Journal of The Korea Society of Computer and Information
Vol. 23 No. 1, pp. 111-116, January 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.01.111

A Secure Decentralized Storage Scheme of Private Information in Blockchain Environments

Seungjin Han*

Abstract

Recently, IoT and Big Data dealing with voluminous and complex sensitive information is one of the key issues in the era of the 4th industrial revolution. There have been a lot of studies to store the collected and processed sensitive information safely in storage data. Especially biometric information, if it is leaked and becomes identity theft, is hard to be corrected and results in serious event. To fix the problem, methods such as FIDO or KFTC have been proposed. In this paper, we propose a modified method of TTAK.KO-12.0098 according to the environment of this paper and propose a method of safely storing the generated disposable template in a block chain. We show that our method is better by comparing the existing method and the security analysis.

▸Keyword: Blockchain, One-Time Template, Biometric, Distributed Ledger

I. Introduction

우리 사회는 향후 몇 년 내에 IoT를 통해 모든 기기들이 서로 연결될 것이고, 이를 통해 축적되는 수많은 데이터와 이를 활용하고자 하는 빅데이터와 관련된 기술이 급속히 발전하고 있다. 악의의 사용자들은 이러한 민감한 정보나 개인 정보를 유출하기 위해 다양한 공격을 시도하고 있다. 공격자들부터 정보를 보호하기 위한 ID, PW와 같은 전통적인 방법을 사용하였으나 최근에는 바이오정보를 이용한 정보보호 방법이 활발히 연구되고 있다[1,2].

바이오인식은 신체의 고유한 특성인 지문, 홍채, 망막, 정맥, 얼굴 등이나 행동적인 특성인 목소리, 서명, 걸음걸이 등을 이용하여 개인을 식별하는 방법이다. 최근에는 심전도, 뇌전도와 같은 생체신호를 이용한 개인의 인증을 시도하는 사례가 있다[3-8]

그러나 사용자의 과실없이 사용자의 바이오정보를 저장한 기관, 회사 혹은 서버로부터 사용자의 바이오정보가 유출된다면 그 파급효과는 상당히 크다. 예를 들어 지문이나 홍채와 같은 바이오정보를 이용하여 인증을 하던 사용자가 기관에서 등록한 바이오정보가 유출되었다면 사용자는 자신의 바이오정보를 이용하여 다른 기관이 서비스를 받을 수 없을 것이다. 따라서 바이오정보를 보다 안전하게 저장하는 방법이 필요하다.

Satoshi Nakamoto가 최초로 제안한 비트코인으로 인해 블록체인이 새롭게 주목을 받기 시작했다[9]. 블록체인은 단순히 금융에서 뿐만 아니라 다양한 분야에서 응용되고 있다[10].

본 논문에서는 [11]을 수정하고 생성된 일회용 템플릿을 보다 안전하게 저장하고자 블록체인을 이용한 개선된 방법을 제안한다. 본 논문은 II장에서는 관련연구를 기술하고, III장에서는 일회용 템플릿을 이용하여 사용자의 바이오정보를 블록체인에 등록, 인증 및 갱신하는 과정을 정의한다. IV장에서는 본 논문에서 제안하는 방법에 대해 보안성 평가를 하고, V장에서는 결론 및 추후 연구과제에 대해서 기술한다.

II. Preliminaries

1. Related works

관련연구에서는 바이오인식을 적용한 표준 및 관련 연구를 살펴보고, 문제점을 기술한다.

• First Author: Seungjin Han, Corresponding Author: Seungjin Han
*Seungjin Han (softman@kiwu.ac.kr), Dept. of Business Administration, Kyung-In Women's University
• Received: 2017. 12. 04, Revised: 2017. 12. 26, Accepted: 2018. 01. 19.

1.1 TTAK.KO-12.0098

TTAK.KO-12.0098에서는 일회용 템플릿 기술을 이용하여 바이오인식 템플릿을 네트워크를 통해 전송할 때 발생할 수 있는 보안취약점을 보강하는 방법을 제안하였다[11]. 인증시스템은 인증 클라이언트와 인증서버로 이루어져 있다고 가정하고, 인증 템플릿은 클라이언트에서 생성되어 네트워크를 통해 인증서버로 전송된다. 그리고 사용자 인증을 위한 템플릿 매칭, 즉 인증 템플릿과 등록 템플릿 비교는 인증서버에서 이루어진다. 네트워크를 통해 전송되는 바이오인식 템플릿은 공격자에 의해 유출될 수 있다. 이 경우, 사용자 바이오인식 정보 노출로 인한 프라이버시 침해가 발생할 뿐만 아니라, 유출된 템플릿은 재사용 공격(replay attack)에 이용될 수 있다.

사용자 바이오인식 정보 노출을 최소화하기 위해, 클라이언트는 변환 함수를 이용하여 원본 템플릿을 변형하고, 변환된 템플릿(transformed template)을 인증 서버에 전송한다. 그리고 인증 서버는 클라이언트로부터 수신된 변환된 템플릿과 인증 서버에 저장된 변환된 템플릿을 비교하여 사용자 인증을 수행한다. 즉, 인증 서버는 원본 템플릿이 아닌 변환된 등록 템플릿을 저장한다. 또한, 매 인증시마다, 새로운 변환 함수를 이용하여 새로운 템플릿을 생성하여 사용자 인증에 이용함으로써, 유출된 템플릿을 이용한 재사용 공격을 방지한다. 일회용 템플릿을 이용한 사용자 서비스는 크게 사용자 등록과 사용자 인증 과정으로 나눌 수 있다.

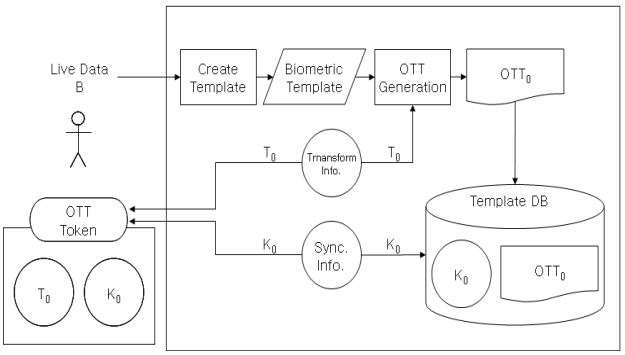

Fig. 1. User Registration and Initiation

그러나, [11]은 단일 서버에 사용자의 바이오정보 템플릿이 저장되어 있기 때문에 해킹으로 인해 사용자의 정보가 노출될 수 있다는 단점이 있다.

1.2 FIDO

FIDO 기술 표준을 제정한 FIDO Alliance는 2016년 4월 현재 250여 업체가 참여하고 있고, 참여업체 수가 꾸준히 늘어나고 있는 거대한 기업 연합체이다[12].

사용자는 사용자가 소지하고 있는 기기가 제공하는 인증 수단을 통해 사용자 로컬 인증을 수행하고 사용자 기기는 인증된 사용자를 대신하여 FIDO 표준 기반의 원격 인증을 수행한다. FIDO 표준의 원격 인증은 이미 많이 사용되어 안전이 입증된 공개키 암호 기술을 사용한다. 공개키 암호에 사용되는 개인키는 사용자의 기기에만 저장되고 외부에 노출되지 않으며, 사용자가 기기에 인증한 경우에만 저장되어 있던 개인키를 이용해 암호문을 생성하고 해당 암호문을 서버에 전송할 수 있다. 서버는 사용자 등록 과정에서 전달받은 저장된 공개키를 이용하여 전송된 암호문을 검증하고 사용자 인증을 완료한다.

FIDO 시스템의 장점은 사용자의 개인식별정보와 무관한 공개키 정보만 FIDO 서버에 저장되기 때문에, 서버의 정보가 해킹 등으로 모두 유출되더라도 사용자 개인의 정보는 유출되지 않는다. 그러나 신뢰성이 있는 제 3기관을 이용하지 않는 기술이기에 공인인증서와 같은 신뢰성을 구축하기 어렵다. 사용자 입장에서는 RP 서버가 적법한 서버인지에 대한 의문점이 있을 수 있고, RP 서버 입장에서는 사용자가 적법한 사용자인지에 대해 공인된 기관에서의 인증이 필요하다.

1.3 Distributed management of biometrics for KFTC

금융결제원(KFTC: Korea Financial Telecommunications and Clearings Institute)의 바이오정보 분산관리는 사용자의 바이오 정보를 나누어 각기 다른 서버에 저장하고 필요한 경우 각 서버로부터 바이오정보를 전송받아 합친 후 대상자를 검증하는 방식이다[13]. 바이오 정보를 분리해서 보관하는 방법은 자사인증서비스와 위탁인증서비스 2가지가 있지만, 이는 바이오 정보를 하나의 서버에 저장하느냐 아니면 2개의 서버에 저장하느냐의 차이일 뿐 근본적인 해결책이 되지 못한다. 금융결제원에 바이오 인증 위탁을 맡긴 금융기관은 5.41%(2017년 7월 26일 기준)에 불과하다[14].

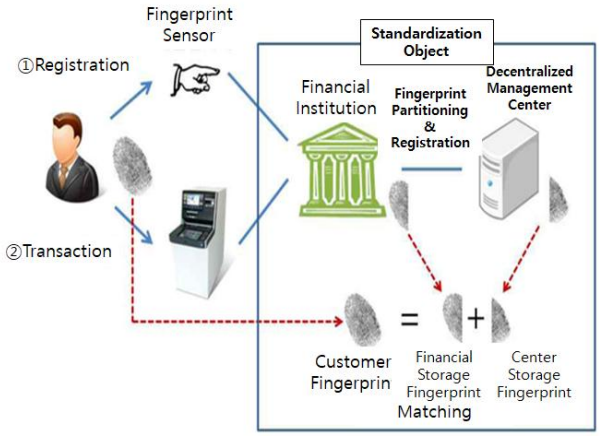

Fig. 2. Standard for distributed management of biometrics(KFTC)

1.4 The others

Seo et., al.은 비트코인의 블록체인 기술을 이용하여 파일을 효율적으로 분산하고 암호화하여 보안을 강화하는 방법을 제안하였다[15]. 제안한 시스템은 블록체인을 이용한 분산 클라우드 스토리지 시스템의 초기 모델로 기본적인 결함 허용성을 보장하지만 내부 로드 밸런싱 등의 안정적인 서비스를 제공하기 위한 몇 가지 구현이 미흡한 상황이다. 또한, 제안한 시스템은

지능화된 캠퍼스의 인프라로 사용될 수 있는 강력한 기반 스토리지 시스템을 제작하는 것이기에 블록체인 데이터베이스에 실제 모델을 적용하였을 때의 확장성, 비용, 성능 이슈를 상용 시스템과 비교하여 충분히 고려되지 못했다.

Masayuki et., al은 중앙 서버 없이 공개된 블록체인의 P2P 네트워크를 기반으로 한 온라인 저장 방법에 대해서 제안하였다[16]. 사용자 데이터는 나누어져 저장되어 있고 P2P 노드에 분산되어 있기 때문에 공격자는 온라인 저장소에서 목표로 하는 사용자의 저장소를 찾을 수 없도록 하였다.

III. The Proposed Scheme

Fig. 3은 본 논문에서 제안하는 방법의 개략도이다. 사용자는 자신의 바이오정보를 센서를 통해서 단말기에 인식시킨다. 단말기는 센서를 통해 획득한 바이오정보를 이용하여 일회용 템플릿 토큰(OTT)을 생성한다.

생성된 OTT는 임의의 블록체인에 저장한다. OTT를 전송받은 블록체인은 자신과 연결된 다른 블록체인에 사용자의 OTT를 전송하고, 이 과정을 모든 블록체인에 저장될 때까지 반복한다.

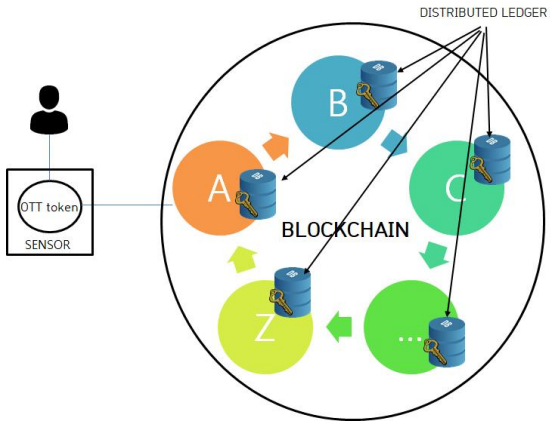

Fig. 3. Overview of proposed scheme

본 논문에서 제안하는 수식을 간단하고 명료하게 하기 위해 다음과 같은 기호를 정의한다.

Table 1. Notations

기호	설명
$\{X \rightarrow Y: M\}$	X sends the message M to Y
$X_H(Y)$	X hashes Y using a strong one-way hash function(H).
$A \| B$	concatenate A and B
$A \oplus B$	exclusive-or A and B
$A \overset{?}{=} B$	compare A with B
$U_H(RN_x)$	U sends the sufficiently long random number from a hash function results to a particular Block Chain.
$BC_H(RN_y)$	A particular Block Chain sends the sufficiently long random number from a hash function results to User Device.
$U_H(RN_x)'$	Block Chain receives the sufficiently long random number from a hash function results from User Device.
$BC_H(RN_y)'$	User Device receives the sufficiently long random number from a hash function results from a particular Block Chain.
U_{PK}	Public Key of User Device
U_{RK}	Private Key of User Device
BC_{PK}	Public Key of a particular Block Chain
BC_{RK}	Private Key of a particular Block Chain

다음은 사용자의 일회용 템플릿을 등록, 인증, 갱신하는 과정이다.

1.1 User registration and initialization step in distributed ledger of blockchain

$$\{U \rightarrow BC_1 : U_{PK}, REG_{req}\} \quad (1)$$

사용자 장치(U)는 블록체인 1(BC_1)에게 자신의 공개키와 함께 등록 요청을 한다.

$$\{BC_1 \rightarrow U : U_{PK}(T_0, K_0, BC_{1_H}(RN_{y_1}), BC_{1_{PK}})\} \quad (2)$$

BC_1은 충분히 긴 난수(RN_{y_1})를 생성하여 해쉬화하고, 바이오 정보 원본(Raw data)을 일회용 템플릿(One-Time Template: OTT)으로 변환하는 함수 생성에 관련 정보인 T_0, U와 BC_1과의 동기화를 위한 정보인 K_0, 그리고 BC_1의 공개키를 식 (1)에서 전송받은 U의 공개키로 암호화하여 등록을 하고자 하는 U에게 전송한다.

U는 BC_1로부터 전송받은 T_0와 K_0를 U_{RK}를 이용하여 복호화한 후 OTT 토큰(token)으로 저장한다.

$$\{U : OTT_G(Bio_T, T_0) \Rightarrow OTT_0\} \quad (3)$$

U는 바이오 정보 획득 장치를 이용하여 사용자의 바이오 정보 원본(Bio_T)을 획득하고, BC_1로부터 (2)에서 전송받은 T_0와 K_0를 이용하여 일회용 템플릿(OTT_0)을 생성한다.

U는 식 (3)을 수행한 후 일회용 템플릿을 생성하는 데 사용한 바이오 정보 원본을 즉시 삭제한다.

$$\{U \rightarrow BC_1 : BC_{1_{PK}}(RN_{x_1}, U_H(RN_{x_1}) \| BC_{1_H}(RN_{y_1})', U_{RK}(OTT_0))\} \quad (4)$$

U는 충분히 긴 난수(RN_{x_1})를 생성하여 해쉬화하고, 이를 식 (2)에서 전송받은 $BC_{1_H}(RN_{y_1})'$과 연결 연산(Concatenation)을 한다. U의 개인키로 암호화한 OTT_0와 RN_{x_1}을 식 (2)에서 전송받은 BC_1의 공개키인 $BC_{1_{PK}}$로 암호

화하여 BC_1로 전송한다.

OTT_0를 전송받은 BC_1은 자신의 개인키($BC_{1_{RK}}$)를 이용하여 복호화한 후 식 (4)에서 U로부터 전송받은 난수(RN_{x_1})와 자신이 U에게 전송한 난수(RN_{y_1})를 이용하여 BC_1은 식 (2)를 전송한 U가 맞는지 검증한다.

$$\{BC_1 \rightarrow U : OK \text{ or } NOK\} \quad (5)$$

검증 후 맞다면 BC_1는 U에게 등록이 성공했음을 알린다.

$$\{BC_1 \rightarrow BC_2 : BC_{1H}(BC_{1RK}(K_0, OTT_0))\} \quad (6)$$

이 후 BC_1은 OTT_0와 K_0를 자신의 개인키로 암호화하고 해쉬화하여 블록체인에서 자신과 연결된 다음 블록으로 전송한다. 다음 블록은 그 다음 블록으로 전송함으로써 블록체인 망 전체에 $BC_{1H}(BC_{1RK}(K_0, OTT_0))$가 저장되도록 한다.

1.2 User authentication

U는 식 (1) ~ (3)과 같은 방법을 이용하여 n번 째 OTT_n을 생성한다.

$$\{U \rightarrow BC_1 : BC_{1_{PK}}(U_{RK}(OTT_n), OTT_n)\} \quad (7)$$

U는 생성한 OTT_n 원본과 자신의 개인키(U_{RK})로 암호화한 OTT_n을 BC_1의 공개키($BC_{1_{PK}}$)로 암호화하여 전송한다.

이후 BC_1은 블록체인의 분산 원장에 저장되어 있는 OTT_n'과 U로부터 전송받은 OTT_n이 일치하는 지 확인하여 결과를 통보한다.

$$\left\{BC_1 : OTT_n \stackrel{?}{=} OTT_n'\right\} \quad (8)$$

$$\{BC_1 \rightarrow U : OK \text{ or } NOK\} \quad (9)$$

1.3 Onetime template update

U에는 입력 장치를 통해 바이오 정보를 획득하기 전까지는 사용자 등록 시 혹은 인증 시 사용 후 즉시 삭제하기 때문에 바이오 정보가 없다. 따라서 바이오 정보를 갱신하기 위해서는 K_n으로부터 생성된 변환함수 정보 T_n'과 이전에 인증에 사용된 템플릿 OTT_n으로부터 생성되고 이를 이용하여 새로운 일회용 템플릿을 갱신해야 한다. 현재 블록체인의 분산 원장에 저장되어 있는 것은 K_n과 OTT_n이고, 사용자 단말기의 OTT 토큰에는 T_n과 K_n이 저장되어 있다.

$$\{U \rightarrow BC_1 : U_{PK}, UPD_{req}\} \quad (10)$$

사용자 장치(U)는 블록체인 1(BC_1)에게 자신의 공개키와 함께 갱신 요청을 한다.

$$\{BC_1 \rightarrow U : U_{PK}(OTT_n, BC_{1_H}(K_n \| RN_{y_n}), RN_{y_n}, BC_{1_{PK}})\} \quad (11)$$

BC_1는 충분히 긴 난수(RN_{y_n})를 생성하여 U와 BC_1와의 동기화를 위한 정보인 K_n와 함께 해쉬화하고, BC_1의 공개키를 식 (10)에서 전송받은 U의 공개키로 암호화하여 갱신을 하고자 하는 U에게 전송한다.

$$\{U : U_H(K_n \oplus RN_{y_n}) \Rightarrow K_{n+1}\} \quad (12)$$

식 (11)을 수신한 U는 자신이 저장하고 있는 K_n과 식 (11)의 RN_{y_n}과 Exclusive-OR 연산을 하고 이에 대한 결과를 해쉬화한다. 결과는 K_{n+1}이 되고, 갱신된 OTT 토큰으로 저장한다.

$$\{U : K_n(T_n) \Rightarrow T_n'\} \quad (13)$$

U와 BC_1와의 동기화를 위한 정보인 K_n과 T_n을 이용하여 T_n'을 생성한다.

$$\{U : G(T_n, T_n') \Rightarrow T_{n+1}\} \quad (14)$$

바이오 정보를 일회용 템플릿으로 변환하는 함수 생성에 관련 정보인 T_n과 U와 BC_1와의 동기화를 위한 정보인 K_n과 T_n을 이용하여 생성한 T_n'을 이용하여 T_{n+1}을 생성한다. T_{n+1}은 갱신된 OTT 토큰으로 저장한다.

$$\{U : OTT_G(OTT_n, T_n') \Rightarrow OTT_{n+1}\} \quad (15)$$

U는 식 (7)에서 전송받은 OTT_n과 식 (13)에서 생성한 T_n'을 이용하여 OTT_{n+1}을 생성한다.

$$\{U \rightarrow BC_1 : BC_{1_{PK}}(RN_{x_n}, U_H(RN_{x_n}) \| BC_{1_H}(RN_{y_n})', K_{n+1}, OTT_{n+1})\} \quad (16)$$

U는 충분히 긴 난수(RN_{x_n})를 생성하여 해쉬화하고, 식 (11)에서 전송받은 RN_{y_n}을 해쉬화하여 연결 연산(Concatenation)을 한다. 식 (12)에서 생성한 K_{n+1}와 OTT_{n+1}, 그리고 연결 연산(Concatenation)한 결과를 $BC_{1_{PK}}$를 이용하여 암호화하여 BC_1에 전송한다. 이후에 BC_1은 식 (6)을 수행하여 블록체인의 분산 원장에 갱신된 내용이 저장되도록 한다.

IV. Security Analysis

보안 분석에서는 본 논문에서 제안하는 방법에 대해 상호 인증의 경우에 대해 안전하다는 것을 입증한다.

Table 2에서는 1.2절에서 설명한 FIDO[12], 1.3절에서 설명한 KFTC[13], FIDO에서 패스워드가 없는 인증 시스템을

제안한 방법[17], 그리고 모바일 장치를 이용하여 생체인식 정보를 획득하고, 비교하고, 저장하기 위한 기술 및 관리적 보안 지침으로써 인 인증 모델을 생체인식 정보 획득, 저장 및 비교의 주체 방식에 따라 12가지 모델을 제시한 ITU-T X.TAM[18]을 본 논문의 보안 특성과 비교한다. 본 논문에서 제안하는 방법은 비교하는 모든 분야에서 보안 요건을 충족함을 알 수 있다.

Table 2. Security property comparison

Security Property	KFTC [13]	J.J Kim [17]	FIDO [12]	ITU-T X.Tam [18]	This Paper
Prevention of Tamper	*No*	*Yes*	*No*	*No*	*Yes*
Prevention of Replay Attack	*partial*	*Yes*	*Yes*	*partial*	*Yes*
use a Certificate	*Yes*	*Yes*	*No*	*No*	*No*
Message Integrity	*Yes*	*Yes*	*partial*	*partial*	*Yes*
Prevention of MITM	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Table 2는 위·변조 방지, 재생 공격 방지, 인증서 사용 메시지 무결성, 중간자 공격 방지에 대해서 본 논문에서 제시하는 방법과 기존의 방법[12,13,17,18]과 비교하였다. 비교 결과 기존의 방법은 일부 항목에서 만족하지 못한 결과(No) 혹은 부분적으로 만족(Partial)하는 결과를 보였다. 그러나 본 논문에서 제시하는 방법은 모든 분야에서 충족함을 보였다.

1.1 Privacy protection

본 논문에서는 사용자의 개인정보(바이오정보)를 원본 데이터 그대로 사용하는 것이 아니라 사용 시마다 일회용 템플릿을 생성하여 사용한다. [11]과 같이 단일 서버에 일회용 템플릿을 저장하는 것이 아니라 블록체인에 암호화되어 저장되어 있기 때문에 해킹이 되더라도 블록체인에 분산 되어 있는 모든 원장을 수정하여야 하기 때문에 사실상 템플릿의 수정은 불가능하다.

또한 식(1)~(16)까지 어디에도 사용자의 개인키 혹은 바이오정보 원본을 전송하지 않기 때문에 전송도중 메시지가 유출되어도 파급효과는 극히 미비하다. 중간에 바이오정보가 유출이 되더라도 일회용 템플릿이므로 보안에 안전하다.

1.2 Replay attack prevention

공격자가 사용자 장치와 블록체인 사이에서 전송되는 $U_H(RN_x)$, $BC_H(RN_y)$, $U_H(RN_x)'$, $BC_H(RN_y)'$를 가로채더라도 사용자 장치, 사용자 장치와 연결된 특정 블록체인의 개인키를 알지 못하므로 재생공격이 불가능하다.

또한 인증 수단인 바이오정보는 일회용 템플릿을 사용하고 있기 때문에 재사용이 불가능하다.

1.3 Man-in-the-middle attack prevention

본 논문에서 제안하는 방식은 공격자가 사용자 장치와 특정 블록체인 사이에서 정보를 가로채더라도 사용자 인증 단계에서 특정 블록체인의 개인키를 알아야 하고 특정 블록체인의 개인키가 노출이 되어도 식 (8)과 같이 블록체인의 분산되어 있는 모든 원장과 비교하여야 하기 때문에 중간자 공격은 불가능하다. 또한 모든 메시지는 암호화와 해쉬화되어 전송되기 때문에 중간자 공격으로부터 안전하다.

1.4 Tamper-proof of transmitting data

사용자의 원본 바이오정보(Bio_T)는 식 (3)을 수행하고 사용자 단말기에서 바로 삭제하기 때문에 Bio_T는 전송되지 않기 때문에 공격자가 중간에 가로챌 수 없다. 식 (4)를 공격하기 위해서는 공격자는 BC_1의 개인키인 BC_{1RK}를 알아야 하고 또한 공격자가 OTT_n을 가로챈다 하더라도 사용자의 개인키 U_{RK}를 알 수 없다. OTT_n을 공격자의 개인키(A_{RK})로 암호화($A_{RK}(OTT_n')$)해서 전송한다 하더라도 식 (1)에서 전송받은 사용자의 공개키 U_{PK}로는 $A_{RK}(OTT_n')$를 복호화할 수 없다. 따라서, 공격자가 전송 중인 메시지를 중간에 가로챈다 하더라도 OTT_n을 위·변조 할 수 없다. 사용자 인증 및 일회용 템플릿 갱신 과정도 마찬가지이다.

V. Conclusions

본 논문에서는 블록체인 환경에서 일회용 템플릿을 사용하여 안전하게 개인정보를 저장하는 방법을 제안하였다. FIDO에서 제안하는 방법은 사용자 단말기에서 바이오정보를 저장하고 획득한 사용자 정보를 이용하여 적법한 사용자인지를 검증하였다. 그러나 본 논문에서 제안하는 방법은 사용자의 바이오정보를 사용하여 일회용 템플릿을 생성하고 이를 이용하여 블록체인에 저장된 바이오정보와 비교하여 적법한 사용자인지를 검증한다. 사용자 장치를 불법으로 탈취하여도 저장된 바이오정보가 없고, 블록체인을 해킹을 한다 하더라도 분산된 모든 원장의 일회용 템플릿을 수정하여야 하기 때문에 사실상 불가능하다.

본 논문에서 제시하는 방법은 보안 분석을 통해 기존의 방법에 비해 보안 특성이 우수하고, 여러 가지 공격에 대해 안전함을 보였다. 블록체인 구조는 가장 일반적인 구조인 공용형, 1개의 단체나 학교 또는 기업에서 적용 가능한 블록체인 구조인 개인형 그리고 은행 연합 및 상호 신뢰할 수 있는 여러 개의 단체 혹은 기관에 적용 가능한 구조인 컨소시엄형태로 나눌 수 있는데, 본 논문에서 제안하는 방법은 블록체인 중 컨소시엄형태(예를 들어 금융권, 글로벌 기업 등)에 적용 시 유용하다.

추후 연구과제로는 공용형 블록체인에서 일회용 템플릿을 일회용 키로 사용하여 개인 정보 혹은 민감한 정보를 보다 안전하게 보호하고 저장할 수 있는 방법에 대해서 연구할 계획이다.

REFERENCES

[1] S. J. Han, “A Robust Mutual Authentication between User Devices and Replaying Server(FIDO Server) using Certificate Authority in FIDO Environments.” Journal of The Korea Society of Computer and Information, The Korea Society of Computer and Information, vol. 21, no. 10, Oct,. 2016.

[2] Tiago Duarte et., al, “Biometric access control systems: A review on technologies to improve their efficiency,” Power Electronics and Motion Control Conference (PEMC), 2016 IEEE International, Varna, Bulgaria, pp.25-28, Sept,. 2016.

[3] A. Kaveh and W. H. Chung, “Temporal and spectral features of single lead ECG for human identification,” Biometric Measurements and Systems for Securityand Medical Applications (BIOMS), 2013 IEEE Workshop on IEEE, pp.17-21, Sept,. 2013.

[4] J. Wang, M. She, S. Nahavandi, and A. Kouzani, “Human identification from ECG signals via sparse representation of local segments,” Signal processing letters IEEE, Vol. 20, Issue 10, pp.937-940, June. 2013.

[5] S. K. Yeom, H. I. Suk, and S. W. Lee, “Person authentication from neural activity of face-specific visual self-representation.” Pattern recognition, Vol. 46, Issue 4, pp.1159-1169, April. 2013.

[6] K. Brigham and B. V. K. V. Kumar, “Subject identification from electroencephalogram (EEG) signals during imagined speech.” Biometrics: theory applications and systems (BTAS), 2010 Fourth IEEE international conference on. IEEE, pp.1-8, Sept,. 2010.

[7] Seoul National University Hospital, Domestic and overseas biological signal identification technology analysis and research DB construction, Technical Report, KISA, 25, Jan,. 2016.

[8] Jason Kim and Sam Lee, “Trend and prospect of telebiometric technology using biosignals,” Review of KIISC, Korea Institute of Information Security and Cryptology, vol. 26, no. 4, pp.41-46, Aug,. 2016.

[9] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Consulted, 1(2012):28, 2008.

[10] Akabane Yoshiharu et., al, Block Chain Structure and Theory, Wikibooks, 2017.

[11] TTA, “Biometric Authentication Framework based on One-Time Template,” TTA Standard, TTAK.KO-12. 0098, 19 Dec,. 2008.

[12] Fido Alliance, https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.pdf

[13] Korea Financial Telecommunications & Clearings Institute, “Standard for distributed management of biometrics,” Korea Financial Telecommunications & Clearings Institute, June. 2015.

[14] Digital Times, http://www.dt.co.kr/contents.html?article_no=2017072702101360053001

[15] Youngdeok Seo et., al, “The implementation of secure decentralized storage system using Bitcoin Blockchain,” Korea Computer Congress 2016, pp.1148-1150, June. 2016.

[16] Masayuki Fukumitsu et., al, “A Proposal of a Secure P2P-type Storage Scheme by using the Secret Sharing and the Blockchain,” 2017 IEEE 31st International Conference on Advanced Information Networking and Applications, Taipei, Taiwan, pp.803-810, 27th-29th March. 2017.

[17] Jaejung Kim, "Study on the password-free certification system using the FIDO (Fast IDentity Online)," Communications of the Korea Information Science Society, KIISE, vol. 33, no. 5, May. 2015.

[18] ITU-T SG17 WG5 Q9, http://www.itu.int/itu-t/workprog/wp_item.aspx?isn=9429

Authors

Seungjin Han received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Inha University, Korea, in 1989, 1992 and 2004, respectively. Dr. Han joined the faculty of the Department of e-Business at Kyung-In Women's University, Incheon, Korea, in 2004. He is currently a Associate Professor in the Department of Business Administration, Kyung-In Women's University. He worked for Research Center of Daewoo Telecommunication as a TDX software developer from Jan. 1992 to Jun. 1996, and National Information Society Agency(NIA) as project manager from Jun. 1996 to Jul. and SKTelecom as project manager from Jul. 1996 to Jan. 1998. He was a lecturer of Inha University from Mar. 2002 to Feb. 2004. He is interested in computer network and security.

His research has always been in the area of MANET and Sensor Networks or technologies which relate to it, such as Security, Protocol and Routing in MANET and USN, Middleware in USN and Security using Biometric Systems.