JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 27, No. 1: 97~102, Jan. 2023

IoT 환경의 단말 인증 시스템

강동연[1] · 전지수[1] · 한성화[2*]

Device Authentication System in IoT environment

Dong-Yeon Kang[1] · Ji-Soo Jeon[1] · Sung-Hwa Han[2*]

[1]Student, Department of Information Security, Tongmyong University, Busan, 48520 Korea
[2*]Professor, Department of Information Security, Tongmyong University, Busan, 48520 Korea

요 약

IoT는 전통적인 정보 서비스뿐만 아니라 다양한 분야에서 활용되고 있다. 특히 스마트 홈, 스마트 해양, 스마트 에너지나 스마트 팜 등 많은 융합 IT 분야에서 IoT 기술을 활용하고 있다. IoT 기반 정보 서비스의 서버에 대하여, 지정된 프로토콜을 사용하는 IoT 단말은 신뢰된 객체이다. 그래서 악의적 공격자는 인가되지 않은 IoT device를 사용하여 IoT 기반 정보 서비스 접근, 인가되지 않은 중요 정보에 접근 후 이를 변조하거나 외부에 유출할 수 있다. 본 연구에서는 이러한 문제점을 개선하기 위하여 IoT 기반 정보 서비스에서 사용하는 IoT 단말 인증 시스템을 제안한다. 본 연구에서 제안하는 IoT 단말 인증 시스템은 MAC address 등의 식별자 기반 인증을 적용한다. 본 연구에서 제안하는 IoT 단말 인증 기능을 사용하면, 인증된 IoT 단말만 서버에 접근할 수 있다. 본 연구는 비인가 IoT 단말의 세션을 종료하는 방식을 적용하므로, 보다 안전한 단말 인증 방식인 접근 차단에 대한 추가연구가 필요하다.

ABSTRACT

IoT is being used in a lot of industry domain such as smart home, smart ocean, smart energy, and smart farm, as well as legacy information services. For a server, an IoT device using the same protocol is a trusted object. Therefore, a malicious attacker can use an unauthorized IoT device to access IoT-based information services and access unauthorized important information, and then modify or extract it to the outside. In this study, to improve these problems, we propose an IoT device authentication system used in IoT-based information service. The IoT device authentication system proposed in this study applies identifier-based authentication such as MAC address. If the IoT device authentication function proposed in this study is used, only the authenticated IoT device can access the server. Since this study applies a method of terminating the session of an unauthorized IoT device, additional research on the access deny method, which is a more secure authentication method, is needed.

키워드 : IoT, 단말 인증, 인증 서버, 아두이노

Keywords : IoT, Device Authentication, Authentication Server, Arduino

Received 28 November 2022, **Revised** 7 December 2022, **Accepted** 14 December 2022

*** Corresponding Author** Sung-Hwa Han(E-mail:shhan@tu.ac.kr, Tel*** - **** - ****)
Professor, Department of Information Security, Tongmyong University, Busan, 48520 Korea

Open Access http://doi.org/10.6109/jkiice.2023.27.1.97 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

IoT(Internet of Things)는 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술이다. 이 IoT는 Web 서비스를 주축으로 하는 정보 서비스를 다양한 분야로 확장하였다. 각종 분야에서 필수적으로 취급하는 정보를 획득하기 위해 센싱(Sensing)하거나 [1], 센싱 데이터를 바탕으로 상태를 분석하여 대응 행동을 결정하고 이행하는데 IoT는 IT 융합 분야에 필수적인 요소이다 [2].

이 IoT 서비스는 크게 IoT 서버와 IoT 단말로 구성된다. IoT 단말은 센싱 데이터의 생성과 전달, 그리고 대응 행동 이행을 담당하고, IoT 서버는 센싱 데이터를 수집하고 저장·분석하여 대응 행동을 결정한다. 이러한 IoT 서비스는 그 목적에 따라 다양한 종류의 단말을 사용하고, 또 서비스 범위에 따라 취급하는 단말의 개수도 많아질 수 있다 [3].

이러한 IoT 서비스는 기본적으로 경량 플랫폼을 추구하기 때문에, 다양한 보안 체계를 갖춘 legacy 정보 서비스보다는 보안에 취약할 수 있다. 악의적 공격자는 이러한 취약점에 집중하여, 인가되지 않은 IoT 단말을 서비스에 접근시킬 수 있다. 이를 통하여, IoT 서비스에 접근, 중요 내부 정보를 변조하거나 외부에 유출할 수 있다. 중요 정보를 변조한다면 IoT 서비스가 오동작하거나, 변조된 센싱 데이터 분석으로 잘못된 대응 행동을 결정하는 등 다양한 피해를 발생시킬 수 있다 [4]. 그러므로 IoT 서비스에는 충분히 검증된 IoT 단말만 서버에 접근할 수 있어야 한다.

본 연구에서는 IoT 서비스에 대하여, 서비스 제공 중 서버에 접근하는 IoT 단말을 식별·인증할 수 있는 시스템을 제안한다. 제안하는 IoT 단말 인증 시스템은 서버와 IoT 단말에서 동작하는 각각의 컴포넌트로 구성된 아키텍처와 보안 요구기능, 그리고 각 보안 기능의 동작 순서이다. 또, 본 연구에서 제안하는 IoT 단말 인증 시스템의 기능을 확인하기 위하여 제안한 아키텍처에 따라 실증 구현하고 목표한 기능을 검증한다.

본 연구에서 제안하는 IoT 단말 인증 시스템을 사용하면, IoT 서버에 접근하는 IoT 단말을 식별하고 인증하여 안전한 서비스를 운영할 수 있을 뿐만 아니라, 비인가 접근을 시도하는 IoT 단말을 식별하여 추가적인 대응을 할 수 있는 장점이 있다.

Ⅱ. 관련 연구

2.1. IoT 서비스 현황

IoT는 사물을 인터넷과 연결하여, 사물에서 발생하는 정보를 인터넷을 통해 수집하고 분석을 통해 새로운 정보를 생성하는 기술이다. IoT 기술은 초기 개념 정립 이후 다양한 분야로 확대되고 있으며, 현재는 사실상 보편화되었다. IoT는 단순히 단말에서 정보를 수집하는 단계를 넘어서, 분석 후 예측에 따른 대응 행동까지 확대되고 있다. 특히 IoT 보편화에 따라 그림 1과 같이 다양한 분야로 확대되고 있다 [5].

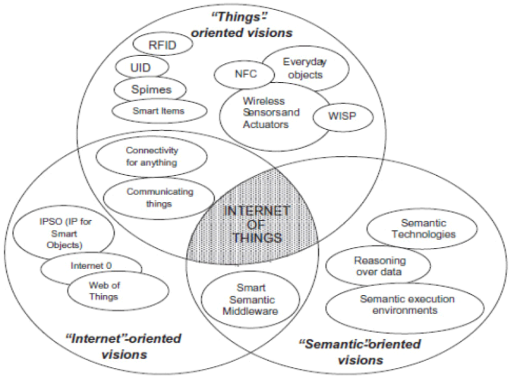

Fig. 1 IoT convergence domains

IoT 서비스는, 그 서비스 목적과 제공 기능, 범위 등에 따라 그 서비스 아키텍처는 달라지지만, 기본적으로 그림 2와 같이 IoT 서버와 IoT 단말로 구성된다. IoT 서버는 IoT 단말에서 전달한 정보를 수집하고 저장·분석하여 대응행동을 결정하는 역할을 수행한다. IoT 단말은 IoT 서비스에서 필요한 정보를 생성하여 IoT 서버에 전달한다 [6].

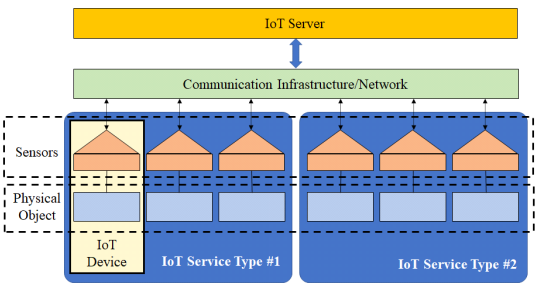

Fig. 2 IoT service architecture

IoT 단말은 다양한 종류의 장치가 적용될 수 있다. Physical Object에서 발생시킨 전기·전자형태의 Signal을 Sensor에서 Digital data로 변환하고 이를 Network을 통해 IoT Server에 전달한다 [7].

2.2. IoT 보안 환경 분석

IoT 서비스는 그 목적상 정보의 수집과 저장, 분석, 대응행동 결정에 집중되어 있다. 그래서 IoT 서비스의 기능 제공 범위는 legacy 정보 서비스와 비교하여 상대적으로 적다. 특히 IT 융합 영역은 legacy 정보 서비스 대비 정보보호에 대한 인식이 낮아 보안 수준이 낮아 표 1과 같은 보안 위협이 발생한다 [8, 9].

Table. 1 Cyber-attack about IoT service

Attack	Description
Device attack	• Compromising critical damage to IoT device
Application attack	• Compromises system applications like web, database or etc.
Network attack	• Compromising intercommunication among server and client by either delaying message forwarding or message loss.
Web interface attack	• Presenting itself as a result of account enumeration, lack of account lockout or weak account credentials.
Data integrity attack	• Compromising system data by inserting, altering or completely deleting data so as to deceive smart device to make wrong decisions or compromise its integrity.

IoT 서비스는 목표한 기능 만족에 집중하여 일반적인 보안 요구사항을 만족하지 않기 때문에, legacy 정보 서비스보다 보안에 취약하다[10].

특히 비인가 IoT 단말을 이용한 공격이 증가하고 있다. IoT 서버는 프로토콜을 만족하는 IoT 단말은 신뢰된 주체이다. 그러므로 IoT 단말이 전달하는 MQTT (Message Queueing Telemetry Transport)나 CoAP (Constrained Application Protocol) method에 따라 동작한다.

여기서 악의적 공격자는 IoT 서비스의 이러한 취약점을 이용한다. 악의적 공격자는 인가되지 않은 단말을 사용하여 IoT 서버에 접속하고, IoT 서버의 중요 정보를 변조하거나 삭제, 비정상 데이터를 추가할 수 있다 [11]. 그러면 IoT 서비스는 비정상 종료되거나, 비정상 데이터 분석을 통해 잘못된 대응 행동을 결정하고 이행할 수 있다 [12].

2.3. IoT 보안 요구사항

이와 같은 IoT 서비스의 보안 취약점에 대하여 IoT 서비스에도 보안 체계의 구축과 운영에 대한 필요성이 제시되었다. 많은 연구가 수행되었으며, 연구에 따라 서로 다른 보안 요구사항을 제시하였으나, 보편적으로 수용되고 있는 보안 요구사항은 표 2와 같다 [13].

Table. 2 IoT service's security requirement

Requirement	Attack/Challenges
Confidentiality	• Replay Attack • Man-in-the-Middle Attack • Timing Attack
Integrity	• Unauthorized Access to the Tags • Malicious Data, Malicious Insider • Tag Cloning
Authentication	• IP Spoofing • Session establishment and resumption
Availability	• Sleep deprivation attack • DOS & DDOS attack • Malicious code injection/virus,worms, trojan horse, spyware
Authorization	• Identity Spoofing • Spear-Phishing attack
Nonrepudiation	• Sybil Attack • Sinkhole Attack
Privacy	• Insecure software/firmware • Insecure interfaces • End-to-end security

IoT 서비스에 보안 체계를 구축하더라도, 구축된 보안 체계가 IoT 서비스 본연의 목표 달성을 저해해서는 안된다. 특히 IoT 서비스는 배터리에 의해 전력을 공급하고 무선 통신을 사용하는 단말을 사용할 수 있으므로, IoT 서비스에서 보안 요구사항을 만족하기 위해 과도한 보안 기능을 적용하는 것은 지양해야 한다.

그래서 IoT 서비스에 보안 체계를 구축할 때에는, 키 관리 체계나 IoT 단말 식별 체계, 보안 체계를 위한 전력 활용 수준, Bigdata 플랫폼 구축 여부, 단말 그룹 관리 방법, 포렌식 지원 수준 등을 고려해야 한다 [14].

Ⅲ. IoT 단말 인증 시스템

IoT 서비스의 기밀성과 무결성, 인증, 권한관리 등의 보안 요구사항을 만족하기 위해서, IoT 서비스 구성요소 간 안전한 정보 송수신이 필요하다. 본 연구에서는, IoT 서비스 구성요소 간 안전한 정보 송수신을 위한 방법으로 IoT 단말 인증 시스템을 제안한다.

3.1. IoT 단말 인증 시스템 아키텍처

본 연구에서 제안하는 IoT 단말 인증 시스템의 구조는 그림 3과 같다.

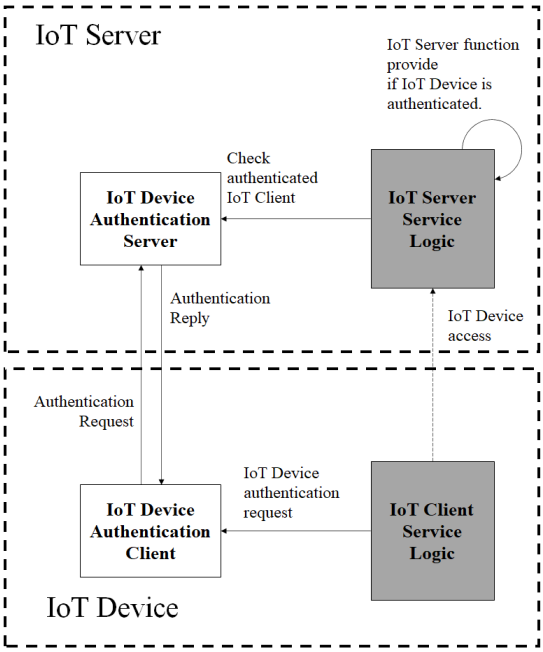

Fig. 3 IoT device authentication system architecture

본 연구에서 제안하는 IoT 단말 인증 시스템은 IoT 서버와 IoT 단말에서 각각 동작하는 2개의 컴포넌트로 구성된다. IoT Device Authentication Client는 IoT Device에서 동작하는 라이브러리 형태의 인증 클라이언트 모듈이다. IoT Device Authentication Server는 IoT 서버에서 동작하는 인증 서버 모듈로 IoT Device Authentication Client를 인증하는 역할을 담당한다.

3.2. IoT 단말 인증 시스템 보안 기능 제공 방법

본 연구에서 제안하는 IoT 단말 인증 시스템은 그 자체적으로 동작하지 않고 IoT 서버나 IoT 단말의 Library 형태로 동작한다.

본 연구에서 제안하는 IoT 단말 인증 시스템의 동작 순서는 그림 4와 같다.

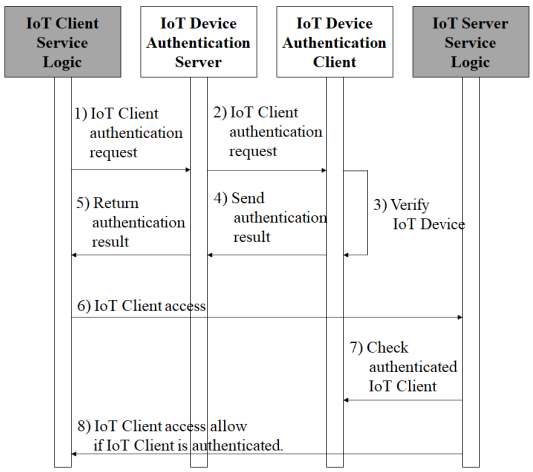

Fig. 4 IoT device authentication system authentication function providing sequence diagram

IoT Device는 IoT 서버에 접속하기 전에, IoT Device Authentication Client에게 단말 인증을 요청한다. 그러면 IoT Device Authentication Client는 IoT Device Authentication Server에 인증 정보를 전달하여 인증을 요청한다. IoT Device Authentication Server는 IoT Device Authentication Client가 전달한 정보를 이용하여 IoT Device를 검증한다. 이후 IoT Device Authentication Server는 인증 결과를 IoT Device Authentication Client에 전달하고, IoT Device Authentication Client는 인증 결과를 IoT Client Service Logic에 return한다.

IoT Device Authentication Client가 인증하는데 사용되는 정보는 다양하다. IoT Device의 MAC Address나 Shared-key, Encrypted String이나 다양한 인증 메커니즘을 위한 수학적 연산 결과가 적용될 수 있다.

본 연구에서 제안하는 방법을 사용하면, 어떠한 Device를 사용하는 IoT 서비스라도, 서비스 자체적으로 인증할 수 있는 장점이 있다.

Ⅳ. 실증 구현 및 검증

4.1. 실증 구현

본 연구에서 제안하는 인증 시스템을 검증하기 위하여, REST 서버와 아두이노(Arduino)가 연동하는 IoT 시스템에 대하여 IoT 단말 인증 시스템을 구현하였다. IoT Server는 REST api 기반 서버이며 CentOS 8.3 운영체제에서 동작한다. IoT Device는 아두이노 CH340 DM72이다. 여기에 본 연구에서 제안한 IoT 단말 인증 기능을 구현하였다.

4.2. 기능 검증 항목

본 연구에서 제안하는 IoT 단말 인증 시스템이 정상 동작하기 위해서는 표 3과 같은 단위 기능이 정상 동작해야 하며, 각 단위 기능을 연계한 통합 기능도 정상 동작해야 한다.

Table. 3 IoT Device authentication system's unit function

Function	Description	Verification ID
Authentication Request	• IoT Device Authentication Client requests authentication from IoT Device Authentication Server.	Verify_F_01
IoT Device Verification	• The IoT Device Authentication Server can determine whether it is an authorized IoT device with the authentication information transmitted by the IoT Device Authentication Client.	Verify_F_02
Authentication Reply	• IoT Device Authentication Client can receive the authentication result.	Verify_F_03
Verification Check	• The IoT Server Service Logic can request confirmation from the IoT Device Authentication Server whether the IoT Client Service Logic requesting access has been authenticated.	Verify_F_04
Positive Function Test	• Checks whether access from authorized devices is allowed.	Intg_F_01
Negative Function Test	• Check whether access of unauthorized devices is denied.	Intg_F_02

4.3. 기능 검증 결과

본 연구에서 제안한 IoT 인증 시스템에 대한 단위 기능이 정상 동작하며, 이를 연계한 통합 기능이 정상 동작하는지를 확인하였다. 먼저 Verify_F_01 ~ Verify_F_04의 기능을 검증한 이후 이를 연계한 통합 기능 Intg_F_01~Intg_F_02를 검증하였다.

단위 기능을 검증한 결과, Verify_F_01 ~ Verify_F_04은 모두 정상 동작함을 확인하였다. Verify_F_01 검증 결과, IoT Device Authentication Server는 IoT Device Authentication Client의 인증 요청을 수신하고, 인증에 필요한 인증 정보를 정상 수신함을 확인하였다. Verify_F_02 검증 결과, IoT Device Authentication Server는 IoT Device Authentication Client를 정상 검증함을 확인하였다. Verify_F_03에서, IoT Device Authentication Server는 IoT Device Authentication Client에게 인증 결과를 정상 전송함을 확인하였다. Verify_F_04를 확인한 결과 IoT Server Service Logic은 IoT Device 접근 요청 시 검증 결과를 정상 수신하는 것을 확인하였다.

Intg_F_01~Intg_F_02의 통합 기능 검증 결과에서도 본 연구에서 제안하는 인증 기능이 정상 동작함을 확인하였다. Intg_F_01에서는 미리 정의된 IoT Device를 정상 인증하고 접속을 허용함을 확인하였다. 반대로 Intg_F_02에서는 정의되지 않은 IoT Device의 접속을 정상 차단함을 확인하였다.

Ⅴ. 결 론

IoT 서비스는 IT 융합 트렌드에 따라 매우 확대되고 있으며, 그 범위는 더욱 넓어질 것이다. IoT 서비스 범위의 확산만큼 IoT 서비스 보안도 중요하다. 이에 따라 많은 연구에서 IoT 보안을 강조하였다.

본 연구에서는 IoT 서비스에 대한 인증 및 권한관리, 무결성, 기밀성 등의 보안 요구사항을 만족할 수 있는 IoT 단말 인증 시스템을 제안하였으며, 그 기능을 검증하였다. 그 결과 본 연구에서 제안하는 IoT 단말 인증 시스템은 정상 동작함을 확인하였다.

다만, 본 연구는 단순한 단말 인증 기능에만 집중하여, 보안 강도를 고려한 다양한 인증 메커니즘에 대한 추가 연구가 필요하다.

REFERENCES

[1] A. Zaslavsky, C. Perera and D. Georgakopoulos, "Sensing as a Service and Big Data," in *Proceedings of International Conference on Advances in Cloud Computing (ACC)*, Bangalore, India, 2013.

[2] T. Yoo and H. Chang, "The IT convergence framework design in the internet of things environment," *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1-10, Feb. 2013. DOI: 10.1186/1687-1499-2013-53.

[3] D. Mohapatra and B. Subudhi, "Development of a Cost Effective IoT-based Weather Monitoring System," *IEEE Consumer Electronics Magazine*, vol. 11, no. 5, pp. 81-86, Sep. 2022. DOI: 10.1109/MCE.2021.3136833.

[4] A. M. Joshi, P. Jain and S. P. Mohanty, "Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework," in *Proceedings of 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Limassol, Cyprus, pp. 440-445, Jul. 2020. DOI: 10.1109/ISVLSI49217.2020.00-17.

[5] D. A. Vyas, D. Bhatt, and D. Jha, "IoT: Trends, Challenges and Future Scope," *International Journal of Computer Science & Communication*, no. 7, vol. 1, pp. 186-197, Sep.-Mar. 2015-2016. DOI: 10.090592/IJCSC.2016.028.

[6] W. Alnahari and M. T. Quasim, "Authentication of IoT Device and IoT Server Using Security Key," in *Proceedings of 2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, Taiz, Yemen, pp. 1-9, 2021. DOI: 10.1109/ICOTEN52080.2021.9493492.

[7] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *Proceedings of 2012 10th international conference on frontiers of information technology*, Islamabad, Pakistan, pp. 257-260, 2012. DOI: 10.1109/FIT.2012.53.

[8] S. Hameed, F. I. Khan, and B. Hameed, "Understanding Security Requirements and Challenges in Internet of Things (IoTs): A review," *Journal of Computer Networks and Communications*, vol. 2019, 9629381, Jan. 2019. DOI: 10.1155/2019/9629381.

[9] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber Security Threats to IoT Applications and Service Domains," *Wireless Personal Communications*, vol. 95, no.1, pp. 169-185, May 2017. DOI: 10.1007/s11277-017-4434-6.

[10] J. Ahamed and A. V. Rajan, "Internet of Things (IoT): Application systems and security vulnerabilities," in *Proceedings of 2016 5th International conference on electronic devices, systems and applications (ICEDSA)*, Ras Al Khaimah, United Arab Emirates, pp. 1-5, Dec. 2016. DOI: 10.1109/ICEDSA.2016.7818534.

[11] B. Ondiege, M. Clarke, and G. Mapp, "Exploring a New Security Framework for Femote Patient Monitoring Devices," *Computers*, vol. 6, no. 1, 11, Feb. 2017. DOI: 10.3390/computers6010011.

[12] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1-44, Jul. 2021. DOI: 10.1145/3453176.

[13] M. Imdad, D. W. Jacob, H. Mahdin, Z. Baharum, S. M. Shaharudin, and M. S. Azmi, "Internet of things (IoT); security requirements, attacks and counter measures," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 3, pp. 1520-1530, Jun. 2020. DOI: 10.11591/ijeecs.v18.i3.pp1520-1530.

[14] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," in *Proceedings of 2015 ieee world congress on services*, New York: NY, USA, pp. 21-28, 2015. DOI: 10.1109/SERVICES.2015.12.

강동연(Dong-Yeon Kang)

동명대학교 정보보호학과 졸업
現 (주)윈스 재직 중
※관심분야 : 취약점 분석, 클라우드 보안

전지수(Ji-Soo Jeon)

동명대학교 정보보호학과 졸업
現 (주)윈스 재직 중
※관심분야 : 네트워크 보안, IoT 보안, 클라우드

한성화(Sung-Hwa Han)

숭실대학교 공학박사
現 동명대학교 정보보호학과 교수
※관심분야 : Zero-Trust, 시스템 보안,
정보보호 컨설팅, 네트워크 보안