Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.343

블록체인 기반 IoT 디바이스 인증 스킴*

박 병 주,[1†] 이 태 진,[2] 곽 진[3‡]

[1]아주대학교 컴퓨터공학과 정보보호응용및보증연구실
[2]호서대학교 정보보호학과, [3]아주대학교 사이버보안학과

Blockchain-Based IoT Device Authentication Scheme*

Byeong-ju Park,[1†] Tae-jin Lee,[2] Jin Kwak[3‡]
[1]ISAA Lab., Department of Computer Engineering, Ajou University
[2]Department of Information Security, Hoseo University,
[3]Department of Cyber Security, Ajou University

요 약

ICT 기술이 발달하며 IoT 환경이 주목받고 있다. 하지만 IoT 디바이스는 다양한 사용 용도만큼 디바이스가 동작하는 CPU의 성능도 다양하지만, 인증에 필요한 암호화가 내장되지 않은 CPU를 사용하거나, 공개키 암호가 동작하지 않는 디바이스도 다수 존재한다. 이에 따라, 본 논문에서는 램포트 해시체인, 램포트 서명, 블록체인을 분석하고, 기존 인증 프로토콜 분석을 통해 인증, 무결성 및 부인 방지 기능을 제공하는 블록체인 기반 IoT 디바이스 인증 스킴을 제안하였다. 본 논문에서 제안하는 스킴은 IoT 디바이스에 단순 해시연산만을 요구하여 저성능 IoT 디바이스에서도 동작이 가능해 IoT 환경에서 안전한 인증을 보장할 수 있다.

ABSTRACT

With ICT technology develops, IoT environment is attracting attention. However, IoT devices have various CPU performance as much as various purpose of use. Some IoT devices use the cpu that doesn't support public key cryptogrphy or crypto acceleration. In this paper, we study Blockchain-based IoT Device Authentication Scheme that provides authentication, integirity and non-repudation through analysis of Lamport Hash-chain, Lamport Signature, Blockchain and existing Authentication protocols. The proposed scheme requires only simple hash operation in IoT devices and it can operate in low performance IoT device, thus ensuring secure authentication in IoT environment.

Keywords: IoT, Blockchain, Authentication, Hash-chain

I. 서 론

최근 ICT 기술의 발달과 함께 목적에 따라 다양한 기능, 성능을 갖는 IoT 디바이스들이 등장하고 있다. Cisco에 따르면, 2018년에는 350억 개, 2020년에는 500억 개의 IoT 디바이스가 인터넷에 연결되어 사용될 것으로 예측되고 있다[1].

IoT 디바이스는 다양한 목적에 사용되는 만큼, 고성능을 필요로 하는 일부 디바이스의 경우, OS가 동작 가능한 고성능의 칩셋을 장착해 대부분의 암호화 프로토콜을 지원한다. 하지만 전등을 on/off 하는 등의 단순 작업을 수행하는 IoT 디바이스들은 OS가 동작하지 않는 저성능의 칩셋을 기반으로 하고 있어, 암호화 프로토콜 지원하지 않거나, 인증서

Received(02. 27. 2017), Modified(03. 28. 2017), Accepted(03. 29. 2017)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT 연구센터육성지원사업의 연구결과로 수행되었음(IITP-2016-R2718160003000102)
† 주저자, bjpark.isaa@gmail.com
‡ 교신저자, security@ajou.ac.kr(Corresponding Author)

를 처리하기에 충분한 성능을 가지지 못해 취약하다고 할 수 있다.

이에 따라, 본 논문에서는 저성능 IoT 디바이스에서도 동작이 가능한 블록체인 기반 IoT 디바이스 인증 스킴을 연구해 보다 안전한 인증 방식을 제안하고자 한다. 본 논문의 2장에서는 블록체인, 램포트 해시체인 및 기존 IoT 인증 절차 및 디바이스 퍼포먼스 등에 대해 분석하고, 3장에서는 2장에서 연구한 내용을 기반으로 블록체인 기반 IoT 디바이스 인증 스킴을 제안한다. 4장에서는 제안한 인증 스킴의 안전성 및 효율성을 분석하고, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 Lamport Hash-chain

램포트 해시체인(Lamport Hash-chain)은 클라이언트에서 생성한 비밀 값으로부터 연속적으로 해시 값을 계산하는 방식으로, 효율적 비동기화 방식의 일회용 패스워드 인증 기법이다. 이를 통한 S/Key 일회용 패스워드 방식이 RFC 2289에 적용되어 있으며, 네트워크상의 도청, 재전송 공격 등으로부터 안전한 개체 인증을 제공한다는 장점이 존재한다[2,3,4].

2.2 Lamport Digital Signature

램포트 서명(Lamport Digital Signature)는 일방향함수를 이용한 디지털 서명 생성 기법으로 256비트의 암호학적 해시 함수와 안전한 난수 발생기로 다음과 같은 절차를 통해 서명을 수행한다[2].

2.2.1 키 생성

개인키를 생성하기 위해, 난수 발생기를 이용해 256개의 랜덤값의 쌍을 만든다. 각각의 랜덤값들은 사용자의 개인키가 되고, 키 하나당 256비트의 길이를 갖는다. $(2\times256\times256bit)$ 크기의 공개키를 생성하기 위해, 사용자는 개인키 쌍들의 해시 값을 각각 구한다. 해시함수를 통해 생성된 512개의 해시값들이 사용자의 공개키가 된다.

2.2.2 메시지 서명

메시지에 서명하고자 하는 경우, 메시지 M에 대한 해시 값을 구하고, 각각의 비트에 대응되는 위치의 개인키 쌍에서 값을 선택한다. 해시 값의 첫 번째 비트 값이 0인 경우, 첫 번째 개인키 쌍의 첫 번째 값을 선택하고, 첫 번째 비트값이 1일 때에는 첫 번째 개인키 쌍의 두 번째 값을 선택한다. 상기 방식으로 순차적으로 진행하여 256개의 값을 개인키 쌍에서 선택할 수 있으며 구해진 값은 앨리스의 서명이 된다. 이 때, 공개된 앨리스의 개인키는 다시 사용되거나, 사용하지 않은 랜덤 값은 공개되거나 사용되지 않아야 한다.

2.2.3 서명 검증

수신자가 서명을 확인하기 위해 우선적으로 메시지 M의 해시 값을 구하고, 얻어진 해시 값을 이용해 송신자의 공개키에서 256개의 값을 선택한다. 그리고 메시지와 함께 공개되어 있는 서명 값들의 해시 값을 구하고 공개키에서 선택한 해시값과 비교한다. 양쪽의 값들이 모두 일치한다면 서명은 올바른 것으로 판단한다.

2.3 블록체인

블록체인은 비트코인을 위해 개발된 기반 기술로, 가상 화폐로 거래할 때 발생 가능한 다양한 위협을 막기 위한 기술로, 사용처에 따라 다양한 형태로 변형되어 사용되고 있지만, 기본적인 구조는 유사하다[5].

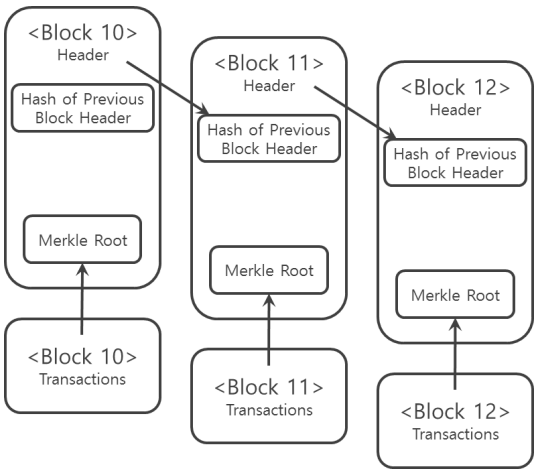

Fig. 1. Blockchain Structure

Table 1. Types of Blockchain and Characteristic

Category	Concepts and Features	Prerequisites
Public Blockchain	• First Blockchain Use Case • A ledger that be opened and can be operated by everyone over the Internet • Devide compute power to the network • Network expansion is difficult and transactions are slow	• Network Effect • Stable Ecosystem • Risk Management
Private Blockchain	• Personalized Blockchain • One entity manages the internal network with Blockchain	• Taking system changed and ensuring safety • Global Branches in one entity
Consortium Blockchain	• Half-center type Blockchain • Only pre-selected entities can participate • Notarized participation through rules agreed upon among the entities • Easy network expansion and fast transaction speed	• Business agreement between participants • Ensure system safety

2.3.1 블록체인 구조

블록체인은 Fig. 1.과 같이 크게는 이전 블록헤더의 해시값, 전자서명, 현재 블록의 해시값, 타임스탬프 등으로 이루어진 블록헤더와 Merkle root, 트랜잭션 등으로 이루어진 블록데이터로 구성되어 있다.

2.3.2 블록체인 종류와 개념 및 특징

블록체인은 사용 용도에 따라서 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain), 컨소시엄 블록체인(Consortium Blockchain) 3가지로 분류가 가능하다. 각각의 블록체인은 전체 및 구조적으로 유사하지만 다른 개념과 특징을 가지고 있으며, 각각의 블록체인을 정의 및 구현하기 위한 선결 요건 또한 존재한다. 퍼블릭 블록체인은 일반적으로 알려진 비트코인을 활용하기 위한 블록체인이며, 프라이빗 블록체인, 컨소시엄 블록체인은 블록체인을 다른 용도로 활용하기 위한 개념이다. 위의 Table 1.은 블록체인의 종류와 개념 및 특징을 나타낸 표이다.

2.3.3 Merkle Tree

머클 트리(Merkle Tree)는 트리 구조의 일종으로 다음 Fig. 2.와 같은 구조를 갖는다. 잎 노드는 파일 등의 데이터를 가리키며, 상위 노드들은 각각 자식 노드들의 해시 값이 된다. 블록체인 구조에서 자료의 유효성을 검사하기 위해 사용된다[6].

최상위 해시값인 Tx_Root 값을 공유한 후, 개별 파일이 전송되는 경우, 개별 파일들의 해시 값들을 통해 Tx_Root 값을 계산하면 보내진 파일의 변조 유무를 검증할 수 있다. 이를 응용하여, 일부의 해시값과 Tx_Root값을 알고 있는 경우에 특정 파일의 변조 유무 또한 검증이 가능하다.

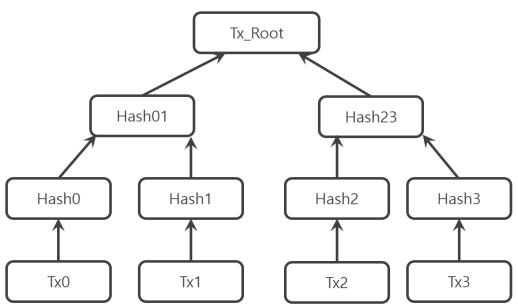

Fig. 2. Merkle Tree Structure

2.4 IoT-device Performance

공개키 암호 방식은 높은 연산량을 필요로 해 높은 오버헤드가 발생해 IoT 디바이스에 부적합하다[7]. IoT 디바이스들은 단순 조명 on/off 센서부터 웨어러블 디바이스 등에 이르기까지 사용 용도에 따라 다양한 성능을 갖는다. 하지만 일부 디바이스의 경우, 낮은 CPU 퍼포먼스로 인해 공개키 암호화를 지원하지 않으며 CPU에 암호화가 내장되어 있지 않은 경우가 많다. 이로 인해, 인증서를 활용한 인증 등을 수

Table 2. IoT device-specific CPU and whether encryption function supports

Name	CPU	Crypto Acceleration	Public Key Encryption
Belkin Wemo Switch	Ralink RT5350F	**No**	Yes
Samsung Smarthings Hub	PIC32MX695f-512H 32bit	**No**	Yes
LIFX Color 1000	Kinetis K22 (ARM Coretex-M4)	**No**	**No**
Philips Hue Lights (Bulb)	ST Microelectronics STM32F100RBT6B (ARM Cortex-M3)	**No**	**No**
Pebble Time	ST Microelectronics STM32F439ZG (ARM Coretex-M4)	Yes	**No**
Fitbit Surge	Silicon Labs EFM32 Giant Gecko (ARM Cortex-M3)	Yes	**No**
Fitbit One	ST Mircroelectronics 32l151C6 Ultra Low Power (ARM Coretex-M3)	**No**	**No**

행할 수 없어 인증 측면에서 취약하다.

위의 Table 2.는 Datamation에서 선정한 home automation iot device 중 임의의 IoT 디바이스들의 CPU 별 공개키 암호화 지원 여부를 분석한 표의 일부이다[8].

2.5 기존 IoT 인증 프로토콜 유형 분석

IoT 환경에서 공격자들은 IoT 디바이스에 위장 공격, 재사용 공격, DoS 공격 등 다양한 공격을 수행해 IoT 환경 내부로 접근하고자 한다.

기존의 IoT 환경에서는 이를 방지하기 위해 다섯 가지 종류의 인증 프로토콜을 사용한다[9]. 아래 Table 3.은 각 인증 기술들의 장단점을 나타낸 표이다.

2.5.1 ID/password 기반 인증

각 사용자의 ID와 패스워드를 서버의 DB에 저장하고 저장된 지식을 기반으로 인증하는 방식으로 주로 서버/클라이언트 인증 환경에서 사용되는 기술이다. 서버에 저장된 패스워드 리스트가 노출되어 인증이 무력화됨을 막기 위해 해시 함수를 통해 값을 저장하는 방식을 채택하는 경우가 많다. 보다 높은 안전성을 보장하기 위해 SSID를 숨기거나, AP와 디바이스 간 WEP키 사용, PAP 인증 방식 채택, RFID 방식을 사용한다. IoT 환경에서의 ID/Password 방식은 다수의 기기가 사람의 개입없이 사용되는 IoT 환경의 특성상 서버의 관리 및 부하 등의 문제점이 있으며, 기기 수정 및 추가 과정에 사람의 개입이 전제되어야 하는 문제점이 있다. 또한 부인방지 기능을 제공하지 못해 IoT 환경에서의 인증 기술로는 적합하지 않다.

2.5.2 MAC Address 기반 인증

네트워크 인터페이스에 할당된 고유의 식별 주소인 MAC(Media Access Control) Address를 활용한 인증 방식으로 주로 인트라넷 환경에서 네트워크 접근제어에 사용된다. 디바이스가 네트워크 접속 요청 시 서버에 등록되어있는 MAC 주소와 디바이스로부터 요청받은 메시지와 함께 전송된 MAC 주소를 비교해 인증하는 절차를 가지며, ID/Password 기반 인증 방식보다 간편하고 속도도 빠르다. 하지만 다양한 디바이스들의 증가 및 IoT의 등장으로 새로운 MAC Address 양식이 규정되어야할 필요성이 제기되고 있으며, EUI-48, EUI-64 등 새로운 표준이 규정되고 있다. 또한, MAC Address는 위조가 가능해 별도의 보안장비 없이는 Spoofing 등의 공격으로 인해 취약하다[10].

2.5.3 암호 프로토콜 기반 인증

공개키 암호, 대칭키 암호를 기반으로 개체를 인증하는 프로토콜로 주로 무선인터넷 보안 프로토콜에서 사용된다. 802.1x/802.11i, WPA 등 다양한 표준을 지원하고 있다. 암호 프로토콜 기반 인증 방식은 사용하는 암호 프로토콜에 따라 ID/Password 기반 인증, MAC 주소 기반 인증, 인증서 기반 기기 인증서 인증 등의 기술을 포함할 수 있다. 또한 다양한 인증 방식을 제공해 사용 환경에 따라 적합한 인증 방식을 선택할 수 있으며, 채택한 암호 프

Table 3. Comparison of advantages and disadvantages of existing authentication technology

Authentication Technology	Advantages and Disadvantages	
ID/Password based Authentication	Advantage	- Easily authenticated if ID/Password are pre-shared
	Disadvantage	- Require additional application or protocol to connect - Non-repudiation is impossible
MAC Address based Authentication	Advantage	- Easy to Connect and additional application or protocol are not required
	Disadvantage	- Re-registration is required when device changed - Should be connected by user's own device - Non-repudiation is impossible
Cryptography Protocol based Authentication	Advantage	- Provides various authentication methods to select suitable method for each environment - Non-repudiation is possible according to designed protocol
	Disadvantage	- Safety relies on encryption protocol
Certificate based Authentication	Advantage	- Reliable device identification is possible - Provide high safety - Non-repudiation is possible
	Disadvantage	- Certificate management required - Processing time is relatively long due to large amount of calculation - Difficult to use on low performance devices
IBE based Authentication	Advantage	- Key predistribution is not required - Non-repudiation is possible
	Disadvantage	- Vulnerable to ID spoofing attack by using public ID

로토콜에 따라 부인방지 기능도 제공이 가능하다.

하지만, 안전성을 기반 암호 기술에 의존하여 암호 기술의 취약점이 발견될 경우, 인증기술의 취약점으로 연결될 수 있다.

2.5.4 인증서 기반 인증

공개키 암호를 이용하는 전자서명을 통해 인증하는 방식으로, 인증서에 전자서명을 위한 정보를 수록하여 이를 기반으로 인증을 수행한다. 국내의 경우, 1999년 제정한 전자서명법을 통해 공인인증서 발급 체계 및 관리와 관련된 규정을 마련하였으며 최상위 인증기관인 Root CA 하에 5개의 공인인증기관을 통해 인증서의 발급 및 인증을 수행하고 있다. 국외의 경우, Verisign사의 기기 인증 서비스를 통한 개인 디바이스, 케이블 모뎀 디바이스 인증, WiMAX 산업 인증서 등이 제공되고 있다. 이 외에도 VoIP, 네트워크 감시카메라 등에서 인증서 기반 인증기술이 사용되고 있으며 그 영역을 점차 넓혀가고 있다.

인증서 기반의 인증기술은 강력한 인증 기능을 통해 높은 안전성을 제공하며, 부인방지 기능 또한 제공한다. 하지만, 기기인증서 처리 소프트웨어 및 알고리즘은 높은 연산 처리량을 필요로 한다. 따라서 저전력, 저성능의 IoT 디바이스에서 사용하기에는 적합하지 않다.

2.5.5 IBE를 이용한 인증

아이디 기반 인증(ID-based Authentication)은 사용자의 이메일 주소, 이름, IP주소 등 사용자의 ID를 공개키로 사용하는 공개키 암호 시스템으로 서명 및 인증을 제공한다. 사전 키 분배가 필요하지 않으며, 연산량이 적고 키 길이가 상대적으로 짧다는 장점이 있지만 ID 위장 공격에 취약하다는 단점이 존재한다. 다른 인증기술에 비해 상대적으로 새로운 개념과 기술로 Hess's Algorithm, Lynn's Algorithm, Gentry and Silverberg's Algorithm 등 다양한 인증 스킴 등이 있다[11].

2.6 IoT 디바이스 인증 보안 요구사항

IoT 환경에서 안전한 인증을 위해서는 보안 요구사항을 분석하여야 한다. 본 논문에서는 저성능의 IoT 디바이스에서도 동작이 가능한 인증 스킴을 위해 블록체인 및 램포트 해시체인 등의 기술을 사용한다. IoT 인증 프로토콜의 보안 요구사항은 다음과 같다.

● 디바이스 인증 제공

IoT 네트워크에 참여하는 각 센서 디바이스들은 최상위 Aggregator에게 자신이 정당한 디바이스가 맞는지를 증명해야 한다.

● 디바이스 무결성 제공

최상위 Aggregator에서는 센서 디바이스가 악성코드에 감염되거나 악의적인 행위를 막기 위해 센서 디바이스가 위·변조되었는지를 확인할 수 있어야 한다.

● 부인방지 제공

센서 디바이스들은 최상위 Aggregator 또는 다른 디바이스들과 상호 동작하는 과정에서 자신이 보낸 메시지에 대한 부인방지를 제공해야 한다.

III. 제안 사항

본 논문에서 제안하는 블록체인 기반 IoT 디바이스 인증 스킴은 다음 Fig. 3.과 같은 일반적인 IoT 네트워크 구조를 따른며, Fig. 4.는 제안사항을 적용한 형태이다. 본 논문에서 제안하는 인증 스킴은 폐쇄적인 네트워크로 구성되어 있으며, 센서 등의 디바이스는 네트워크에 참여하기 전에 최상위 Aggregator에게 그룹키를 나눠받는 사전 절차를 거친 후에 네트워크에 추가될 수 있다. 일반적인 IoT 네트워크상에서의 최상위 Aggregator는 Fig. 2.의 머클 트리 중 최상위 노드 역할을 수행한다. 또한, 최상위 노드의 해시값인 Tx_Root와 이전 블록의 해시값 등 다양한 정보를 통해 다음 블록을 생성한다.

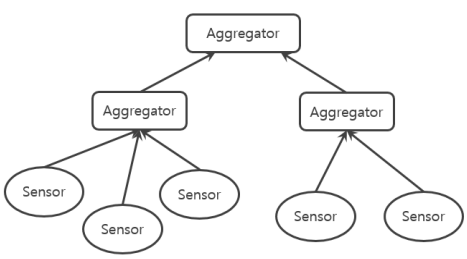

Fig. 3. General IoT Network Structure

3.1 기호 및 표기

본 논문에서 제안하는 스킴에 사용되는 기호 및 표기는 다음의 Table 4.와 같다.

그룹 키의 경우, 사전에 생성되어 있으며 네트워크에 참여하고자 하는 노드가 있을 때, 최상위 Aggregator에서 분배한다.

Table 4. Notation

Notation	Description
pk_i	Public key of sensor i
x_i	Hash value of merkle tree node
l	Length of hash-chain
n	Number of device
$h(\,)$	Hash function
K_G	Grout key

3.2 공개키 생성 과정

센서 디바이스에서 인증을 위해 사용하는 그룹 키는 램포트 해시체인을 이용해 다음과 같은 절차를 통해 생성된다.

사용자는 순차적인 해시 값을 인덱스의 역순으로 다음 수식 (1, 2)와 같이 생성한다.

$$pk_l <- (0,1)^n \tag{1}$$

$$pk_i <- h(pk_{i+1}) \text{ for } i \in (l-1, l-2, ..., 0) \tag{2}$$

각각의 pk값들은 각 센서들의 공개키가 되며, pk_1부터 역순으로 나타난다.

그룹키 pk_i를 검증하기 위해서는 pk_0가 실제로 i번째 해시인지 검증한 후, pk_i의 해시값 검증을 수행한다. 그룹키 pk들은 해시체인의 특성으로 인해 공격자가 i번째 키를 알고 있어도, 다음 $i+1$번째 키를 예측하기가 어렵다.

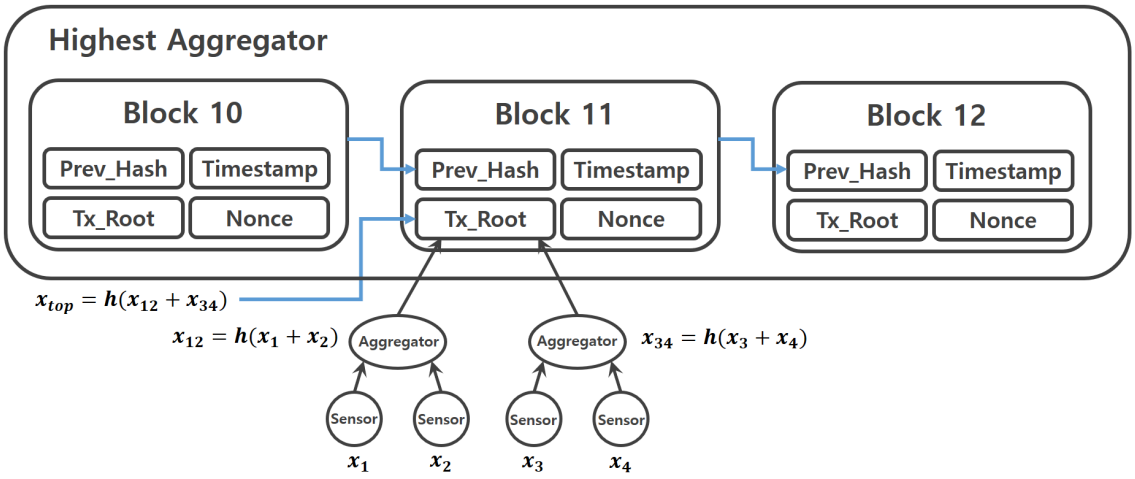

Fig. 4. Proposed Blockchain-based IoT Device Authentication Scheme

3.3 머클 트리 생성

머클 트리를 생성해 Tx_Root 값을 생성하기 위하여 각각의 센서들은 다음과 같은 수식을 통해 해시값을 생성한다.

$$x_i = H(Data \| K_G \| H(pk_i)^n), H(pk_i)^{n-1} \quad (3)$$

각 센서 디바이스에서는 수식 (3)과 같이, 자신의 데이터, 사전에 공유한 그룹키, 램포트 서명을 통해 생성한 공개키 등을 통해 머클 트리를 구성하는데 사용될 해시 값을 생성한다.

3.4 인증 및 검증 과정

본 논문에서 제안하는 블록체인 기반 IoT 디바이스 인증 스킴에서는 디바이스를 인증하기 위해 사전에 정의했던 수식 (3)의 값을 이용한다. 최상위 Aggregator에서 다음 블록을 생성하기 위해 주변 센서 디바이스들로부터 해시값을 전송받아 Tx_Root 값을 생성한다. 이때, 최상위 Aggregator에서는 미리 보유하고 있던 해시체인을 통해 각 디바이스에서 생성하는 공개키를 생성하고, 그룹키와 센서 디바이스의 정보를 계산해 센서 디바이스들로부터 전송받은 x_i값으로 생성된 Tx_Root값이 정당한 값인지 검증하고, 전송받은 x_i값의 유효성을 검증한다.

$$Tx\_Root = h(h(x_1 + x_2) + h(x_3 + x_4)) \quad (4)$$

수식 (4)와 같이 Tx_Root 값은 x_i값들의 최종 해시값이므로, 임의의 x_i를 다른 x_i들을 통해 검증할 수 있다. Tx_Root 값이 정당할 경우, 센서 디바이스들로부터 전송받은 공개키와 디바이스 정보 또한 유효하므로, 센서 디바이스에 대한 인증, 무결성 검증 및 부인방지가 가능하다.

IV. 안전성 및 효율성 분석

4.1 안전성 분석

본 논문에서 제안하는 블록체인 기반 IoT 디바이스 인증 스킴은 IoT 디바이스 인증을 위한 보안 요구사항을 만족하기 위해, 블록체인, 램포트 해시체인, 램포트 전자서명 등의 기술을 활용한다. 제안하는 스킴에서 각각의 센서에서 생성하는 x_i값들은 센서의 상태에 따라 다른 값을 가지게 되어, 새로운 블록을 생성할 수 있다. 또한, 큰 폭의 변화를 갖는 경우 센서 디바이스 점검을 수행하는 등 추가적인 보안 조치를 취할 수 있다.

● 디바이스 인증

센서 디바이스들은 자신을 최상위 Aggregator에게 증명하기 위해 네트워크에 참여할 때 부여받은 램포트 해시체인을 통해 생성된 공개키를 포함해 머클 해시 트리 값을 생성한다. 최상위 Aggregator는 여러 센서들로부터 전송받은 해시값으로 Tx_RooT값을 생성하고 각 센서들의 머클 트리 값이 맞는지 검

증한다. 해당 과정에서, 해당 머클 트리 값은 센서 디바이스별로 다르므로 적합한 머클 트리 값을 가지고 있다면 인증을 수행할 수 있다.

● 디바이스 무결성

제안하는 논문에서는 블록체인을 생성하는 과정에서 머클 트리를 통해 디바이스의 인증을 수행한다. 머클 트리를 검증하는 과정에서 센서 디바이스들의 해시값인 x_i의 위·변조 검증을 통해 디바이스 내부 데이터의 무결성을 보장할 수 있다.

● 부인방지

센서 디바이스들은 램포트 해시체인을 통해 생성된 공개키와 디바이스 정보 등을 통해 머클 트리 값을 생성한다. 센서 디바이스에서 생성한 각각의 머클 트리 해시값은 각 디바이스에서만 생성할 수 있으므로 부인방지 기능을 제공할 수 있다.

4.2 효율성 분석

기존 IoT 인증 프로토콜의 경우, 주로 암호 프로토콜 및 인증서를 기반으로 인증을 수행한다. 하지만 암호 프로토콜 또는 인증서를 기반으로 하는 인증은 연산량이 높은 공개키 암호를 채택하고 있어, CPU에 암호화 기능을 내장하고 있지 않거나 성능이 낮은 일부 디바이스에서는 부적합하다. 하지만 본 논문에서 제안하는 블록체인 기반 IoT 디바이스 인증 스킴은 최상위 Aggregator에서 공개키 검증, 해시체인 생성 등 대부분의 연산을 수행하고 IoT 디바이스에는 단순한 해시연산만을 요구한다. 이에 따라, 암호 프로토콜 및 인증서를 기반으로 인증을 수행하는 기존 인증 방식에 비해 효율성을 보장할 수 있다.

V. 결 론

ICT 기술이 발달함에 따라, IoT 환경 또한 주목을 받고 있으며, 연구가 활발히 일어나고 있다. IoT 환경은 개인정보와 밀접한 관련이 있으며, 디바이스의 수가 많고, 모든 디바이스가 인터넷과 연결되어 있어 인증에 대한 고려가 필요하다. 하지만 기존 IoT 인증 프로토콜의 경우 암호화가 내장되지 않은 CPU를 사용하거나, 공개키 암호 연산이 불가능한 저성능 디바이스에 대한 고려가 미흡하다. 따라서, 본 논문에서는 블록체인 및 램포트 해시체인 등을 활용하여 안전하고 경량화된 블록체인 기반 IoT 디바이스 인증 스킴을 제안하였다.

본 논문에서 제안하는 인증 스킴의 경우, 인증 외에도 무결성 및 부인 방지 기능을 제공한다. 또한 IoT 디바이스에 단순 해시연산만을 요구해 저성능 디바이스에서도 동작이 가능해 IoT 환경에서 안전한 인증을 제공할 수 있다.

References

[1] Cisco, "11th annual Visual Networking Index: Global IP Traffic Forecast Update," Dec. 2015

[2] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report SRI-CSL-98, SRI International Computer Science Laboratory, Oct. 1979.

[3] RFC 2289, A One-Time Password System, Feb. 1990. https://www.ietf.org/rfc/rfc2289.txt

[4] L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM (24.11), pp 880-772., 1981.11.24.

[5] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.10.31.

[6] Ralph C. Merkle, "A digital signature Based on a Conventional Encryption," Advances in Cryptology, Crypto `87. CRYPTO 1987.

[7] Aaron Aridiri, "Is it possible to secure micro-controllers used within IoT?," EvoThings, 2014.08.27.

[8] Cynthia Harvey, "75 Top IoT Devices," Datamation, 2016.07.25

[9] KIISC, "Research on efficient authentication system for machine-to-machine communications," 2010.09.30.

[10] Enos Letsoalo, Sunday Ojo, "Survey of Media Access Control address spoofing attacks detection and prevention techniques in wireless networks," IST-Africa

Week Conference, 2016.05.11.
[11] H. Kupwade Patil, D. Willis, "Identity based authentication in SIP," IETF draft 2008.02.18.

〈저 자 소 개〉

박 병 주 (Byeong-ju Park) 학생회원
2016년 2월: 순천향대학교 정보보호학과 학사
2016년 3월~현재: 아주대학교 컴퓨터공학과 석사과정
〈관심분야〉 Fintech 보안, 암호프로토콜, 응용시스템 보안, IoT 보안

이 태 진 (Taejin Lee) 종신회원
2003년 2월: POSTECH 컴퓨터공학과 학사
2003년~2017년: 한국인터넷진흥원 정보보호R&D팀장
2008년 2월: 연세대학교 컴퓨터공학과 석사
2017년 2월: 아주대학교 컴퓨터공학과 박사
2017년~현재: 호서대학교 정보보호학과 조교수
〈관심분야〉 악성코드 분석, 침해사고 탐지/대응

곽 진 (Jin Kwak) 종신회원
2000년 8월: 성균관대학교 학사
2003년 2월: 성균관대학교 석사
2006년 2월: 성균관대학교 박사
2006년 4월~2006년 11월: 일본 큐슈대학교 방문연구원
2006년 8월~2006년 11월: 일본 큐슈시스템정보기술연구소 특별연구원
2006년 11월~2007년 2월: 정보통신부 정보보호기획단 개인정보보호팀 통신사무관
2007년 3월~2015년 2월: 순천향대학교 정보보호학과 교수
2008년 1월~현재: 한국정보보호학회 상임이사
2011년 1월~현재: 한국정보처리학회 이사
2015년 3월~현재: 아주대학교 사이버보안학과 교수
〈관심분야〉 자동차 보안, 암호프로토콜, 응용시스템보안, 클라우드 컴퓨팅 보안, 개인정보보호, 정보보호제품평가