The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 4, pp.43-48, Aug. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.4.43
JIIBC 2017-4-6

사물인터넷 보안 기술 분석

Analysis of Security Technology for Internet of things

이호태*

Ho-Tae Lee*

요 약 현대 사회는 정보통신기술(ICT)의 발달로 제4차 산업혁명이 가져오는 지능정보사회에 다가가고 있다. 우리 주변의 사람과 사물, 사물과 사물 등은 사물인터넷 기술의 발달로 공간에 제약을 받지 않고 네트워크로 연결되어 빅데이터가 산출되고 서로 정보를 송·수신 할 수 있게 되었다. 그러나 단말기 분실 및 물리적 파괴, 무선신호 교란 정보유출, 데이터 위·변조, 서비스 거부 등 기존의 통신환경에서 생성되는 위협들은 정보보안의 3대 요소인 기밀성, 무결성, 가용성을 침해하여 사물인터넷의 보안을 위협할 수 있다. 이런 위협에 대비하여 사물인터넷에 대한 보안과 정보유출 등의 정보보호 기술을 강화해야 한다. 본 논문에서는 사물인터넷의 구성과 활용 분야를 알아보고 각기 다른 구성요소에서 나타나는 보안 취약점이 발생할 때 대응할 수 있는 사물인터넷 보안기술을 센서와 디바이스, 네트워크와 서버, 플랫폼과 앱의 3가지 구성으로 나누어 안전성 확보를 위한 보안 기술을 분석하였다.

Abstract Today our society is approaching new intelligence information society, which has been caused by the Fourth Industrial Revolution along with the development of information and communication technology(ICT). And this has just opened a new era of Internet of Things(IoT) that connects between human and objects and between objects through network, allowing transmission and reception of information beyond the limits of space. However, many crises occurred in the existing communication environment may threaten the security of Internet of Things, by violating the three components of information security. In this paper, this study aims to analyze security technology to achieve advanced security by dividing IoT security technology for coping with security vulnerability found in different components into three groups.

Key Words : Security Technology, Internet of things, Network/Server Security, Platform/App, Sensor/Device

Ⅰ. 서 론

사물인터넷(Internet of things)은 1999년 MIT의 Auto-ID Center 에서 전망하면서 처음 사용한 것으로 알려져 있다. 사물인터넷기술은 인터넷과 연결을 되지 않았던 일상 사물들이 네트워크로 연결되어 사람과 사물, 사물과 사물들이 서로 데이터를 주고받는 기술을 말한다.[4][10]

최근 사물인터넷 기술은 미국 정보 기술연구 자문 회사인 가트너사에서 발표한 2016년 10대 전략기술 트렌드로 선정되었다.

표 1은 최근 3년간 가트너의 10대 전략 트렌드를 알 수 있다. 또한, 시스코 시스템즈는 2020년에는 500억 개 이상의 사물이 인터넷에 연결될 것이고 1경 400조 규모

*정회원, 부산대학교 IT응용공학과
접수일자: 2017년 7월 16일, 수정완료: 2017년 8월 3일
게재확정일자: 2017년 8월 11일

Received: 16 July, 2017 / Revised: 3 August, 2017
Accepted: 11 August, 2017
*Corresponding Author: htlee@pusan.ac.kr
Dept. of Applied IT and Engineering, Pusan National University, Korea

의 거대 시장으로 성장하게 될 것 이라고 발표하였다.[1],[3],[4]

표 1. 최근 카트너 10대 전략기술 [12]
Table 1. Recent Gartner 10 Strategic Technology

2015년	2016년	2017년
컴퓨팅 에브리웨어	디바이스메시	인공지능과 고급 머신 러닝
사물인터넷	앰비언트 사용자 경험	지능형 앱
3D 프린팅	3D 프린팅 소재	지능형 사물
차세대 첨단분석	만물정보	가상현실 및 증강현실
콘텍스트 리치 시스템	진보된기계학습	디지털 트윈
스마트머신	자율 에이전트 및 사물	블록체인과 분산장부
클라우드/ 클라이언트 컴퓨팅	능동형 보안 아키텍처	대화형 시스템
SW정의 인프라와 애플리케이션	첨단 시스템 아키텍처	메시 앱 및 서비스
웹스케일IT	메시앱 및 서비스 아키텍처	디지털 기술 플랫폼
위험 기반 보안과 자기방어	사물인터넷 아키텍처와 플랫폼	능동형 보안 아키텍처

이에 따라 기존에 사용하던 장치들이 사물인터넷 환경에서 인터넷과 접속되어 기존의 인터넷 환경에서 발생할 수 있는 모든 위협과 취약점들이 사물인터넷에서 발생할 수도 있다.[10],[12],[20]

사물인터넷환경의 구성은 네트워크 통신방식이 (ZigBee, RFID, WiFi 등) 상이하고 각각의 네트워크들이 서로 다른 처리 능력을 갖추고 있다. 그리고 이들의 보안 시스템은 개별적으로 호환 가능한 통합적인 기술이 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 사물인터넷 구성과 활용분야를 알아보고 3장에서는 사물인터넷 보안 위협을 서술한다. 4장에서는 사물인터넷 정보보호 종류와 기술의 분석하고 5장에서는 본 연구의 결론을 맺는다.

II. 사물인터넷 구성과 활용 분야

1. 사물인터넷의 구성요소

사물인터넷을 구성하는 기술적 요소는 다음과 같이 크게 4가지로 구분할 수가 있다.[2-9],[11],[13-21]

가. Sensor 기술

센서기술은 사람을 대신하여 필요한 사물이나 장소에서 정보를 수집하여 실시간으로 전달, 공유하는 핵심 기술이다. 최근에 기술의 발달로 사람의 오감영역 보다 뛰어난 센서들이 개발되어 기술영역을 확장 시켜주고 있다.

나. Network 인프라 기술

사물인터넷의 네트워크 인프라는 사물과 사람이 인터넷에 연결되도록 지원하는 기술로, 기존의 WiFi, Bluetooth, 3G/4G/LTE, Zigbee, 등 유선과 무선으로 주고받는 모든 매체가 될 수 있다.

다. 서비스 인터페이스 기술

서비스 인터페이스 기술은 사물인터넷으로 연결된 정보를 생성, 수집, 공유, 활용하는 역할을 하고 Open API 기반의 서비스를 제공하여, 대량의 정보를 수집하고 분석하여 처리하는 Big Data 기술이 여기에 포함된다.

라. 보안 기술

네트워크, 서버 및 디바이스 및 센서 등 사물인터넷 구성 요소에 해킹 및 악성코드 전의 개인 정보 유출, 서비스거부 등 이를 방지하기 위한 기술이며, 적용 분야별로 기능과 애플리케이션, 인터페이스 등이 다르기 때문에 그에 따른 적합한 보안 기술 적용이 요구된다.

2. 사물인터넷 활용 분야

사물인터넷 활용 분야는 교통, 의료, 가전, 자동차 등 다양한 분야에서 활용되고 있으며 표 2와 같이 분류하고 있다.

표 2. 사물인터넷 활용 분야[3]
Table 2. Internet of Things Application Fields

적용분야	적용 유형
자동차	-차량관리, 네비게이션, 교통정보, 통행료, 원격 차량진단 등 -무인주행, 신호등 시스템 등
원격관리 제어	-가스, 물, 전기, 등 사용량의 원격 검침 -산업자동화, 유통망관리 -고객관리, 수요관리

물류/유통/금융	-물류관리시스템, 유통망관리, NFC결제,택배서비스나 배달 서비스 등
보안/공공안전	-지능형교통망, 무선보안시스템, 감시시스템 CCTV보안,
의료	-U-헬스, 의약품관리, 생체신호모니터링, 독거노인지원, 원격의료 등
가전	-가정용에너지, 원격관리, TV, 에어컨, 동/식물
원격유지보수	-교량, 빌딩 등 유지 모니터링
환경감시	-하천오염도 측정, 대기오염 모니터링, 해수 측정 등

Ⅲ. 사물인터넷 보안 위협

사물인터넷은 각기 다른 기술요소들의 공동체이며, 기존의 통신 환경에서 생성되는 보안위협들을 가지고 있다. 정보보안의 3대 요소인 CIA, 즉 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 침해하는 보안 위협들이 나타날 수 있다. 표 3은 사물인터넷의 각 구성요소에서 발생할 수 있는 보안위협을 정리하였다.[3],[7-9],[13-21]

표 3. 사물인터넷 구성요소별 보안위협[13]
Table 3. Internet of Things Component-Specific Security Threats

구분	보안위협
단말기	물리적 파괴, 분실/도난
애플리케이션	정보유출, 데이터 위·변조, 서비스거부
네트워크	정보유출, 무선신호 교란, 서비스 거부 ,데이터 위변조

1. 단말기 분실 및 물리적 파괴

사물인터넷 서비스를 위해 설치된 센싱 노드들이 분실되거나 물리적인 접근 또는 파괴되었을 때 통신 기능의 상실로 인한 사물인터넷 서비스가 중단될 수 있다.

2. 무선신호 교란

사물인터넷은 대부분 무선네트워크 통신환경으로 되어있으며 최근 3G/4G/LTE, GPS, RF 등의 대상으로 다양한 전파 차단 장치들이 등장하고 있다. 이때 인가받지 않은 불법 무선통신 교란 장비로 인해 정상적인 서비스를 방해할 수 있다.

3. 정보유출

정보유출은 기존 유·무선 통신구간에서의 스푸핑, 백도어, 스니핑등의 비인가 접근을 통해 이루어질 수 있다. 이로 인해 개인정보 등의 중요정보가 유출될 경우 프라이버시 침해 등의 피해가 일어 날수 있다.

4. 데이터 위·변조

데이터 위·변조 위협은 허가받지 않은 단말기 또는 센서를 통해 데이터를 유·무선 네트워크상에서 가로채어 위·변조 한 뒤 정상적인 경로를 통해 송신한 것으로 위장할 수 있다.

5. 서비스 거부

사물인터넷 환경에 설치된 단말/센서들은 정상적인 서비스 제공하기 위해 단말/센서 간의 관리하는 게이트웨이를 통하여 상시 연결요청을 수행한다. 공격자는 이를 악용해 임의로 대량의 패킷을 전송하고 전력 또는 데이터 처리에 과부하가 되어 필요한 서비스를 불가능하게 만들 수 있다.

Ⅳ. 사물인터넷 정보보호 기술

사물인터넷 정보보호 기술은 다음과 같이 분류하여 보안대책을 제시하였다.[5],[6],[11],[13-21]

1. 센서/디바이스 보안대책

센서/디바이스에 관련된 위협으로는 분실, 도난, 파손 그리고 디바이스의 좀비단말화, 불법복제와 악성코드에 관한 보안 대책을 세워 각종 센서와 디바이스들의 보안 위협에 대응하여야 한다.

아래 표 4는 센서/디바이스에 관한 보안 대책과 대응방안의 세부적인 내용을 정리하였다.

표 4. 센서/디바이스 보안대책과 방안
Table 4. Security Measures and Countermeasures for Sensors and Devices

보안위협	보안대책과 대응방안
분실과 도난,	- 도난, 분실 시 단말기 잠금 또는 원격 파일

파괴	삭제 기능을 탑재 - 암호설정과 초기화 MDM 기능을 제공
좀비 단말화	- 서버와 데이터 전송을 통제하고 허가받은 매체만 사용가능 하도록 통제 - 디바이스 앱 또는 웹 방식의 모바일 어플리케이션 이용 시 정보저장과 다른 프로세스의 실행을 제한
불법복제와 악성코드	- 단말기 불법 복제 시 구동이 불가능한 도구 설치 - 악성코드나 웜바이러스 보안프로그램설치 운용 - 비인가자의 파라메타 설정이나 수정 금지

2. 네트워크/서버 보안대책

네트워크와 서버 관련 보안대책은 기존의 유·무선 네트워크 기반의 디바이스들이 접속하는 서버에 관한 보안 대책으로, 세부내용을 정리하면 표 5와 같다.

표 5. 네트워크/서버 보안대책과 방안
Table 5. Security Measures and Countermeasures for Networks and Servers

보안위협	보안 대책과 대응 방안
무선신호교란	- 불법적인 전파 차단/교란 장비이용, 접속불능 상태로 전이 차단을 위한 교란 추적 장비보유 운영 - 허용가능 이상의 전파전송으로 위한 장비가동 불능 상태를 차단하기 위한 과전파 차단장치 설치운영
패킷 가로채기와 DDoS공격	- 방화벽 운용, 인증서, 로그관리, 비인가 포트 차단 및 접근권한 통제 강화 - 패킷 가로채기와 DDoS 공격 등에 대응가능한 서버 침입탐지 시스템 설치 운용 - 사물네트워크 환경에서 실시간 프로세서 제어 보안기술 개발
악성코드전이	- OS나 프로토콜, 미들웨어, 플레폼등의 보안 취약점을 대비하여 정기적인 보안 업데이트 실시 강화 - 악성코드 탐지와 치료 가능한 안티바이러스 등의 도구 설치 운영과 주기적인 업데이트 실시 - 비인가된 접근과 I/O접근 통제 강화와 악성 코드의 탐지 및 치료가능 시스템 설치 운용

3. 플랫폼/앱 보안대책

플랫폼과 앱의 보안 위협은 악성코드 전의 웜바이러스/안티바이러스 등이 있으며 이에 관한 보안대책을 세워 적절하게 대응해야 한다.

표 6은 플랫폼과 앱의 보안대책을 정리하였다.

표 6. 네트워크/서버 보안대책과 방안
Table 6. Security Measures and Countermeasures for Platforms and Apps

보안대책	보안 대책과 대응 방안
플랫폼의 취약성 공격	- 방화벽과 침입탐지 시스템 구축 운용, 비밀번호 또는 인증서, 로그관리, 비인가 포트 차단 및 접근 권한 통제 강화
웜바이러스/안티바이러스	- 웜바이러스와 부적절한 안티바이러스 사용으로 인한 보안약화를 방지하기 위해 검증된 정상 S/W와 도구 사용 - 안티바이러스 설치와 부적절한 관리 등의 보안역량 약화 요인제거 가능한 강력한 보안정책 도입필요
악성코드 전이	- 웜바이러스, 스파이웨어 등의 악성코드에 의한 보안위협에 대비하여 적절한 안티바이러스 솔루션 도입 - 백신 프로그램 설치 및 자동 업데이트, 원격 패치 관리용 보안 솔루션을 제공 - 비정상적인 접속 시도되면 강제 세션 종료 및 자동 로그 정보수집 시스템 개발

V. 결 론

앞에서 살펴본 봐, 사물인터넷은 주변의 수많은 디바이스와 센서가 네트워크 연결되어 있고 그중 하나가 문제가 생길 경우 연속적으로 다른 센서들 또는 단말기까지 영향을 받을 수 있다. 따라서 실시간으로 통신 상태를 점검할 수 있어야 하고 문제가 발생 시 즉각 적인 조치와 복구가 이루어져야 한다. 그리고 외부공격에 대한 대비와 내부 발생 문제에 대한 매뉴얼과 대응책 마련으로 사물인터넷 안전성을 확보하여야 한다.

사물인터넷 환경의 특성상 개인정보 유출과 데이터 위·변조, 단말분실 또는 파손, 서비스 거부 등 보안 위협 요인들이 있다. 이를 해결하기 위해서는 사물인터넷 환경의 구성요소별 보안 인증체계 구축이 중요하며 이를 위해 저전력, 저손실의 암호화 기법의 개발이 필요하다. 그리고 물리적인 위협에 대응하기 위한 단말/센서들의 잠금장치와 비인가자들의 접근을 불가능하도록 접근통제가 이루어지는 공간에 설치되어야 하며, 상황 인지 기

반으로 설계·구축 하여 추후 오동작 시 이를 파악하고 신속하게 대처를 할 수 있어야 한다.

그리고 무엇보다 사물인터넷의 안전한 환경 구축을 위한 국가적인 지원과 신규보안 기법 개발 및 표준화 연구가 필요하겠다. 본 논문에서 분석하고 제시한 보안방안들이 안전한 사물인터넷환경을 제공하는데 기초자료가 되어 도움이 될 수 있을 것이라 기대한다.

References

[1] Nam-Hui Kang, “Standards and Technology Trends for the Internet of Things security”, The Journal of The Korean Institute of Communication Sciences, Vol. 31, No.9, pp. 40-45, Aug 2014.

[2] Yu-Jae Won, “IoT (Internet of Things) information security technology development direction”, The Journal of The Korean Institute of Communication Sciences Vol.32, No.1, pp. 24-27, Jan 2015.

[3] Dong-Hui Kim, Seok-Ung Yun, Yong-Pil Lee, "Security for IoT Services" The Journal of The Korean Institute of Communication Sciences, Vol. 30, No. 8, pp. 53-59, Jul 2013.

[4] Seoung-Chan Chol, Min-Woo Ryu, Nam Jin, Jae-Ho Kim, “Internet of Things platform and service trends”, The Journal of Communications and Networks, Vol. 31, No. 4, pp. 20-27, Mar 2014.

[5] Ministry of Science, ICT and Future Planning, “Internet of Things Information Security Roadmap”, http://www.msip.go.kr/web/msipContents/contentsView.do?cateId=mssw11211&artId=1287656, Oct 2014.

[6] Korea Internet & Security Agency, “Internet of Things (IoT) password authentication technology used in the environmental handbook”, http://seed.kisa.or.kr/iwt/ko/guide/EgovGuideDetail.do?bbsId=BBSMSTR_000000000011&nttId=89&pageIndex=1&searchCnd=&searchWrd= Apr 2016.

[7] Dong-Hui Sin, Jae-Yeol Joung, Seong-Hyeon Kang, “Internet of Things and Future Trends”, The Journal of Internet Computing and Service Vol. 14, No. 2, pp. 32-46, Jun 2013.

[8] Cheol - Sik Pyo,, “Internet of Things Technology Trends”, The Journal Of Korean Institute of Electromagnetic Engineering and Science, Vol. 25, No. 4, pp. 49-58, Jul 2014.

[9] Se-Hyeong Kim, "Internet of Things(IoT : Internet of Things)Technology," The Magazine of the IEEE, Vol. 43, No. 3, pp. 64-71, Mar 2016.

[10] Gartner Inc. http://www.gartner.com

[11] Bong-Im Jang, Chang-Su Kim, “A study on the security Technology for the Internet of Things”, Journal of Security Engineering Vol. 11, No. 5, pp. 429-438, Oct 2014.

[12] Cisco Systems Inc. http://www.cisco.com/

[13] Seong-Ryeol Kim, “Security threats and Countermeasure Technology of the Internet of Things”, Journal of Industrial science researches, Vol. 34, No. 2, pp. 137-142, Feb 2017.

[14] Dong-Hyeok Lee, Nam-Je Park, “Proposal of Technology and Policy Post-Security Management Framework for Secure IoT Environment”, Journal of Korean Institute of Information Technology, Vol. 15, No. 4, pp. 127-138, Apr 2017.
DOI: https://doi.org/10.14801/jkiit.2017.15.4.127

[15] Wan-Jin Chang, Yong-Tae Shin, “A Study on the Network and Security for the Internet of Things”, Proceedings of KIIT Summer Conference, pp.19-21, Jun 2015.

[16] Hyung-Jin Mun, Gwang-Houn Choi, Yooncheol Hwang, “Countermeasure to Underlying Security Threats in IoT communication”, Journal of Convergence for Information Technology, Vol. 6, No. 2, pp.37-44, Jun 2016.
DOI: https://doi.org/10.22156/cs4smb.2016.6.2.037

[17] Yong-Hyeog Kang, “A Study on Security Requirements and Security Protocols for Internet of Things ”, Proceedings of Symposium of the Korean Institute of communications and Information, Vol. 2017, No. 1, pp. 1141-1142 Jan

2017.

[18] Sick-Yong Jung, Jea-Sang Cha, "IoT device security check standards", The Journal of The Korean Institute of Communication Sciences, Vol. 34, No. 2, pp. 27-33, Jan 2017.

[19] Jung-Nyeo Kim, Seung-Heon Jin, "Internet(IoT) Security Technology for Security Threats in Second Connection Environment", The Journal of The Korean Institute of Communication Sciences, Vol. 34, No. 3, pp. 57-64, Feb 2017.

[20] Dong-Hui Kim, Seok-Ung Yun, Yong-Pil Lee, "Security for IoT Services" The Journal of The Korean Institute of Communication Sciences, Vol. 30, No. 8, pp. 53-59, Jul 2013.

[21] Myong-Yeal Lee, Jae-Pyo Park, "Analysis and Study on Invasion Threat and Security Measures for Smart Home Services in IoT Environment", The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol. 16, No. 5, pp. 27-32, Oct 2016.
DOI: https://doi.org/10.7236/jiibc.2016.16.5.27

[22] Se-Hwan Park, Jong-Kyu Park, "IoT Industry& Security Technology Trends", The International Journal of Advanced Smart Convergence(IJASC), Vol. 5, No. 3, pp. 27-31, Sep 2016.
DOI: https://doi.org/10.7236/ijasc.2016.5.3.27

[23] Mi-Young Kang and Ji-Seung Nam, "A Study on Smart Network Utilizing the Data Localization for the Internet of Things," Journal of the Korea Academia-Industrial cooperation Society(JKAIS), Vol. 18, No. 6, pp. 336-342, Jun, 2017.
DOI: https://doi.org/10.5762/KAIS.2017.18.6.336

[24] Sunhwa A. Nam, Hyokyung Bahn. "Real-time Task Scheduling Methods to Incorporate Low-power Techniques of Processors and Memory in IoT Environments." The Journal of the Institute of Internet, Broadcasting and Communication(JIIBC), Vol, 17, No. 2, pp. 1-6, Apr 2017.
DOI: https://doi.org/10.7236/jiibc.2017.17.2.1

저자 소개

이 호 태(정회원)

- 2009년: 밀양대학교 정보통신공학과 (공학사)
- 2012년: 부산대학교 바이오메디컬공학과(공학석사)
- 2015년 ~ 현재: 부산대학교 IT응용공학과 박사과정

<주관심분야 : 이동통신, 전자기학, 무선통신, 정보보안>

※ 이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음.