Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 10 pp. 815-821, 2023

https://doi.org/10.5762/KAIS.2023.24.10.815
ISSN 1975-4701 / eISSN 2288-4688

스마트 홈 디바이스를 위한 무인증서 인증 메커니즘 설계

민소연[1*], 이재승[2]
[1]서일대학교 정보통신공학과, [2]숭실대학교 컴퓨터학과

Design of Certificate-less Authentication Scheme for Smart Home Devices

So-Yeon Min[1*], Jae-Seung Lee[2]
[1]Dept. of Information and Communication Engineering, Seoil University
[2]Dept. of Computer Science and Engineering, Soongsil University

요 약 스마트 홈 환경에서 IoT 디바이스의 증가와 복잡성이 높아짐에 따라 새로운 인증 메커니즘의 필요성이 부각되고 있다. 전통적인 PKI 기반 인증 방식은 복잡한 인프라와 중앙화된 인증서 관리의 부담으로 스마트 홈 환경에 적합하지 않을 수 있다. 이러한 배경에서 본 논문은 스마트 홈 IoT 디바이스를 위한 무인증서 인증 기법을 제안한다. 제안하는 프로토콜은 중앙 키 생성 센터(KGC)를 도입하여 디바이스 별 키를 생성 및 관리한다. 디바이스가 첫 연결 시 KGC에 인증 요청을 하면, KGC는 디바이스의 고유 정보와 함께 특정키를 생성하고 이를 디바이스에 전달한다. 이후 디바이스와 서비스 제공자 간의 통신에서 이 키를 활용하여 상호 인증을 진행한다. 이 무인증서 인증 기법은 디바이스의 수가 증가함에 따라 확장성 있게 설계되었으며, 키 관리의 중앙화로 인한 보안 위험을 최소화한다. 또한, 실제 스마트 홈 환경에서의 성능 테스트 결과, 제안하는 방법은 기존 방식과 비교했을 때, 디바이스가 증가할수록 데이터 전송량에서 큰 차이를 보였으며, 응답 시간의 경우 디바이스 수의 따라 약 100~120%의 성능이 향상되었다. 또한, 오버헤드에서도 디바이스 수의 따라 90~110% 이상이 향상되었다. 본 논문은 제안하는 인증 기법을 통해 스마트 홈 환경에서 효율성 있는 인증 및 키 관리 방안에 대해 작성하고 검증하였다.

Abstract With the proliferation and increasing complexity of IoT devices in smart home environments, there is growing emphasis on the need for novel authentication mechanisms. Traditional PKI-based authentication approaches may not be suitable for smart home settings because of their intricate infrastructure and the challenges of centralized certificate management. Against this backdrop, this paper proposes a certificate-less authentication scheme tailored specifically for smart home IoT devices. The proposed protocol introduces a Central Key Generation Center (KGC) to generate and manage keys for each device. Upon their initial connection, devices send an authentication request to the KGC, which then generates a specific key, incorporating the unique information of the device and conveying it back to the device. Subsequent communications between the device and service providers leverage this key for mutual authentication. This certificate-less authentication approach has been designed for scalability, particularly as the number of devices grows, minimizing the security risks associated with centralized key management. Furthermore, in actual performance tests within a smart home environment, the proposed approach showed a significant difference in data transmission volume as the number of devices was increased compared to the conventional method. Regarding response time, the performance improved by approximately 100-120% depending on the number of devices. In addition, there was 90-110% improvement in overhead depending on the number of devices. This paper reports an efficient authentication and key management solution for a smart home environment using the proposed scheme.

Keywords : SmartHome Authentication, Certificate-less Authentication, Key Management, IoT Authentication, IoT

본 논문은 서일대학교 학술지원비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
email: symin@seoil.ac.kr
Received September 01, 2023 Revised October 5, 2023
Accepted October 6, 2023 Published October 31, 2023

1. 서론

스마트 홈 환경은 최근 몇 년 동안 기술의 중심 역할을 해 왔으며, 사용자의 생활 품질 향상을 위한 다양한 기능과 서비스를 제공하고 있다. 스마트 홈의 핵심은 다양한 IoT(Internet of Things) 기기와 연결성이며, 이러한 연결성은 다양한 기기 간의 통신과 데이터 공유의 기초가 된다. 하지만 이런 연결성에는 크나큰 위험성이 도사리고 있다. 이러한 위험성 중 가장 중요한 것은 보안 문제로, 특히 인증 및 키 관리에 관한 것이다. 전통적인 인증 방법 중 하나는 인증서 기반의 방식이다. 하지만 이 방법은 복잡한 설치 및 관리 프로세스가 필요하고, 인증서의 유효기간, 갱신 및 취소 등의 문제점이 있다[1,2]. 또한, 스마트 홈 환경에서 다양한 기기의 수가 급격히 증가함에 따라, 인증서 기반의 방식이 효과적이지 않을 수 있다. 이에 따라, 무인증서 기반의 인증 및 키 관리 방법의 필요성이 대두되고 있다. 무인증서 방식은 전통적인 인증서의 복잡함을 제거하면서도 안전한 연결을 유지할 수 있는 방법을 제공한다. 이러한 방식은 스마트 홈 환경에서의 다양한 기기 간의 빠르고 안정적인 통신을 지원하며, 효율적인 보안 관리를 가능하게 한다.물론 무인증서 기반의 방식도 모든 부분에서 완벽하지 않다. 이 방식의 안전성, 효율성, 그리고 구현의 복잡성 등에 대한 근본적인 문제점들이 여전히 존재한다. 이러한 문제점들을 극복하고, 무인증서 기반의 방식을 스마트 홈 환경에 적용하기 위해서는 깊은 연구와 개발이 필요하다[3,4].

본 논문은 스마트 홈 환경에서 무인증서 기반의 인증 및 키 관리 방법에 관한 연구를 제안하며, 논문의 구성은 다음과 같다. 2장에서는 무인증서 인증 기법에 대한 설명과 장점, 스마트 홈 환경에서 보안의 중요성에 대해 기술하였으며, 3장에서는 스마트홈 환경에서 무인증서 기반의 새로운 인증 기법을 제안하였다. 4장에서는 해당 연구의 성능 검증을 통해 우수성을 확인하였으며, 5장 결론을 통해 연구의 장점, 향후 연구 계획에 대한 내용을 기술하였다. 이 연구를 통해, 무인증서 방식의 장점을 파악하고, 효과적인 구현 방법을 통해 스마트 홈 환경에서의 보안성을 높이고, 사용자의 정보와 기기를 안전하게 보호할 수 있는 방법을 제안한다.

2. 관련 연구

2.1 무인증서 인증 기법

무인증서 인증(Certificate-less Authentication)은 전통적인 PKI(Public Key Infrastructure)의 한계점을 극복하고자 나온 개념이다. 전통적인 인증방식인 PKI와의 차이로는 PKI의 경우 각 사용자는 CA(Certification Authority)로부터 발급받은 공개키 인증서를 가지고 있어야 한다. 이 인증서는 사용자의 공개키와 이를 식별할 수 있는 정보(ID 등)를 포함하며, CA에 의해 서명 된다. 무인증서의 경우 사용자는 인증서를 보유하고 있지 않으며, 대신 인증서 없이도 다른 당사자를 신뢰할 수 있는 메커니즘을 제공한다. IoT 장치와 같은 대규모 네트워크에서 수많은 장치들에게 인증서를 할당하고 관리하는 것은 복잡하고 비효율적일 수 있으며, 무인증서 인증은 이러한 복잡성을 줄일 수 있다. 또한, 장치들이 인증서를 저장할 필요가 없으므로, 저장 공간에 대한 강점을 가진다. 이는 특히 저장 공간이 제한적인 장치에 유용하며, 인증서의 검증 과정 없이 더 빠르게 인증을 수행할 수 있다. 인증서 기반 시스템에서는 인증서의 만료와 갱신 관리가 중요한 이슈이며, 일부 무인증서 인증 체계에서는, KGC(Key Generation Center)에 의해 생성된 부분 키가 손상되더라도, 사용자의 다른 개인 정보 없이는 완전한 개인 키로 사용될 수 없어서, 더 나은 보안성을 제공할 수 있다. 다만 사용자의 개인키와 공개키 간의 관계를 안전하게 유지하고, 중앙 키 생성 센터(KGC)와 같은 엔터티의 신뢰성을 보장해야 한다. KGC를 활용한 무인증서 인증 절차는 대략적으로 다음과 같은 단계로 구성된다[5-7].

먼저, 사용자는 KGC에 등록을 원하는 자신의 신원 정보(ID)와 관련된 정보를 제공한다. KGC는 이 정보와 KGC의 마스터 키(master key)를 사용하여 사용자의 개인 키(private key)를 생성한다. 이후, KGC는 안전한 방법으로 사용자에게 개인 키를 전달한다. 이는 직접적인 방법이나, 암호화된 채널 등 다양한 방법으로 이루어질 수 있다. 인증이 필요할 경우 사용자 A가 다른 사용자 B와 안전하게 통신하고자 할 때, A는 자신의 신원 정보와 통신을 시작하고자 하는 메시지를 B에게 전송한다. 키 생성 및 메시지 암호화를 위해 B는 A의 신원 정보(ID)와 KGC에서 미리 받아둔 자신의 개인 키를 활용하여 일시적인 공유 키(temporary shared key)를 생성한다. B는 이 공유 키를 사용하여 메시지를 암호화하고 A에게 응답한다.메시지 복호화 및 인증 완료를 위해 A는 동일한 방법으로 일시적인 공유 키를 생성하고 이 공유 키를 사용하여 B로부터 받은 암호화된 메시지를 복호화하고, 안전한 통신 채널이 형성된 것을 확인한다. 마지막으로 통신 종료 후 키 폐기를 위해 통신이 종료되면 일시

적으로 사용한 공유 키는 폐기된다.

KGC의 장점은 중앙에서의 키 관리와 사용자의 편의성을 제공한다는 것이다. 사용자는 별도의 인증서나 키 교환 절차 없이도 안전하게 통신할 수 있다. 단, KGC가 공격자로부터 보호받아야 하며, KGC가 손상될 경우 시스템 전체의 보안이 위협받을 수 있기 때문에 이에 대한 주의가 필요하다[8-10].

2.2 스마트 홈

스마트 홈의 토대가 되는 기술은 1970년대의 X10, 초기 원거리 통신 프로토콜을 통한 기본적인 집 내 장치 제어에서 시작되었다. 1990년대에는 인터넷의 상업적 성장에 따라 웹 연결을 통한 홈 자동화 솔루션의 가능성이 태동하였고, 2000년대 초에는 Wi-Fi, Zigbee, Z-wave와 같은 무선 통신 기술의 발전으로 스마트 홈 장치 간의 연결성이 크게 향상되었다. 2010년대에 들어, 스마트폰의 급속한 보급과 함께 클라우드 기반 서비스의 연동을 통한 스마트 홈 플랫폼들이 대중화되었고, 이를 통해 사용자는 어디서나 집의 다양한 IoT 장치들을 통합적으로 제어하게 되었다. 이러한 연속된 발전으로 현재 스마트 홈은 다양한 센서, 스마트 스피커 등의 IoT 장치들과의 연동을 통해 진보된 홈 환경을 제공하게 되었다. 스마트 홈은 연결된 장치와 시스템을 활용하여 주거 공간의 편의성, 안전성, 및 에너지 효율성을 극대화하는 현대적인 접근법을 표현한다. 주요한 기술적 원동력은 IoT로, 여기에는 원격 제어를 가능하게 하는 스마트폰과 같은 디바이스, 그리고 집의 조명, 온도, 보안 시스템 등을 제어하는 다양한 센서와 장치가 포함된다. 또한, 인공 지능과 머신러닝 기술은 스마트 홈 장치가 사용자의 습관과 선호도를 학습하여 최적화된 서비스를 제공하는 데 기여하며, Wi-Fi, Zigbee, Z-Wave 등의 무선 통신 기술은 장치 간의 연결성을 강화한다. 이러한 기술적 발전은 스마트 홈 시장의 급속한 확장을 이끌고 있다[11,12].

스마트 홈 기술의 발전은 우리의 일상에 편의성을 가져다주지만, 여러 보안 이슈에 직면하고 있다. 많은 장치들은 기본 패스워드나 약한 암호화를 사용하면서, 공격자의 침입에 취약해지고 있으며, 이런 장치들 간의 무선 통신은 암호화되지 않아 중간자 공격에 쉽게 노출될 수 있다. 추가로, 스마트 홈의 센서와 카메라는 사용자의 개인 정보와 생활 패턴에 관한 데이터를 수집하여, 이러한 정보가 부적절하게 취급되면 큰 프라이버시 침해 이슈로 이어질 수 있다[13]. 예시로 스마트 홈 기기들의 보안 취약성은 과거부터 다양한 해킹 사례로 그 심각성을 나타났는데, 2019년에는 Ring 도어벨의 보안 취약점이 노출되어, 외부인이 사용자의 집 안 활동을 무단으로 감시하는 사례가 발생했으며 Google의 Nest 보안 카메라도 유사한 문제를 경험했다. 사용자의 집안 상황에 무단으로 접근하거나 스피커를 통해 사용자와 소통하는 해킹 사례가 있었다. 2016년에는 Mirai 봇넷 악성 코드의 등장이 있었는데, 이 봇넷은 다수의 스마트 홈 장치를 감염시켜 대규모 DDoS 공격을 실시하였고, 이로 인해 여러 주요 웹사이트들이 서비스가 중단 되었다. 또한, 일부 스마트 온도 조절기는 해커의 원격 조작을 통해 집의 온도가 변경되는 등의 피해를 보는 사례도 있었으며, 보안 취약성을 가진 스마트 플러그는 전력망 공격의 도구로 사용되어 이로 인해 연결된 장치들의 제어가 위협받거나 전력망에 큰 영향을 주는 사례도 발생했다. 이런 사례들은 스마트 홈 장치의 보안이 얼마나 중요한지에 대해 지속적인 논의의 필요성을 보여준다[14,15].

3. 제안 내용

본 논문은 다음과 같은 절차를 기반으로 프로토콜을 작성하였다. 초기 KGC 인증 절차와 스마트 디바이스 등록 절차, 타임스탬프의 사용은 기본으로 정의되었음을 가정하고 진행한다. KGC 초기화를 위해 KGC는 공개 키와 비밀 키 쌍을 생성한다. 공개 키는 모든 스마트 디바이스와 중계 라우터, 서비스 제공자에게 공유하며 스마트 디바이스는 제조 시점에서 고유한 ID와 초기 비밀 키를 가지게 된다. 디바이스는 KGC에 자신의 ID와 초기 정보를 전송하여 인증을 요청하고, KGC는 디바이스의 정보를 검증하고 인증 토큰 및 세션 키를 디바이스에게 전송하여 통신에 활용된다. 중계 디바이스는 KGC에 인증을 요청하고 인증 후, 주변의 스마트 디바이스와 페어링을 시도한다. 스마트 디바이스와 중계 라우터는 상호 인증 절차를 수행하는데, 이 과정에서 KGC에서 제공받은 세션 키가 사용된다. 서비스 제공자는 KGC에 인증을 요청하고 인증이 성공하면, 서비스 제공자는 중계 라우터를 통해 스마트 디바이스와의 통신을 시작한다. 서비스 제공자와 스마트 디바이스는 상호 인증 절차를 수행한 후, 암호화된 통신 채널을 확립한다. 주기적으로, 또는 보안 정책에 따라, KGC는 새로운 세션 키를 생성하여 중계 라우터와 스마트 디바이스에 전송하며 비정상적인 활동이 감지될 경우 해당 키를 폐기하고 새로운 키를 생성, 배포한다.

Table 1. Proposed Notation

Notation	Meaning
KGC	Key Generation Center
N_r	Nonce
H_n	Hash Function
ID	Device ID
p,q,z	Prime Number
ID	Node ID
G_n	Elliptic Curve Group over a Finite Field
P,Q	point on G_n

3.1 디바이스 초기 인증

상기에서 서술한대로 디바이스 ID, 초기 데이터 값 등의 공유절차는 생략한다.

Step 1. KGC는 Master-Key s 및 G_1, G_2를 이용해 소수쌍 q, e, 그리고 P를 선택한다. 이후 P_0를 계산한 뒤 해시 함수와 난수를 선택하여 $H_1, H_2, G_1, G_2, P, P_0, e, n$을 이용하여 $param$ 값을 만든다.

Step 2. Service Provider와 KGC는 인증 절차를 위해 기본 데이터를 공유 한다.

Step 3. 인증을 위한 값 Q_A, D_A를 계산하고 $e(D_A, P) = e(Q_A, P_0)$를 증명한다.

Step 4. 인증을 요청한다.

Step 5. $e(D_A, P) = e(Q_A, P_0)$를 증명하고 X_A를 계산한다. 이후 키 쌍을 만들어 공개키를 공유한다.

Step 6. 이후 절차는 스마트 디바이스와의 아이디 및 증명 값을 주고 받으며 이상이 없을 경우 초기 인증을 마무리 한다.

3.2 디바이스 인증 및 키 관리

상기에서 서술한대로 초기에는 공유 값을 통해 요청을 받은 것을 가정하고 진행한다.

Step 1. KGC는 소수 p, q와 g, x를 선택하고 y를 계산한다. 이후 해시 함수와 난수 n을 선택하고 해당 값들을 이용하여 $Param$값을 생성한다. 해당 값은 공유 된다.

Step 2. 중계 라우터는 U_x와 r을 선택하고 r_{id}, r'_{id}, 그리고 g^x를 이용하여 U_{id}를 만든다. 이후 $r_{id} + xH_1(ID, U_{id})$를 통해 D_{id}를 만들어 저장하고 v_{ID}, P_{ID}를 연산한다.

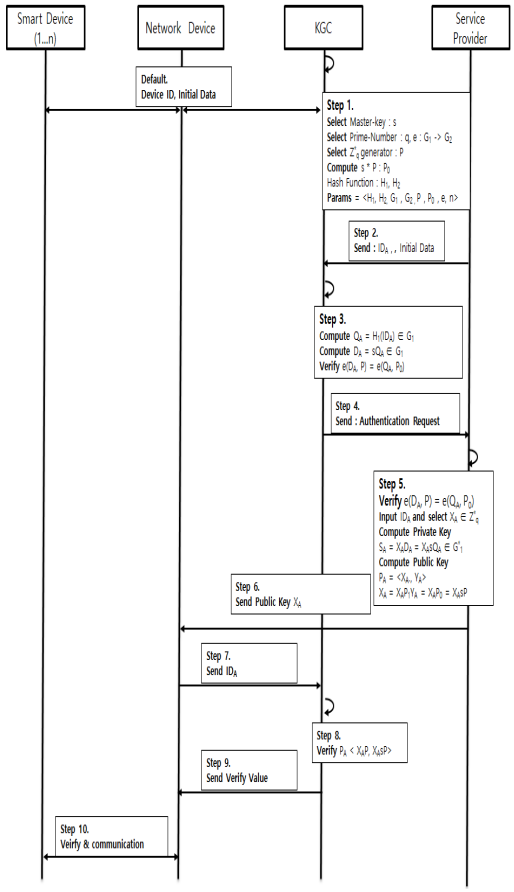

Fig. 1. Initial Authentication Process

Step 3. 디바이스 ID와 z를 선택하고 S_{ID}를 계산한다. 이후 $P_{ID,} S_{ID}$를 전달한다.

Step 4. 전달 받은 데이터를 전달하여 검증을 요청 한다.

Step 5. 검증 기관은 U_x를 계산한 후 r을 선택하고 U_{ID}를 생성한 다음 $v_{ID,} p_{ID}$를 연산하여 키 DK_{ID}를 생성한다. 검증이 완료되면 디바이스는 μ_{ID}를 계산하고 해당 값을 이용해서 PK_{ID}를 생성한다.

해당 결과는 응답 메시지를 통해 개인키및 공개키 생성 과정을 종료한다.

Step 6. 마지막 검증 절차로 디바이스는 $v_B y^{H_1(b, U_b, v)}$를 검증하고 난수를 생성하여 해시 값 h, h`를 생성한다 $H_{3..4}(m, t, \mu'_r, U_B^r y^{H_1(B, \omega B)} r, \mu_{ID,} U_A, \mu_B, U_B)$ 이후 h, h'를 이용해 s와 (c, s, t)를 계산한다.

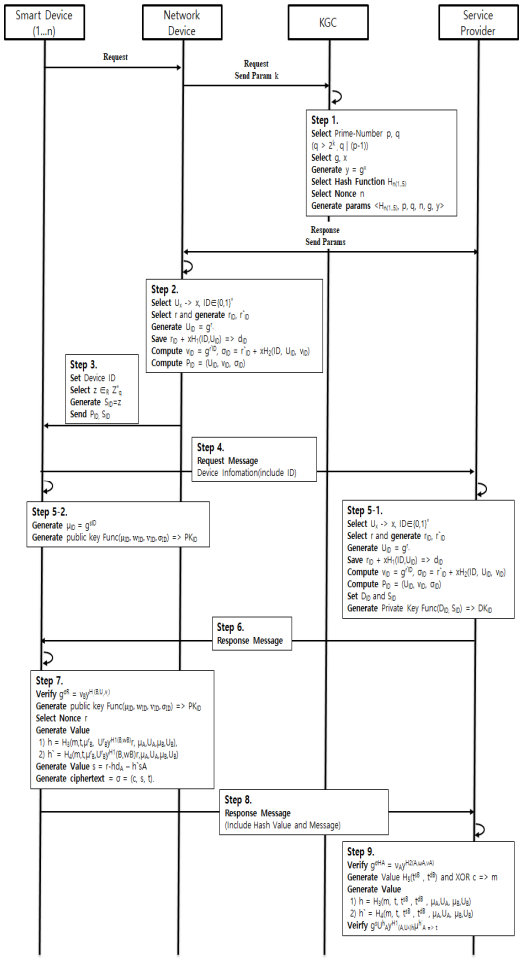

Fig. 2. Device Authentication

Step 6. $g^{\sigma A}$를 계산 후 h, h' 해시 값을 검증한다. $H_{3..4}(m,t,t^{sB},t^{dB},\mu_A,U_A\mu_{B,}U_B)$ 이후 t를 계산해 증명 후 종료한다.

4. 성능 평가

4.1 효율성 검증

본 논문에서는 제안방식의 실험 분석을 위해 다음과 같은 가상 환경을 구성하여 검증하였다.

성능 테스트를 위해 Table 2, Table 3, Table 4와 같이 가상의 환경을 구성하였으며, 스마트 홈 환경에서 사용되는 디바이스의 성능을 고려한 가상의 센서를 배치하여 실험을 진행하였다. 실험은 인증 및 키 관리 과정에서 발생하는 데이터 전송량, 연산량, 인증 시간을 기준으로 배치된 센서를 랜덤으로 선택하여 인증 횟수에 따른 결과를 도출하였다.

Table 2. Hardware Environment

PC Specifications	
Processor	Intel Core i7-9700K @ 3.60GHz
RAM	16GB DDR4
Storage	512GB NVMe SSD
Network Card	Gigabit Ethernet

Table 3. Software Environment:

Software Environment	
Operating System	Windows 10 Pro (64-bit)
Virtualization Tool	VMware Workstation 16
IoT Emulation Software	ns-3
Network Monitoring Tool	Wireshark

Table 4. Communication Environment:

Communication Environment	
Communication specifications:	Virtual network environment simulating 4G/LTE modules
Internal network	Ethernet virtual network.

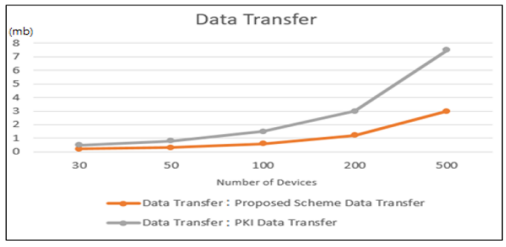

Fig. 3. Experimental result of Data Transfer

실험 결과, Fig. 3은 데이터 전송량이 기존 잘 알려진 PKI 시스템 대비 2배 정도의 차이가 나며, 횟수가 많아질수록 디바이스에 가중되는 부담이 가파르게 개선되었음을 확인할 수 있었다.

Fig. 4는 연산량의 비교를 나타내며 약 인증 횟수에 상관없이 꾸준히 2배 정도의 차이가 개선되었음을 나타내고 있다.

평균 인증 시간의 경우에도 Fig. 5에서 나타내듯 기존에 제안하는 방법과 비교했을 때 약 2~2.5배의 효율성을 가짐을 확인할 수 있었다.

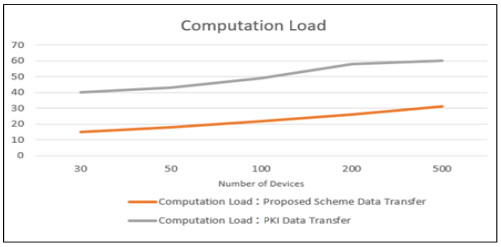

Fig. 4. Experimental result of Computation Load

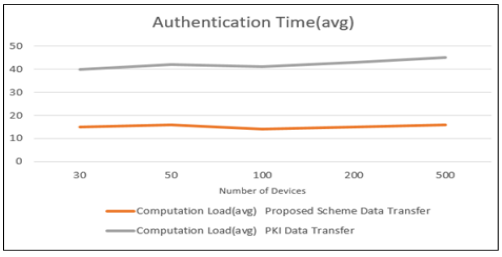

Fig. 5. Experimental result of Authentication Time

5. 결론

스마트 홈 환경이 지속적으로 발전함에 따라 IoT 디바이스의 수가 급증하고 시스템의 복잡성이 증가하면서 보다 간결하고 효율적인 인증 메커니즘의 필요성이 점점 커지고 있다. 전통적인 공개키 기반 인증 방법은 복잡한 인프라 구조와 중앙화된 인증서 관리로 인해 스마트 홈 환경에는 적합하지 않을 수 있다. 이러한 문제점을 극복하기 위해 본 연구에서는 스마트 홈 IoT 디바이스에 특화된 무인증서 인증 스키마를 제안한다. 이 제안된 프로토콜은 중앙 키 생성 센터(KGC)를 도입하여 각 디바이스의 키를 중앙에서 생성 및 관리한다. 디바이스가 첫 연결 시 KGC에 인증 요청을 하면, KGC는 해당 디바이스의 고유 정보를 바탕으로 특정 키를 생성하여 디바이스에게 전송한다. 이후, 디바이스와 서비스 제공자 간의 통신에서는 이 키를 활용하여 인증 과정을 수행한다. 이 무인증서 인증 스키마는 디바이스의 수가 계속해서 증가함에도 불구하고 확장성 있게 설계되었으며, 중앙화된 키 관리 방식은 보안 위험을 크게 줄인다. 실제 스마트 홈 환경에서의 성능 테스트 결과 기존의 인증 방식에 비해 전송량, 응답 시간, 시스템 오버헤드 등에서 약 2~2.5배의 뛰어난 성능을 보였다. 본 연구는 이렇게 제안된 인증 스키마를 통해 스마트 홈 환경에서의 인증 및 키 관리에 대한 효율적인 해결책을 제시하고 그 유효성을 검증하였다. 스마트 홈 환경에서 우수성을 확인하였으므로, 향후 연구를 통해 확장성 있는 프로토콜을 구현하여 스마트 홈 뿐만 아니라 웨어러블이나 스마트 더스트 등 다양한 IoT 환경에서 적용될 수 있을 것으로 기대된다.

References

[1] MENG, Yan; ZHU, Haojin; SHEN, Xuemin. Literature Review of Security in Smart Home Network. Security in Smart Home Networks, 2022, pp.21-35. DOI: https://doi.org/10.1007/978-3-031-24185-7_2

[2] ALI, Waqar, et al. IoT based smart home: Security challenges, security requirements and solutions. In: 2017 23rd International Conference on Automation and Computing (ICAC). IEEE, 2017. pp.1-6. DOI: https://doi.org/10.23919/iconac.2017.8082057

[3] MANDAL, Shobhan, et al. Certificateless-signcryption-based three-factor user access control scheme for IoT environment. IEEE Internet of Things Journal, 2020, 7.4: pp.3184-3197. DOI: https://doi.org/10.1109/jiot.2020.2966242

[4] DU, Hongzhen, et al. A new provably secure certificateless signature scheme for Internet of Things. Ad Hoc Networks, 2020, 100: 102074. DOI: https://doi.org/10.1016/j.adhoc.2020.102074

[5] LIU, Jingwei, et al. Certificateless remote anonymous authentication schemes for wirelessbody area networks. IEEE Transactions on parallel and distributed systems, 2013, 25.2: pp.332-342. DOI: https://doi.org/10.1109/tpds.2013.145

[6] NKURUNZIZA, Egide, et al. ECAAP-SG: Efficient certificateless anonymous authentication protocol for SG. Security and Privacy, 2023, 6.1: e273. DOI: https://doi.org/10.1002/spy2.273

[7] BARBOSA, Manuel; FARSHIM, Pooya. Certificateless signcryption. In: Proceedings of the 2008 ACM symposium on Information, computer and communications security. ACM, pp.369-372 2008. DOI: https://doi.org/10.1145/1368310.1368364

[8] WU, Chenhuang; CHEN, Zhixiong. A new efficient certificateless signcryption scheme. In: 2008 International Symposium on Information Science and Engineering. IEEE, pp.661-664. 2008. DOI: https://doi.org/10.1109/isise.2008.206

[9] XIE, Wenjian; ZHANG, Zhang. Efficient and provably secure certificateless signcryption from bilinear maps. In: Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on. IEEE, pp. 558-562. 2010. DOI: https://doi.org/10.1109/wcins.2010.5541841

[10] XIE, Wenjian; ZHANG, Zhang. Certificateless Signcryption without Pairing. IACR Cryptology ePrint

Archive, 2010: p.187. 2010.
DOI: https://doi.org/10.3724/sp.j.1001.2011.03891

[11] DOMB, Menachem. Smart home systems based on internet of things. In: Internet of Things (IoT) for automated and smart applications. IntechOpen, 2019. DOI: https://doi.org/10.5772/intechopen.84894

[12] TASTAN, Mehmet. Internet of things based smart energy management for smart home. KSII Transactions on Internet and Information Systems (TIIS), 2019, 13.6: pp.2781-2798. DOI: https://doi.org/10.3837/tiis.2019.06.001

[13] YU, Rui; ZHANG, Xiaohua; ZHANG, Minyuan. Smart home security analysis system based on the internet of things. In: 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). IEEE, 2021. pp.596-599. DOI: https://doi.org/10.1109/icbaie52039.2021.9389849

[14] BASTOS, Daniel; SHACKLETON, Mark; EL-MOUSSA, Fadiali. Internet of things: A survey of technologies and security risks in smart home and city environments. 2018. DOI: https://doi.org/10.1049/cp.2018.0030

[15] YE, Chenghao; INDRA, Praburam Prabhakar; ASPINALL, David. Retrofitting security and privacy measures to smart home devices. In: 2019 sixth international conference on internet of things: systems, management and security (IOTSMS). IEEE, 2019. pp.283-290. DOI: https://doi.org/10.1109/iotsms48152.2019.8939272

민 소 연(So-Yeon Min) [종신회원]

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신공학과 교수

〈관심분야〉
통신 및 신호처리, 정보통신, 임베디드 시스템

이 재 승(Jae-Seung Lee) [정회원]

- 2013년 2월 : 평생교육진흥원 컴퓨터학과 (공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2015년 3월 : 숭실대학교 컴퓨터학과 박사수료
- 2019년 ~ 2022년 : (주)IOSYS 연구소 연구원

〈관심분야〉
시큐어코딩, Sensor Network, IoT Security