JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 2, pp. 113-122, February 2020
https://doi.org/10.9708/jksci.2020.25.02.113

IoT Authentication System Using Blockchain and TOTP

Ho-Gyun Kim*, Soon-Ho Jung*

*Student, Dept. of Computer Engineering, Pukyong University, Busan, Korea
*Professor, Dept. of Computer Engineering, Pukyong National University, Busan, Korea

[Abstract]

In this paper, we propose the terminal authentication system using blockchain and TOTP(Time-based One-time Password Algorithm) to sustain a continuous authentication between user device and service device. And we experiment this system by using door-lock as a terminal of IoT(Internet of Things). In the future, we can apply this result to several devices of IoT for convenience and security. Although IoT devices frequently used everyday require convenience and security at the same time, it is difficult for IoT devices having features of the low-capacity and light-weight to apply the existing authentication technology requiring a high amount of computation. Blockchain technology having security and integrity have been used as a storage platform, but its authentication cannot be performed when the terminal cannot access any network. We show the method to solve this problem using Blockchain and TOPT.

▸ **Key words**: IoT, Authentication Technology, Blockchain, Ethereum, Smart Contract

[요 약]

이 논문에서는 블록체인과 TOTP(Time-based One-time Password Algorithm)를 이용하여 사용자 장치와 서비스 장치 사이의 지속적인 인증을 유지하는 단말기 인증 시스템을 제시하고 이 사물인터넷의 단말기로서 도어-록에 적용하여 실험하였다. 앞으로 IoT의 여러 장치들에 편리와 보안을 위하여 이 시스템을 적용할 수 있다. 사물인터넷(IoT, Internet of Things) 기술이 발전하면서 사물인터넷 장치들의 편의성과 보안성이 동시에 요구되고 있다. 사물인터넷 장치들은 저용량, 경량의 특징을 가지고 있으나 높은 연산량을 요구하는 기존의 인증기술을 적용하기 어렵기 때문에 사물인터넷 보안에 위협이 되고 있다. 최근 위변조가 불가능한 블록체인 기술로 보안성과 무결성을 제공하는 저장 플랫폼을 적용하였으나 단말기가 네트워크에 접속할 수 없을 때 블록체인을 이용한 인증을 수행할 수 없다. 이 문제점을 블록체인과 TOPT를 이용하여 해결하는 시스템을 보여준다.

▸ **주제어**: 사물인터넷, 인증 기술, 블록체인, 이더리움, 스마트 계약

• First Author: Ho-Gyun Kim, Corresponding Author: Soon-Ho Jung
*Ho-Gyun Kim (hogyoon.kim@gmail.com), Dept. of Computer Engineering, Pukyong National University
*Soon-Ho Jung (snow@pknu.ac.kr), Dept. of Computer Engineering, Pukyong National University
• Received: 2019. 12. 26, Revised: 2020. 01. 14, Accepted: 2020. 01. 20.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

최근 4차 산업혁명(4IR, Fourth Industrial Revolution)이 진행되면서, 세상의 모든 사물을 연결시키고 지능화하여 사용자에게 유용한 서비스를 제공하는 사물 인터넷(IoT, Internet of Things)에 관한 연구가 활발히 진행되고 있으며 사용 또한 급격하게 증가하는 추세이다. 하지만 사물인터넷은 하드웨어, 플랫폼, 통신방식의 이종성으로 인해 다양한 보안 위협으로부터 노출되어 있고 일상생활과 밀접한 관련이 있어 보안 문제가 발생했을 때 큰 부작용을 초래할 수 있다. 한편, 중앙기관 없이 분산 원장을 통해 데이터의 위변조가 불가능한 블록체인 기술이 등장하였고, 블록체인 기술을 통해 신뢰성을 확보하려는 다양한 시도가 진행 중이다.

본 논문에서는 분산 원장을 통해 위변조가 불가능한 성질을 가지고 있는 블록체인 기술과 시간 동기화 방식으로 일회용 패스워드를 생성하는 TOTP(Time-based One-time Password) 알고리즘 이용하여 네트워크, 게이트웨이에서의 사물인터넷의 기밀성(Confidentiality), 무결성(Integrity), 가용성(availability)을 충족하는 사물인터넷 인증 시스템을 개발한다. 이 기술을 통해 플랫폼, 센서/디바이스에 대한 보안 문제는 해결할 수 없으나 보안 위협과 보안 요구사항에 대한 범위를 개인키 노출에 대한 범위로 한정시킬 수 있다는 이점이 있다.

2장에서는 관련연구로 사물인터넷, 블록체인, OTP, 보안 공격, 사물인터넷 기기 보안 요구사항, 기존의 사물인터넷 인증 시스템에 대해 기술하고, 3장에서는 블록체인과 TOTP를 이용한 사물인터넷 인증 시스템을 제안하며, 4장에서는 IoT의 단말기로서 디지털 도어록을 적용한 실험 및 평가에 대해 기술하고, 5장에서는 본 논문에 대한 결론을 제시한다.

II. Related Work

1. IoT and Security Technology

사물인터넷(Internet of Things)의 개념은 1999년 메사추세츠공대(MIT)의 오토아이디센터(Auto-ID Center) 소장이었던 캐빈 애쉬튼(Kevin Ashtonin)이 “RFID와 기타 센서가 사물에 탑재된 사물 인터넷이 구축될 것”이라고 처음으로 언급한 것으로 시작된다. 2005년 ITU가 사물인터넷에 관한 보고서를 발간하면서 표준 관점에서 논의가 이슈화되기 시작하였고 2008년부터 Intel, Cisco, Qualcomm, Aricson 등의 글로벌 기업들이 사물인터넷을 산업 유망 아이템으로 선정하면서 산업적으로 관심을 받게 되었다. 사물인터넷의 의미는 전문가마다 해석이 상이하지만 보통 사람, 사물, 공간 등 모든 사물들이 네트워크에 연결되어 정보가 생성, 수집, 공유, 활용되는 것을 말한다.

하지만 사물인터넷 기술이 발전하면서 이기종 단말, 네트워크, 어플리케이션 간의 연동이 늘어남에 따라 다양한 보안 위협에 노출되면서 정보 보안의 3대 요소인 기밀성, 무결성, 가용성이 침해될 가능성이 높아지고 있다. 사람과 사물이 직접 연결되는 사물인터넷의 특성상 사생활 노출, 경제적 손실, 인프라 마비, 신변 위협 등 수준 높은 사회 문제를 초래할 수 있다.

이처럼 다양한 사물이 연결되어야 하는 사물인터넷 환경은 상호운용성 지원을 위한 표준이 필수적이다. [Table 1]에서 보는 바와 같이 최근에는 인터넷/이동통신망 기반의 사물인터넷 표준기술을 ITU-T, ISO, IETF, oneM2M, 3GPP 등을 통해서 새로운 국제 표준으로 추진하고 있다. 구체적으로 공적 표준화기구로는 ITU-T, ISO/IEC JTC1이 있으며, 사설 표준화 기구로는 oneM2M, IEEE, IETF, ETSI, 3GPP, W3C 가 있으며, 표준 협의체로는 OCF, AllSeen Alliance, Thread Group 등이 있다[4].

Table 1. IoT Standardization Organization

Group	Value
ITU-T	Discuss security standards for Network(SG 13), Security(SG17), IoT and applications(SG20), etc.
ISO/IEC JTC1	Discuss standards for automatic identification(JTC1/SC31), Information and communication(SC6), Sensor Network(WG7), IoT(WG10), etc.
oneM2M	As a de facto standardization organi zation for the IoT/M2M common service support layer, development of standards such as structure, require ments, protocols, security, and semantic technologies.
IEEE	As a de facto standardization organization for wireless LAN/PAN technology, standard development such as smart metering, outdoor low-power short-range, and long-distance com munication
IETF	As a de facto standardization organization related to Internet protocol, development of standards such as adaptation layer and CoAP for low power wired and wireless network.
ETSI	Discuss standardization of IoT reference structure, interoperability, and smart city centering on issues that are not interoperable

3GPP	Focus on standardizing cellular com munications from the physical layer to the transport layer. leading standards development including Load management, network operating structure, low power cellular communication
W3C	Create a new interest group called Web-of-Things to lead relevant technical research and semantic data and object standards.
OCF	Consortium developing both device and resource interoperability standards and open source to provide universal IoT connectivity framework connecting various industries.
AllSeen Alliance	Established to promote device connectivity and interoperability through All Joyn open source. currently launching new IoT application service through AllJoyn Platform with more than 200 members.
Thread Group	Through IP based wireless communication network protocol and thread development for smart ho me, established a thread group to implement interoperable IoT.

한편, 최근 ITU-T SG17(국제전기통신연합 정보통신부문 연구반 17)회의에서 “Security frame work for the Internet of things based on the gateway model“ 국제 표준이 X.1361로 최종 채택되었다. 국제 표준 X.1361에서는 사물인터넷에서 보안을 센서/디바이스, 게이트웨이, 네트워크, 플랫폼을 보안을 수행하는 주요 개체로 식별하고, 각 개체에 대한 보안 위협과 해결하기 위한 보안 요구사항을 제시하였다[1].

2. Blockchain

블록체인의 개념은 Satoshi Nakamoto라는 가명의 개발자가 작성한 논문 <Bitcoin: Peer-to-Peer Electronic Cash System>에서 처음으로 등장하였다. 논문에서는 블록체인 기술을 통해 제 3자의 개입 없이 거래 당사자 사이에서 거래가 가능한 전자화폐를 구현하고 있으며, 블록체인은 모든 참여자가 거래 내역과 순서를 공유하고 있어 이중지불과 위조, 변조, 해킹이 불가능한 특징을 가지고 있다.

[Fig. 1]과 같이 이전 거래 내역 및 다음 소유자 공개키의 해시값에 전자 서명하여 만들어진 디지털 서명의 사슬을 통해 전자 화폐에 대한 소유권을 검증 할 수 있으나, 수금자는 이전 소유자들이 화폐를 이중지불 했는지 알 수 없다는 문제가 발생한다.

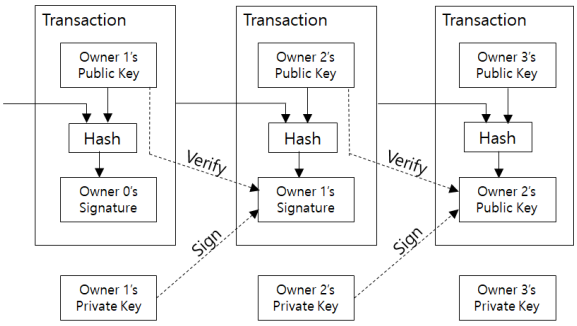

Fig. 1. Electronic coin as a chain of digital signatures

이중지불 문제를 해결하기 위해서는 이전 소유자가 어떤 거래에도 서명하지 않았음을 수금자에게 알릴 수단이 필요함을 알 수 있다. 즉, 모든 거래를 공개하고 거래의 순서를 단일 이력에 합의하는 시스템이 필요하다. 거래의 순서를 합의하기 위해 타임스탬프 서버가 필요해졌고, 개인 대 개인 기반의 분산 타임스탬프 서버를 구현하기 위해 논문에서는 Adam Back의 Hashcash와 유사한 작업 증명 시스템을 사용하였다[13].

작업증명(Proof-of-Work)은 블록안의 임의 값인 nonce 를 찾는 과정을 말하며, 이 과정에서 컴퓨팅 파워가 요구된다. nonce 값을 찾으면 블록이 생성되며 모든 참여자에게 전파되어 [Fig. 2]와 같이 체인을 형성하고 검증된 블록들은 과반에 합의를 통해 확정된다.

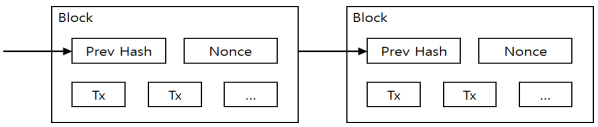

Fig. 2. Structure of Blockchain

타임스탬프에 의해 블록은 약 10분 주기로 생성되고, 블록 내에는 거래 내역들이 기록되는데 [Fig. 1]과 같이 디지털 서명의 사슬형태로 구성된다.

이처럼 사토시 나카모토는 거래 시간순의 전산적 증명을 생성하는 개인 대 개인 간 분산 타임스탬프 서버를 사용하여 이중지불 문제를 해결할 수 있는 블록체인을 제시하였고, 정직한 노드가 공격자 노드의 협력 그룹보다 총체적으로 더 많은 컴퓨팅 파워를 통제하는 한 블록체인 기술이 보안상 안전하다는 것을 주장하였다[9].

3. One-Time Password(OTP)

One-Time Password(OTP)는 비밀 pass-phrase를 사용하여 일회성 비밀번호를 생성하는 기술이다. OTP 시스템을 사용하면 사용자의 암호가 네트워크를 통과 할 필요가 없기 때문에 보안상 이점을 얻을 수 있다.

네트워크 시스템에 대한 하나의 공격 수법은 네트워크 연결을 도청하면서 인가된 사용자의 로그인 ID 및 비밀번호와 같은 인증정보를 얻는 것이다. 이 인증정보가 캡쳐된다면, 캡처된 인증 정보는 이 후에 시스템 인가를 얻기 위해 사용될 수 있다. 이러한 공격은 리플레이 공격(replay attack)[16]이라고 하며, OTP 시스템은 일회성 비밀번호를 생성하므로, 이러한 유형의 공격에 대응할 수 있도록 설계된 시스템이다.

그러나, OTP 시스템은 중간자가 개인정보에 접근하거나 피싱과 같은 사회 공학적 공격(social engineering) 또는 IP 스푸핑 및 세션 하이재킹과 같은 능동적 공격(active attacks)[15]은 막을 수 없다는 한계점을 가진다[14].

OTP 알고리즘은 크게 두 가지로 HOTP(HMAC-based One-Time Password) 알고리즘과 TOTP(Time-based One-Time Password) 알고리즘으로 나뉜다. HOTP는 이벤트 기반의 OTP 알고리즘이며, 이동 계수(moving factor)가 이벤트 카운터(event counter)로, 카운터 값이 증가할 때 마다 서로 다른 패스워드를 생성하는 방식을 의미한다. TOTP는 시간 기반의 OTP 알고리즘이며 보안을 강화하기 위해 짧은 시간을 주기로 서로 다른 패스워드를 생성한다[12][8].

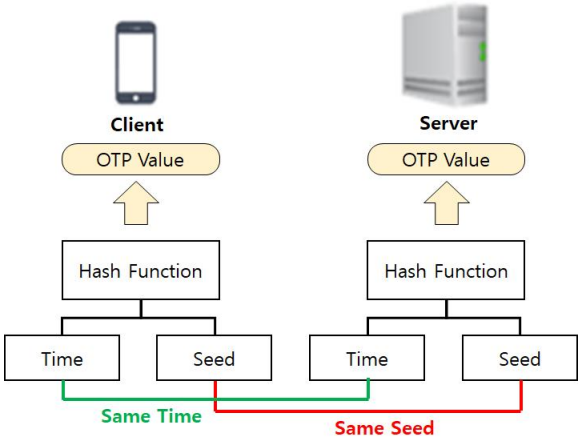

Fig. 3. Principle of Time-based One-Time Password

4. Security Attack

정보보안이 목표로 하는 세 가지 핵심적인 원칙은 기밀성, 무결성, 가용성 이다. 각 원칙을 위협하는 대표적인 공격 방법은 다음과 같다.

4.1 Confidentiality Attack

기밀성이란 합법적인 정보만 읽을 수 있도록 보호하는 서비스를 의미하며, 전송되는 메시지 내용, 트래픽 흐름 분석, 도청으로부터 전송 메시지를 암호 알고리즘을 이용하여 완벽하게 보호하여 비인가자가 정보의 실제 내용을 볼 수 없도록 방지하는 것을 의미한다. 기밀성을 위협하는 대표적인 공격으로는 스누핑(Snooping), 트래픽분석, 가로채기(Interception) 등이 있다.

4.2 Integrity Attack

무결성이란 합법적인 실체만 수정할 수 있도록 보호하는 서비스를 의미하며, 정보가 불법적으로 변형되지 않고 원래의 정보 또는 신호가 전송, 저장, 변환 중에 또는 그 후에도 동일함을 유지하는 것을 의미한다. 무결성을 위협하는 공격으로는 불법수정(Modification), 위조(Fabrication), 시간성 변경, 가장(Masquerading), 재연(Replaying), 부인(Repudiation) 등이 있다.

4.3 Availability Attack

가용성이란 정보에 대한 접근과 사용이 적시에 확실하게 보장되는 상태를 의미한다. 가용성을 위협하는 공격으로는 서비스 거부(DoS), 차단(Interruption) 등이 있다.

5. Traditional IoT Authentication System

5.1 ID/Password Authentication

ID/Password 인증 방식은 사용자와 서버가 미리 지정해놓은 인증 정보를 통해 인증하는 방법으로 지식 기반(knowledge-based) 인증의 한 형태이다. 사용자가 직접 인터페이스를 통해 입력하기 때문에 직접적인 관찰에 의해 비밀번호를 알아내는 숄더 서핑(Sholder Surfing) 공격에 대한 위협이 있으며, 지식 기반 인증의 특성상 사용자가 동일한 지식을 여러 인증시스템에 사용하는 경향이 있으므로, 인증 정보가 노출되었을 때 다른 시스템 또한 무력화되는 문제가 있다.

5.2 Biometric Authentication

생체 인증 기술은 지문 인식, 홍채 인식, 얼굴 인식 등이 존재하며 기존의 비밀번호보다 보안이 향상된 기술이지만, 생체 정보의 저장 및 관리 방식이 기존의 비밀번호 방식과 다르지 않아 노출의 가능성이 높다. 특히 비밀번호 방식은 노출되더라도 재설정 가능하지만, 생체 인증 정보는 한번 노출된 경우 재설정이 불가능하다는 심각한 문제점이 있다.

생체 인증 기술은 사진에 의해서도 복제가 가능한 것으로 알려져 있다. 지문 인식의 경우 유럽의 카오스 컴퓨터 클럽(CCC) 소속의 해커가 손가락 사진을 이용해서 독일 국방장

관의 손가락 지문을 복제했다는 것을 발표하였다[17]. 뿐만 아니라 지문을 스캔하여 Apple 사의 지문 잠금 해제 기능인 Touch ID 해킹을 시연하였다[6]. 홍채 인식은 야간 촬영이 가능한 적외선 카메라로 사람 얼굴을 촬영하고 홍채를 추출하여 컬러 레이저 프린터로 출력한 뒤, 콘택트렌즈에 올리는 방식으로 인증을 우회할 수 있다[3]. 얼굴 인식은 사진이나 동영상 속의 상대방의 얼굴을 3D 프린터를 통해 렌더링 하는 방식으로 인증 우회를 할 수 있다. 실제로 베트남의 보안 회사인 Bkav는 이러한 방식으로 iPhone X의 얼굴 인증 시스템인 Face ID를 우회하였다[18].

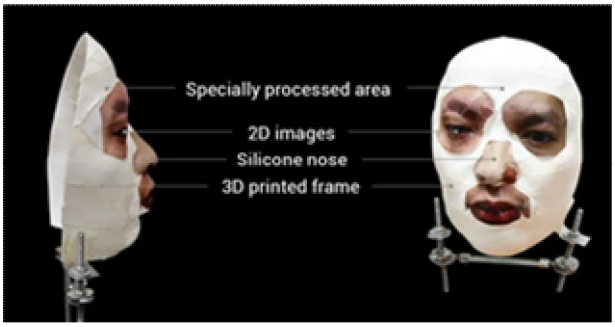

Fig. 4. Face ID hack with mask by Bkav

5.3 RFID Authentication

RFID(Radio-Frequency Identification)는 주파수를 이용하여 ID를 식별하는 방식으로 일명 전자태그로 불린다. RFID 태그와 RFID 리더기가 전파를 통해 먼 거리에서도 정보를 인식하는 기술을 말한다. RFID 통신을 이용하여 인증하는 방식은 편리하여 실생활에서도 많이 접할 수 있지만, 비교적 쉽고 저렴한 방법으로 RFID 태그를 복제하여 인증을 우회할 수 있으며[10], 이외에도 물리적으로 RFID 태그를 변조하여 조작하거나 교체하여 인증하는 물리적 공격(physical attack) 방법, 동의 없이 RFID 태그 정보를 전자적으로 복사하는 스키밍 공격(skimming attack), 정당한 리더기로 위장하여 RFID 태그에 질의함으로써 인증정보를 얻거나 위조된 태그를 생성할 수 있는 스푸핑(Spoofing) 공격, RFID 무선 주파수 방해를 통한 서비스 거부 공격(DoS) 등 다양한 보안 위협이 존재한다[11].

5.4 Bluetooth Authentication

블루투스는 2.4GHz의 무선 주파수를 사용하여 고속으로 데이터를 주고받을 수 있는 통신 프로토콜로, 저가격, 저전력으로 근거리 무선 통신에 활용하기 위해 고안되었다. 이전에는 단말기와 노트북을 연결하기 위해 별도의 케이블이 필요하였으나, 블루투스가 상용화되면서 케이블 없이 기기 간의 연결이 가능하게 되었다. 최근 사물인터넷이 발전하면서 블루투스 통신 기반으로 인증을 수행하거나 상호 통신하는 장치가 늘고 있는 추세이다.

그러나 블루투스 무선 통신 장치는 DoS 공격, MITM 공격, 도청, 메시지 변조, 자원 착복 등의 공격에 취약하다. 대표적으로는 대상 장치에 무단으로 정보에 액세스하는 블루스나핑(Bluesnarfing), 대상 장치에 원치 않는 메시지 보내는 블루재킹(Bluejacking), 대상 장치의 명령을 사용하여 임의의 동작을 실행하는 블루버깅(Bluebugging)이 있으며 이외에도 단말을 반복적으로 재부팅하여 서비스 이용을 방해하는 DoS 공격 등 다양한 보안 위협이 존재한다.[7]

5.5 Authentication Server

인증 서버(Authentication Server)는 단말 장치에 대해 신원확인 및 신원증명 서비스를 제공하며, 이를 위해 사용자의 인증 정보를 중앙집중식 데이터베이스에 저장 및 관리하는 제 3의 신뢰 받는 인증용 서버를 의미한다. 인증 서버는 단말기의 권한의 부여 및 접근 제어를 구현하기 용이하며 관리가 편리하다는 장점이 있으나, 다양한 공격에 의해 중앙 서버가 해킹당할 경우 인증을 우회하거나 인증 정보가 유출되는 문제가 발생할 수 있다.

5.6 Blockchain Authentication

독일의 스타트업인 슬록잇(slock.it)은 사물인터넷 장치의 인증 과정을 블록체인을 통해서 수행하도록 하여, 인가를 받은 사용자가 블록체인을 통해 잠금장치를 열 수 있는 내용으로 특허 출원 및 등록하였다[2]. 그러나 두 단말기가 노이즈 및 주파수 위변조 등으로 인한 서비스 거부 공격(DoS)에 의해 블록체인 네트워크에 연결 할 수 없는 상황이라면, 인증 서비스를 이용할 수 없는 가용성 문제가 발생한다.

III. The Proposed Scheme

본 장에서는 제안하는 사물인터넷 인증 시스템을 설계하고 IoT의 단말기로서 디지털 도어록에 적용하여 구현한 내용에 대하여 기술한다. 서론에서 기술한 바와 같이 사물인터넷을 안전하게 이용하기 위해서 센서/디바이스, 플랫폼, 네트워크, 게이트웨이에 대한 보안 요구사항을 만족할 수 있어야 한다. 또한 2장에서 살펴 본 바와 같이 기존의 사물인터넷 인증 시스템들은 비밀번호 유출, 리플레이 공격, 무작위 공격, 중앙 서버에 대한 다양한 해킹 공격, 피싱과 같은 사회적 공학 해킹, DoS 공격, 네트워크 단절 등의 다양한 보안 위협으로부터 기밀성, 무결성, 가용성을 모두 만족시키기 어려웠다.

제안하는 시스템은 분산 장부에 기록된 데이터는 위변조가 불가능하고 비대칭 키 암호화 방식을 사용하는 블록체인의 성질을 이용하여 데이터 기밀성과 접속 제어(access control)을 구현한다. 특히 블록체인 데이터를 비대칭키로 암호화하여 데이터를 전송하면, 권한이 없는 사용자는 데이터에 접근할 수 없음을 보장할 수 있으며 중간자(MITM, man in the middle)공격에 대응할 수 있어 네트워크, 게이트웨이, 서버에 대한 기밀성과 무결성을 보장할 수 있다. 또한 튜링 완전 프로그램인 스마트 계약을 수행하더라도 수수료가 발생하기 때문에, DoS 공격에 대한 가용성은 보장할 수 있으며, 블록체인 네트워크를 이용할 수 없는 경우 OTP 방식을 통해 인증 서비스에 대한 가용성을 제공할 수 있다.

1. System Architecture

이 시스템의 전체적인 구조는 [Fig. 5]과 같이 블록체인에서 단말기의 OTP의 seed 값과 단말기의 권한 정보는 블록체인에 기록하고 스마트 계약(smart contract)에 의해서 관리된다. 또한 제안하는 시스템은 두 가지의 장치로 구분되며, 사용자 장치로 부터 인증 정보를 받고 인증 여부를 결정하는 서비스 장치(service device)와 스마트 폰처럼 보편적으로 사용자가 소유하며 인증 정보를 가지고 서비스 장치에 인증을 요청하는 사용자 장치(user device)로 구분할 수 있다.

권한을 부여 받은 사용자 장치 또는 서비스 장치는 블록체인에 자신의 공개키로 서명된 seed 값, 권한 정보, 시간 동기화 정보를 개인키로 복호화 하여 얻을 수 있다. 각 장치는 시간과 seed 값을 이용하여 일회성 비밀번호를 생성하고 두 장치의 비밀번호를 비교하여 인증을 여부를 확인할 수 있다. 이러한 방법을 통해 두 단말기는 네트워크 단절 등의 이유로 블록체인 서비스를 이용할 수 없는 경우에도 단말기 간 인증을 이용 할 수 있으며, 기존의 블록체인 인증 방법에서 가용성을 측면에서 이점을 얻을 수 있다.

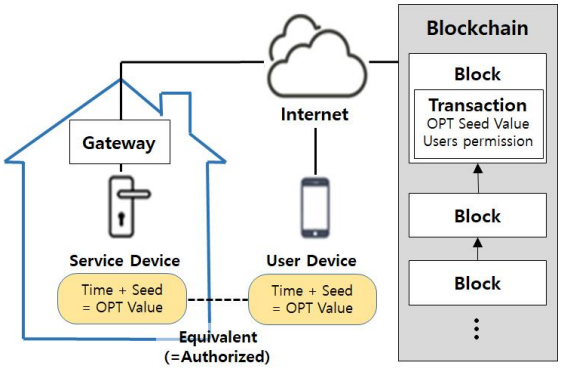

Fig. 5. System Architecture

2. Smart Contract

권한을 부여 받은 서비스 장치와 사용자 장치는 OTP의 seed 값을 초기화 및 동기화하거나 사용자 권한을 수정할 수 있다. [Fig. 6] 과 같이 seed 값 초기화 또는 사용자 권한을 수정 요청할 때 스마트 계약을 사용하며, 스마트 계약에 해당하는 EVM 코드가 실행되어 블록체인 상에 기재된 정보를 갱신한다.

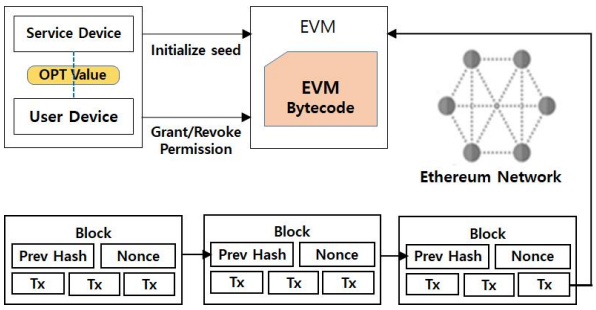

Fig. 6. Query execution using smart contract

2.1 Initialize OTP seed

소프트웨어를 안정적으로 운영하기 위해 본 연구에서는 OTP seed 값을 초기화해야 하는 경우를 3가지로 지정했으며 각각 다음과 같다. 장치가 시작 되었을 때, seed 값을 발급하고 오랜 시간이 지났을 때, 사용자에 대한 권한이 수정되었을 때이다. 이 경우에서 서비스 장치는 스마트 계약을 통해 OTP seed 값 초기화 작업을 요청한다.

OTP seed 값을 초기화 하는 과정은 [Fig. 7] 과 같다. 서비스 장치는 스마트 계약을 통해 OTP seed 초기화 작업을 요청한다. 스마트 계약은 새로 발급받은 OTP seed 값, 현재 사용자의 권한 정보, 시간 동기화 정보 등을 권한을 부여받은 각 장치의 공개키로 서명하여 블록체인 상에 각각 기재한다. 권한을 부여받은 각각의 장치들은 각 장치의 개인키로 복호화 하여 정보를 열람한다.

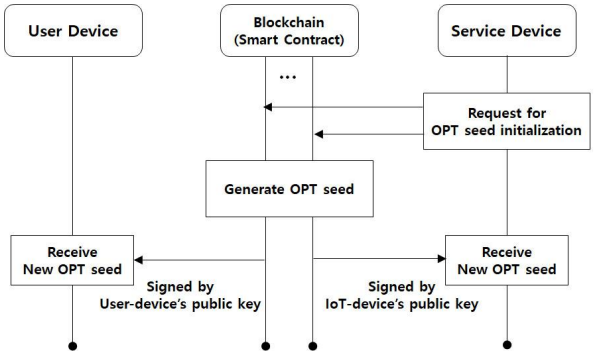

Fig. 7. initialize OTP seed

한편, Dapp에서 난수를 생성하는 문제는 일반적인 컴퓨터 과학보다 어려운 문제에 속하는데, 마이너가 채굴한 블록에서 난수에 의해 불리한 결과가 발생했을 때 네트워크에 해당 블록을 전파하지 않는 방법을 사용 할 수 있기 때문이다. 따라서 본 연구에서는 Signidice Algorithm 방식을 사용하여 난수를 생성 하였다[19].

2.2 Grant/Revoke Permission

권한을 부여 받은 장치는 다른 사용자 장치에 대한 권한을 수정할 수 있다. 권한을 부여받은 장치는 스마트 계약을 통해 다른 사용자 장치에 대한 권한 정보를 수정하여 전달할 수 있다. 서비스 장치는 블록체인 네트워크에서 사용자 권한 정보가 수정된 것을 감지한다. 서비스 장치에서는 새로운 사용자 권한 정보를 적용하고, OTP seed 초기화를 요청한다. OTP seed 초기화가 완료되면 수정된 권한 정보가 반영된다.

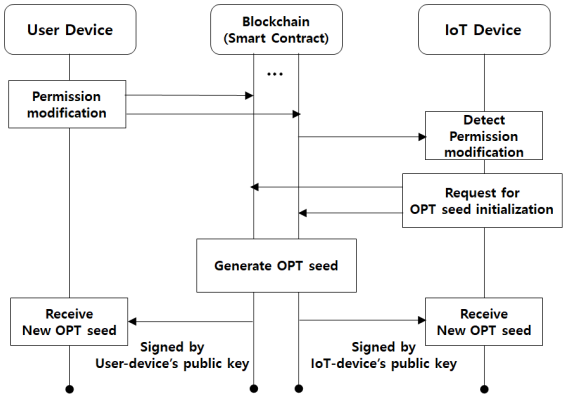

Fig. 8. Grant/Revoke permission

3. Service Device

이 시스템의 서비스 장치 동작과정은 [Fig. 9]와 같다. 장치가 처음으로 시작되면 OTP seed 값과 시간 정보를 동기화하여 인증을 위한 TOTP가 정상 동작 할 수 있도록 환경을 구성한다.

OTP seed 값을 초기화해야 하는 경우는 장치가 시작된 경우 이외에도 오랜 시간 동안 같은 OTP seed를 사용했거나, 사용자의 권한이 변경된 경우이다. 사물인터넷 장치는 이러한 상황을 감지했을 때, 스마트 계약을 통해 OTP seed 초기화를 요청한다.

만약 사용자 장치로부터 인증 신호가 감지되었다면, OTP seed 값과 시간 정보를 통해 일회용 비밀번호를 발행한다. 사용자 장치에서 보낸 OTP 값과 일치한다면, 인증된 사용자이므로 인가된 동작을 수행한다. 만약 일치하지 않는다면, 인가된 동작을 수행할 수 없다.

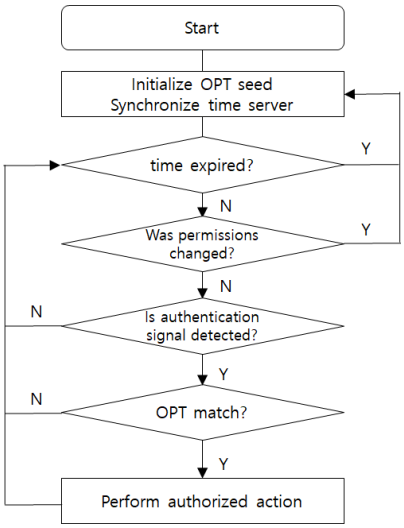

Fig. 9. Flowchart of service device

4. User Device

사용자 장치는 서비스 장치에 인증을 요청해야 하는 경우 인증 신호를 전달한다. 인증 신호에는 사용자 장치에 동기화된 시간과 seed 값을 이용하여 만들어진 일회용 비밀번호가 포함된다. 서비스 장치에서 일회용 비밀번호의 일치 여부를 확인하면 인증 과정은 완료된다.

IV. Implementation and Evaluation

1. Implementation

3장에서 설명한 서비스 장치, 사용자 장치를 각각 라즈베리파이 및 모바일 디바이스에서 구현하고 테스트한 결과를 기술한다.

1.1 Service Device

인증 서비스를 제공하는 사물인터넷 장치를 구현하기 위해 디지털 도어락을 구현하였다. [Fig. 9] 와 같은 장치의 동작을 구현하고 수행하기 위해 라즈베리파이 2 보드에 Python 3.7 환경으로 프로그램을 작성하였으며, 디지털 도어락의 개폐부의 열림과 닫힘 기능을 알고리즘에 맞게 조작하기 위해 라즈베리파이의 GPIO 5 핀에 트랜지스터를 연결하였다.

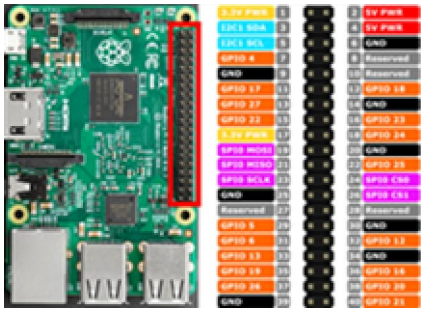

Fig. 10. Raspberry Pi GPIO pin map

아래의 [Fig. 11]는 라즈베리파이와 트랜지스터를 이용하여 도어락 장치의 개폐부와 연동한 모습이다.

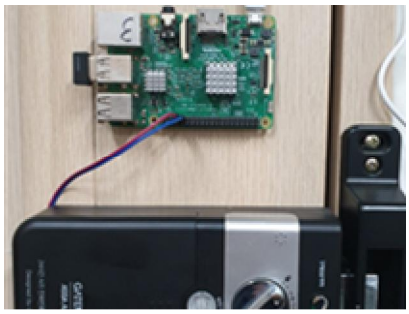

Fig. 11. Digital door lock with Raspberry Pi

1.2 User Device

사용자 장치는 두 가지 기능을 제공하며 각각 인증 요청과 사용자 권한 수정 기능이다. [Fig. 12]의 좌측 사진은 이 사용자 장치에서 인증 가능한 서비스 장치들의 목록을 보인 화면이며, 서비스 장치에 대한 인증 요청을 위해 Signal 버튼을 눌렀을 때 생성된 일회용 비밀번호를 서비스 장치에 전달함과 동시에 토스트 메시지를 띄운 화면이다. 우측 화면은 Home 서비스 장치에 대한 권한을 부여받은 사용자 목록을 조회 한 것이며, 버튼을 통해 새로운 사용자 장치를 추가하거나 각 사용자 장치에 대한 권한을 변경 또는 삭제 요청을 스마트 계약을 통해 할 수 있다. 본 논문에서는 사용자 장치를 구현하기 위해 갤럭시 노트 S5 디바이스에서 Android 7.0 (Nougat) 운영 환경에서 프로그램을 작성하였고 테스트하였다.

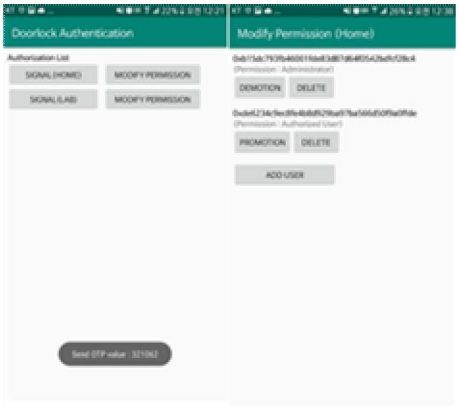

Fig. 12. Android application for authentication

2. Evaluation

블록체인은 비대칭키 기반의 암호화를 사용하기 때문에, 전송 중인 데이터를 암호화하면 권한이 없는 사용자가 데이터에 접속할 수 없게 된다. 따라서 도청, MITM, 메시지 변조와 같은 보안 공격은 성공할 가능성이 거의 없는 것이 보장된다. 블록체인에서 DDoS(Distributed Denial of Service) 공격은 스마트 계약 실행을 위한 수수료로 사용되어 실행되기 어렵다. 차단 및 방해로 인하여 네트워크가 단절된 경우 서버 기반의 인증 시스템들은 서비스 이용이 불가능하지만, 이 인증시스템은 seed 와 시간 정보를 통해 인증 정보를 확인하므로, 네트워크가 단절된 상황에서도 인증 서비스를 이용할 수 있다는 장점을 가진다. [Table. 2]는 기존의 인증 시스템과 본 논문에서 제안하는 시스템에 대해서 각 보안 위협 내용을 비교한 것으로 여러 보안공격에 대한 여러 문제점들을 해결하였음을 보여준다.

Table 2. Comparison of security threats

security attack	Proposed Scheme	Bluetooth	Slock.it
Wiretapping	**impossible**	weak	impossible
MITM	**impossible**	weak	impossible
Message Modification	**impossible**	weak	impossible
DoS	**available**	unavailable	available
Network Disconnection	**available**	unavailable	unavailable

V. Conclusions

본 논문에서는 이종성 문제로 인해 다양한 보안 위협에 노출되어있는 사물인터넷의 문제를 해결하기 위하여 위변조가 불가능한 블록체인과 스마트 계약을 이용하여 발생

가능한 보안 위협을 줄였고, 또한 네트워크가 단절된 상황에서도 인증에 대한 가용성을 확보하기 위해 TOTP를 이용하는 방법을 제안하고 그 결과를 기술 하였다.

전 세계적으로 사물인터넷 보안에 대한 표준 확립 및 보안 서비스를 제공하는 연구가 진행 중이다. 일상생활의 모든 개체가 인터넷에 연결되면 상호 운용성을 보장하기 위해 동일한 프로토콜을 사용해야 하므로, 사물인터넷 성공을 위해서 표준화된 프로토콜이 반드시 필요하다[5]. 그러나, 사물인터넷은 센서/디바이스, 게이트웨이, 플랫폼, 네트워크라는 다양한 주체에 대해 다양한 보안 위협이 존재하고 또한 저용량, 경량의 특징을 가지는 사물인터넷 장치 특성상 모든 보안 요구사항을 만족하는 보안 프로토콜 및 보안 서비스를 적용하는 것이 쉽지 않을 것이다.

본 논문에서 제안한 기술은 사물인터넷 장치를 위변조가 불가능한 블록체인 기반으로 구성하고 스마트 계약을 통해 인증/인가, 접근 제어를 수행하여 기밀성, 무결성을 만족시키고, 스마트 계약의 실행에 대한 수수료를 부과하는 방식으로 DoS 공격에 대응 가능하고 TOTP를 이용하여 네트워크 단절 시에도 인증 기능을 이용할 수 있으며, 블록체인이 분산 네트워크라는 점에서 가용성을 높일 수 있다. 또한 실질적인 프로그램 수행은 스마트 계약을 통해 이루어지므로, 플랫폼 및 센서/디바이스에서는 개인키 노출과 관련한 보안 위협과 보안 요구사항으로 줄일 수 있다는 점에서 기술적 가치를 가진다. 실제로, ITU-T SG20에서, 2017년 3월 연구과제의 일환으로 “Framework of blockchain of thins as decentralized service platform”을 제안하였으며, 블록체인 기반의 사물인터넷 표준화에 대한 논의는 계속해서 진행 중에 있다.

블록체인은 탈중앙화 환경에서 신뢰성을 보장하는 기술이다. 따라서 다양한 사물이 연결되는 사물인터넷의 보안 문제는 블록체인 기술이 대안이 될 가능성이 높다. 향후 블록체인 기술 기반으로 사물인터넷의 인증, 권한 부여, 접근 제어 등의 무결성 및 기밀성에 대한 표준화와 관련된 연구를 진행할 계획이다.

ACKNOWLEDGEMENT

This work was supported by a Research Grant of Pukyong National University(2018).

REFERENCES

[1] ITU-T, “Security framework for the Internet of things based on the gateway model”, ITU-T Recommendation X. 1361, pp.4, September 2018.

[2] Slock.it, Inc, “BLOCK-CHAIN ENABLED SERVICE PROVIDER SYSTEM”, US 2018/0191714 A1, Dec. 28, 2017, Jul. 5, 2018.

[3] 46halbe, “Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8”, CCC, https://www.ccc.de/en/updates/2017/iriden, 2017.

[4] Park. Byungju, “IoT industry trends and development prospects”, IITP, Weekly Technology Trend 1759 issue, 14p~23p, 2016.

[5] S. Keoh, S. Kumar, H. Tschofenig, “Securing the internet of things: A standardization perspective,” IEEE Internet of Things Journal, Vol. 1, No. 3, pp. 265-275, June 2014.

[6] frank, “Chaos Computer Club breaks Apple TouchID”, CCC, https://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid, 2013.

[7] J. Padgette, K. Scarfone, “Guide to Bluetooth Security”, NIST Special Publication 800-121 Revision 1, June 2012.

[8] D. M'Raihi, S. Machani, M. Fei, J. Rydell, “TOTP: Time-Based One-Time Password Algorithm”, RFC 6238, May 2011.

[9] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, October 2008.

[10] A. Juels, “RFID Security and Privacy: A Research Survey”, IEEE Journal On Selected Areas In Communications, 381-394, March 2006.

[11] H. Torstein, “Security and Privacy in RFID Applications”, Norwegian University of Science and Technology (NTNU), June 2006.

[12] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen, “HOTP: An HMAC-Based One-Time Password Algorithm”, RFC 4226, December 2005.

[13] A. Back, “Hashcash - a denial of service counter-measure”, http://www.hashcash.org/papers/hashcash.pdf, August 2002.

[14] N. Haller, C.Metz, P.Nesser, M. Straw, “A One-Time Password System”, RFC 2289, Faburary 1998.

[15] Computer Emergency Response Team (CERT) , “IP Spoofing and Hijacked Terminal Connections”, CA-95:01, January 1995.

[16] Haller, N., and R. Atkinson, “On Internet Authentication”, RFC 1704, October 1994.

[17] Seth Rosenblatt, “Hacker claims you can steal fingerprints with only a camera”, cnet, http://www.cnet.com/news/hacke r-claims-you-can-steal-fingerprints-with-only-a-camera/

[18] BBC, “Face ID iPhone X 'hack' demoed live with mask by Bkav”, BBC, https://www.bbc.com/news/av/technology-41992 610/face-id-iphone-x-hack-demoed-live-with-mask-by-bkav

[19] gluk256, “The Signidice Algorithm”, Github, https://github .com/ gluk256/misc/blob/master/rng4ethereu m/signidice.md

Authors

Ho-Gyun Kim is currently a senior student of the Department of Computer Engineering, Pukyong National University, Busan, Korea. He currently works as a S/W development director at a venture company, MROCOMMERCE, Seoul, Korea.. He is interested in Computer Security, Algorithms, and Blockchain Technology & Application.

Soon-Ho Jung received the B.S. degree in Mathematics Education from Seoul National University in 1982 and M.S. and Ph.D. degrees in Computer Science from KAIST in 1982 and 2000 respectively. He is currently a Professor in the Department of Computer Engineering, Pukyong National University. He is interested in Embedded Intelligent System, Computer Security and Machine Learning.