The Journal of the Convergence Culture Technology (JCCT)
Vol. 2, No. 4, pp.77-82, November 30, 2016. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2016.2.4.77
JCCT 2016-11-11

사물인터넷(IoT) IP의 노출과 위협에 대한 연구

A Study on the Exposures and Threats for Internet of Things(IoT) IP

김유진*, 이누리*, 신성은*, 송승연*, 정다영*, 장영현**, 문형남***

Yu-Jin Kim*, Nu-Ri Lee*, Seong-Eun Shin*, Seung-Yeon Song*, Da-Young Jung*, Young-Hyun Chang, Hyung-Nam Moon*****

요 약 가트너가 2013년부터 2015년까지 3년 연속 'IT 10대 전략기술' 의 하나로 선정한 사물인터넷(IoT) 기술은 사람과 사물의 상호작용을 가능하게 하면서 고도화된 스마트사회를 구현할 수 있다. IoT 장비들이 인터넷으로 연결되어 있는 특성에 따라 해킹으로 인하여 무선신호 교란, 정보 유출, 데이터 위·변조와 서비스 거부 등 개인의 사생활 노출로부터 국가의 중요 기밀과 시설에 대한 위협까지의 중차대한 보안상 문제들이 나타날 수 있다. 본 논문에서는 IoT 장비들의 IP 노출에 대한 보안위협 사례들을 조사하고 문제점을 분석하여 개인의 사생활 노출이나 국가 기반시스템에 대한 피해 등 IP 노출로 인한 보안위협을 최소화하기 위한 방안을 제안한다.

주요어 : 사물인터넷(IoT), 인터넷프로토콜(IP), IP 노출(exposures), IoT 취약성, IoT 보안

Abstract IoT technology was selected as one of IT 10 strategic technologies by gartner from 2013 to 2015, and implements advanced smart society while enabling interaction between people and things. Because IoT devices are connected to the Internet, they are involved in issues including exposure of private lives, for example, hacking to result in wireless signal interference, data theft, data modification and forgery and service denial, and critical security issues including threat to national confidential information and facilities. This study aims to suggest a method for examining threats to security through IP exposure of IoT devices and examining related problems to minimize threats to security through IP exposure including exposure of private lives or damages to the national infrastructure system.

Key Words : IoT, Internet Protocol, IP Exposures, IoT Vulnerability, IoT Security

I. 서 론

공상과학 영화에는 자동으로 문이 열리고 전등이 켜지며, 간단한 음성인식으로 커피포트가 끓고 텔레비전이 켜지는 등의 장면이 나온다. 과거에서는 상상이고 현재에서는 현실이 되고 있다. 사물인터넷(Internet of Things: IoT) 기술의 발달 때문이다. 가트너 선정 2015년도 '10대 IT 전략기술' (Top

*준회원, 배화여자대학교 스마트IT학과
**정회원, 배화여자대학교 스마트IT학과
***정회원, 숙명여자대학원 정책산업대학원 IT융합비즈니스전공
접수일자: 2016년 10월 12일, 수정완료일자: 2016년 10월 26일
게재확정일자: 2016년 11월 4일

Received: 12 October, 2016 / Revised: 26 October, 2016
Accepted: 4 November, 2016
***Corresponding Author: ebiztop@gmail.com
Dept. of IT Convergenc Business, Sookmyung Women's University

10 Strategic IT Trends)에도 중요한 위치(2013: 사물인터넷 4위, 2014: 만물인터넷 3위, 2015: 사물인터넷 2위)로 선정된 IoT 기술의 발달은 사람과 사물의 상호작용을 가능하게 하고, 생활을 스마트하고 편리하게 만들고 있다. 실제로도 최근에 LG U+에서 IoT Home 서비스를 실시하여 집 안에 있는 에어컨, 스위치, 냉장고 등의 사물들을 인터넷으로 연결하여 시공간을 초월하여 내부 상태를 확인할 수 있게 만든다.[1] 이처럼 스마트 홈 기술 및 서비스가 적용된 홈 네트워크를 통해 연결되어 사람과 자연스러운 상호작용으로 인간 중심의 서비스 환경에서 유익한 서비스를 제공함으로써 삶의 질을 향상시키고 보다 스마트한 가정환경을 누릴 수 있게끔 돕는다.[7] 하지만 IoT 기술의 발달이 항상 긍정적인 모습만을 보여주는 것은 아니다. 최근 중소기업청이 중소기업 정보화 수준을 평가한 결과에 따르면 기업들의 IT업무 활용도에 있어서 개인 업무 활용(56.7%), 사내 네트워크 활용(53.4%), 기업간 네트워크 활용(47.1%)으로 아직까지 기업들이 구축된 정보시스템인프라를 50% 수준으로 밖에 제대로 활용하지 못하고 있으며, 제조업의 경우도 ICT와 IoT를 활용한 생산성 혁신과 경쟁력 제고가 미흡한 설정이고 회계, 인사 등 기업 내부 전산화 수준에 머물러 있는 것이 현실이다.[6] 또한 다양한 보안 위협들로 인해 IoT 장비들의 해킹에 대한 위험성이 높아지고 있고, IoT 장비들의 특성상 인터넷으로 연결되어 있어 무선신호 교란, 정보 유출, 데이터 위.변조, 서비스 거부 등의 장비 해킹으로 인한 보험위협으로, 개인의 사생활 노출로부터 시작하여 국가의 중요 시설에 대한 위협까지 확대될 수 있다.

IoT에 대한 위협의 가장 중요한 원인은 IoT 장비에 할당되어있는 IP(Internet Protocol)주소의 노출(exposures)이라 할 수 있다. IoT 장비는 인터넷에 연결되므로 고유의 IP주소를 가지고 있기 때문에 IP주소 노출에 대한 문제가 심각하게 나타난다. IP주소는 공격자가 해당 IP주소에 대한 권한만 획득할 수 있다면 쉽게 접근이 가능하고, 위에서 언급한 데이터 위·변조, 서비스 거부 등의 공격 또한 쉽게 이루어질 수 있기 때문에 노출에 대한 위험성이 더욱 크다.

시장조사 기관인 가트너는 IoT 산업에 대해 2020년에는 260억 개의 사물이 연결되어 약 1조 9000억 달러에 달하는 시장이 창출될 것이라고 예측했다. 아울러 미국국제전략연구소(CSIS)는 해킹으로 인한 경제적 손실을 연간 약 4천 450억 달러로 추정했다. 우리가 왜 IoT 디바이스 보안에 관심을 갖고 준비를 해야 하는지에 대한 답은 바로 여기에 있다.

본 연구에서 IoT 장비들의 IP 노출에 대한 보안 위협 사례들을 조사하고 문제점을 분석하여 IP 노출로 인한 사생활 노출이나 국가 기반 시스템에 대한 피해 등의 IP주소 노출에 따른 보안 위험성을 예방하기 위한 IP노출 위협 예방 시스템에 대해 연구한다.[1]

II. IoT 보안 취약성 국내외 사례 분석

2.1 한국 IoT 취약성 사례

국내에서는 이혼한 남편이 전 부인 집 보일러를 앱으로 조정해 가스 요금 폭탄을 맞게 한 사건도 벌어졌다. 스마트폰 앱이 악성코드를 실행해 연결된 네트워크 공유기 DNS를 변조시켜 파밍사이트로 만든 사례도 있었다.

융합제품이나 융합서비스에 활용하는 IoT 기기 70%가 암호화되지 않은 네트워크로 데이터를 전송하는 것으로 파악됐다. 제품과 서비스 생산자가 보안에 관심이 낮거나 보안기능을 탑재하는데 상당한 비용과 시간이 소요되는 이유로 보안 내재화 미흡이 문제이다.[3]

2.2 미국 IoT 취약성 사례

스마트홈 가전 및 스마트 오피스 장치들의 등장으로 실생활은 편리해졌지만 보안 취약점으로 인해 노출되는 정보에 의해 물리적 침입 등의 위협이 실제로 발생했다.

실제로 미국 보안서비스업체인 프루프포인트는 2013년 말부터 2014년 초까지 전 세계에서 75만 건의 '피싱'과 '스팸' 메일이 스마트 가전 해킹을 통해 발송됐다고 밝혔다. 공격 대상은 기업과 개인이었고, 가정에 설치한 인터넷 라우터, TV나 냉장고와 같은 비교적 관리가 소홀한 통신 기능이 내장된 가전제품들이 공격에 사용됐다. 이 공격은 단일 인터넷프로토콜(IP) 주소로 보내는 이메일 건수를 최대 10건으로 제한하는 수법을 썼다. 때문에 발송 위치를 파악해 공격을 차단하는 방법을 사용하기가 쉽지 않다.

PC나 모바일 기기에 비해 인터넷에 연결된 스마트 가전기기들은 보안 조치가 허술하게 되어 있어 표적이 되기 쉽지만 해킹에는 무방비 상태라는 지적이 많다.[4]

2.3 중국 IoT 취약성 사례

그림 1은 체중계가 인터넷에 연결되고 각종 분석 기능과 다양한 서비스와 연동이 가능한 사물인터넷 제품/서비스 사례를 보여주고 있다. 사용자가 측정한 체중 정보는 서비스 제공업체의 클라우드에 전송되며 해당 정보를 사용자는 스마트폰과 같은 단말에서 앱을 통해 확인할 수 있다. 언급한 체중 정보 흐름은 단순해 보이지만 개인의 체중 정보는 매우 다양한 형태의 서비스에 활용될 수 있다. 예를 들어, 어떤 사물인터넷용 체중계는 측정한 개인의 체중 정보를 개인의 선택에 따라 트위터와 같은 SNS에 업로드할 수 있다. 서비스 업체에 저장된 개인의 체중 정보가 악의적인 목적으로 사용될 수도 있으며, 서비스 업체가 자사의 이익을 위해서 분석·가공을 통해 회사 입장에서는 부가가치가 높은 다른 정보로 변환할 수도 있을 것이다. 어떤 경우에든 원래의 데이터 소유 주체의 의사에 반하는 형태로 데이터가 활용되는 것이므로 프라이버시 침해가 발생하게 되는 것이다. 이런 상황에서 체중계 사용자(체중정보 소유자)가 자신의 정보에 대한 통제권을 확보하고자 하는 경우, 현재의 사물인터넷 서비스 환경에서는 쉽게 자기정보통제권을 얻을 수 있을지 의문이다. 업체에서 자사가 보유하고 있는 정보를 가공하여 제3의 업체에 판매한 경우, 판매 이후에는 정보를 제공한 업체에서는 해당사용자의 정보를 통제할 수 없을 것이며, 가공된 정보는 원래의 정보라고 볼 수 없기 때문에 최초의 체중 정보 소유자가 이 경우에 해당 정보에 대한 통제권을 가진다고 볼 수도 없게 된다. 지금까지 단일 업체에 의한 정보 처리 및 관리가 이뤄졌고 사물인터넷 환경처럼 여러 주체가 관계되는 경우는 없었기 때문에 기존의 프라이버시 관련 법과 체계는 새로운 사물인터넷 환경에 맞게 정비될 필요가 있다. 언급한 프라이버시 침해 가능성뿐만 아니라[그림 1]에서 보듯 체중계에서 센싱되어 무선통신채널로 전송되는 정보를 악의적인 공격자가 가로챈다면(sniffing), 공격자는 해당 정보를 활용하여 사용자의 신체적 특성을 유추하여 이를 악의적인목적에 사용할 수 있을 것이다. 많은 사물인터넷 디바이스와 플랫폼에는 접근 제어, 인증·인가 기술에 있어서 높은 등급의 기술이 구현되지 않기 때문에 상대적으로 공격에 취약하다. 체중계에 동작센서(motion sensor)가 있다면 공격자는 취약한 보안 체계를 뚫어서 해당 센서에 대한 제어권을 확보하여, 개인의 체중 정보 뿐만 아니라, 댁내 거주 여부도 쉽게 알 수 있게 된다.[2]

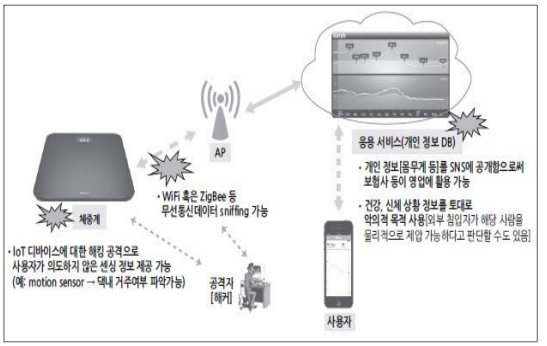

그림 1. 사물인터넷 제품(체중계) 보안 취약성
Fig 1.

2.4 기타 IoT 취약성 사례

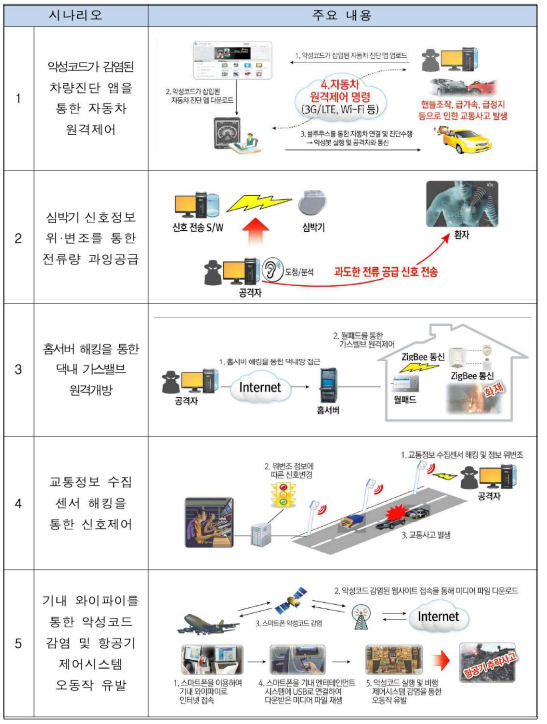

그림 2. IoT서비스 환경에서 발생 가능한 보안위협 시나리오
Fig 2.

그림 2는 IoT서비스 환경에서 발생 가능한 보안위협별 5가지 시나리오 사례를 보여주고 있다. 차량진단, 심박기 신호위·변조, 홈IoT 원격조정, 교통정보 신호제어, 항공기제어시스템 오동작시나리오의 피해사례가 있다. [그림 2]의 시나리오1은 악성코드가 감염된 차량진단 앱을 통한 자동차 원격제어 시나리오는 다음과 같다. 해커가 악성코드가 삽입된 자동차 진단 앱을 업로드하게 되면 사용자가 악성코드가 삽입된 자동차 진단 앱을 다운로드하게 되고 블루투스를 통한 자동차 연결 및 진단수행 등 자동차를 원격제어 하여 핸들조작, 급가속, 급정지 등으로 인한 교통사고를 유발할 수 있다. [그림 2]의 시나리오2는 심박기 신호정보 위·변조를 통한 전류량 과잉공급 시나리오이다. 심박기 신호정보를 받는 소프트웨어를 해커가 데이터 위·변조로 신호정보를 도청, 분석하여 환자에게 과도한 전류 공급 신호를 전송하여 심각할 경우 사망으로 이르게 할 수 있다. [그림 2]의 시나리오3은 홈 서버 해킹을 통한 댁내 가스밸브 원격개방 시나리오이다. 해커가 홈 서버 해킹을 통한 사용자의 IoT 홈서비스 망에 접근하여 월패드를 통한 가스밸브를 원격 제어하여 사용자의 집에 화재를 유발할 수 있다. [그림 2]의 시나리오4는 교통정보 수집 센터 해킹을 통한 신호제어 시나리오이다. 신호등은 신호제어 센서를 통해 변경이 진행된다. 여기서 공격자는 각종 교통 수집 센서를 수집한 후 해킹하여 교통 정보를 위변조 할 수 있다. 위변조한 정보를 통해 실제 신호등을 공격자 마음대로 제어하여 교통사고를 유발하고 시민들을 위험에 빠트릴 수 있다. [그림 2]의 시나리오5는 기내 와이파이를 통한 악성코드 감염 및 항공기 제어시스템 오동작 유발 시나리오 이다. 먼저 비행기에 탑승한 사용자들이 스마트폰 또는 노트북 등 휴대용 기기를 이용하여 기내와이파이에 접속 한 후, 연결된 와이파이를 활용하여 각종 홈페이지를 접속하고 미디어 파일을 다운로드 받게 된다. 이 때 다운로드 받은 파일에는 악성코드가 감염되어 있어 이 사실을 모르는 사용자는 다운로드 파일을 실행시키고자, 비행기 내부에 있는 USB 단자에 연결한다. 감염된 파일이 다운로드 되어있는 USB를 단자에 연결시킴과 동시에 악성코드가 실행되며, 비행기 제어시스템까지 통제 할 수 있게 된다. 이렇게 비행기 제어시스템이 악성코드에 감염되고 비행기가 오작동 되어 심각한 위험에 빠질 수 있다. [5]

이러한 보안위협 시나리오는 한 국가의 IoT기간망을 오류를 통하여 국가전체를 마비시킬 수 있는 상태로 유발한다.

III. 사물인터넷 보안 위협에 대한 방안

사물인터넷은 여러 요소 기술의 융합으로 기술의 취약점 발생 가능성뿐 만 아니라 기술이 융합되어 발생하는 새로운 취약점까지 대비해야한다. 따라서 본 논문에서는 각 분야에서의 보안 기술을 제안한다.

3.1 하드웨어 기반 데이터 암호화

복잡한 암호와 알고리즘은 기존 개인컴퓨터 환경에 초경량·저전력·저성능을 가진 디바이스가 인터넷과 연결되었을 때 사물인터넷(IoT) 장치에서 구현하기 힘들다. 사물인터넷 서비스를 절도, 파괴, 화재 등과 같은 각종 물리적인 위협으로부터 보호하는 방법은 존재하지만 IoT 네트워크 통신 신호를 교란하는 장비를 이용해 불법 무선통신 신호를 보내 서비스를 방해하는 무선신호 교란이나 데이터를 중간에 가로채어 위·변조 한 뒤 정상적인 기기가 이를 송신한 것으로 위장하는 네트워크 보안 위험 요소들이 있다. 이러한 네트워크 보안을 위협하는 제약들을 소프트웨어 기반에서는 완벽히 차단하기 어려움으로 하드웨어에서 송·수신하는 데이터를 암호화 처리 방식을 적용하여 해커들의 우회공격을 차단하고 디바이스 성능 저하와 배터리 소모율을 최소화 할 수 있게 한다.

3.2 AI 인공지능(머신러닝) 상용화

사물인터넷 서비스를 해킹 위험으로 보호하는 최상의 방법은 악성코드가 침입하기 전에 예방하는 것이다. 알파고와 같은 인공지능이나 인공지능의 전 단계인 머신러닝(Machine Learning) 기술을 보안 분야에 접목시키려는 시도가 본격적으로 진행되고 있다. 아직 인공지능과 보안 분야와의 접목은 구체화되지 못한 상태이다. 머신러닝에 기반을 두어 보안에 특화된 알고리즘과 각종 공격의 침투 방식을 학습하여 해킹으로부터 사전에 미리 사물인터넷을 보호한다.

3.3 사물인터넷 보안 교육 활성화

고등학생, 대학생 및 IT종사자 등 IoT보안을 전문적으로 하는 인력을 양성시켜 기존 보안기술 보다 상향된 IoT보안기술로 안전한 사물인터넷(IoT)을 사용할 수 있게 한다.

교육을 활성화시켜 초기부터 바로잡아 안전하게 IoT를 사용 할 수 있고 IP 노출 시 빠르게 대처할 수 있도록 하는 것이다. IoT제품과 서비스를 설계 시 정보를 보호하고 개인정보(privacy)를 강화시키기 위한 교육, 소프트웨어와 하드웨어를 안전하게 적용할 수 있는 교육, 안전한 운영·관리를 위한 교육, 보안문제가 생기기전에 초기보안설정에 힘쓰도록 교육, IoT제품 및 서비스의 보안프로그램·보안시스템을 계속적으로 업데이트 하는 교육을 통해 사물인터넷(IoT)의 IP노출과 위협을 방지한다.

3.4 인증 체계 강화

IoT(사물인터넷) 이용에 제일 중요한 핵심인 인증체계를 강화하여 보다 체계적이고 안전한 IoT 사용환경을 구성한다.

먼저 IoT 제품을 실행시킬 때 사용자에 대한 고유키 관리를 하여 1차적으로 사용자를 식별하고 1차 키 관리와 더불어 보조키를 생성하여 총 2차에 거친 이중 관리로 사용자 인증을 거치게 함으로써 번거롭지만 보다 안전한 IoT를 사용할 수 있도록 인증체계를 구축해야하며, 요즘 다양한 IT업계들이 주목하고 있는 홍채인식을 접목하는 방안도 있다. 사람마다 고유한 특성을 가진 안구를 활용한다. IoT 제품에 휴대용 기기를 추가적으로 연동하여 IoT 제품을 이용하고자 하는 사용자가 연동된 휴대용 기기로 홍채인식을 인증하는 방안이다. 이처럼 사용자 인증 관리를 이중화하고 다양한 인식체계를 수립하여 보안의 취약성을 대비할 수 있다.

또, 사용자 인증과 더불어 IoT 제품 간의 상호간의 인증을 체계하는 방안도 있다. IoT 제품은 신호를 주고받으며 연동되는 것이기 때문에 보안에 제일 취약할 수밖에 없다. 이 부분은 인증을 상호작용하게 하여 대비할 수 있다. 예를 들어 신호등과 해당 신호등을 제어할 수 있는 노트북이 있다. 일반적으로 노트북에서 신호등에게 신호를 보내 한 번의 신호로 신호등이 변화한다고 하면 인증의 상호작용은, 노트북에서 신호등에게 신호를 보내고, 이를 받은 신호등이 다시 노트북에게 신호를 보내 서로의 신호가 인증 된다면, 그때 작동하는 것이다. 인증을 거칠 수 있는 시스템을 개발하여 신호등에 장착하고 이 같은 상호작용 인증을 실현시킨다. 이 같이 방안들로 강화하여 인증 체계 시스템을 구축함으로써 IoT 보안 취약점 해결하고 보안성 높은 IoT 제품을 사용할 수 있다.

3.5 개인정보 보호를 위한 사이버 보안에 유의

대부분의 소비자들이 컴퓨터나 스마트폰이 악성코드에 감염될 수 있다는 것을 깨닫고 있지만, 다른 디바이스에 대한 위협에 대해서는 인식하지 못하고 지나치는 경우가 많다.

IoT제품은 긴밀히 연결된 사회 속에서 만들어진다. 따라서 사물인터넷(IoT)는 개인정보 및 프라이버시를 보호하기 위해 사이버보안에 각별히 유의해야 할 것이다.

인터넷 사이를 연결해주는 모뎀 · 라우터를 안전하게 보호하는 것이 가장 중요하며, 방화벽 구성이 제대로 되어있는지를 확인해야한다.

모든 디바이스의 보안 설정에 주의를 기울여야 하며, 비밀번호를 나만 아는 비밀번호나 문자, 숫자, 기호 등을 조합한 강력한 조합을 사용해야한다.

확인되지 않은 콘텐츠나 소프트웨어를 내려 받거나 실행하지 않으며 불법 콘텐츠가 유통되는 웹사이트에 방문하지 않는다.

사물인터넷 보안 위협에 대해 스스로가 보안에 예방하기 위해 지속적으로 관심을 갖고, 디바이스 관련 보안 교육을 충실히 이행한다.

3.6 보안 3대 요소에 기반을 둔 대안

원론적으로 보안의 3대 요소인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 측면에서 생각했다.

우선 기밀성 측면에서 보자면 국제 데이터 암호화 알고리즘 을 통해 인가된 기기 및 신호에 대해서만 허용하는 원천적 방어가 필수적이다. 국제데이터 암호화 알고리즘(International Data Encryption Algorithm, IDEA)은 스위스에서 1991년에 제작된 블록 암호 알고리즘이다. 현재 가장 안전하고 최고라고 여겨지는 알고리즘으로, 블록 초당 177Mbit의 빠른 처리가 가능하다.

무결성 측면에서는 맬웨어의 공격 및 감염으로 부터 보호하기 위한 Secure Boot를 사용해 비인가, 무허가 시도를 원천적으로 차단, 관리해야 한다. 이는 신뢰할 수 있는 하드웨어, 펌웨어 및 운영체제 로더 코드를 식별하는 키 목록을 미리 만들어 놓음으로써 부팅될 때 PC는 ROM, UEFI drivers, UEFI apps 등을 조사하여 키 목록과 비교하여 유효한 것으로 판단될 때 부팅하여 잠재적인 위협을 차단할 수 있다.

마지막으로 가용성 측면에서는 디바이스 간 통신방식을 다양하게 지원하고 Unique ID 기반 자산관리를 강화해야 한다.

IV. 결 론

본 논문에서는 사물인터넷 국·내외 보안 취약성 사례들과 IoT서비스 환경에서 발생 가능한 보안위협 해결방안을 분석하였다. 사물인터넷은 여러 요소 기술의 융합으로 발생하는 새로운 취약점에 대한 현재 보안 해결책은 미비한 상태이다. 보안이 취약한 공통적인 이유는 사용자의 IP가 노출되어 문제가 생긴다. 하드웨어 기반 데이터 암호화를 통하여 해커들의 우회 공격을 차단하고 사물인터넷에 인공지능(머신러닝)을 상용화하여 침투 방식을 학습한다. 안전한 IoT 사용 환경을 구성하도록 인증체계를 강화하고 암호를 강력한 조합을 사용해 개인정보 보호를 위한 사이버 보안에 유의한다. 보안 3대 요소에 기반을 둔 대안을 활용하여 해킹으로부터 사전에 미리 사물인터넷을 보호하고 사물인터넷 보안 교육을 활성화시켜 보안 기술을 상향시킨다면 사물인터넷을 보안 위협으로부터 보호할 것으로 기대된다. 향후 연구에서는 본 논문에서 제안한 IP노출 위협 예방 시스템을 기반으로 정부의 적극적인 지원과 함께 사물인터넷 제품과 통신망을 보유하고 있는 국내 대기업 및 통신업체들과의 상생환경을 조성하는데 적극 참여해야 될 것으로 판단된다.

References

[1] Bae Sang Tae, Kim Jin Kyung, "Paradigm Shift of Development and Security of Internet (IoT) “, 2016

[2] Kim, Ho-Won, "Security / Privacy Issues in the Internet Environment", TTA Journal, p36~p37, 2014

[3] http://www.etnews.com/20151207000287, 2015

[4] http://biz.chosun.com/site/data/html_dir/2014/01/19/2014011900725.html, 2014

[5] Ministry of Science, ICT and Future Planning, "Internet of Things-Information Protection Roadmap", 2014

[6] Yoon Kyungbae, Chang Younghyun, “IOT-based SMEs producing standardized information system model analysis and design “, The Journal of the Convergence on Culture Technology (JCCT), Vol. 2, No. 1, pp.87-91, February 2016.

[7] Lee Myung-Ryul, Park Jae-Pyo, “Analysis and Study on Invasion Threat and Security Measures for Smart Home Services in IoT Environment IoT(Internet of Things)” , 2016