The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 19, No. 2, pp.103-109, Apr. 30, 2019. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2019.19.2.103
JIIBC 2019-2-15

분산 클러스터 기반 IoT 디바이스 경량 인증 방법에 대한 연구

A Study on Light Weight Authentication Method of Distributed Cluster-based IoT Devices

김성환*, 김영곤**

Sung-hwan Kim*, Young-gon Kim**

요 약 ICT 기술이 발달로 인하여 주변에 존재하는 사물들을 네트워크로 연결하고, 사물에 대한 정보를 이용하여 다양한 분야에서 활용하기 위한 IoT 환경이 주목받고 있으며, 보안 위협 또한 증가하는 추세이다. IoT 환경에서 증가되는 보안 문제를 해결하기 위해 민간 분야에서 인증서, 암호화, 해쉬연산, 블록체인 등을 활용한 방법들을 연구하고 있으나, 디바이스 간의 성능 격차를 극복하고 다양한 장치에서 호환성을 가지는 보안인증 방식은 현재까지 구체화 되어 제안되고 있지 않은 상황이다. 본 논문에서는 IoT 장치 환경에 따른 영향을 최소화하여 호환성을 폭넓게 확보할 수 있는 인증 방식을 제안하고자 한다.

Abstract Due to the development of ICT technology, the IoT environment for connecting objects in the vicinity to networks and utilizing information about objects in various fields is getting attention, and security threats are also increasing. In order to solve the increasing security problem in IoT environment, we are studying methods that use certificate, encryption, hash calculation and block chain in the private sector. However, the security authentication method which overcomes the performance gap between devices and has compatibility with various devices It has not been proposed yet. In this paper, we propose an authentication method that can achieve wide compatibility by minimizing the influence of IoT device environment.

Key Words : Authentication, OTP, Blockchain, IoT, Auth, MQTT

Ⅰ. 서 론

ICT 기술이 발달로 인하여 주변에 존재하는 사물들을 네트워크로 연결하고, 사물에 대한 정보를 이용하여 다양한 분야에서 활용하기 위한 IoT 환경이 주목받고 있다. IoT 서비스는 스마트폰, 스마트 워치, 스마트 밴드 등의 개인 휴대 장치와 센서, 데이터 수집 장치, 가전제품, 모니터링 장치, 산업용 장비 등 다양한 분야에 적용되어 사용이 확산되고 있으며, IoT 기술은 네트워크 환경과 디바이스 에서 활용 가능한 확장성을 제공하지만 여러 종류의 각기 다른 특성을 가지는 시스템 및 센서 장치들과 이들이 연결된 다양한 형태의 네트워크 구성으로 인한 복잡한 운영환경에서 사용되고 있는 특성을 가지고 있어 보안을 위협할 수 있는 요인 또한 다수 존재하며, 이들의 취약성을 통한 외부로 부터의 보안 위협은 지속적으로 증가하고 있다.

*김성환, 한국산업기술대학교 컴퓨터공학과
접수일자 2019년 1월 18일, 수정완료 2019년 3월 3일
게재확정일자 2019년 4월 5일

Received: 18 January, 2019 / Revised: 3 March, 2019 / Accepted: 5 April, 2019
*Corresponding Author: ykkim@kpu.ac.kr
Korea Polytechnic University Department of Computer Engineering

IoT 환경에서의 보안 문제를 해결하기 위해 민간 분야에서 인증서, 암호화, 해시연산, 블록체인 등을 활용한 방법들을 연구하고 있으며, 다양한 장치에 적용할 수 있는 보안 인증 방식을 구현하여 IoT 환경에서 보편적인 보안 서비스 제공을 위한 다양한 방법들을 제시하고 있다. 그러나, IoT 디바이스는 다양한 용도와 비례하여 디바이스의 CPU 연산능력, 네크워크 환경, 암호화 미지원, 저장 용량의 한계 등의 다양한 제약 요인들로 인하여 다양한 장치에 호환성을 가지는 인증방법의 구현에 어려움이 있다. 따라서 본 논문에서는 IoT 장치 환경에 따른 영향을 최소화하여 호환성을 폭넓게 확보할 수 있는 인증 방안을 제시하고자 한다.

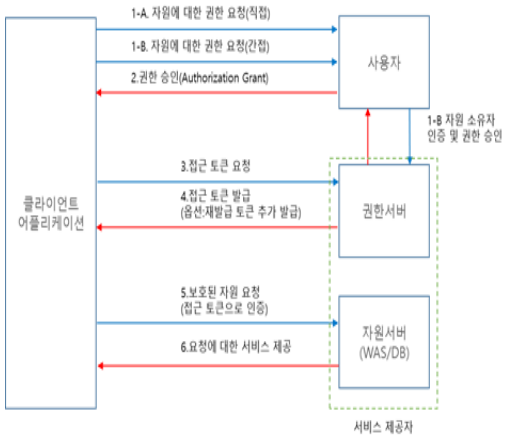

그림 1. OAuth 2.0 승인 프로세스
Fig. 1. OAuth 2.0 authentication process

II. 관련 연구

다수의 Device가 연동되는 IoT의 특성상 장치 간 인증이 필수적으로 요구되고 있다. 다양한 분야에서 활용되는 IoT 인증 방식은 아래와 같이 제안되고 있다.

1. OAuth

OAuth는 인증을 위한 오픈 스탠더드 프로토콜로, 다른 애플리케이션 또는 서비스에 사용자의 아이디와 암호가 노출되지 않도록 하면서 접근 위임을 하는 방식으로 Facebook, Twitter와 같은 특정 인터넷 서비스의 가입자가 다른 애플리케이션(데스크톱, 웹, 모바일 등)를 사용할 때 API 접근 위임 방식을 통해 특정 인터넷 서비스의 계정을 사용하여 인증할 수 있는 기존의 방식들이 있었으나, 표준화가 되어있지 않아 2007년에 비공식 논의체에 의해 OAuth 1.0이 표준화를 목적으로 개발되었으며, 2008년 IETF에서 표준안에 대한 논의가 있었고 2010년 IETF OAuth 워킹그룹에 의해 이 프로토콜이 IETF 표준 프로토콜로 발표 되었다. 현재까지 가장 최근에 출시된 OAuth 2.0은 드래프트 단계에 있는 것으로, IETF OAuth 워킹그룹이 주축이 되어 만든 것이며, OAuth 2.0 프로코콜은 이전 버전인 OAuth 1.0과 호환되지 않지만, 인증 절차가 간략한 장점이 있어 여러 인터넷 서비스에서 OAuth 2.0을 사용하고 있으며, IoT 환경에서도 활용하기 위한 연구가 활발한 상태이며, OAuth 2.0의 인증과정은 다음 그림 1의 Oauth 2.0 승인 프로세스와 같다[1],[2],[3],[4].

2. Kerberos

Kerberos는 미국 MIT대의 Athena Project에 의해 개발된 대칭키 방식에 의한 인증 시스템으로 신뢰받은 제3자 기반의 인증 시스템의 초기 구현 형태로 가장 대중적으로 도입되어 활용되고 있으며, 사용자와 서버 간 인증을 할 수 있는 중앙 집중식 인증 서버를 제공하며, Kerberos 서버, TGS(Ticket Granting Server), 티켓, 인증자로 구성되며, 다음 그림 2의 Kerberos 인증 프로세스와 같다[5].

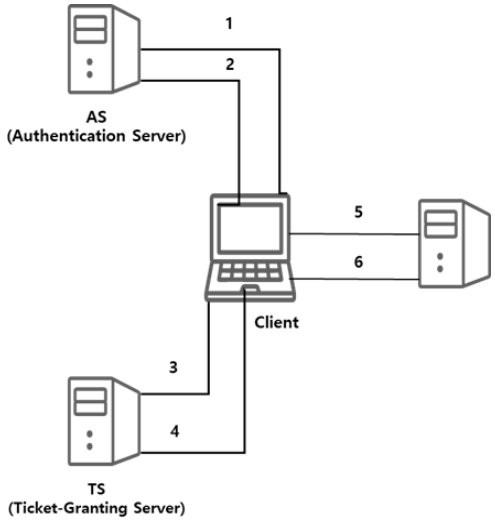

그림 2. Kerberos 인증 프로세스
Fig. 2. Kerberos authentication process

3. MQTT

IBM 에 의해서 개발되었고 2014년 국제 민간 표준기구인 오아시스에 의해서 표준으로 제정된 프로토콜로 경량화가 가능해서 통신 대역폭이 제한적인 사물인터넷에 적합하기 때문에 이를 활용하는 연구가 활발하게 이루어지고 있다. MQTT는 MQTT Broker, Publish, Subscribe로 구성되어 있으며, Publisher가 Hi 라는 메시지를 보내면 Subscribe 가 Broker를 통해 메시지를 받는 구조로 구독하지 않은 토픽과 Subscriber는 메시지를 받을 수 없는 특징을 가지고 있으며, 구성도는 다음 그림 3 MQTT Broker 구성도와 같다[6],7],[8].

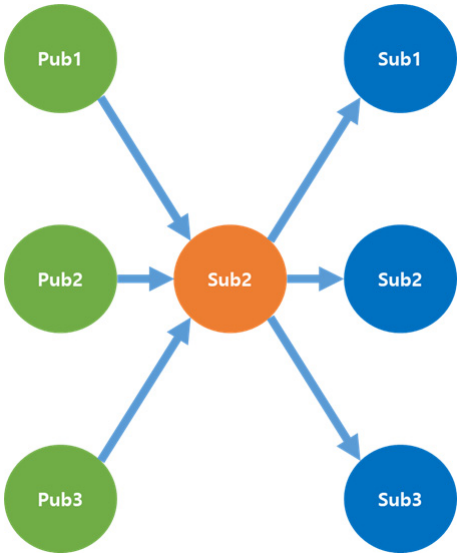

그림 3. MQTT Broker 구성도
Fig. 3. MQTT Broker diagram

4. 블록체인 기술

블록체인은 가상화폐 중 가장 많이 사용되고 활성화되어 있는 '비트코인'을 유지하는 기반 보안 기술이다. 비트코인에서 블록체인은 주기적으로 발행하는 화폐인 비트코인의 이동 이력을 저장하는 일종의 분산된 디지털 장부라고 할 수 있다. 이 장부는 위변조할 수 없는 암호학적 기술로 만들어지며 비트코인의 소유권 이동을 위해 비트코인의 거래(Transaction) 과정과, 발생한 거래를 모아 시간이 매우 오래 걸리는 특정 조건의 해시 값을 갖게 하는 난수(Nonce) 찾기 문제로 거래 내용의 위변조를 방지할 수 있는 작업증명(Proof of Work) 단계 등으로 만들어지며, 그림 4의 과정을 통해 합의인증 과정을 가진다.

분산장부 시스템을 통한 투명한 거래로 보안, 감독, 규제 비용 절감 가능 하며 P2P 네트워크 방식을 기반으로 참여자간 직접 거래가 이루어지기 때문에 중개기관 수수료가 발생하지 않는 장점이 있다.

블록체인은 탈 중앙화 구조이기 때문에 다수 참여자의 인프라를 공유하여 사용할 수 있어 대규모의 IT 장비와 인력으로 구성된 인프라를 요구하지 않는 장점을 가지고 있으나, 분산성과 익명성을 보장하는 시스템의 구조상 직접적인 통제가 필요한 시스템에 적용하기 어려운 문제가 있으며, 분산 원장 기술은 거래와 관련된 모든 데이터가 참여자들에게 공개하는 특성을 가지고 있기에, 정보 공개를 원하지 않거나 법 제도상 공개되지 않아야 하는 정보를 가지고 있는 환경에는 적용할 수 없는 문제가 있어, 이러한 문제점은 프라이빗 블록체인 기술들을 활용할 수 있는 대안이 연구되고 있다[9],[10].

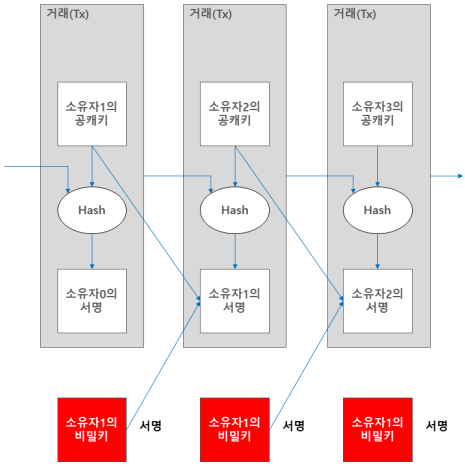

그림 4. 블록체인 인증 프로세스
Fig. 4. Blockchain authentication process

Ⅲ. 3장 본문

본 논문에서는 기존의 IoT 환경에서의 인증기술들이 가지는 문제점들을 해결하기 위한 방법으로 기기간의 효율적인 인증을 위해 ID와 패스워드를 입력 받지 않고 Device의 고유한 정보 값을 사전에 입력하고 값을 비교하여 인증 절차를 완료하는 방법과 사전 정의된 SeedWords 기반 난수표를 IoT 디바이스에 사전 배포한 상태에서 Challenge and Response 방식으로 검증 절차를 가지는 IoT to Gateway 방식과 블록체인의 다자합의

인증 방식을 활용한 Gateway to 서버 인증 방식을 제안하고자 한다.

1. Device 등록 및 인증방법

Device의 고유정보를 사전에 등록하여 인증 절차를 완료하는 방법은 인증과정이 간단하면서도 보안성이 우수한 서비스 이용 환경을 제공할 수 있으며, Device의 고유 값을 보안설정의 일부로 필드를 추가로 구현이 가능하며, 그림4와 같은 절차를 통해 인증을 수행한다.

이 방식은 기기가 게이트웨이에 접속을 시도할 경우 게이트웨이에서 사전 입력된 Device의 고유 정보를 대조 후 일치 여부를 확인되면 인증을 완료하는 과정을 가지며, Device 사전 등록 인증 프로세스는 다음 그림 5와 같다.

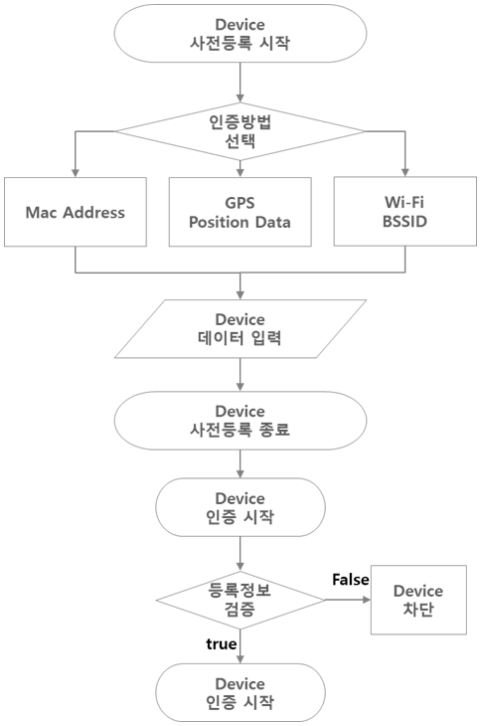

그림 5. Device 사전 등록 인증 프로세스
Fig. 5. Device preregistration authentication process

2. IoT to Gateway Authentication

IoT와 Gateway가 인증하는 방식은 Device의 사전 등록을 위한 인증 프로세스가 종료된 이후 IoT 장치와 서버간의 데이터 교환을 위해 IoT 장치가 서버와 연동하기 위해 인증 요청을 하는 인증 프로세스에서 Challenge anf Response 방식으로 수행하는 일련의 과정을 제안하였다. IoT 디바이스가 서버에 인증 요청을 OTP 카드번호를 전송하면 서버는 난수를 생성하여 challenge로 IoT 디바이스에 전달한다. 이와 동시에 IoT 장치 식별 번호에 해당하는 Seed Words 키를 데이터베이스에서 추출한 후 추출된 키를 이용하여 난수의 암호화를 시작한다. challenge 를 받은 IoT 장치는 IoT 장치에 내장되어 있는 Seed Words 값을 반환하며. IoT 장치로부터 Response를 받은 서버는 서버가 계산한 값과 수신한 값이 일치하는 경우에 장치를 정당한 권한을 가진 것으로 인증하게 된다. 본 인증과정은 다음 그림6의 Challenge and Response 방식 인증 프로세스와 같다.

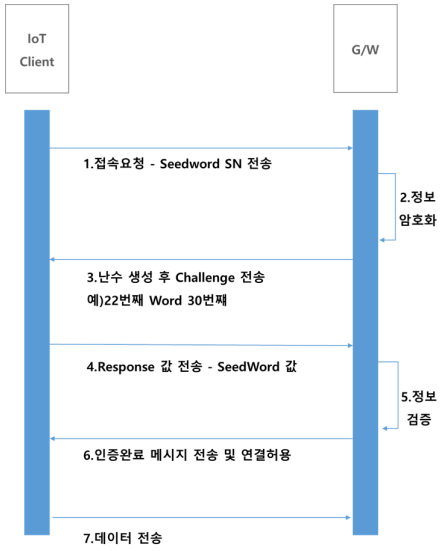

그림 6. Challenge and Response 방식 인증 프로세스
Fig. 6. Challenge and Response authentication process

본 논문에서 난수표의 단점을 보완하기 위해 제안된 Seed Words는 숫자, 알파벳 소문자, 알파벳 대문자를 조합하여 6자리로 4개의 조합된 단어를 생성하는 기법을 적용하였다. 제안되는 기법은 기존에 널리 사용되는 난수표에서 생성되는 코드와 비교했을 때 무작위 생성된 단어의 조합되어 있어 유추 또는 연산을 통한 해킹이 어렵고, 코드 생성 과정에서 복잡한 연산처리를 요구하지 않는 특성을 가지고 있으므로 시스템에서 요구하는 기본적인 보안성능은 유지하면서 디바이스의 연산능력에 대한 영향을 최소화 할 수 있어 초소형 저성능 시스템에도 적용할 수 있다. 제안되는 인증방법은 다음 그림7 IoT to Gateway 인증 알고리즘과 같다.

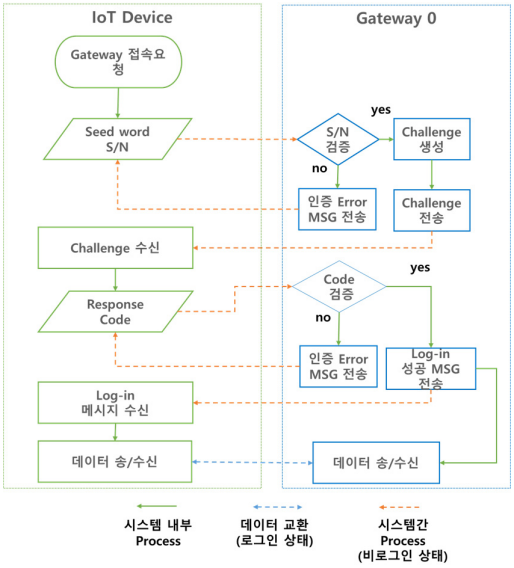

그림 7. IoT to Gateway 인증 알고리즘
Fig. 7. IoT to Gateway authentication Algorithm

3. Gateway to Server Authentication

Gateway와 서버 간 인증 과정은 Private 블록체인인 하이퍼레저 패브릭 기반으로 사용자 정의 알고리즘을 적용하여 아래 인증과정을 통해 역할을 수행한다.

제안되는 Gateway와 서버간의 인증을 위해 단계별로 수행되는 절차는 다음 그림8 G/W<-> 서버 인증 프로세스와 같다.

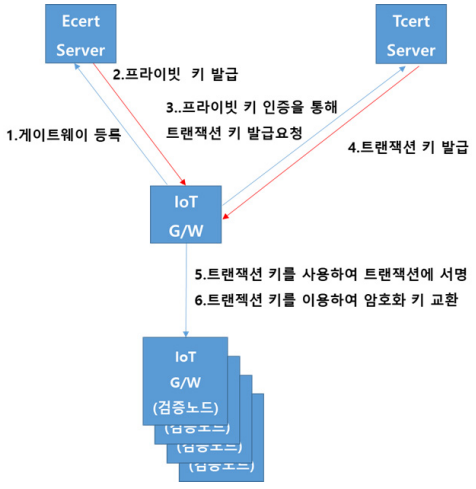

그림 8. G/W<-> 서버 인증 프로세스
Fig. 8. Gateway to Server authentication process

- Ecert 발급서버 - 개인키
- Tcert 발급서버 -1회용 트랜잭션 키
- Gateway는 Ecert 발급
- Gateway는Tcert를 발급
- Gateway는 Tcert를 이용하여 서버에 접속
- Gateway는 개별적으로 검증 노드 역할을 수행

본 논문에서 제안되는 Private 블록체인 아키텍처는 일반적인 형태의 PBFT 알고리즘에 추가로 사용자가 알고리즘을 정의한 후 시스템에 적용하여 사용할 수 있는 특징을 가지기 때문에 시스템이 가지는 목표에 최적화된 구조를 제공하며, 외부에 노출되지 않는 프라이빗 형태의 환경을 제공할 수 있다. 이러한 블록체인 아키텍처는 G/W와 서버 간의 데이터 교환을 위한 인증 과정에서 원장을 공유하는 방식은 차이가 없으며, 네트워크에 연결되는 사용자와 디바이스의 정보는 암호화 기술을 통해 보호하는 방식으로 정보 공개를 최소화 하여 보안 성능을 강화할 수 있으며, 제안되는 개선된 알고리즘에는 아래와 같이 디바이스를 인증하기 위한 프로세스가 추가되며, 다음 그림9의 Private 블록체인 아키텍처를 가지고 있다.

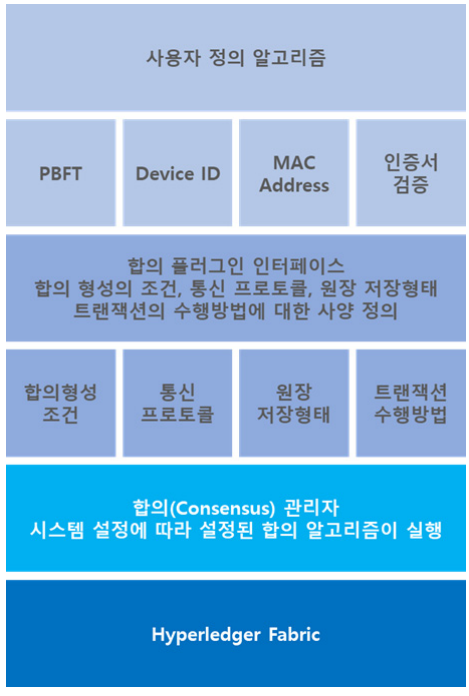

그림 9. Private 블록체인 아키텍처
Fig. 9. Private Block Chain architecture

제안되는 블록체인 기반 인증 알고리즘에는 아래와 같이 Gateway를 인증하기 위하여 보안 및 인증 절차가 강화된 프로세스가 추가된다.,

- 보안규칙 - 등록된 장치(Device ID, MAC Address, IP 모두 일치)만 접근 가능
- IoT Client가 최초로 G/W에 접속하면 키 발급
- 보안을 위해 접속 시 1회용 인증키를 발급한다.
- IoT 장치와 G/W간 통신은 MQTT 프로토콜 사용
- Gateway는 인접 G/W에 인증 무결성 확인을 위해 블록체인 네트워크를 통해 검증하는 절차를 가진다.

본 논문에서 제안하는 게이트웨이와 서버 간의 인증을 위한 알고리즘은 사전에 등록된 장치의 정보, 개인키, 1회용 트랜잭션 키를 이용한 인증과정과 이를 블록체인 네트워크에서 검증하는 과정을 가지며, 다음 그림 10의 G/W to 서버 인증 알고리즘과 같다.

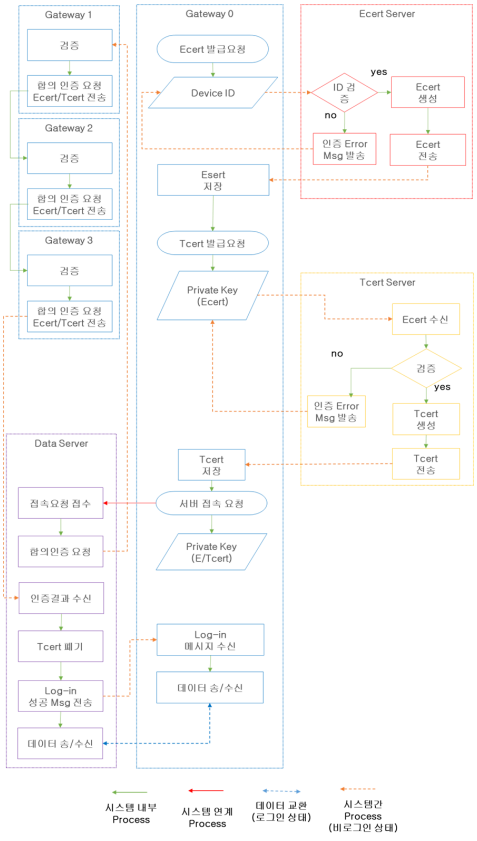

그림 10. G/W to 서버 인증 알고리즘
Fig. 10. Gateway to Server authentication Algorithm

Ⅳ. 결론

ICT 기술의 발달로 인하여 주변에 존재하는 사물들을 네트워크로 연결하고, 사물에서 수집되는 정보를 다양한 분야에서 활용하기 위한 IoT 환경에 대한 관심이 증가하고 있으며, 이를 활용하기 위한 목적의 연구가 활발하게 이루어지고 있다. IoT 환경은 네트워크에 연결되어 있어 보안성을 유지할 수 있어야 하며, 다양한 성능 및 운영체제를 사용하는 장치들에 폭 넓은 호환성을 확보할 수 있는 인증 방식이 요구된다.

본 논문에서는 다양한 디바이스, 네트워크, 운영체제 환경에서 원활한 운영이 가능하도록 호환성을 확보하고, 다양한 운영환경에 의한 보안 취약점이 발생하지 않도록 보안 성능을 확보할 수 있는 분산 클러스터 기반 IoT 디바이스 경량인증 방법을 제안하였다.

본 논문에서 제안한 인증 방식은 IoT와 게이트웨이간의 보안인증 과정을 경량화하여 낮은 사양의 IoT 장치의 인증에 활용할 수 있도록 호환성을 확보하여 다양한 센서 장치들을 활용한 IoT 네트워크 구성이 가능하다. IoT와 게이트웨이간의 인증을 경량화의 영향으로 보안 성능이 저하되는 것을 보완하기 위하여 IoT 디바이스에 외부로 부터의 접근을 할 수 없도록 게이트웨이를 통해서만 접속 할 수 있는 네트워크를 구성하였다.

또한 G/W와 서버간의 인증은 트렌젝션 키를 활용하여 키의 유출이나 침해로부터 보호할 수 있으며, 프라이빗 블록체인 기반 환경에서 게이트웨이가 네트워크에 참여하여 다수의 게이트웨이들이 검증하는 방식을 통해 허가 받지 않은 장치 및 외부로 부터의 침해 위협으로 부터 시스템을 안전하게 보호할 수 있는 보안환경을 제공할 수 있다.

본 논문에서 제안한 IoT to G/W, G/W to Server 인증 방식을 활용한다면 저성능의 센서 디바이스 및 다양한 기기들로 구성되는 분산 클러스터 IoT 네트워크를 효율적으로 구축 할 수 있으며, 보안성이 요구되는 시스템 환경에 사용될 수 있을 것으로 기대한다.

References

[1] J. Richer (Ed.), "OAuth 2.0 Token Introspection," RFC 7662, Oct. 2015.

DOI:10.17487/RFC7662

[2] D.Hart, "The OAuth 2.0 Authorization Framework," IETF RFC 6749, Oct. 2012.
DOI: 10.17487/RFC6749

[3] Jung Kyu-Won, Shin Hye-seong, Park, Jong Hwan. Integrated Authentication Protocol of Financial Sector that Modified OAuth2.0. Journal of the Korea Institute of Information Security and Cryptology, 27(2), 373-381, Apr 2017.
DOI: https://doi.org/10.13089/JKIISC.2017.27.2.373

[4] Sung-Tae Yu, Soo-Hyun Oh. OAuth-based User Authentication Framework for Internet of Things Journal of the Korea Academia-Industrial cooperation Society, Vol. 16, No. 11, pp.8057-8063, Nov 2015.
DOI: https://doi.org/10.5762/KAIS.2015.16.11.8057

[5] Cheol-hyun Kim, Yon-Sik Lee. A study on Kerberos Authentication mechanism. Journal of Korea Institute of Information Security and Cryptology, 15(3), 53-64, Jun 2005.

[6] Hwang Ki-tae, Park Hey-jin, Kim Ji-su, Lee Tae-yun, Jung In-hwan. An Implementation of Smart Gardening using Raspberry pi and MQTT. The Journal of The Institute of Internet, Broadcasting and Communication (IIBC) Vol. 18, No. 1, pp.151-157, Feb 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.1.151

[7] OASIS "MQTT version 3.1.1 Standard"

[8] Geo-Su Yim. IoT MQTT Security Protocol Design Using Chaotic Signals. The Korea Institute of Information & Electronic Communication Technology, Vol. 11, No. 6, pp.778-783, Dec 2018
DOI: https://doi.org/10.5762/KAIS.2015.16.11.8057

[9] Satoshi Nakamoto, "Bitcoin: A Peer to Peer Electronic Cash System", Oct 2008.

[10] Yoo Soon-duck, Kim Ki-heung. A Study on Improvement for Service Proliferation Based on Blockchain. The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 18, No. 1, pp.185-194, Feb 2018.
DOI: https://doi.org/10.7236/JIIBC.2018.18.1.185

저자 소개

김 성 환(정회원)

- 2009년 2월: 열린사이버대학교 정보통신공학과(공학사)
- 2017년 8월: 한국산업기술대학교 소프트웨어융합공학과(공학석사)
- 2017년 9월~현재: 한국산업기술대학교 컴퓨터공학과 박사과정
- 관심분야 : 소프트웨어공학, 정보통신 시스템, 임베디드 시스템

김 영 곤(정회원)

- 1983년 2월: 경북대학교 전자공학과(공학사)
- 1985년 2월: 연세대학교 본대학원 전자공학과(공학석사)
- 2000년 2월: 한국과학기술원 전산학과(공학박사)
- 1985년~2007년: KT 수석연구원
- 2007년~현재: 한국산업기술대학교 컴퓨터공학과 교수
- 관심분야 : 소프트웨어공학, 정보통신시스템, 객체지향 분석 및 설계