산업융합연구 제18권 제5호 pp. 23-29, 2020
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2020.18.5.023

사물인터넷 디바이스를 위한 AES 기반 상호인증 프로토콜

오세진, 이승우*
경운대학교 항공소프트웨어공학과 교수

A Study on AES-based Mutual Authentication Protocol for IoT Devices

Se-Jin Oh, Seung-Woo Lee*
Professor, Dept. of Aeronautical Software Engineering, College of Aeronautical Engineering, Kyungwoon University

요 약 사물인터넷(IoT)은 다양한 디바이스와 일상적인 물건을 인터넷 연결하여 인터넷을 확장한 것이며, 전자제품에는 인터넷 연결이 가능하고 다양한 형태의 하드웨어가 내장되어 있다. 이러한 사물인터넷은 디지털 생태계에 중대한 위험을 초래한다. 이들 기기 중 상당수는 공격자의 공격을 막기 위한 보안 시스템이 내장되지 않은 상태로 설계되어 있기 때문이다. 본 논문에서는 사물인터넷 디바이스를 위한 대칭키 기반의 상호인증 프로토콜을 제안한다. 제안 프로토콜은 대칭키 암호 알고리즘을 사용하여 무선상에 전송되는 데이터를 안전하게 암호화한다. 아울러 암호화에 사용된 비밀키는 매 통신마다 디바이스가 생성하는 난수를 비밀키로 사용하여 고정적으로 사용되는 비밀키를 가변적으로 사용함으로써 보안성을 높였다. 제안 프로토콜은 무선상에서 데이터를 전송하기 전에 상호인증 과정을 거쳐 인증된 디바이스만 데이터를 전송하기 때문에 공격자를 차단하고 정상적인 디바이스가 통신이 가능하도록 하였다. 마지막으로 제안된 프로토콜을 공격유형별 시나리오를 통해 도청 공격, 위치추적, 재전송 공격, 스푸핑 공격, 서비스 거부 공격에 안전함을 확인하였다.

키워드 : 보안, 인증, 프로토콜, 사물인터넷, 암호학

Abstract The Internet of things (IoT) is the extension of Internet connectivity into various devices and everyday objects. Embedded with electronics, Internet connectivity and other forms of hardware. The IoT poses significant risk to the entire digital ecosystem. This is because so many of these devices are designed without a built-in security system to keep them from being hijacked by hackers. This paper proposed a mutual authentication protocol for IoT Devices using symmetric-key algorithm. The proposed protocol use symmetric key cryptographic algorithm to securely encrypt data on radio channel. In addition, the secret key used for encryption is random number of devices that improves security by using variable secret keys. The proposed protocol blocked attacker and enabled legal deives to communicate because only authenticated devices transmit data by a mutual authentication protocol. Finally, our scheme is safe for attacks such as eavesdropping attack, location tracking, replay attack, spoofing attack and denial of service attack and we confirmed the safety by attack scenario.

Key Words : Security, Authentication, Protocol, IoT, Cryptography

1. 서론

과거 유비쿼터스(Ubiquitous) 시대를 시작으로 스마트 시대, 사물인터넷으로 이어져 최근 4차 산업 혁명이 주목받고 있다. 4차 산업 혁명은 사물인터넷(Internet of Things)의 이슈로 연구 개발 및 다양

*Corresponding Author : Seung-Woo Lee(swlee@ikw.ac.kr)
Received July 29, 2020 Revised August 29, 2020
Accepted October 20, 2020 Published October 31, 2020

한 제품으로 판매되고 있는 실정이다[1-3].

사물인터넷은 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하여 많은 데이터를 송수신하여 사용자에게 의미 있는 데이터로 제공하는 서비스를 말한다. 첨단 기술, 편리함, 인공지능 활용 등으로 우리 일상 깊은 곳에 자리 잡으려 하고 있으며, 편리함이 늘어가는 반면에 IoT 보안 위협도 증가하고 있다. 과거 유비쿼터스의 핵심이라 할 수 있는 RFID/USN의 경우 보안 프로토콜의 취약성으로 인해 많은 보안 문제와 보안 연구가 이루어졌다. 사물인터넷에서도 마찬가지로 보안 기법이 적용된 Wi-Fi, 블루투스 등과 같이 보안 기법이 적용된 경우는 보안에 강하지만 무선 주파수를 이용하는 사물인터넷의 경우 유비쿼터스때와 마찬가지로 보안에 취약하다 할 수 있다. 특히 ISO 18000 규격을 사용하는 사물인터넷의 경우 별도의 보안 프로토콜의 부재로 공격자의 공격에 매우 취약하다. 한국인터넷진흥원은 IoT 기기를 개발하는 기업과 이를 이용하는 사용자 모두 보안 예방의 노력이 필요함을 강조하며, 기업과 사용자 관점에서 반드시 조치해야 할 보안 대응 요소를 포함한 'IoT 소형 스마트홈 가전 보안 가이드'를 발간하였다.

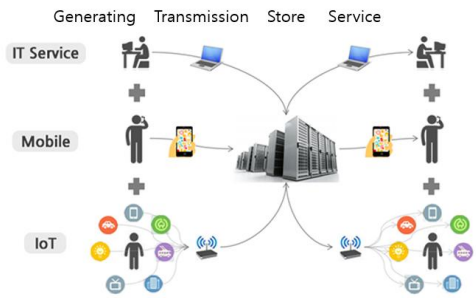

Fig. 1. IoT Connectivity and Services

사물인터넷의 다양한 센서들로부터 많은 데이터를 수집하게 되는데 이때 많은 양의 데이터들은 유무선 네트워크를 통하여 전송된다. 특히, 무선을 이용한 데이터 전송은 공격자의 공격에 매우 취약하다. 공격자는 도청, 위치추적, 재전송 공격, 스푸핑 공격, 서비스 거부 공격 등 다양한 공격으로 개인정보 유출, 시스템 파괴 등과 같은 위험이 초래되고 있다[4-6].

2. 관련연구

본 장에서는 사물인터넷과 관련한 제품 유형 군과 이에 대한 보안 위협 및 원인에 대해 알아본다.

사물인터넷을 제품 유형별로 나누어 보면 멀티미디어 제품, 생활가전 제품, 네트워크 제품, 제어 제품, 센서 제품 등으로 나누어 볼 수 있다.

멀티미디어 제품의 주요 제품으로는 스마트 TV, 스마트 냉장고 등이 있으며, PC 환경에서의 모든 악용 행위와 카메라, 마이크 내장 시 사생활 침해가 있다.

생활가전 제품은 청소기, 인공지능 로봇 등이 있으며, 알려진 운영체제의 취약점 및 인터넷 기반 해킹 위협이 존재한다. 그리고 로봇청소기에 내장된 카메라를 통해 사용자의 집을 불법적으로 모니터링이 가능하다.

네트워크 제품에는 홈 캠, 네트워크 카메라와 같은 제품이 있으며, 카메라의 특성으로 인해 사진 및 동영상을 공격자의 서버 및 이메일로 전송하거나 불법적으로 모니터링할 수 있는 공격이 있을 수 있다.

Table 1. Type of Security Threats

Type	Cause of Security Threats
Multimedia	Absence of Authentication Protocol, Weak Password, Firmware Update Vulnerabilities, Physical Security Vulnerabilities
Household Appliances	Absence of Authentication Protocol, Firmware Update Vulnerabilities, Physical Security Vulnerabilities
Network	Absence of Access Control, Absence of Radio Data Security, Physical Security Vulnerabilities
Control	Absence of Authentication Protocol, Weak Password, Absence of Access Control, Physical Security Vulnerabilities, Non-encrypted Authentication Information, absence of radio data security,
Sensor	Absence of Radio Data Security, Absence of Data Integrity, Physical Security Vulnerabilities

제어 제품으로는 디지털 도어락, 가스 밸브, 모바일 앱 등이 있으며, 제어 기능 탈취로 인해 도어락의 임의 개폐, 앱 소스 코드 노출로 사물인터넷 제품 제어 기능을 탈취할 수 있다. 마지막으로 센서 제품에는 온습도 센서와 같은 센서 정보를 취득하는 제품은 잘못된 센서 정보를 제공하는 데이터 위변조 공격이

있을 수 있다[7,8]. Table 1은 앞서 언급한 사물인터넷 유형별 주요 보안 위협 원인을 나타낸 것이며, 그림 2는 센서와 디바이스 간 구성도를 나타낸 것이다.

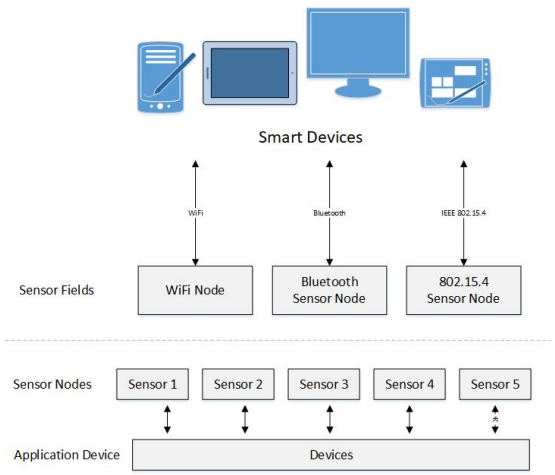

Fig. 2. Configuring Sensors and Devices

한국인터넷진흥원의 '연도별 IoT 취약점 신고 현황'에 따르면 2015년 130건에서 2016년 362건으로 2.7배 이상 증가하여 사물인터넷 보안에 대한 우려는 끊임없이 제기되고 있다.

이는 최근 기술 발달로 사물인터넷 제품이 폭발적으로 늘어났음에도 사물인터넷 기기의 보안 강화가 제대로 이뤄지지 않고 있다는 것을 의미한다. 한국인터넷진흥원이 발표한 최근 사물인터넷 기기 보안 침해 대표 사례를 보면 2014년 냉난방 관리용 셋톱박스 취약점을 이용한 DDoS(Dynamic Denial of Service) 공격, 공유기의 보안취약점을 통해 SK브로드밴드의 DNS(Domain Name System) 서버가 DDoS 공격을 받았으며, 2016년에는 CCTV를 해킹하여 인터넷으로 생중계되었으며, 2017년에는 보안에 취약한 사물인터넷 기기에 미라이(Mirai) 악성코드에 감염된 기기들이 국내에서 다수 발견되는 사례가 있었다.

Fig. 3은 연도별 사물인터넷 취약점 신고 현황이며, Fig. 4는 사물인터넷 이용자 통계를 표로 나타낸 것이다.

사물인터넷의 경우 다양한 디바이스가 연결된 환경으로 인해 네트워크 구성에 있어 많은 변화를 지니고 있다. 이에 다양한 보안 위협에 노출되어 있으므로 안전한 인증 기법들이 연구되고 있다. 그러나 일부 보안 프로토콜의 경우 기밀성, 무결성, 익명성, 상호인증과 같은 보안 요구사항을 만족하지 못해 공격 취약성을 지니고 있다[9-12].

Porambage[13] 등은 ECC(Elliptic Curve Cryptography) 기반의 인증 프로토콜을 제안하였다. ECC 특성상 개인 키와 공개 키를 관리해야 하는 단점과 개인 키를 추측할 수 있는 문제가 존재한다. Baruah[14] 등은 프로토콜은 생체정보를 활용하는 프로토콜이다. 이때 사용되는 R1 값의 유출로 인해 스푸핑 공격에 취약성을 가지고 있다[15]. 그러므로 효율적인 암호 알고리즘과 안전한 상호인증 설계를 통해 공격자의 공격을 방어해야 할 것이다.

본 논문에서는 사물인터넷에 사용되는 디바이스 간 데이터 전송 시 안전하게 데이터를 전송하는 상호인증 프로토콜을 제안하고 제안 프로토콜에 대한 안전성을 분석한다.

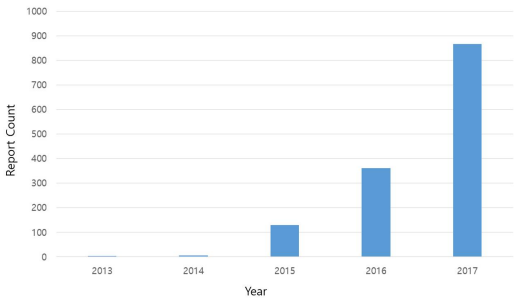

Fig. 3. The current state of IoT vulnerability

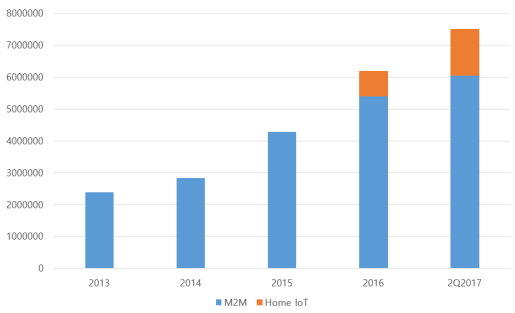

Fig. 4. IoT User Statistics

3. 제안 프로토콜

본 장에서는 사물인터넷 디바이스를 위한 상호인증 프로토콜을 제안한다. 제안 프로토콜은 다음과 같은 표기법과 가정사항을 갖는다.

디바이스 A와 디바이스 B는 ISO 18000 기반의 사물인터넷 장치이며, 무선을 통하여 데이터를 전달하여 공유할 수 있다.

- 디바이스 A와 디바이스 B는 무선 채널을 이용하여 데이터를 공유하므로 보안에 취약하다.
- 디바이스 A와 디바이스 B는 사전에 동일한 비밀키를 공유하고 있다.
- 디바이스 A와 디바이스 B는 미국 표준 암호 AES(Advanced Encryption Standard) 암복호화와 난수 생성이 가능하다.

Table 2. The Notations of proposed Protocol

Variable	Definition
Key	Secret Key
Data	Non-encrypted Data
R_A	Random Number generated by device A
R_B	Random Number generated by device B
||	Concatenation
$E_k()$	Encryption
$D_k()$	Decryption
Query	Request Message

본 논문에서 제안하는 프로토콜은 디바이스 A로부터 시작하며, 요청 질의어 Query를 디바이스 B에게 전달로 시작한다. 제안 프로토콜의 상호인증 과정은 그림 5와 같다.

먼저 디바이스 A가 디바이스 B에게 요청 신호 Query를 송신한다. Query를 수신받은 디바이스 B는 난수 R_B를 생성하고 AES 알고리즘으로 암호화된 $\alpha = E_k(R_B)$를 디바이스 A에게 전달한다. α를 전달받은 디바이스 A는 AES 복호화 연산, $D_k(\alpha)$를 연산하여 R_B를 추출하고 난수 R_A를 생성한 후 $E_k(R_A \| R_B)$를 연산하여 β를 디바이스 B에게 전달한다.

β를 전달받은 디바이스 B는 $D_k(\beta)$를 복호화 연산하여 R_A와 R_B를 추출하여 디바이스 B가 소유한 R_A, R_B와 추출된 R_A와 R_B를 비교하여 인증과정을 진행한다. R_A와 R_B값이 같으면 디바이스 A를 정상적인 디바이스로 인증한다. 그렇지 않으면 공격자로 간주하고 통신을 중단한다.

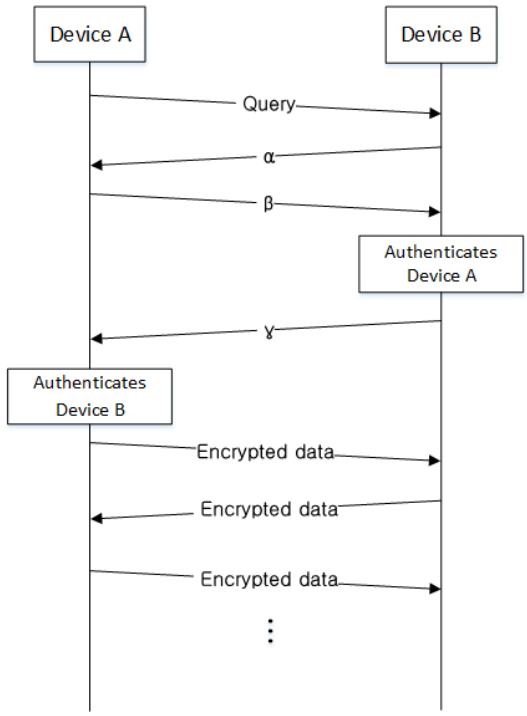

Fig. 5. The Proposed Protocol

디바이스 A를 인증한 후 디바이스 B를 인증하기 위하여 $E_k(R_B \| R_A)$를 연산하여 γ를 디바이스 A에게 전송한다.

γ를 전송받은 디바이스 A는 $D_k(\gamma)$를 연산하여 R_B와 R_A를 추출하여 디바이스 A가 소유한 R_B와 R_A와 추출된 R_B와 R_A를 비교하여 같으면 디바이스 B를 인증한다. 그렇지 않으면 통신을 종료한다.

이로써 인증과정 이후 디바이스 A와 디바이스 B간 상호인증이 완료되었으므로 데이터 전송을 안전하게 할 수 있게 된다. 이후 데이터는 암호화하며, 디바이스 A는 R_B를 비밀키로 사용하여 전송하며 디바이스 B는 R_A를 비밀키로 사용하여 데이터를 암호화하여 전송한다. 제안 프로토콜의 세부 연산 과정은 다음과 같다.

- Step 1.
  Device A : generates Query
  Device A → Device B : Query

- Step 2.
  Device B : generates R_B
  $\alpha = E_k(R_B)$ with Key

Device B → Device A : α

- Step 3.
  Device A : generates R_A
  $D_k(\alpha)$ with Key
  $\beta = E_k(R_A \| R_B)$ with R_B
  Device A → Device B : β

- Step 4.
  Device B : R_A and $R_B = D_k(\beta)$ with R_B
  if R_A and R_B then
  authenticates Device A
  $\gamma = E_k(R_B \| R_A)$ with R_A
  else
  exit
  Device B → Device A : γ

- Step 5.
  Device A : R_B and $R_A = D_k(\gamma)$ with R_A
  if R_B and R_A then
  authenticates Device B
  else
  exit

- Step 6. ~ Step n.
  Device A : use R_B to encrypt data
  Device B : use R_A to encrypt data

4. 안전성 분석

본 장에서는 제안 프로토콜의 안전성을 분석한다. Table 3은 제안 프로토콜의 안전성을 공격유형별 표로 나타낸 것이다.

제안 프로토콜은 디바이스 간 송수신 시 전달되는 데이터는 미국 표준 암호 알고리즘은 AES 대칭키 알고리즘으로 안전하게 암호화되어 있어서 도청 공격에 안전하다. 또한, 암호화 데이터는 난수를 암호화하기 때문에 통신 때마다 값이 변화하므로 위치공격 안전하다. 그리고 공격자가 암호화 데이터를 복호화하더라도 매 통신 생성되는 난수이므로 의미 없는 값이고 뿐만 아니라 매 통신 암호화 키는 난수이므로 공격자가 인증과정을 통과하기에는 매우 불가능하다. 그리고 상호인증과정을 진행하여 정당한 개체인지를 확인하므로 위장 공격과 같은 공격을 사전에 차단할 수 있다. 그러므로 인증과정을 통해 재전송 공격과 스푸핑 공격, 서비스 거부 공격의 안전성을 확보하므로 두 공격에 안전하다 할 수 있다.

Table 3. The Security Analysis of proposed protocol

Type of Attacks	Description (Solution)
Eavesdropping	Safe (Encryption)
Location Tracking	Safe (Variable Data)
Replay Attack	Safe (Authentication)
Spooing Attack	Safe (Authentication)
DoS Attack	Safe (Authentication)
Authentication	Mutual Authentication
Steps	3 Step
Encryption	3 Times
Decryption	3 Times
Symmetric Key	Variable
Data Transmission	384 bits
Random Number	2

디바이스 A와 B가 서로 간 인증과정을 진행하므로 상호인증을 지원한다. 또한, 인증과정 중 암복호화 횟수는 각각 3회를 하였고, 이때 사용되는 암복호화 키는 다음 통신 때 난수이므로 가변적이라 할 수 있다. 그리고 인증과정에 사용되는 데이터양은 384bit로 경량 인증 프로토콜에 사용할 수 있다. 사물인터넷은 수많은 디바이스들 간의 연결점을 고려할 때 데이터양은 매우 중요한 쟁점이 될 것이다. 디바이스 증가에 따른 전송량을 Fig. 6과 같이 나타났다.

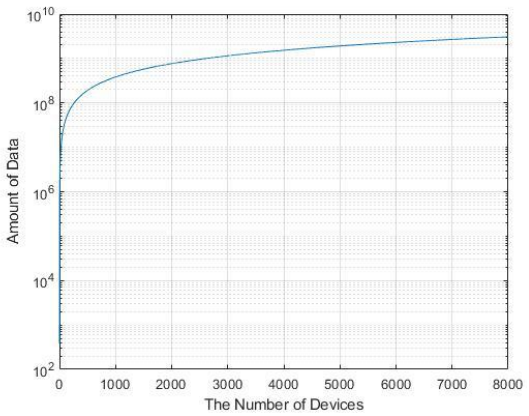

Fig. 6. Data Length in proposed Protocol

5. 결론

최근 4차 산업혁명 기술 중 사물인터넷은 다양한 센서들과의 연결을 기반으로 하여 많은 양의 데이터를 생성 및 가공한다. 다양한 디바이스와 사물인터넷과의 융합은 실세계와 가상세계를 하나로 묶는 새로운 ICT(Information and Communication Technology) 융합 산업을 창출하는 데 큰 역할을 하고 있다. 사물인터넷의 다양한 센서 및 디바이스의 사용은 매년 빠른 속도록 증가하면서 이에 대한 보안 위협이 비례하여 증가하고 있다. 그뿐만 아니라 사물인터넷의 다양한 센서들의 데이터 송수신과정에서 무선 통신을 사용하는 특성은 공격자의 공격에 취약하고 새로운 응용 및 서비스 개발에 반드시 주의해야 할 부분이다 [16,17].

본 논문에서 제안한 사물인터넷 디바이스를 위한 상호인증 프로토콜은 사물인터넷의 다양한 디바이스 간 데이터 전송 시 대칭 키 기반의 암호 알고리즘을 사용하여 안전하게 데이터를 암호화하며, 상호인증 과정 및 암호화 데이터를 난수를 이용하여 공격자의 공격을 방어하고 데이터를 안전하게 전송한다.

사물인터넷과 같은 새로운 기기 및 서비스는 ICT 발전과 동시에 새로이 나타날 것이다. 이에 새로운 보안기술과 기존 보안기술과의 효율적 보안능력을 향상하게 시킬 연구가 진행되어야 할 것이다.

REFERENCES

[1] J. M. Blythe & S. D. Johnson. (2018, March). The consumer security index for IoT: A protocol for developing an index to improve consumer decision making and to incentivize greater security provision in IoT devices. *Living in the Internet of Things: Cybersecurity of the IoT - 2018.* (pp. 1-7). London : IET.

[2] R. Gurunath, M. Agarwal, A. Nandi & D. Samanta. (2018, August). An Overview: Security Issue in IoT Network. *2018 2nd International Conference on I-SMAC(IoT in Social, Mobile, Analytics and Cloud).* (pp. 104-107). Palladam : IEEE.

[3] D. D. Lopez et al. (2018). Shielding IoT against Cyber-Attacks: An Event-Based Approach Using SIEM. *Wireless Communications and Mobile Computing, 2018, 1-18.* DOI:10.1155/2018/3029638

[4] A. A. Hezam & D. Konstantas (2019). A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *Journal of Sensor and Actuator Networks, 8(22),* 1-38. DOI : 10.3390/jsan8020022

[5] Springer. (2019). *Big Data and Internet of Things Security and Forensics: Challenges and Opportunities.* [Handbook of Big Data and IoT Security]. Cham : A. Azmoodeh, A. Dehghantanha & K. R. Choo.

[6] K. Tsai, Y. Huang, F. Leu, I. You, Y. Huang & C. Tsai. (2018). AES-128 based Secure Low Power Communication for LoRaWAN IoT Environments. *IEEE Access, 6,* 45325-45334. DOI : 10.1109/ACCESS.2018.2852563

[7] A. Sadeghi, C. Wachsmann & M. Waidner. (2015, June). Security and privacy challenges in industrial internet of things. *52nd ACM/EDAC/IEEE Design Automation Conference,* (pp. 1-6). San Francisco : ACM.

[8] D. H. Kim, J. Y. Cho, J. I. Lim & B. G. Lee. (2016). Developing iot security requirements for service providers. *Information, 19(2),* 595-603.

[9] H. U. Kim. (2017). *A Design of Mutual authentication protocol between heterogeneous services in the internet of things Environment.* Doctoral dissertation. Soongsil University, Seoul.

[10] K. H. Lee & J. S. Lee. (2018). Mutual Authentication Method for hash Chain Based Sensors in IoT Environment. *Journal of the korea Academia-Industrial cooperation Society, 9(11),* 303-309.

[11] S. Y. Min & J. S. Lee. (2018). Device Mutual Authentication and Key Management Techniques in a Smart Home Environment. *Journal of the korea Academia-Industrial cooperation Society, 9(10),* 661-667.

[12] S. J. Yu, K. S. Park, Y. H. Park & Y. H. Park. (2018). Lightweight User Authentication and Key Agreement Scheme in Wireless Sensor Network Environments. *The Journal of Korea Information and Communications Society, 43(12),* 2215-2229. DOI : 10.7840/kics.2018.43.12.2215

[13] M. S. Farash, M. Turkanović, S. Kumari & M. Hölbl. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet

of Things environment. *Ad Hoc Networks, 36(1),* 152-176.
DOI : 10.1016/j.adhoc.2015.05.014

[14] K. C. Baruah, S. Banerjee, M. P. Dutta & C. T. Bhunia. (2015). An Improved Biometric-based Multi-server Authentication Scheme Using Smart Card. *International Journal of Security and Its Applications, 9(1),* 397-408.
DOI : 10.14257/ijsia.2015.9.1.38

[15] K. H. Lee & J. S. Lee. (2018). Mutual Authentication Method for Hash Chain Based Sensors in IoT Environment. *Journal of the Korea Academia-Industrial cooperation Society, 19(11),* 303-309.
DOI : 10.5762/KAIS.2018.19.11.303

[16] M. El-hajj, A. Fadlallah, M. Chamoun & A. Serhrouchni. (2019). A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors, 19(5),* 1-43.
DOI : 10.3390/s19051141

[17] M. Husamuddin & M. Qayyum. (2017, March). Internet of Things: A study on security and privacy threats. *2017 2nd International Conference on Anti-Cyber Crimes (ICACC).* (pp. 93-97). Abha : IEEE.

오 세 진(Se-Jin Oh) [정회원]

· 2009년 2월 : 경운대학교 컴퓨터공학과(공학사)
· 2011년 2월 : 경북대학교 전자전기컴퓨터학부(공학석사)
· 2014년 8월 : 경북대학교 컴퓨터학부(공학박사)
· 2017년 3월 ~ 현재 : 경운대학교 항공소프트웨어공학과 교수
· 관심분야 : 정보보안, 임베디드 시스템, 사물인터넷
· E-Mail : sjoh@ikw.ac.kr

이 승 우(Seung-Woo Lee) [정회원]

· 2009년 2월 : 경일대학교 컴퓨터공학과(공학사)
· 2013년 2월 : 경북대학교 컴퓨터학부(공학석사)
· 2020년 8월 : 경북대학교 컴퓨터학부(공학박사)
· 2020년 3월 ~ 현재 : 경운대학교 항공소프트웨어공학과 교수
· 관심분야 : 플래시 메모리, 핫 데이터, FTL
· E-Mail : swlee@ikw.ac.kr