ISSN 2586-1816
Journal of Convergence for Information Technology e-ISSN 2586-4440
Vol. 8. No. 3, pp. 85-90, 2018 DOI : https://doi.org/10.22156/CS4SMB.2018.8.3.085

블록체인을 이용한 생체정보와 OTP 기반의 안전한 인증 기법

문형진
성결대학교 정보통신공학부

Biometric Information and OTP based on Authentication Mechanism using Blockchain

Hyung-Jin Mun
Department of Information & Communication Engineering, Sungkyul University

요 약 블록체인 기술은 분산된 신뢰구조를 제공하고, 위변조가 불가능한 시스템 구현이 가능하고, Smart Contract 등 이 가능하면서 인터넷 차세대 보안 기술로 발전하고 있다. 블록체인 기술이 차세대 보안기술로 부각되면서 무결성 뿐만 아니라 인증을 비롯하여 다양한 보안 서비스에 대한 연구가 진행되고 있다. 인터넷 기반의 다양한 서비스는 패스워드 기반의 사용자 인증으로 이루어지고 있지만 클라이언트나 네트워크에서 가로채기가 가능하고, 패스워드 정보가 저장된 서버가 해킹의 위험에 노출되어 있다. 따라서 무결성을 보장할 수 있는 블록체인 기반 기술과 OTP 기반의 안전한 인증 기법을 제안한다. 특히, 이중 인증(Two-Factor Authentication) 은 OTP 기반의 인증과 사용자가 가지고 있는 생체인증의 결합으로 패스워드 없이 안전한 인증이 가능하다. 제안기법은 인증에 필요한 생체정보를 식별할 수 없도록 다중 해시함수를 적용하여 트랜잭션을 생성하여 블록에 담기 때문에 서버로부터 분리되어 서버 공격에 안전하다.

주제어 : 블록체인, 사용자인증, 생체정보, OTP, 이중 인증

Abstract Blockchain technology provides distributed trust structure; with this, we can implement a system that cannot be forged and make Smart Contract possible. With blockchain technology emerging as next generation security technology, there have been studies on authentication and security services that ensure integrity. Although Internet-based services have been going with user authentication with password, the information can be stolen through a client and a network and the server is exposed to hacking. For the reason, we suggest blockchain technology and OTP based authentication mechanism to ensure integrity. In particular, the Two-Factor Authentication is able to ensure secure authentication by combining OTP authentication and biometric authentication without using password. As the suggested authentication applies multiple hash functions and generates transactions to be placed in blocks in order for biometric information not to be identified, it is protected from server attacks by being separate from the server.

Key Words : Blockchain, User Authentication, Biometric, OTP, Two-Factor Authentication

1. 서론

ICT의 발달로 인해 다양한 서비스가 인터넷을 기반으로 제공되고 있다. 특히 스마트 폰의 하드웨어 발전과 사용자의 급증으로 인해 다양한 서비스가 인터넷을 통해 가능하게 되었다. 사용자가 인터넷 서비스를 받기 위해 합법적인 사용자임을 증명할 필요하다. 사용자 인증을 위해 패스워드나 보안카드 등 OTP을 이용하여 합법적인

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received May 30, 2018 Revised June 12, 2018
Accepted June 20, 2018 Published June 30, 2018

사용자여부를 확인한다.

하지만 다양한 인터넷 서비스에서 아이디/패스워드 기반의 인증이지만 안전하지 않은 채널을 통해 아이디/패스워드 탈취 가능성이 높다. 암호화폐에 대한 수요가 급증하면서 기반 기술인 블록체인 기술에 대해 많은 관심을 갖고 있다. 블록체인 기술을 통해 분산된 신뢰구조를 제공하고, 무결성을 기반으로 위변조가 불가능한 시스템 구현이 가능하다. 블록체인 기술을 활용한 분야로 암호화폐, Smart Contract, 보안 및 기록유지가 가능하여 차세대 인터넷 기술로 발전하고 있다[1,2].

보안이 고려되지 않는 인터넷 기술이 블록체인 기술과 접목하면서 데이터의 무결성을 비롯한 보안 서비스가 적용되는 인터넷 생태계로 변화시켜줄 시대가 도래하고 있다. 블록체인 기술은 트랜잭션을 암호화 기술로 보호하고 블록에 담아 체인으로 연결되어 분산 저장하고 짧은 시간에 계속적으로 블록을 생성하는 방식으로 공격자가 공격에 필요한 시간과 자원을 확보할 수 없게 되므로 안전성을 보장 받는다. 특히, 블록체인 기술을 통해 분산 저장되므로 데이터의 무결성이 보장되어 위변조의 위험을 원천적으로 차단할 수 있는 기술이다. 블록체인 기술을 활용하여 사용자 인증에 필요한 정보를 블록에 담아 무결성을 보장받고, 인증정보를 누구도 볼 수 없게 다중으로 해시값 형태로 저장함으로써 블록체인 시대에 맞는 사용자 인증 매커니즘을 제안하고자 한다. 제안 모델을 통해 중요한 인증정보가 서버의 DB에 저장되지 않으므로 DB관리자에 의한 유출 및 정보 오남용이나 해킹된 회원테이블의 rainbow table 공격으로부터 보호를 받을 수 있다[3,4].

본 논문은 다음과 같이 구성된다. 2장에서는 블록체인의 블록을 소개하고, 패스워드 기반의 인증과 커버로스 인증시스템의 개념을 소개하고, 3장에서는 이중 인증과 OTP 기반의 사용자 인증 기법에 대해 설명하고, 4장에서는 블록체인 기술을 활용하여 패스워드 기반 이중 인증과 OTP 기반 이중인증을 제안하고, 제안기법에 대한 평가를 실시하고, 마지막으로 5장에서는 결론과 향후 연구를 기술한다.

2. 관련연구

2.1 블록체인의 블록 구조

블록체인 기술의 기본이 되는 블록은 Table 1과 같이 4개의 논리적 구성요소를 가진다[5]. 블록의 크기는 215byte~1Mbyte 이다. 블록의 헤더에는 6가지의 정보로 구성되어 블록의 모든 정보와 모든 트랜잭션의 요약정보가 담겨있다. 특히, 블록의 헤더에는 이전 블록의 해시값을 저장하고 있고, 현재 블록이 이전블록을 참고하고, 그 이전 블록은 그 이전 블록을 참조하는 체인으로 형성되어 있다. 또한 머클트리 루트는 모든 트랜잭션의 정보를 32byte로 요약된 정보이다. 머클트리 루트를 통해 2,000~3,000개의 트랜잭션 중에 하나라도 변조될 경우 바로 탐지가 가능하다. 블록은 주어진 난이도에 맞는 문제를 푼 노드에게 블록생성권한을 부여하기 때문에 헤더에 블록을 만들어진 시간과 난이도 정보가 담겨 있다. 세 번째는 트랜잭션의 개수가 가변적인 길이로 작성이 되고, 네 번째는 모든 거래내역이 트랜잭션의 형태로 작성되어 있다. 블록을 생성한 노드에게 수수료를 주기 때문에 최대한 많은 트랜잭션을 담아 블록을 생성한다.

Table 1. Structure of Block

size of block (4byte)
header of block (80byte) Version, PreviousHash, MerkHash, Time, Bits, Nonce
count of transaction (1~9 byte)
content of transaction (the rest)

2.2 패스워드 기반 인증 기법

인터넷 서비스를 제공하기 위해서는 사용자가 정당한 사용자인지를 확인하는 사용자 인증이 필요하다. 대부분의 서비스에서 사용자 인증으로 편리성 때문에 아이디/패스워드 기반 인증을 사용하고 있다. 패스워드 인증 기법은 Fig. 1과 같이 웹브라우저 등을 통해 사용자가 아이디와 패스워드를 입력하면 패스워드의 해시값을 서버에 전달하고, 전달된 해시값이 등록 당시에 제공한 패스워드의 해시값과 비교하여 검증하는 방식이다[6].

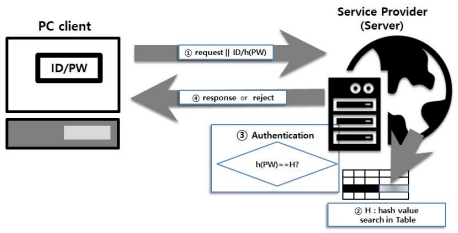


Fig. 1. Password based Authentication Method

패스워드 기반 인증의 안전성은 패스워드가 저장된 DB 보안의 안전성에 달려 있다. 내부자와 연계된 공격자가 회원정보가 담겨있는 DB 테이블을 유출하여 사용자의 패스워드를 알아내는 사례가 있다. DB 테이블의 유출로부터 안전하게 패스워드를 보호하기 위해 사용자가 등록한 패스워드를 그대로 저장하는 것이 아니라 입력된 패스워드를 일방향 함수인 해시함수의 결과값을 DB에 저장한다. 128비트의 해시값을 생성하는 MD5 의 충돌 가능성 등 취약점이 발생하여 SHA-256 이나 SHA-512 등 안전한 해시함수로 대체되고 있다. 하지만 패스워드를 안전한 해시값으로 교체해서 저장해도 사용자의 입력할때 공격이 여전히 가능하다. 즉 사용자가 패스워드를 입력할 때 어깨넘어로 훔쳐보기나 구글 글래스 등으로 패스워드를 입력할때 녹화할 수 있다. 뿐만 아니라 사용자 정보를 기반으로 하는 사회공학적 공격이나 패스워드 무작위 대입 공격도 가능하다. 패스워드가 저장된 회원정보 테이블이 유출될 경우 사전에 생성한 해시값을 이용한 Rainbow Table 공격으로 사용자의 패스워드를 유출할 수 있다[3,4]. 편리성을 가장하다보니 패스워드가 단순하거나 패스워드 길이가 짧아 무작위 대입 공격이나 Rainbow Table 공격이 가능해져서 일정한 횟수만큼만 패스워드를 입력하도록 제한하거나 패스워드를 등록할 때 복잡하고 길이가 긴 패스워드만 등록이 가능하도록 시스템에서 제한을 하고 있다.

최근에는 사용자의 스마트 폰을 이용한 SMS 인증이나 OTP 인증을 요구하거나 포털이나 다른 웹사이트 계정정보를 이용하여 대신 인증하거나 공인인증서 또는 IPin 등을 통해서 인증하는 시스템으로 발전하고 있다.

2.3 커버로스 인증

커버로스 인증은 MIT에서 Project Athena 팀에 의해 개발된 분산환경에서 인증 서비스로 제 3의 인증서버를 이용해 사용자 간의 인증을 한다. 분산환경에서 사용자가 분산된 서버에 서비스를 요청할 때마다 인증을 요구한다. 신분의 확인을 커버로스 내의 인증서버를 통해서 인증을 하고, 인증결과로 티켓을 발급한다. 커버로스 시스템은 인증 서버(AS:AuthenticationServer)와 티켓 승인 서버(TGS:TicketGrantingServer)로 구성되어 있다. 커버로스 인증은 사용자가 클라이언트를 통해 커버로스 서버에 접근할 때 사용자의 계정을 요구한다. 사용자의 ID와 패스워드, 서버의 ID를 서버에 전달한다. 서버에서는 정당한 사용자인지 확인 후 서비스 서버에 접근할 수 있는 서비스 티켓을 TGS에서 발급하여 클라이언트에 제공한다. 발급된 티켓은 사용자의 ID, 사용자의 네트워크 주소, 서비스 서버의 ID를 세션키로 암호화하여 생성된다. 세션키는 인증서버와 서비스 서버간에 설정된 대칭키라서 티켓의 내용은 인증서버와 서비스 서버만이 복호화할 수 있기 때문에 공격자 뿐만 아니라 사용자도 내용을 보거나 변조할 수 없다. 서비스 서버는 티켓을 복호화하여 사용자 ID와 네트워크 주소로 사용자를 확인하고, 서비스 서버의 ID를 확인한 후 서비스를 제공한다[7].

커버로스 인증의 장점으로 네트워크 상에서 티켓을 사용하므로써 클라이언트와 서비스 서버사이에서 전달되는 패스워드가 없고, 티켓을 기반하기 때문에 스푸핑을 방지할 수 있다. 상호 인증의 장점을 가지고 있지만 사용자가 인증서버의 정당한 사용자로 한번의 인증만 요구되고, 또한 인증할 때 패스워드 기반으로 인증하기 때문에 공개된 네트워크에서 취약점이 존재한다.

3. OTP 기반 이중 인증기법

3.1 이중 인증

이중 인증(two-factor authentication)는 사용자가 아는 요소(1단계)와 사용자가 가지고 있는 요소(2단계)를 이용하여 인증하는 방식이다. 서비스에 접근하려면 사용자는 두 가지 요소를 모두 가지고 있어야 한다. 요청/응답 프로세스에서 인증을 할 때 사용자임을 증명할 수 있는 시스템이 요구하는 개인 정보를 가질 때 인증이 완료된다[8].

안전이 요구되는 서비스에서는 이중 인증을 사용하고 있다. 1단계 인증으로 아이디와 패스워드와 같이 자신이 아는 요소를 사용하고, 2단계 인증으로 SMS나 OTP 또는 보안 카드와 같이 가지고 있는 요소를 활용하여 사용자 인증을 사용하고 있다. 안전하지 않는 채널을 통해 1단계의 패스워드가 노출되더라도 사용자가 소지하고 있는 요소를 분실하지 않는 다면 2단계 인증을 해결 할 수 없어 기술적인 측면에서 안전하다.

3.2 OTP 이용한 이중 인증

Fig. 2와 같이 모바일 단말기를 이용한 이중 인증을 통해 사용자의 계정과 단말기의 실시간으로 동적인 정보를

이용하여 인증을 수행한다. 사용자는 서비스 제공자의 서버로 ID/PW를 입력하면 서버는 OTP 모듈을 이용하여 OTP(One-Time Password)를 생성하고, 이를 등록된 폰으로 SMS 형태로 송신하면 사용자는 수신된 OTP를 서버에 전달하여 폰 소유를 검증한다. OTP 모듈을 앱의 형태로 설치된 모바일 단말기나 OTP 기기를 통해 OTP를 생성하여 서버에 전달하여 동기화된 OTP와 비교하여 검증한다. 이는 OTP 모듈을 가진 기기 소유를 검증한다. 폰이나 OTP 기기와 같이 물리적 매체를 분실한 경우 이중 인증에 위협이 가능하다[9-11].

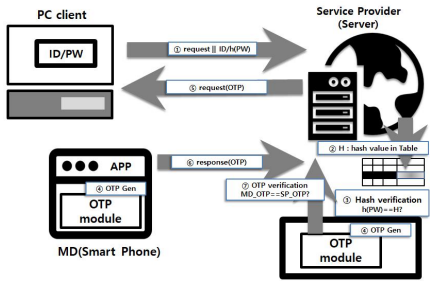


Fig. 2. OTP based Authentication Method

4. 제안기법

4.1 블록체인을 이용한 생체정보 이중 인증

사용자 인증을 위해 패스워드나 사용자의 비밀정보를 서버 대신에 블록체인에 저장하여 사용자 인증을 위한 비밀정보의 위변조를 방지 할 수 있고, 중앙관리시스템에서 벗어날 수 있는 새로운 인증 모델을 제안한다.

최근 스마트 폰의 사양이 좋아지면서 지문이나 홍채 등 사용자의 생체정보를 채취가 가능하다[11-13]. 스마트 폰의 지문이나 홍채 정보를 이용하여 스마트 폰의 사용을 위한 인증이나 카드 사용시 인증에 활용된다. Fig. 3은 블록체인의 블록에 익명화된 생체정보를 삽입하고, 사용자 인증을 할 때 해당 생체정보를 이용하여 정당한 사용자인지를 확인하는 과정을 보여주고 있다.

사용자는 서비스 제공자인 서버에 패스워드 기반으로 인증을 하고, 서버에서는 사용자의 스마트 폰을 통해 생체정보를 요청하여 해시값을 생성한다. 생체정보를 해시값을 생성하고, 블록체인에서 해당 블록을 검색하여 블록에 있는 해시값을 요청하여 그 해시값을 비교하여 검증을 완료하다.

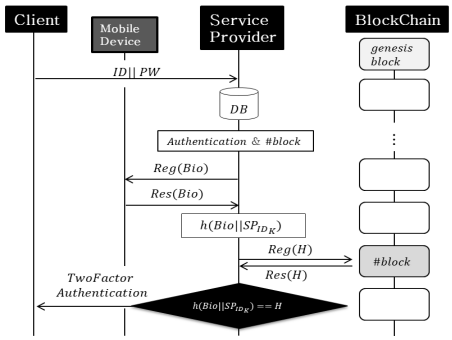


Fig. 3. Bio-Information based Authentication Model Using Two-Factor Authentication

Fig. 3는 사용자가 서비스를 제공하는 서버에 아이디/패스워드를 입력하면 서버에 저장된 DB에서 아이디를 검색하고, 패스워드로 인증한다. 해당 아이디로 생체정보가 저장된 블록을 확인한다. 서버는 사용자로 하여금 생체정보를 요구하면 사용자는 모바일 단말기를 통해 지문이나 홍채 등의 생체정보를 제공하고, 서버에서 생체정보와 사용자, 서비스 등의 정보로 해시값을 생성한다. 블록체인에서 생체정보가 저장된 블록을 찾아 해시값과 사용자로부터 받은 정보를 기반으로 생성한 해시값을 비교한다. 해시값이 같으면 인증이 완료된다.

사용자의 생체정보를 측정하기 위해 스마트 폰을 이용하여 홍채나 지문 등을 수집하여 그 정보를 알 수 없도록 해시함수를 통해 사용자의 정보의 내용을 확인할 수 없도록 한다. 이 정보가 노출되더라도 해시함수로 인해 해당 정보를 확인할 수 없고, 오직 서버에서 해당 정보에 대한 식별할 수 있도록 익명성을 보장하는 기법이다.

4.2 제안기법의 검증 및 평가

제안기법은 사용자 검증을 위해 최소한의 정보를 서버의 DB에 저장하고, 블록체인의 블록으로부터 생체인증정보의 해시값과 비교 검증하여 인증을 수행한다.

Fig. 4는 서비스 제공자 서버의 Table 구조의 일부를 보여주고 있다. 서버는 사용자의 아이디인 hong을 DB에서 식별하고 패스워드가 맞는 지 인증을 한 후에 블록 번호인 해시값을 확인하다. 블록 번호는 hong의 생체정보가 저장된 블록으로 생체정보는 ID와 서비스 제공자(SP)의 식별자, 난수(N) 등에 대한 해시값을 생성하여 익명처리를 한다. 서비스 제공자만이 익명화된 생체정보를 조회할 수 있다.

no	ID	IDpadding	h(PW)	blockHash	txid	TimeStamp
101	hong	hong#0512	h(pw1)	bHash1	txid1	N1

Fg. 4. Member table in the Service Provider

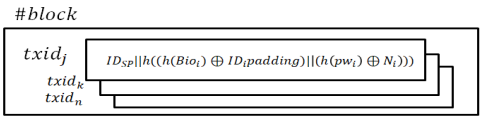
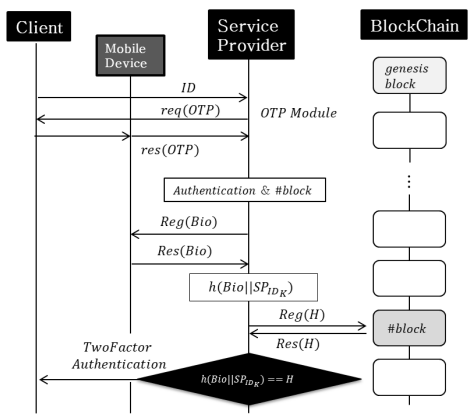


Fig. 5. j-th transaction contents in block

Fig. 5와 같이 생체정보는 해시값의 형태로 블록의 트랜잭션 안에 저장되어 있다. 서비스 제공자는 생체정보를 서버의 식별정보와 난수 등과 함께 서비스 제공자의 개인키로 암호화하여 트랜잭션을 생성하여 블록에 등록하는 방식으로 블록체인에 연결한다. 이를 통해 사용자의 생체정보는 분산된 저장공간을 사용할 수 있다. 3장에서 언급한 것과 같이 패스워드가 아닌 OTP를 이용하여 1단계 인증을 하고, 사용자의 생체정보를 2단계 인증으로 사용할 수 있다. Fig. 6은 패스워드 기반이 아닌 OTP 기반으로 인증하는 과정을 보여주고 있다.



Fg. 6. Authentication process using OTP and biometrics

제안 모델은 OTP 와 생체정보를 결합한 새로운 인증 모델로 패스워드 기반의 인증보다 안전성이 보장된다. 특히, OTP와 생체정보는 사용자가 가지고 있는 스마트폰을 이용하여 인증하므로써 저장된 패스워드 유출로 인해 공격이 어렵다. 특히, 생체정보가 안전한 해시값을 이용하므로 무결성을 보증하고, 사용자의 폰의 소유를 기반으로 한 기밀성을 보증한다.

제안기법은 3가지 측면에서 장점을 가진다.

첫 번째 생체인증정보가 블록에 담겨져 있어 분산 저장되어 누구나 접근이 가능하지만 하지만 서비스 제공자의 확인 없이는 누구의 소유인지를 확인하기 어렵다.

두 번째 서비스 제공자의 서버가 생체인증정보를 가지지 않는다. 인증관련 정보를 가직고 있지 않기 때문에 공격자로부터의 공격을 회피할 수 있다.

세 번째 기존기법은 사용자가 패스워드를 주기적으로 변경해야 하는 단점이 있지만 제안기법에서 서비스 제공자에 의해 블록에 저장된 생체인증정보를 주기적인 변경이 가능하다.

5. 결론

많은 웹사이트나 시스템 접근시 사용자를 인증하고 있다. 대부분 아이디는 이메일로 사용되어 패스워드만 알게 되면 해당 시스템에 인증이 가능하며 다양한 공격에 취약하다. 인터넷 서비스를 이용하여 위해 패스워드 기반으로 인증을 하지만 공개된 환경이라 취약점이 많다. 이 취약점을 보완하기 위해 OTP와 모바일 단말기를 인용한 생체정보를 기반으로 블록체인 기술을 활용한 새로운 인증모델을 제안하였다.

최근 차세대 기술로 블록체인기술 관련 산업이 급격한 성장을 하고 있다. 블록체인 기술은 거래내역을 해시값과 서명을 통해 블록에 담아 블록을 생성하는 저장하는 기술이다. 블록체인 기술은 비트코인의 1세대에서 이더리움의 2세대, 이오스 등으로 이어지는 3세대까지 발전하고 있다. 블록체인 기술을 통해 데이터를 중앙 집중화 하지 않고 데이터를 분산 저장하는 기술로 대두되고 있다. 특히, 분산 저장되고 위변조가 불가능하고, 정보의 익명화까지 제공하고 있다.

사용자 대부분이 사용하고, 휴대하고 있는 모바일 단말기를 통해 사용자의 생체정보를 쉽게 습득하고, 이를 기반으로 이중 인증이 가능한 모델을 제시하였다.

서비스 제공자에 저장된 정보는 사용자의 생체정보와 같은 민감한 정보는 저장하지 않고, 익명성이 보장된 블록내의 트랜잭션에 있는 정보의 소유자를 확인하는 수단으로 활용된다.

향후 연구로는 서버에 저장된 블록의 번호 등의 기존 인증시스템보다 안전한 정보를 보호할 필요가 있다. 또한, 블록에 저장된 다중 해시된 생체정보에 대한 안전성 평가에 대한 연구가 필요하다.

REFERENCES

[1] J. H. Yang. (2018). A Study on the Effect of Block Chain Application and Legal Issue in Logistics Industry. *Journal of Convergence for Information Technology, 8(1)*, 187-199.
DOI : 10.22156/CS4SMB.2018.8.1.187

[2] D. Y. Lee, J. W. Park, J. H. Lee, S. R. Lee & S. Y. Park. (2017). Blockchain Core Technology and Domestic and Foreign Trends. *Communications of the Korean Institute of Information Scientists and Engineers, 35(6),* 22-28.

[3] H. J. Mun & S. Oh. (2016). Injecting subject policy into access control for strengthening the protection of personal information. *Wireless Personal Communications*, 89(3), 715-728.
DOI : 10.1007/s11277-015-3094-7

[4] H. J. Mun, S. H. Hong & J. P. Shin. (2017). A novel secure and efficient hash function with extra padding against rainbow table attacks. *Cluster Computing*, 1-13.
DOI : 10.1007/s10586-017-0886-4

[5] S. H. Hong & S. H. Park. (2017). The Research on Blockchain-based Secure IoT Authentication. *Journal of the Korea Convergence Society, 8(11),* 57-62.
DOI : 10.15207/JKCS.2017.8.11.057

[6] H. J. Mun & K. Y. Jin, (2017) Empowering Information Subject to Control Information Use to Protect Personal Information, *Indian Journal of Forensic Medicine & Toxicology. 11(2),* 530-534.
DOI : 10.5958/0973-9130.2017.00181.5

[7] W. Stallings (1988). Cryptography and Network Security. UK : Pearson Education

[8] C. T. Li, C. Y. Weng & C. Fan. (2012). Two-Factor User Authentication in Multi-Server Networks. *International Journal of Security and Its Applications, 6(2)*, 261-268.

[9] Namu. (2018). *OTP*. Namu. https://namu.wiki/w/OTP

[10] Y. S. Jeong, S. H. Han & S. S. Shin. (2012). A Study on Mobile OTP Generation Model. *Journal of Digital Convergence, 10(2),* 183-191.

[11] W. J. Jang & H. W. Lee. (2010). Biometric One-Time Password Generation Mechanism and its Application on SIP Authentication. *Journal of the Korea Convergence Society*, *1(1)*, 93-100.

[12] K. H. Lee. (2013). A Study of Authentication Scheme using Biometric-Based Effectiveness Analysis in Mobile Devices. *Journal of Digital Convergence, 11(11),* 795-801.
DOI : 10.14400/jdpm.2013.11.11.795

[13] S. H. Yun. (2017). The Biometric Authentication Scheme Capable of Multilevel Security Control. *Journal of the Korea Convergence Society, 8(2)*, 9-14.
DOI : 10.15207/JKCS.2017.8.2.009

문 형 진(Mun, Hyung Jin) [종신회원]

- 2002년 2월 : 충남대학교 수학과 (이학석사)
- 2008년 2월 : 충북대학교 전자계산학(이학박사)
- 2009년 3월 ~ 2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신공학부 조교수, 부교수
- 2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수
- 관심분야 : 정보보안, 암호학, 프라이버시보호, 블록체인
- E-Mail : jinmun@gmail.com