https://doi.org/10.33778/kcsa.2024.24.3.165

베터리 전력 환경 IoT 디바이스 경량 인증 프로토콜 연구

한 성 화*

요 약

IT융합 트렌드에 의해, 많은 산업 분야에서는 필요한 IoT 기술을 개발하고 있다. 특히 대용량 베터리와 모바일 통신 기술 발전으로, IoT는 스마트 팜이나 스마트 환경, 에너지 등을 포함한 다양한 분야로 확대될 수 있었다. 이러한 서비스들은 서비스 유지 시간 확보를 위해 목표한 기능에만 집중하며, 상대적으로 전력 소모가 많은 보안 기술 도입에 소극적이다. IoT 서비스의 IoT 단말의 취약한 보안 환경은 안정적인 서비스 제공에는 부적절하다. 안전한 IoT 서비스 제공을 위해서는, 베터리 전력 소모를 고려한 보안 기술이 요구된다. 본 연구에서는 IoT 서비스에 대한 다양한 보안 요구사항 중, 전력 소모를 최소화하는 IoT 단말 인증 기술을 제안한다. 제안하는 기술은 Diffie-Hellman 알고리즘 기반의 단말 인증 기능으로, 전송 구간에서 인증 정보가 유출되더라도 해당 단말을 위장할 수 없는 장점이 있다. 또 제안하는 인증 기술 실효성을 검증하기 위해 ID/PW 기반 인증 기술과 베터리 전력 소모율을 비교 검증한 결과, 본 연구에서 제안하는 인증 기술이 상대적으로 적은 전력을 소모하는 것으로 확인되었다. 본 연구에서 제안하는 단말 인증 기술이나 이를 준용한 인증 기술을 IoT 단말에 적용한다면, 더 안전한 IoT 보안 환경을 확보할 수 있을 것으로 예상된다.

Study on Battery Power based IoT Device Lightweight Authentication Protocol

Sung-Hwa Han*

ABSTRACT

Due to the IT convergence trend, many industrial domains are developing their own IoT services. With batteries and lightweight devices, IoT could expand into various fields including smart farms, smart environments, and smart energy. Many battery-powered IoT devices are passive in enforcing security techniques to maintain service time. This is because security technologies such as cryptographic operations consume a lot of power, so applying them reduces service maintenance time. This vulnerable IoT device security environment is not stable. In order to provide safe IoT services, security techniques considering battery power consumption are required. In this study, we propose an IoT device authentication technology that minimizes power consumption. The proposed technology is a device authentication function based on the Diffie-Hellman algorithm, and has the advantage that malicious attackers cannot masquerade the device even if salt is leaked during the transmission section. The battery power consumption of the authentication technology proposed in this study and the ID/PW-based authentication technology was compared. As a result, it was confirmed that the authentication technique proposed in this study consumes relatively little power. If the authentication technique proposed in this study is applied to IoT devices, it is expected that a safer IoT security environment can be secured.

Key words : IoT, Battery Power, Wireless-Device, Authentication Protocol, Light-weight

접수일(2024년 07월 11일), 수정일(1차: 2024년 08월 21일), (2차: 2024년 09월 04일), 게재확정일(2024년 09월 30일)

* 동명대학교/Dept. Information System and Security

1. 서 론

IoT(Internet of Things)는 다양한 사물을 인터넷으로 연결하는 개념이다. 사물에 센서를 부착, 장치에서 발생하는 물리·화학적 정보를 수집하여 이를 인터넷을 통해 전송·분석한다. 필요한 경우 컨트롤러를 사물에 장착하여 사물을 제어한다. 다양한 정보 수집·분석하고 각종 장치를 제어할 수 있는 디바이스 개발로, IoT 서비스는 스마트 환경이나 스마트 에너지, 스마트 팜(Farm), 스마트 해양 등으로 확대되고 있다 [1]. 특히 고용량 베터리와 무선 통신 기술 발전으로 웨어러블 디바이스를 사용하는 스마트 의료나 스마트 헬스케어 등의 IoT 서비스가 출시되었다 [2].

이 웨어러블 디바이스를 사용하는 스마트 의료나 스마트 헬스케어 등의 IoT 서비스는 서비스 제공 시간 확보를 위해 경량화를 지향한다 [3]. 그러나 이러한 IoT 서비스는 보안 기술 도입에 매우 소극적이다. 매우 간단한 보안 기술만 적용하거나 심지어 보안 기술 일체를 적용하지 않기도 한다. 이와 같은 취약한 IoT 서비스는 다양한 보안 위협에 노출되어 있어, 악의적 공격에 의해 안정적인 서비스를 제공하지 못할 수 있다 [4].

이러한 IoT 서비스 보안 현황이 지적되면서 IoT 서비스에 대한 디바이스 인증이나 기밀성, 무결성 등의 보안 요구사항이 제안되었으며, 관련 보안 기술도 제시되었다. 그러나 legacy 정보서비스와 같은 수준의 보안 기술을 적용한다면, 상대적으로 연산이 많은 보안 기술 제공으로 전력 소모가 증가하여 IoT 서비스 제공 시간이 단축되는 문제점이 있다 [5].

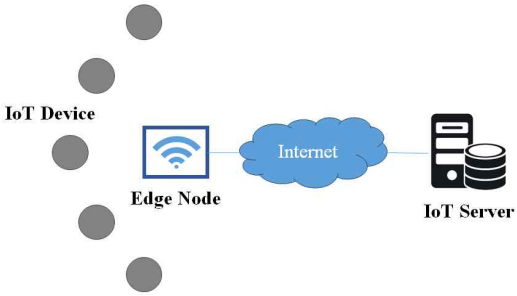
본 연구에서는 IoT 서비스 목표 달성을 지원하며 안전한 서비스 환경을 제공할 수 있는 베터리 전력 환경의 IoT 디바이스 인증 기술을 제안한다. 제안하는 IoT 디바이스 인증 기술은 Diffie-Hellman 알고리즘을 적용하며, IoT 서버에 대한 IoT 디바이스 접근을 통제한다. 본 연구에서는 제안하는 IoT 디바이스 인증 기술의 실효성을 검증하기 위해, 기능을 확인하고 전력 소모 수준을 비교한다.

본 연구에서 제안하는 IoT 디바이스 인증 기술은, legacy 디바이스 인증 기술 대비 전력 소모를 최소화한다. 본 연구에서 제안하는 인증 기술이나, 이를 준용한 유사 인증 기술을 베터리 전력 기반 IoT 서비스에 적용하면 인가된 IoT 디바이스만 서버에 접근할 수 있으며, 악의적 공격자에 의한 IoT 디바이스 위장 공격을 차단할 수 있는 장점이 있다.

2. 관련 연구

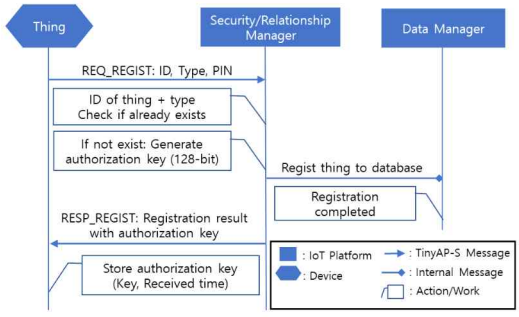
2.1 IoT 디바이스 인증 기능 적용 현황

IoT 서비스는 (그림 1)과 같이 IoT 디바이스에서 생성·전달되는 정보를 수집, 저장, 분석하는 IoT 서버와 원격지에서 동작하는 IoT 디바이스로 구성되며, 서비스 특성에 따라 IoT 디바이스를 서버와 연결하기 위한 Edge node를 사용하기도 한다 [6, 7].



(그림 1) IoT 서비스 네트워크

IoT 서비스는 인가된 디바이스의 접근만을 허용하기 위해서 디바이스 인증 기능을 사용한다. 이때 인증 정보 유출 방지를 위해 암호화 채널 사용 등의 부가적인 보안 기술을 적용한다. (그림 2)는 대표적인 IoT 디바이스 인증 메커니즘이다 [8].



(그림 2) IoT 디바이스 인증 구조

(그림 2)와 같이, 많은 IoT 서비스는 IoT 디바이스 ID와 authorization key 등의 인증 토큰(Token)을 사용하는 메커니즘을 채택한다.

그러나 IoT 서비스 중 스마트 의료나 헬스케어 서비스 개발자는, 사용자의 충분한 IoT 서비스 사용 시간 확보를 위해 IoT 디바이스 인증 메커니즘을 매우 간소화하거나 적용하지 않기도 한다. IoT 디바이스 이름이나 ID를 사용하는 단순 메커니즘을 적용하거나 심지어 인증 메커니즘 일체를 생략하기도 한다 [9].

이러한 보안 환경에서는 IoT 서비스에 인가되지 않은 IoT 디바이스가 서버에 접속할 수 있다. 악의적 공격자는 잘못된 정보를 주입할 수 있으며, IoT 디바이스를 경유하여 서버에 있는 중요 정보에 접근할 수 있는 위험이 있다 [10].

2.2 IoT 보안 요구사항

일반적으로 IoT 서비스는 기계, 에너지, 환경 등의 다양한 융합 산업 분야에 활용된다. 그러므로 전통적인 정보서비스 대비 정보보안에 취약하다. 특히 산업 분야 특징상 IoT 서비스가 보안 위협을 받을 경우, 기기의 오동작 및 고장이 발생하거나, 심지어 인명 피해가 발생할 수 있다.

이러한 환경을 고려하여 IoT 서비스에 대한 보안 연구가 진행되어 왔으며, <표-1>과 같은 보안 요구사항이 제시되었다 [11].

<표 1> IoT 서비스 보안 요구사항

보안 요구사항	설명
디바이스 인증	• IoT 서버나 Edge node에서 IoT 디바이스 검증
키 분배/관리	• IoT 디바이스 인증·데이터 보호에 사용되는 암호키 분배·보관
메시지 보호	• 서비스에 사용되는 전송 데이터의 기밀성 및 무결성 보장
부인 방지	• 전송 데이터 송수신 거부 방지
프라이버시 보호	• 전송 데이터 중, 개인 식별 정보나 민감 정보의 노출 방지
형상 관리	• IoT 서비스에 적용되는 SW의 버전 및 변경 관리

상기 IoT 서비스 보안 요구사항 외에, IoT 디바이스 물리적 보안이나 디바이스 자체 안정성 확보, 모니터링 등의 보안 요구사항도 제시되고 있다 [12].

2.3 IoT 디바이스 인증 기능 적용 고려사항

IoT 서비스를 제공하는 데 있어, 안정적인 서비스 제공을 위해 IoT 디바이스 인증 기술은 필수적이다. 그러나 이 인증 기능을 구현하는 데 있어 legacy 정보서비스와 같은 수준의 인증 기술을 적용하게 되면, 해시 알고리즘 같은 암호 연산으로 베터리 소모가 증가하여 IoT 서비스 유지 시간이 단축되는 단점이 있다.

3. 베터리 전력 기반 IoT 디바이스 경량 인증 기술

3.1 IoT 디바이스 경량 인증 기능 요구사항

보안 기술이 IoT 서비스 본연의 목적 달성을 저해할 수는 없다. 그러므로 베터리를 사용하는 IoT 디바이스를 사용하는 IoT 서비스에 디바이스 인증 기능을 구현할 때는, IoT 디바이스에 전원을 공급하는 베터리 소모를 최소화하는 IoT 디바이스 인증 기술이 요구된다.

본 연구에서는 이러한 IoT 서비스 환경을 고려하여 <표-2>와 같은 경량 인증 요구사항을 도출하였다.

<표 2> IoT 디바이스 경량 인증 요구사항

인증 요구사항	설명
암호 연산 최소화	• 베터리 기반 전력 사용 최소화를 위해 암호 연산을 사용하지 않거나 가급적 최소화
인증 정보 노출 극복	• 전력 사용 최소화를 위해 인증 정보 전송 시 가능한 평문으로 전송
최소한의 인증 정보 사용	• 인증에 사용되는 디바이스 정보 등 사용 정보의 최소화
인증 정보 재사용 방지	• 디바이스 위장 공격 방지

IoT 디바이스 경량 인증 요구사항은 인증 기능 제공에 필요한 리소스 사용을 최소화하여 IoT 서비스 유지 시간을 확보한다.

3.2 IoT 디바이스 경량 인증 프로토콜

본 연구에서는 도출한 IoT 디바이스 경량 인증 요구사항을 만족할 수 있는 경량 인증 프로토콜을 제안

한다. 제안하는 프로토콜은 (그림 3)과 같이 IoT 디바이스 등록을 위한 Register 과정 a)와, 등록을 완료한 이후 IoT 디바이가 IoT 서버나 Edge Node에 접근할 때 적용되는 Authentication 과정 b)로 나뉜다.

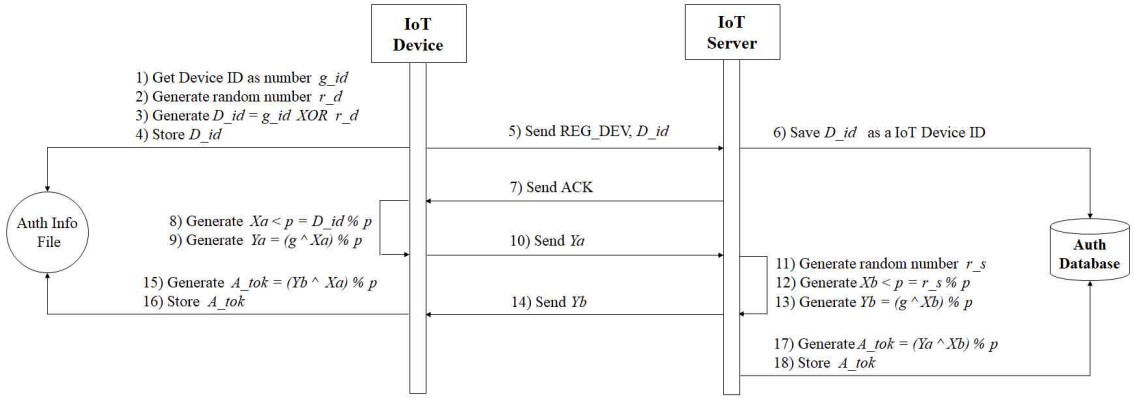
Register 과정에서 IoT 디바이스는 Device ID(*g_id*)를 획득하고, Random Number(*r_d*)를 생성하여 *D_id*를 생성, 이를 저장한다. 이후 <표 2>에 기술된 요구사항을 만족하기 위해 Diffie - Hellman 알고리즘을 적용하여 상호 공유된 IoT 디바이스 등록키 *A_tok* 를 생성하며 그 과정은 수식 (1)과 같다.

$$\begin{aligned} Xa\_a &= r\_da \ \% \ p \\ Ya\_a &= (g \ \hat{} \ Xa\_a) \ \% \ p \\ Tk\_a &= (Yb\_a \ \hat{} \ Xa\_a) \ \% \ p \end{aligned} \quad (1)$$

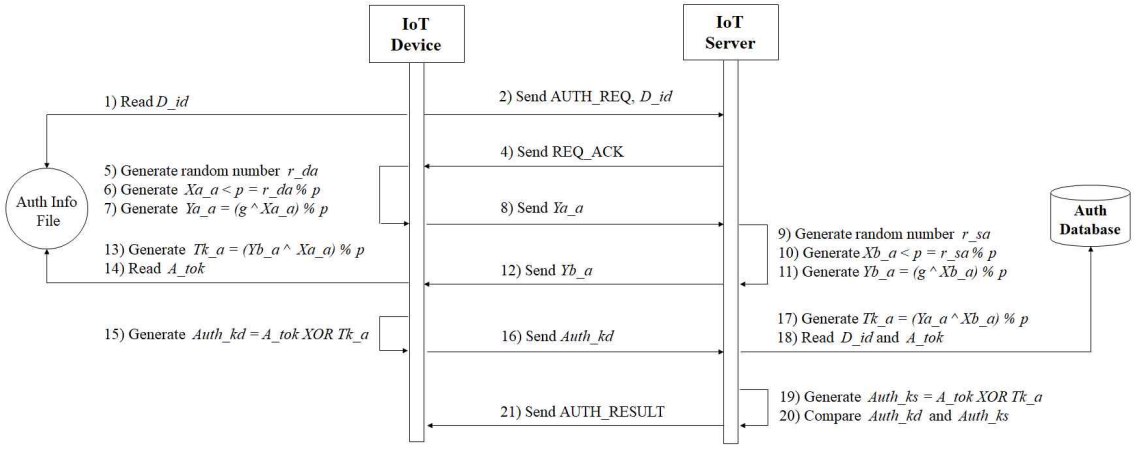
여기서 p는 소수(Prime Number)이며, Xa와 Xb는 각각 IoT 디바이스와 서버의 Diffie-Hellman 알고리즘의 개인키이며, Ya와 Yb는 공개키이다.

Authentication 과정에서 IoT 디바이스는 사전 등록한 D_id 를 IoT 서버에 전달, 인증을 요청한다. 이후 IoT 디바이스와 서버는 수식 (2)와 같이 Diffie-Hellman 알고리즘을 적용하여 각각 임시 토큰인 *Tk_a*를 생성한다.

$$\begin{aligned} D\_id &= g\_id \ XOR \ r\_d \\ Xa &= D\_id \ \% \ p \\ Ya &= (g \ \hat{} \ Xa) \ \% \ p \\ A\_tok &= (Yb \ \hat{} \ Xa) \ \% \ p \end{aligned} \quad (2)$$



a)



b)

(그림 3) IoT 디바이스 경량 인증 프로토콜 구조

a) IoT 디바이스 Register 과정, b) IoT 디바이스 Authentication 과정

최종적으로 IoT 디바이스는 수식 (3)과 같이 저장된 인증키 A_tok와 Tk_a를 사용하여 인증을 위한 Auth_kd를 생성하고 이를 IoT 서버에 전달한다. 서버는 이를 수신하고, 자체적으로 생성한 *Auth_ks* 와 비교하여 IoT 디바이스의 인증 여부를 판정한다.

$$Auth\_kd = Auth\_ks = A\_tok\ XOR\ Tk\_a \quad (3)$$

전체 인증 과정은 Diffie-Hellman 알고리즘에 적용되는 이산대수 원리에 따라 Register 과정에서 전송되는 공개키 *Ya, Yb*와 Authentication 과정에서 전송되는 *Ya_a, Yb_a*를 공격자가 획득하더라도, 각각 생성되는 *A_tok*이나 *Tk_a*를 산출할 수 없다. 그러므로 MIMA (Man-in-the-Middle-Attack)에 안전하다 [13].

4. 검증

4.1 기능 검증

본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜의 기능 검증을 위해 <표-3>과 같은 단위 기능 검증 항목을 도출하였다.

<표 3> IoT 디바이스 경량 인증 프로토콜 기능 검증 항목

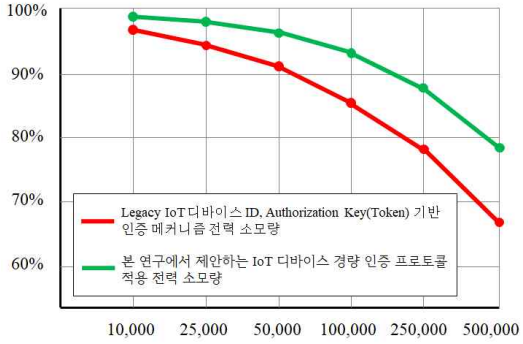
검증 항목	검증 사항
Func_Reg_1	• IoT 디바이스를 IoT 서버에 등록 시, IoT 디바이스 등록키 A_tok의 생성 및 등록
Func_Auth_1	• IoT 디바이스에서 IoT 서버에 접근 시, 인증키 Tk_a의 생성 확인
Func_Auth_2	• IoT 디바이스가 생성된 Tk_a를 전달하여 IoT 서버의 인증 여부 확인

위의 기능 검증 항목을 확인한 결과, 각 단위 기능 검증 항목별 정상 동작함을 확인하였다. 그러므로, 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜은 기능상 정상 동작함을 확인하였다.

4.2 성능 검증

본 연구의 최종 목적은 IoT 디바이스의 단말 인증 시, legacy 인증 기술 대비 전력 소모를 최소화하는 것이다. 그러므로, IoT 서비스에서 일반적으로 사용되는 RESTful 모델의 경량 프로토콜에서 사용되는 IoT 디바이스 인증 메커니즘의 전력 소비보다, 본 연구에서 제안하는 인증 프로토콜의 전력 소비가 적어야 한다.

이를 확인하기 위하여, 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜의 전력 소모량과 아두이노(Arduino) 단말에 COAP(Constrained Application Protocol) 환경의 인증 프로토콜을 구현 후 여기서 사용되는 전력 소모량을 비교 측정하였다. COAP 환경은 ID/Password 인증 메커니즘을 적용하였으며, Password는 SHA-256 알고리즘을, MIMA 대응을 가정하여 ECDHE-RSA-AES256-GCM-SHA256 Cipher Suite를 적용한 암호 채널을 사용하였다. 전력 소모량 측정은, 아두이노 단말에 전원을 공급하는 베터리(500mA)의 잔여 전력량으로 선정하였으며, 인증 회수 별 10회를 측정한 평균값을 적용하였으며, 그 결과는 (그림 4)와 같다.



(그림 4) 전력 소모량 측정 결과

(그림 4)는 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜의 전력 소모량은 Legacy 단말 인증 프로토콜에서 사용하는 전력 소모량 대비 20.86%의 전력을 덜 소모하는 것으로 확인되었다.

그러므로 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜은 전력 소모량 절감 관점에서 효과적인 것으로 확인되었다.

4.3 검증 결과 비교 분석

본 연구에서 제안한 IoT 디바이스 경량 인증 프로토콜은, <표-2>에서 제시한 요구사항에 대하여 legacy IoT 디바이스 인증 프로토콜 대비 <표-4>와 같은 장점이 있다.

<표 4> IoT 디바이스 경량 인증 프로토콜 검증 결과 분석

항목	Legacy IoT 디바이스 인증 프로토콜	본 연구에서 제안한 IoT 디바이스 경량 인증 프로토콜
암호 연산	• 기존 암호 알고리즘 사용	• DH 알고리즘 사용
인증 정보 노출	• 인증 정보 보호를 위해 암호 채널 사용	• DH 알고리즘 적용에 따른 MIMA로부터 안전
인증 정보 사용 범위	• 디바이스 ID, 인증 토큰	• 디바이스 ID
인증 정보 재사용	• 인증정보 재사용 가능	• 인증정보 재사용 불가

Legacy IoT 디바이스 인증 프로토콜은 암호 알고리즘 적용에 따라, 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜 대비 전력 사용량이 높은 것으로 확인되었다.

그러므로 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜은 기능 및 성능적으로 충분히 효과가 있는 것으로 확인되었다.

5. 결론

웨어러블 서비스는 수명 연장과 건강 유지를 위해 그 종류는 더 다양해질 것으로 예상된다. 그러나 IoT 서비스는 서비스 유지 시간 확보를 위해 보안 기술 도입에 소극적이다. 이러한 보안 환경으로 인해 IoT 디바이스의 보안 취약점을 이용한 보안 위협이 증가하고 있다. 스마트 헬스케어나 스마트 의료 서비스는 사용자의 중요 정보를 취급하므로, IoT 디바이스 인증 기술 적용이 요구되고 있다. 그러나 legacy 단말 인증 기술을 적용하면, 전력 소모가 증가하여 서비스 유지시간이 짧아지는 단점이 있다.

본 연구에서는 이러한 웨어러블 디바이스 기반 서비스를 포함한 베터리 전력 기반 IoT 서비스의 서비스 유지 시간을 보다 증가시킬 수 있는 IoT 디바이스 경량 인증 프로토콜을 제안하였다. 제안하는 인증 프로토콜은 Diffie-Hellman 알고리즘에 기반하여 연산 과정을 최소화하였으며 MIMA 공격에 대응할 수 있는 장점이 있다. 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜의 기능 검증 결과, 목표한 기능이 정상 제공되는 것을 확인하였다. 전력 소모량 측정 결과, 본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜은 legacy 단말 인증 기술 대비 전력을 덜 소비하는 것으로 확인되었다.

본 연구에서 제안하는 IoT 디바이스 경량 인증 프로토콜은 Diffie-Hellman 알고리즘 적용에 따라 인증 토큰 생성을 위한 정보 교환 회수가 많다. 그러므로 정보 교환 회수 축소를 위한 추가 연구가 후속되어야 한다.

참고문헌

[1] P. Gokhale, O. Bhat and S. Bhat, “Introduction to IOT,“ International Advanced Research Journal in Science, Engineering and Technology, vol.5, no.1, pp.41-44, 2018.

[2] M. A. Tunc, E. Gures and I. Shayea, “A survey on iot smart healthcare: Emerging technologies, applications, challenges, and future trends,“ arXiv preprint arXiv:2109.02042, 2021.

[3] T. Y. Wu, L. Wang and C. M. Chen, “Enhancing the security: A lightweight authentication and key agreement protocol for smart medical services in the ioht,“ Mathematics, vol.11, no.17, pp.3701, 2023.

[4] 김정태, “사물인터넷과 융합한 헬스케어 시스템에서의 보안 이슈 및 취약점 분석“, The Journal of the Convergence on Culture Technology (JCCT), vol.9, no.4, pp.699-706, 2023.

[5] M. Kumar and S. Chand, “A secure and efficient cloud-centric internet-of-medical-things-enabled

smart healthcare system with public verifiability“, IEEE Internet of Things Journal, vol.7, no.10, 10650-10659, 2020.

[6] M. Wazid, A. K. Das, S. Shetty, J. JPC Rodrigues and Y. Park, “LDAKM-EIoT: Lightweight device authentication and key management mechanism for edge-based IoT deployment,“ Sensors, vol.19, no.24, pp.5539, 2019.

[7] 신광철, “사물인터넷을 위한 경량화된 센서 네트워크 인증 프로토콜“, 한국정보기술학회 논문지, vol.20, no.1, pp.103-111, 2022.

[8] 유명한 and 김상경, “소셜관계 기반의 새로운 IoT 플랫폼 구현”, 한국통신학회논문지, vol.44, no.11, pp.2131-2145, 2019.

[9] E. K. Elsayed, L. S. Diab and A. A. Ibrahim, “Formal verification of an efficient architecture to enhance the security in iot,“ International Journal of Advanced Computer Science and Applications, vol.12, no.3, 2021.

[10] A. Alkhresheh, K. Elgazzar and H. S. Hassanein, “DACIoT: Dynamic access control framework for IoT deployments,” IEEE Internet of Things Journal, vol.7, no.12, pp.11401-11419, 2020.

[11] Y. H. Jeon, “사물인터넷 (IoT) 기반 스마트 그리드 보안 특성 및 쟁점 분석”, Review of KIISC, vol.24, no.5, pp.59-65, 2014.

[12] H. W. Kim and D. K. Kim, “IoT 기술과 보안”, Review of KIISC, vol.22, no.1, pp.7-13, 2012.

[13] A. Abusukhon, M. N. Anwar, Z. Mohammad and B. Alghannam, “A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm,” Journal of Discrete Mathematical Sciences and Cryptography, vol.22, no.1, pp.65-81, 2019.

〔저자소개〕

한 성 화 (Sung-Hwa Han)
동명대학교 정보보호학과 교수
숭실대학교 공학박사
관심분야 : IT융합보안, 시스템보안, 인공지능, 악성코드 탐지, 제로트러스트 보안
email: shhan@tu.ac.kr