 초연결 시대가 실현될 것으로 예상되고 있다. 사물인터넷은 다음과 같이 기구별로 다양하게 정의되고 있다[11].

'국제전기통신연합(ITU)'은 언제 어디서나 어느 것과도 연결될 수 있는 새로운 통신환경으로 인간과 인간, 인간과 사물, 사물과 사물을 연결하는 '객체의 제약'을 해결하는 것이 핵심이다'고 정의하고 있다.

'유럽통신표준협회(ETSI)', '미국전기전자학회(IEEE)'는 M2M을 인간의 개입이 없는 상태에서 기기사이에서 발생하는 정보 교환으로 정의하고 있다. 그리고 '한국인터넷진흥원'은 사물인터넷 기술을 초연결사회의 기반 기술로서 사물간 인터넷 혹은 개체간 인터넷으로 정의하였고, 고유 식별이 가능한 사물이 만들어낸 정보를 인터넷을 통해 공유하는 환경이라고 정의하고 있다[11].

2.2 사물인터넷 서비스실태

사물인터넷 서비스의 활용은 냉동·냉장 창고 모니터링, 프랜차이즈 매장관리, 백신 냉장고 온도 모니터링, 스마트화분 모니터링, 무선통신 기지국 관리, 스마트 홈 게이트웨이 등 여러 분야에서 커뮤니케이션하는 환경을 제공해 주는 것이다. 그리고 사물인터넷의 핵심은 인간을 둘러싼 사물들이 서로 연결되면서 인간에게 새로운 편의 혹은 가치를 부여하는 것이다. 스마트 폰이 인간을 중심으로 하여 언제 어디서든 연결될 수 있는 환경을 만들어 주었다면 사물인터넷은 인간 주변의 모든 사물을 연결하고 인간과 상호 소통할 수 있도록 만들어 줄 것이다[11, 12].

그림 1. 향후 사물인터넷기반 파급전망
Figure 1. Future Internet of Things based on the ripple views

<그림 1>과 같이 사물인터넷은 가전, 의료, 교통 등 모든 분야에 적용될 것으로 전망됨에 따라 대부분의 기기에 정보 획득 및 네트워크 연결기능이 탑재되고 이를 바탕으로 스마트 홈, 스마트 가전, 스마트 카, 스마트 헬스케어, 스마트 시티, 스마트 물류, 스마트 그리드 등 다양한 분야에서 새로운 제품과 서비스가 출현될 것이다.

3. 사물인터넷 보안위협 및 보안기술

3.1 사물인터넷 보안위협

사물인터넷 서비스는 디지털과 아날로그가 만나온·오프라인 경계를 허무는 O2O (Online to Offline)의 역할을 하기위해 여러 가지 기술요소가 통합되어 사용된다. 즉, 사물인터넷은 정보를 센싱하기 위한 센서 기술과 센싱된 정보에 대한 원활한 통신·네트워킹을 위한 기술, 사물인터넷 디바이스 자체를 위한 칩 기술, 기능 구현을 위한 OS 기술·임베디드 시스템 기술, 디바이스의 자율 동작과 지능적 동작을 위한 플랫폼 기술, 대량의 데이터를 처리하는 빅데이터 기술, 유용한 정보 추출을 위한 텍스트 마이닝 기술, 사용자 중심의 사물인터넷 서비스를 위한 웹 서비스·응용 서비스 기술, 오픈 API 기술 등 다양한 형태의 기술이 사용된다. 이처럼 다양한 기술이 어우러진 사물인터넷 서비스는 기술 자체 혹은 구현하는 방법의 문제점으로 인해 다양한 보안 취약점이 존재할 수 있다[14].

사물인터넷의 보안 위협으로 데이터 위·변조, 비 인가된 서비스 및 사용자 접근, 인증 방해, 신호 및 데이터의 기밀성·무결성 침해, 정보유출, 복제 공격 등의 형태로 발생 가능하며, 이러한 보안 취약점과 더불어 개인 프라이버시 침해 문제도 심각하다고 할 수 있다[8, 9, 10].

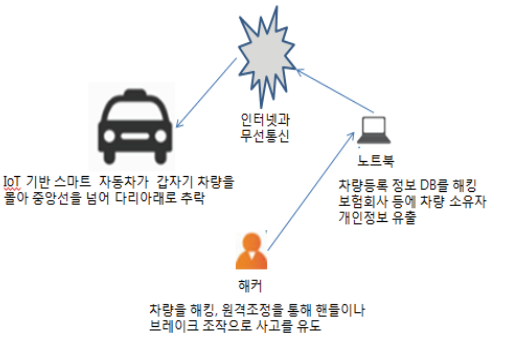

그림 2. 사물인터넷에 연결된 자동차의 보안 취약성
Figure 2. Car security vulnerabilities associated with the Internet of Things

3.2 사물인터넷 보안기술

① 사물인터넷(IoT) 칩셋 보안

대부분의 칩셋은 전자제품에 삽입되어 전자제품의 두뇌역할을 하는 핵심 칩으로 단순 시간예약에서부터 특수한 기능에 이르기 까지 제품의 다양한 특징이 있어서 해킹에 취약성을 가지고 있다.

② 사물인터넷(IoT) 통신네트워크 인프라 보안

사물인터넷에서 주로 사용되는 통신기술은 블루투스, 와이기그(WiGig), 지그비(ZigBee), RF 메시(Mesh) 등을 포함한 근거리 통신기술, 와이파이(WiFi)·4G 롱텀에볼루션(LTE), 스몰셀 등 무선·이동통신 기술과 이더넷 등의 유선통신 기술이 다양하게 활용될 것으로 보인다.

저전력 저손실 네트워크(LLN) 라우팅 프로토콜, IP와 이더넷을 기반으로 하는 유무선 통합 인프라에서도 수용이 가능할 것으로 예상되나, 통신할 수 있는 정보량이 한정되어 있어 높은 수준의 보안 기술을 적용하기 어렵다는 문제점을 가지고 있다[13].

불루투스 또한 무선으로 통신이 이루어지기 때문에 보안 위협으로부터 노출되어 있다. 사용 시

통신 데이터의 암호화가 되어 있지 않을 경우, 허가되지 않은 액세스 등의 해커의 공격이 발생할 수 있다.

와이기그는 60㎓ 대역을 사용해 데이터를 최대 7Gbps 속도로 전송할 수 있어 와이파이에 비해 12배가량 빠른 속도로 전송할 수 있는 기술이다. 와이기그도 무선 근거리통신기반 이기 때문에 해킹 등의 보안 위협으로부터 정보유출이 발생할 수 있다.

③ 사물인터넷(IoT) 플랫폼/서비스 보안

IoT는 기기, 사용자, 서비스 등 다양하게 발생하는 서비스를 활용하여 신규로 서비스가 발생하는 구조를 갖는다. 따라서 위장된 사물 간 서비스, 기능이 변조된 사물 등의 서비스, 비인가 접속을 차단하기 위한 디바이스 간 인증, 접근제어 및 키 관리, 프라이버시 침해를 방지하기 위한 보안기술이 요구되고 있다.

④ 사물인터넷(IoT) DB 보안

사물인터넷에서 발생한 정보는 공격자가 비인가 단말 및 센서를 통해 정식 사용자로 위장하여 데이터를 전송하거나 데이터를 가로채 위·변조하여 정당한 정보로 전송되는 경우에는 인증절차를 통과하여 공격할 수 있다. 따라서 데이터보안은 곧 정보 수집 및 저장하는 단계에서 프라이버시 침해와 뗄 수 없는 관계로 보인다. 사물인터넷은 사람·사물 간의 데이터 교환을 근간으로 하는 시스템이므로 개인정보(이름, 생년월일, 전화번호, 주소 등)가 시스템 접근 절차에서 요구되기도 하고, 시스템을 통해 유출될 가능성도 있다[15].

개인정보를 이용하여 접근한 후 시스템을 조작하거나 신용카드 및 비밀번호 등 더 많은 정보를 유출시킬 수 있어 프라이버시 침해는 사용자에게 더욱 위협적일 수 있다.

표 1. IoT 서비스 제공을 위한 시스템 구성 요소별 보안
Table 1. System-specific security components for the IoT services

유형	내용
칩셋보안	- 유무선 환경에서 보안터널을 만들어 오가는 데이터를 모두 암호화함으로써 적합한 보안 요구사항 만족
통신네트워크인프라 보안	- IoT에 연결되는 모든 사물과 사용자에 유일한 ID(인증서)를 부여 보안 요구사항 만족 - 서비스 이용과 타 사물접근시 기기를 인증해 사용이나 접근 권한 제어
플랫폼/서비스보안	- 사이버 공격과 내부 위협으로부터 고객의 주요 비즈니스 서비스 및 애플리케이션을 보호하는 보안 요구 사항 만족
DB보안	- 중요 데이터에 접근이 가능한 외부경로인 웹 애플리케이션 보안에서부터 파일 및 데이터베이스에 대한 중요도를 파악하고 사용자별 권한에 따른 움직임을 모니터링하며 이를 통제

4. 사물인터넷 보안전략 방안

4.1 IoT 환경에서 센서/칩셋 보안

주로 사용되고 있는 습도, 열, 초음파 센서, 온도 등에서부터 동작인식 센서, 원격 감지 등 유형 사물과 주위 환경으로부터 정보를 얻을 수 있는 물리적 센서에 표준화된 인터페이스와 센싱한 데이터로부터 특정 정보를 추출하는 버츄얼 센싱 인터페이스에 물리적 요소부터 접근이 불가능하도록 통제해야 한다. 주로 신호간섭 제어, 신호에너지 분석, 임의 해시 잠금기술 등이 있으며, 가장 기본적으로 디바이스와 통신할 때 장치인증과 칩셋 표준암호화 알고리즘과 정당하게 전송된 데이터의 프로토콜 디지털 서명 기술 방식이 있다.

4.2 IoT 환경에서 통신네트워크 보안

네크워크 보안의 기본전제 중에 하나는 키 관리로서 비밀 키 생성, 유통, 저장, 갱신 및 키 분배가 대부분이다. 키 관리 알고리즘을 경량으로 설계하여 합법적인 사용자들의 안전을 보장할 수 있는 한정된 자원을 비밀 키 분배 방식으로 지원할 수 있을 것이다.

무선통신 네트워크에 공개키 암호화 알고리즘을 실시하고, 네트워크의 각 노드는 자신의 개인키를 보유해야 하며, 기지국에서 공개키 인증서 알고리즘을 사용하여 전체 네트워크의 보안을 보장할 수 있다.

또한 개인키를 제공하는 어려움을 극복하기 위해 무선센서 네트워크에 사용되는 주로 두 가지 알고리즘이 있다. 대칭 암호와 알고리즘과 비대칭 암호와 알고리즘이 고강도 보안을 제공하지만 현재는 실험단계에 있다.

4.3 IoT 환경에서 플랫폼/서비스 보안

사물인터넷 환경은 플랫폼과 서비스에 대한 접속이 간단해서, 체계적이고 안전한 인증기술과 암호체계를 적용한다 해도 키(Key)를 소프트웨어로 저장할 경우 쉽게 해독이 가능하여 위험에 노출될 가능성이 높다. 일반적으로 키의 복제나 변조가 불가능하도록 하드웨어 기술을 사용해야 하는데 국제표준 보안 전용 TPM을 사용하고 있다. TPM은 디바이스의 식별과 인증을 위해서 암호화 장치 무결성을 보장하고 있다. TPM은 다양한 응용과 보안성이 우수하나, 가격이 높은 단점이 있다. 대안으로 가격부담 없이 암호와 기능과 체계적인 인증을 적용할 수 있는 AES(Advanced Encryption Standard) 같은 소형 암호인증 전용칩을 활용할 수 있다.

4.4 IoT 환경에서 DB 보안

사물인터넷은 다양한 종류의 정보를 네트워크에서 수집하여 해당 서비스에 적합하게 가공하여 수요자에게 제공하고 있다. 따라서 데이터를 처리함에 있어서 허가받지 않은 사용자로부터 정보유출을 방지하고, 데이터의 보안을 위해서 반드시 암호화 및 접근제어 기술이 요구되고 있다. 하지만 데이터베이스의 검색속도가 지연될 수 있는 원인이 될 수 있다.

따라서 검색이 신속하게 데이터를 가공하며, 보안성을 제공 할 수 있는 암호화 기술이 필요하다. 암호화된 자료를 복제하지 않은 상태에서도 필요한 자료를 검색할 수 있게 해주는 대표적인 기술로 검색가능 암호기술(Searchable Encryption Technique)이 있다.

5. 결 론

사물인터넷 환경에서 보안 위협은, 사람과 사물이 네트워크화 되면서 사회적 혼란을 야기할 수도 있으며, 그 피해 속도와 규모도 상상할 수 없을 정도로 커질 수도 있어 사회적 비용이 기하급수적으로 증가할 수밖에 없다. 사물인터넷 보안에 대한 우려는 사물인터넷 산업 성장을 저해하는 가장 큰 요인으로 작용하기 때문에 완벽한 보안이 반드시 실현되어야 한다. 사물인터넷 보안은 기존 PC, 모바일기기 중심의 네트워크에서 모든 사물이 확장 연결되어 보호대상 범위, 보호방법, 보안담당 체계, 대응방법 등에 있어 새로운 관점에서 접근해야 한다.

사물인터넷 플랫폼 및 서비스는 설계 단계부터 보안 기법을 적용해야 하며, 사물간 접속 및 정보의 가공 활용단계 및 전송 시에도 인증・인가 기법, 접근 제어 및 권한 제어 기법, ID(Identification)

관리 기법, 키 관리 및 분배 기법, 신뢰 제어 기법 등 다양한 보안 기법이 선행되어야 한다. 또한 사물인터넷 기반 장치에 대한 지속적인 보안기술 적용뿐만 아니라 개인정보보호를 위한 적극적인 보호 조치를 취하는 것이 필요한 상태이다. 따라서 새로운 보안 위협에 대한 신속한 탐지와 분석을 통해 사전에 보안 위협을 회피하고 방지할 수 있는 종합적인 대응체계를 마련할 필요가 있다.

References

[1] J-M. Galerie, *The internet of things: Top five threats to IoT devices*, Business Horizons, Vol. 58, No. 4, pp. 431-440, 2014.

[2] O. Vermesan, and P. Friess, *New mocana atlas and security solutions for the internet of things to be showcased at RSA conference 2014*, Win. com, pp. 10-16, 2014.

[3] C. Folk, *Seedgen Co, domestic and foreign objects into Internet security threats and solutions, security report*, pp. 122-130, 2014.

[4] J. Wan, J. Lu, and D. Qiu, *Benefits analysis of GSMA embedded SIM specification on the mobile enabled M2M industry*, pp. 34-36, 2014.

[5] F. Burkitt, *Internet of things(IoT) information security roadmap, Ministry of Science, ICT and future Planning*, pp. 289-296, 2014.

[6] T. Levitt, *Internet of things IoT governance, Privacy and Security Issues*, pp. 13-32, 2015.

[7] H. D. Cameron, *Government office for science, The internet of things: making the most of the second digital revolution*, pp. 12-25, 2014.

[8] J. Carlson, J. Montgomery, *Hewlett packard enterprise, Internet of things research study*, 2015 Report, pp.3-6, 2015.

[9] M. B. Barcena, *Symantec, Insecurity in the internet of things,* Version 1.0, Ma. 12, pp. 7-14, 2015.

[10] S. T. Bae, J. G. Kim, *Internet of things (IoT) paradigm shift in the development and security,* KISTEP, pp. 40-55, 2014.

[11] G. H. Jo, *To quicken virtual reality (VR) market - HMD status and current issues*, IITP, 2015.

[12] KISA, *Things internet security threat trends*, www.kisa.or.kr, Vol. 5, 2014.

[13] ETRI, *Global trends in information security industry,* Article 30 Electronic Communications Trend Analysis No. 2, pp. 69-76, 2015.

[14] KIET, *Internet of things era safety net, fused security industry*, pp. 2-12, 2014.

[15] MSIP, *Internet of things (IoT) information security roadmap*, pp. 3-9, 2014.

사물인터넷 보안전망 및 대응기술 연구

김동혁[1], 신기철[2]

[1] *한밭대학교 산업경영공학과*

[2] *중소기업진흥공단 전북지역본부*

요 약

최근 사물인터넷(Internet of Things: IoT)이라는 개념으로 사람과 사물, 서비스를 통합하여 실생활을 편리하게 하기위한 다양한 제품과 서비스가 개발되고 있다. 사물인터넷은 다양한 기술의 복합적 특성으로 인해 기존 서비스와는 다른 특징을 가진다. 사물인터넷은 여러 가지 복합적인 요소기술이 통합되어 특정 서비스를 구성하기 때문에 각 요소 기술 자체의 보안

취약성과 네트워크로 연결되어 정보가공에 따른 새로운 보안 취약성 등이 발생할 가능성이 매우 높다. 때문에 인증/인가 기법, 접근 제어/권한 제어 기법, ID관리 기법, 키 관리 및 분배 기법, 신뢰 제어 기법 등 다양한 보안 기법이 요구되고 있다. 이에 본 논문에서는 안전하고 신뢰할 수 있는 사물인터넷 서비스를 제공하기 위한 사물인터넷 서비스 구성 기술 요소 각각에 대한 보안 기술을 체계적으로 살펴보았고, 사물인터넷 서비스 환경의 안전성 확보를 위한 보안 전략을 제시하였다.

Dong Hyuk Kim received the bachelor's degree in computer engineering from the Hanbat University in 1985. He received the M.S. degree and the Ph.D. degree in the Department of Computer Engineering from Hannam University in 2002 and 2004, respectively. From 2005 to 2008 he was a Hannam University Dedicated professors teaching. He is a professor in the Department of industrial Management Engineering at Hanbat University since 2013. He is a current research areas are Web-database, Education-engineering, data mining, and web programming. He is a life member of the KKITS.

E-mail address: dhkim3s@hanbat.ac.kr

Ki-Chul Shin received the bachelor's degree in Public Administration from University of Seoul in 1989. He received the M.S. degree in Advertising & PR from Korea University and the Ph.D. degree in the Business Administration from Soongsil University in 1999 and 2006, respectively. He was a adjunct professor in the Department of Business Administration at Soongsil University 2001, 2006, 2007. His research areas of interest include New Product Development and Venture Business Start-up Program.

E-mail address: skc@sbc.or.kr