JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 8, pp. 73-79, August 2020
https://doi.org/10.9708/jksci.2020.25.08.073

A Survey Analysis of Internet of Things Security Issues and Combined Service

HyunHo Kim*, HoonJae Lee**, YoungSil Lee***

*Professor, Division of Computer Engineering, Dongseo University, Busan, Korea
**Professor, Dept. of Information and Communication Engineering, Dongseo University, Busan, Korea
***Professor, Computer Engineering department in International College, Dongseo University, Busan, Korea

[Abstract]

Since the start of the 4th industrial revolution, technologies have been developed in the Internet of Things (IoT), artificial intelligence (AI), virtual reality (VR), and 5G. Compared to other technologies IoT is currently being commercialized more than other technologies where the numbers of connected things are increases every year. The IoT has a huge advantage to provide convenience and lots of information to users, but security cannot keep up with the speed of development. IoT services continue to provide services for related devices, but at present, more and more types of new services are being combined with other technologies by utilizing the services of devices. This paper reviews and analyzes research on security issues and services related to the Internet of Things to explore how security trends and service delivery will develop in the future.

▸ **Key words**: Internet of Things, IoT Security Issues, IoT Service, IoT Trend

[요 약]

최근 4차 산업혁명의 시작으로 사물인터넷, 인공지능, 가상현실, 5G 등 분야의 기술이 많이 발전하고 있다. 그 중 사물인터넷의 경우 다른 기술들에 비해 현재 상용화가 많이 되어 있으며, 계속해서 사물의 연결 수는 매년 증가하고 있다. 이렇게 계속해서 증가하고 있는 사물인터넷은 사용자의 편의성과 많은 정보를 제공하는 큰 장점이 있지만, 보안은 발전 속도와 비교하면 따라가지 못하고 있다는 것으로 나타났다.

사물인터넷 서비스는 관련 기기마다 서비스를 계속해서 제공하고 있지만, 현재는 기기의 서비스를 활용하여 다른 기술과 결합해서 새로운 서비스를 제공하는 유형도 늘어가고 있는 것으로 나타났으며, 앞으로도 더욱 더 넓은 범위의 서비스가 생겨날 것으로 예상한다. 이렇게 다방면으로 빠르게 발전하고 있는 사물인터넷 기술의 발전방향을 파악하여 안전하게 사물인터넷을 사용할 수 있도록 관련된 보안연구가 필요하다. 이에 따른 연구의 결과는 하드웨어 업그레이드나 소프트웨어적인 패치로 안정성을 보장할 수 있었다. 본 논문에서는 사물인터넷에 관련된 보안 이슈와 서비스에 관한 연구를 조사하여 발전방향을 분석한 후 현재 트랜드를 알아보고 이와 관련하여 필요한 보안요소 앞으로의 보안방향 및 서비스제공이 어떠한 형태로 발전되어 나아갈지 알아본다.

▸ **주제어**: 사물인터넷, IoT 보안, IoT 이슈, IoT 서비스, IoT 트랜드

• First Author: HyunHo Kim, Corresponding Author: YoungSil Lee
*HyunHo Kim (feei20@gdsu.dongseo.ac.kr), Division of Computer Engineering, Dongseo University
**HoonJae Lee (hjlee@dongseo.ac.kr), Dept. of Information Communication Engineering, Dongseo University
***YoungSil Lee (lys0113@dongseo.ac.kr), Computer Engineering department in International College, Dongseo University
• Received: 2020. 04. 22, Revised: 2020. 06. 09, Accepted: 2020. 08. 13.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

4차 산업혁명의 시작으로 사물인터넷(IoT : Internet of Things), 인공지능(AI : Artificial intelligence), 가상현실(VR : Virtual Reality), 5G 통신, 로봇 등 분야의 기술이 집중적으로 발전하고 있다. 이러한 분야 중 IoT 분야의 경우 다른 분야에 비해 상용화 빠른 편이며, IoT와 관련된 제품이 많이 출시하고 있다.

사물인터넷이란 사물과 사물이 서로 인터넷을 통해 연결되어 구성된 인터넷이라고 표현할 수 있으며[1], 현재 유·무선 인터넷으로 연결되어 사용되고 있는 대표적인 모바일, 컴퓨터와 다르게 모든 사물(자동차, 책상, 전등 등)이 연결되어 구성된 인터넷이라고 할 수 있다. 사물인터넷을 활용한 사용자의 관점에서는 이전보다 더 편리하고 스마트한 일상생활을 할 수 있으며, 산업체에서는 보다 높은 생산성 및 안전성이 향상될 것으로 생각된다.

가트너에 따르면 2018년도에 비해 2019년도는 21.5%증가한 48억 개의 엔드포인트가 사용될 것으로 전망하였고, 2020년 엔터프라이즈 및 자동차 관련 IoT 시장이 2019년과 비교하면 약 21% 증가한 58억 개의 엔드포인트로 성장할 것으로 예측하고 있다. 이 중 사물인터넷 엔드포인트를 가장 많이 사용될 것으로 꼽히는 분야는 유틸리티가 1위, 침입 탐지와 실내 감시용 장치 사용과 같은 물리적 보안 분야가 2위, 정부 기관을 3위로 꼽았다[2]. 이처럼 점점 커져가는 사물인터넷의 발전을 위해서는 사용자로부터 편리하고 안전하게 사용할 수 있는 신뢰가 인식되어야 한다.

사물인터넷의 특성상 휴대성, 무게, 디자인 등과 같이 일반적인 장비보다는 소형화되어 나오는 제품이 많으며, 이러한 제한적인 요소 때문에 사물인터넷에서의 보안영역은 크게 제한적인 것이 해결해야 하는 큰 과제이다. 산업연구원의 조사에 따르면 IoT 제품의 해킹 및 보안 피해 규모는 2020년 17조 7,000억원, 2030년 26조 700억원으로 예상하고 있다[3].

점차 늘어나는 사물인터넷 시장에서는 이제 제품개발뿐만 아니라 사물인터넷 관련된 서비스도 다양하게 제공하려고 노력하고 있으며, 더 나아가 사물인터넷 기술이나 서비스를 클라우드, 가상현실, 인공지능 등과 같이 다른 기술과도 결합하여 새로운 사물인터넷 서비스를 제공하기도 한다. 이처럼 사물인터넷과 결합하여 만들어진 서비스는 인공지능 스피커, 스마트 센서, 스마트 시티, 헬스 케어, 영상기반 가상현실을 예로 들 수 있다[4].

본 논문에서는 사물인터넷과 다른 서비스가 결합한 서비스들의 동향을 비교·분석하고 분석된 결과를 바탕으로 사물인터넷 서비스의 발전 방향을 알아보고자 한다.

본 논문의 구성은 Ⅱ장에서 사물인터넷 보안 이슈 동향에 대해 살펴보고 Ⅲ장에서는 사물인터넷 서비스에 대해 알아본다. 그리고 Ⅳ장에서는 Ⅱ,Ⅲ장에서 살펴본 동향을 분석하고 발전 방향을 살펴보고 끝으로 Ⅴ장에서 결론을 맺는다.

II. IoT Security Issues

사물인터넷 보급이 빠르게 확산됨으로 인해 사물인터넷 관련 보안 이슈도 계속해서 늘어나고 있다. 이에 따라 전 세계적으로 대책을 세우고 있으며, 미국의 경우 R&D 우선 과제로 지정하고 IoT 분야 프로젝트에 대한 연구투자를 지원하고 있다[5].

현재 국내외 사물인터넷에 관련한 연구 중 프레임워크에 관련한 연구와 보안 요구사항 연구가 많이 이루어지고 있다. 대표적인 사물인터넷의 플랫폼은 oneM2M(Machine to machine), Azure IoT, Cisco IoT Cloud Connect, IBM Watson IoT 등 많은 플랫폼이 있으며, 이러한 플랫폼 중 oneM2M 플랫폼을 제외한 나머지 플랫폼은 대부분 MQTT와 CoAP, TLS, DTLS 보안 기술을 적용하여 사용한다[6].

본 장에서는 사물인터넷 보안 및 위협요인을 분석하기 위해 사물인터넷 보안 이슈와 관련된 연구 동향을 알아보고자 한다.

1. IoT Security Threat

oneM2M은 전 세계의 사물인터넷 서비스 플랫폼을 표준화 된 플랫폼으로 개발하기 위한 목적으로 세계 주요 7개의 기관이 참여하여 설립한 표준 단체이며, 6개의 WG(Working Group)으로 구성되어 있다. 이들은 사물인터넷 분야의 주요 기술 규격과 기술보고서를 작성하고 배포하였다[7]. 대표적인 기술 규격과 기술보고서는 아래 Table. 1(TS-0008-Security Technical Specification), Table. 2(TS-0002-Requirements Security Countermeasures)와 같다.

TS-0008-V2.0.0 기술보고서에서는 IoT 및 M2M시스템에서 발생 가능한 보안 취약점을 21가지로 분류하여 작성되어 있으며, Table. 1에서는 그 중 데이터 탐지 및 인가되지 않은 어플리케이션이 디바이스 내 메모리에 생기는 문제점을 나열하였다.

Table 1. TS-0008-V2.0.0 oneM2M Technical Report (Security)[8]

ID	Vulnerability
1	Discovery of Long-Term Service-Layer Keys Stored in M2M Devices or M2M Gateways
2	Deletion of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways
3	Replacement of Long-Term Service-Layer Keys stored in M2M Devices or M2M Gateways
4	Discovery of Long-Term Service-Layer Keys stored in M2M Infrastructure
5	Deletion of Long-Term Service-Layer Keys stored in M2M Infrastructure equipment
6	Discovery of sensitive Data in M2M Devices or M2M Gateways
10	Unauthorized or corrupted Applications or Software in M2M Devices/Gateways

Table 2. TS-0002-V2.7.1 one M2M Technical Specification(Requirements)[9]

Requirement ID	Countermeasures
SER-002	The oneM2M System shall be able to ensure the Confidentiality of data.
SER-003	The oneM2M System shall be able to ensure the Integrity of data.
SER-008	The oneM2M System shall support countermeasures against unauthorized access to M2M Services and M2M Application Services.
SER-010	The oneM2M System shall be able to support mechanisms for protection against misuse, cloning, substitution or theft of security credentials.
SER-011	The oneM2M System shall protect the use of the identity of an M2MStakeholder within the oneM2M System against discovery and misuse by other stakeholders.
SER-012	The oneM2M System shall be able to support countermeasures against Impersonation attacks and replay attacks.
SER-013	The oneM2M System shall be able to provide the mechanism for integritychecking on boot, periodically on run-time, and on software upgrades for software/hardware/firmware component(s) on M2M Device(s).
SER-023	Where a Hardware Security Module (HSM) is supported, the oneM2M System shall be able torely onthe HSM to provide local security
SER-024	The oneM2M System shall enable M2M Applications to use different and segregated security environments.

TS-0002-V2.7.1 기술 규격에서는 IoT 및 M2M시스템에서 발생 가능한 보안 취약점 26가지에 대응하기 위한 요구사항으로 총 26가지를 제시하고 있으며 그 중 Table. 2는 Table. 1에 대한 대응방안에 대해 나타낸 것이다.

박세환[10]의 연구에 따르면 IoT 기기의 70%가 수집된 정보를 암호화하지 않은 상태로 전송하고 있으며, IoT 기기의 60%는 보안에 취약한 웹 인터페이스를 적용하고 있다고 한다. 또한, 소프트웨어 업데이트를 할 때 60%가 암호화나 접근 권한에 대한 취약점이 드러난 것으로 조사되었다.

Table 3. IoT Device Security Risk[10]

Device list	Security risk(%)
Smartphone	41.3
Tablet PC	10.7
Car	9.4
Home IoT	8.8
Wearable Device	8.3
Medical Device	7.2

Table 3과 같이 보안리스크가 가장 높은 항목은 스마트폰(41.3%)으로 조사되었으며, Tablet PC(10.7%), 자동차(9.4%), 홈 IoT(8.8%), 웨어러블 기기(8.3%), 의료기기(7.2%) 순으로 결과가 나왔다. 추가로 IoT 네트워크 보안 관련 설문조사 중 전체 응답자의 약 66%는 개인정보 노출, 시스템 보안에 대해 우려하고 있었다.

2. A Study on Priority of Certification Criteria for IoT Security Certification Service[11]

본 연구에서는 사물인터넷 보안역량 강화 및 활성화를 위해 보안 인증 기준을 중요도에 대한 우선순위를 도출하여 가이드라인을 제시한다.

사물인터넷 보안 인증 기준 항목의 상대적인 중요도를 위해 한국인터넷진흥원의 IoT 보안 시험인증 기준을 준수하여 아래 Table. 4와 같이 계층별로 연구모형을 분류하였다.

Table. 4 Research model

Class 1	Class 2
Authentication	User authentication, Safe use of authentication information, Product Certification
Password	Use secure password algorithm, Secure key management, Safe random number generation
Data Security	Information flow, Privacy, Secure session management, Use a secure password algorithm
Platform Security	Software security, Secure update, Security management, timestamp
Physical Security	Physical interface protection, Stepless defense

위의 Table 4는 설문조사 항목 중 IoT 보안 인증서비스 평가항목 중 하나이며, 2019년 3월부터 4월 초까지 보안 인증 관련 담당자(전문가)를 대상으로 설문 조사를 실시하였다. 그리고 설문은 총 12부의 설문을 배부하여 10부의 설문을 회수하였으며, 설문 조사의 답을 기준으로 계층별 중요도와 우선순위를 정한다. 이를 통해 도출된 평가항목의 중요도 최종우선순위는 데이터 보호 항목의 개인정보보호가 가장 높은 항목이며, 가장 낮은 항목은 인증항목으로 나타났다.

한국인터넷진흥원에서 조사한 IoT 기기에 대한 보안 위협 인식도 설문 조사에서는 IoT 사용자 564명이 참여하였으며, 2018년 2월 23일부터 3월 27일까지 “IoT 기기 사용 현황 및 IoT 보안에 대한 인식도”, “안전한 IoT 기기 사용을 위한 활동 현황과 보안 위협 체감 정도”, “안전한 IoT 기기 사용을 위한 활동 현황과 보안 위협 체감 정도”의 3개 카테고리, 총 9개의 항목으로 구성하였다. 설문에 참여한 사용자 중 IoT 기기 사용자는 1개 이상에서 94%의 응답률을 보였으며, 이 중 최근 1년 이내 접속 횟수에서는 80%가 최소 1회 이상 접속하였다고 응답하였다. 또한, 같은 기간(1년) 암호 변경 여부에 대해서는 67% 이상이 최소 1회 이상 변경하고 있다고 응답하였다. 끝으로 해킹이 의심되는 정황에 대해서는 78%가 “전혀 없다”로 응답하였다[12].

III. IoT Service Trend

현재 IoT에 관련된 연구는 단말기, 보안, 네트워크 등 매우 다양한 방면으로 연구가 진행 중이며, 그중 보안은 각종 해킹 사건으로 인해 더 집중하여 연구될 필요가 있다고 생각된다. 하지만 IoT 기기 특성 및 제원으로 볼 때 일반적인 보안을 적용하는 것과 다르게 저전력, 저용량과 같은 요소로 인해 일반적인 보안요소와 같은 보안을 만들기에는 한계점이 존재한다.

본격적으로 사물인터넷이 보급이 시작된 이후 사물인터넷 서비스는 주로 웨어러블 디바이스와 홈 IoT 및 스마트 서비스 시장이 크게 늘어나고 있다. 한국정보화진흥원의 보고서에 따르면 하루 평균 12.3시간을 집에서 보내고 있다고 조사되었으며, 그만큼 집에서 보내는 시간이 편하다고 인식한다고 해석해 볼 수 있다[13]. 이와 같은 결과는 앞으로의 사물인터넷 서비스 중 홈 IoT 분야는 크게 발전할 것으로 생각해 볼 수 있다.

본 장에서 기존 분야별 다양한 연구들의 분석을 통해 문제점 및 개선해야 할 부분을 분석하고, 이에 따른 공통점과 문제점 알아본다.

1. Smarthome Service

계속해서 발전하는 통신 기술과 스마트폰의 보급으로 인해 모니터링 및 기타 제어 장비와 같이 수많은 기기의 연결성이 크게 증가하였다. 이를 바탕으로 스마트폰, 통신업체 등 제조사들은 서로 협력하여 새로운 서비스를 제공하는 데 노력하고 있다. 그중 하나의 서비스인 스마트홈 서비스는 현재 사용자들에게 크게 관심받는 서비스 중 하나로 자리 잡고 있다.

이학준[14]의 연구내용에 따르면 미국에서는 개인 주택이 차지하는 비율이 높아서 개별 가정의 보안과 에너지 비용 절감에 관해 관심이 높다고 말하고 있으며, 이를 기반으로 스마트홈의 서비스 방향도 보안이 강화되고 에너지 비용을 절감하는 방향으로 개발되고 서비스를 제공하고 있다고 말한다.

사용자의 설문 조사에서는 스마트홈에서 가장 가치 있는 분야는 보안 부분으로 확인되었으며, 서비스 부분에서는 침대에서 가전기기들을 제어하거나, 원격으로 온도 조절을 할 수 있는 기능을 원하는 사용자가 많은 것으로 조사되었다.

이와 관련하여 IoT 서비스 시장에서는 스마트 홈 리모컨[13], 음성기반 홈 IoT[15], 전용 통신망을 이용한 사물인터넷 무선통신시스템[16], 스마트 센서[17]와 같은 서비스가 큰 인기를 끌고 있다.

2. Services combined with IoT technology

최근에는 IoT의 시장에서는 IoT 기술과 새로운 서비스가 결합하여 새로운 서비스를 제공하고 있다. 이는 각각의 기기 간의 활용성이 합쳐져서 새로운 서비스를 만들어 제공한다는 의미이기도 하다. 대표적으로 IoT 기술과 VR[18], 자동차(전기이륜차)[19], 방범[20], AI(지능형)[21], 산업 등이 있으며, 이와 같은 서비스들의 시작점은 스마트폰이 그 중심에 있으며, 많은 전문가도 앞으로의 미래가 사물인터넷과 인공지능 등의 기술이 산업적으로도 새로운 패러다임으로 잡을 것으로 예상하고 있다.

IoT 기술을 활용한 VR 서비스의 이전의 VR기기를 통해 한정적인 부분을 개선한 서비스라고 할 수 있으며, 언제든지 촬영한 영상이나 이미지를 사용자가 서버에 공유하고 공유된 서버를 통해 VR기기를 가지고 있는 사용자는 영상을 공유받아 실제 있는 장소나 사이버 공간을 VR기기를 통해 체험할 수 있는 서비스를 말한다.

자동차(전기이륜차)는 스마트폰의 무선통신 방식을 이용하여 클라우드 서비스를 통해 주차 위치, 원격조정(시동, 도어락 등), 배터리 상태 등을 파악할 수 있다. 방범에서는 IoT를 기반으로 클라우드 서비스를 통해 얼굴인식을 하여

사용자에게 알려주는 알림 및 탐지 서비스가 있다.

산업에서는 인공지능과 결합하여 이용되는 경우도 많지만, 인공지능의 한계점과 불완전성을 극복하기 위해 최근에는 인공지능보다 사물인터넷을 적용하는 방향으로 바뀌어 가고 있는 추세이다.

IV. IoT Security and Service Analysis

본 장에서는 Ⅱ장과 Ⅲ장에서 알아보았던 동향 및 연구 내용을 기반으로 보안과 서비스 동향을 분석하고 앞으로의 사물인터넷의 발전 방향을 알아보고자 한다.

현재 IoT 보안 관련에서는 주로 프레임워크에 대한 연구가 가장 많이 이루어지고 있었으며, 그 이유는 플랫폼과 관련이 많았다. 이에 따라 IoT 관련 제품이나 서비스가 서로 연계하거나 협업하여 지능형 서비스를 제공하는 데 필요하기 때문으로 분석된다. 그리고 이와 관련된 플랫폼은 oneM2M, MQTT와 CoAP, TLS, DTLS 보안 기술 등의 연구가 활발히 진행되고 있었으며, 이 중 oneM2M이 가장 많이 사용되고 있는 보안 기술로 나타났다. 특히 oneM2M은 사물인터넷 플랫폼 표준화를 위한 목적을 크게 가지고 있으며, 6개의 WG로 구성되어 있다. 또한, IoT에 대한 기술보고서(TS-0008) 및 관련한 보안 요구사항(TS-0002) 외 사물인터넷이 관련하여 권고하는 문서를 제공하고 있었다.

IoT 기기에 대한 보안에서는 대다수의 기기가 수집된 정보를 암호화하여 전송하지 않는다는 문제, 취약한 인터페이스를 적용하는 문제, 소프트웨어 업데이트 중 암호화 및 접근 권한이 있었으며, 관련하여 보안리스크가 가장 큰 장치는 스마트폰, 태플릿 PC와 같이 사용성 및 휴대성이 높은 기기가 최고 리스크가 큰 것으로 나타났다.

IoT 관련된 서비스에서는 기기에 따라 단일서비스도 여러 가지 서비스를 제공하고 있지만, 헬스케어, 스마트홈, 스마트공장, IoT 방범 등 IoT와 결합한 형태의 서비스도 계속해서 증가하고 있는 것으로 나타나고 있다. 이를 바탕으로 앞으로의 IoT 서비스는 다른 플랫폼 및 서비스와 결합하여 새로운 서비스가 많이 만들어질 것으로 예상해 볼 수 있으며, 발전 방향 또한 결합한 서비스 및 관련한 보안으로 맞추어 나아갈 것으로 사료된다.

V. Conclusions

4차 산업혁명이 시작되고 새로운 분야의 기술들이 많이 등장 했다. 대표적인 기술은 사물인터넷, 인공지능, 가상현실, 5G 무선통신기술, 로봇 등이 있다. 이 중 사물인터넷은 현재 가장 많이 상용화되어 있으면서, 관련 기기와 서비스도 매년 계속해서 늘어나고 있다. 이와 관련하여 가트너에서는 가장 많이 사용되는 엔드포인트 1위로 유틸리티 2위는 침입 탐지 3위는 정부 기관으로 조사된 바 있으며, IoT 제품의 해킹 및 보안 피해 규모에 관련해서 산업연구원에서는 2020년도 17조 7,000억 원, 2030년도는 26조 700억 원으로 예상하고 있다. 이러한 근거로 인해 사물인터넷의 규모와 서비스 발전은 매년 크게 상승하는 것을 예상해 볼 수 있다.

신뢰 있고 안전한 사물인터넷 발전을 위한 연구는 계속해서 진행되고 있으나, 대부분 프레임워크를 중심으로 연구가 진행되고 있으며, 서비스 보안 연구는 미비한 것으로 나타났다. 이에 따라 본 논문에서는 사물인터넷 보안과 서비스에 관련하여 연구된 자료들을 분석하고 발전 방향을 알아보고자 하였다.

사물인터넷 보안은 계속해서 발전하는 결합서비스를 대응하기 위해 현재 프레임워크를 중심으로 많이 연구되고 있는 것으로 나타났으며, 대표적으로 스마트폰, 웨어러블 디바이스, 태블릿 PC와 같이 휴대성이 좋고 확장성이 좋은 기기를 중점으로 제공되는 서비스가 많았다. 하지만 그 밖에 대부분의 IoT 기기는 보안이 취약하다는 문제가 많았으며, 그 이유는 IoT 기기 특성상 스펙 및 암호화의 한계로 인해 일반적인 기기들에 비해 보안이 떨어질 수밖에 없는 것으로 분석된다. 대표적으로 취약한 인터페이스와 정보를 암호화하여 전송하지 않는 문제가 꼽혔으며, 이와 같은 문제는 하드웨어적인 업그레이드나 소프트웨어 업데이트 및 보안 패치와 같은 방법으로 문제 대부분이 해결될 수 있을 것으로 생각된다.

사물인터넷 서비스는 단독적인 서비스도 충분히 유용하게 사용될 수 있지만, 최근 동향을 살펴볼 때 다른 기술과 결합하여 새로운 형태의 서비스가 늘어나는 추세이며, 이에 따라 안전한 서비스를 제공하기 위한 연구도 늘어나고 있었다. 하지만 IoT 기기 특성으로 생긴 보안 취약점은 일반적으로 대응하는 보안방법을 적용하는 데 한계가 있었지만, 다른 방법으로 해결할 수 있는 방향이 존재했다. 이와 같은 연구의 발전으로 앞으로의 사물인터넷 서비스의 종류와 사용범위는 매우 늘어날 것으로 예상하며, 또한 본 논문을 통해 앞으로의 IoT 기기 및 서비스 연구에 도움이 될 것으로 사료된다.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (grant number: 2018R1C1B5043135). and Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology (grant number: NRF-2016R1D1A1B01011908).

REFERENCES

[1] H. C. Lee, “A Study on the Security Solution for IoT Communication Protocols, ” Proceedings of Symposium of the Korean Institute of Communication and Information Sciences, pp. 284-285, Nov. 2019.

[2] CIO Korea, New Technology and Future, 2019. 4. Available: http://www.ciokorea.com/news/130210

[3] S. J. Yun, J. D. Kim, “A Study on Security Requirments Analysis through Security Threat Modeling of Home IoT Appliance,” The Jounal of Society for e-Business Studies, vol. 24, no. 2, pp. 113-124, May. 2019.

[4] V. Sindgura, P. Ramya, “An IoT Based Smart Mobile Health Monitoring System,” 2nd International Conference on Inventive Communication and Computaltional Technologies, 2018.

[5] D. H. Lee, N. J. Park, “IoT product security certification and security maintenance,” Information and Communications Magazine, vol. 33, no. 12, pp. 28-34, 2016.

[6] H. Y. Kim, J. H. Ji, A. M. Awaludin, H. W. Kim, “Linking device security and platform security for secure IoT services,” Korea Institute Of Information Security And Cryptology, vol. 28, no. 5, pp. 26-30, Otc. 2018.

[7] K. Y. Lee, B. S. Kim, J. S. Cho, “Design and Implementation of Security System for Providing Secure Boot and Firmware Update,” Journal of Korean Institute of Information Scientists and Engineers, vol. 45, no. 4, pp. 321-331, Apr, 2018.

[8] OneM2M partners, "TR-0008-V2.0.0: Security," oneM2M Technical Report, Aug. 2016.

[9] OneM2M partners, "TS-0002-V2.7.1: Requirements," oneM2M Technical Specification, Aug. 2016.

[10] S. H. Park, “IoT Security Issues and Domestic and Foreign Security Technology Development Trends”, The Magazine of the IEEE, vol. 44, no. 5, pp. 18-22, May. 2017.

[11] D. Y. Kang, J. H. Hwang, “A Study on Priority of Certification Criteria for IoT Security Certification Service,” Journal of The Korea Contents Association, vol. 19, no. 7, pp. 13-21, Jul. 2019.

[12] KISA, “KISA Cyber Security Issue Report,” Apr. 2018.

[13] A. S. Oh, “Design and Implementation of Smart Home Remote Control Based on Internet of Things Service Platform, ”, Journal of the Korea Institute of Information and Communication Engineering, vol. 22, no. 12, pp. 1563-1570, Dec. 2018.

[14] H. J. Lee, “IoT based smart home,” The Journal of The Korean Institute of Communication Sciences, vol. 32, no. 4, pp. 44-49, Mar. 2015.

[15] S. G Kim, J. Y. Yun, “A Study of Voice Interactive Home IoT Service to Improve User’s “Ability”, ” The Human Computer Interaction Society of Korea, pp. 881-885, Feb. 2019.

[16] I. S. Sohn, “5G IoT Technology Trend and Prospect,” The Magazine of the IEEE, vol. 46, no. 4, pp. 56-63, Apr. 2019.

[17] S. Kang, Daehyeon Yim, Sungho Cho, “Smart sensor development and service implementation for smart IoT environment,” Proceedings of Symposium of the Korean Institute of communications and Information Sciences, pp. 426-427, Jan. 2018.

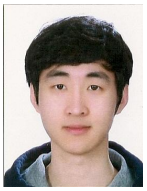
[18] D. H. Kim, D. H. You, “A Study on virtual reality (VR) service technology based on photorealistic video using Internet of Things (IoT) technology, ” The Journal of The Korean Institute of Communication Sciences, vol. 35, no. 9, pp. 3-11, Aug. 2018.

[19] C. M. Park, N. J. Kim, J. Y. Paek, D. G. Lee, J. E Lee, H. P. Jang, K. H. Ro, S. H. Kim, J. S. Lee, S. D. Zu, “A Study on Bettery Swapping Electric Two-wheeler Vehicle Service based on the Internet of Things, ” Proceedings of the Korean Society of Computer Information Conference, pp. 508-511, Jul. 2018.

[20] I. S Kim, J. H. Lee, W. H. Nam, “Implementation of IoT Home Security Service in Cloud-Based Mobile Environment, ” Proceedings of The Institute of Electronics and Information Engineers, pp. 1250-1252, Jun. 2018.

[21] D. G. Jeong, D. U. Song, “Characteristics of IoT-Artificial Intelligence Technologies and Their Related Industry Trend, ” Korea Institute of Information Technology Magazine, pp. 29-39, Dec. 2017.

Authors



HyunHo Kim is an visiting professor of the Division of Computer Engineering at Dongseo University, Rep. of Korea. He received his Ph.D. degree in 2020 at the Dongseo University Graduate School, BS's and Master's Degree from the Dongseo University. His research interests are Digital Forensic Information Security Network Security Internet of Thing(IoT)

HoonJae Lee received his BS, MS, and PhD. degrees in Electrical Engineering from Kyungpook National University, Daegu, South Korea, in 1985, 1987, and 1998, respectively. He is currently a professor in the Department of Information and Communication Engineering at Dongseo University. From 1987 to 1998, he was a research associate at the Agency for Defense Development (ADD). His research interests include developing secure communication system side channel attack and ubiquitous sensor network/radio frequency identification security.

YoungSil Lee is an assistant professor of the Computer Engineering department in International College at Dongseo University, Rep. of Korea. She received a Ph.D. degree in 2015 at the Dongseo University Graduate School and she got her BS's and Master's Degree from the same University. Her research interests are cryptography information security sensor network body area network healthcare, artificial intelligence and cloud computing.