벤처혁신연구 제2권 제2호(통권4호) http:www.kavi.or.kr
Journal of Venture Innovation, Vol.2. No.2, December. 2019, pp.21-29

DID를 사용한 인증서 암호 복구

김형욱(한국전자인증)[1] 김상진(청운대학교 학부)[2] 김태진(청운대학교 학부)[3] 유형근(청운대학교 학부)[4]

국 문 요 약

한국에서 흔히 사용하는 공인인증서 기술에서 사용자들은 그 비밀번호를 기억하지 못했을때 항상 다시 설정해야하는 번거로운 문제점을 지니고 있다. 본 논문에서는 이 문제점에 대한 해결책으로 분산저장을 위한 블록체인과 PKI, DID를 활용하여 안전한 공인인증서 암호 복구 프로토콜을 제안한다. DID는 블록체인 시스템에서 블록 ID를 보호하기 위한 스키마이다. PKI에서 사용되는 개인키를 사용자의 생체인식, 예를 들어 지문으로 하여 복잡한 개인키를 기억하는 것을 완벽히 대체할 수 있도록 구성한다.

이를 위해, 현재 대부분의 사용자들이 이용하는 스마트폰에 탑재된 FIDO 인증 기술을 기반으로 블록 내부 데이터에 접근하기 위해 사용자를 인증하는 과정을 거쳐 공격자가 데이터를 탈취하는 위험성을 최소화 한다.

■ 중심어: Block-chain, DID(Decentralized Identifier), PKI, FIDO

Ⅰ. 서 론

현재 한국에서만 사용하는 공인인증서는 그 비밀번호를 기억하지 못하거나 분실했을 경우 재발급 외에는 방법이 없다. 공인인증서는 공개키기반구조(이하 PKI)의 기술을 사용하고 있으며 미국 국가안보국(NSA)이나 미국 국립표준기술연구소(NIST)로부터 최고 수준의 보안 등급을 인정받았으나 공인인증서가 존재하는 별도의 USB나 핸드폰 혹은 PC와 공인인증서의 비밀번호가 해킹당하면 그대로 정보를 보호함에 위협을 받을 수밖에 없다. 본 논문은 구조적인 한계에서 찾아오는 보안 위협을 해결하기 위해 지문을 이용한 개인 데이터를 저장하고 D.I.D(Decentralized Identify)를 사용해 지문 지문데이터를 분산시켜 비밀번호 복구가 필요할 경우 데이터를 검증하고 정상적인복구를 진행할 수 있는 프로세스를 제안한다.

Ⅱ. 관련 연구

1)저자: 숭실대학교 컴퓨터학과 공학박사, do3196@naver.com
2)공동저자: 청운대학교 졸업예정, kespanate@gmail.com
3)공동저자: 청운대학교 졸업예정, kimtj319@naver.com
4)공동저자: 청운대학교 졸업예정, kjhgfd6702@naver.com
· 투고일: 2019-10-18 · 수정일: 2019-11-22 · 게재확정일: 2019-12-16

2.1 PKI

PKI 공인인증서는 기본적으로 PKI 방식을 사용한다. 공개키 암호화는 암호화가 필요한 컴퓨터 분야의 거의 모든 곳에서 사용된다. PKI는 이런 개인 키-공개 키를 보다 효율적으로 관리할 수 있게 하는 환경이다. 이해를 돕기 위해 간단한 예시를 들겠다.

첫째. 앨리스는 공개 키와 개인 키를 발급받고 싶어 한다. PKI 환경은 앨리스에게 공개키 쌍을 만들어 줄 수 있다.

둘째. 앨리스가 공 키를 사용하려 할 때, 앨리스는 그 공개 키에 맞는 개인 키를 가진 사람이 누구인지알고 싶어 한다. 이 경우 PKI 환경은 공개 키의 주인이 누군지 쉽게 알 방법을 제공한다.

셋째. 앨리스는 밥이 보낸 메시지의 서명을 인증하기 위해, 또는 밥의 공개 키를 사용하여 메시지를 암호화 한 후 밥에게 보내기 위해서 앨리스는 밥의 공개 키를 알고 싶어 한다. 이것을 PKI 환경이 제공한다.

넷째. 앨리스가 밥의 공개 키를 얻었지만, 그 공개 키가 정말 밥의 것인지 알고 싶어 한다. PKI 환경은 공개 키와 키의 주인을 인증할 수 있게 한다.

이상의 설명을 통한 PKI의 구조를 사용하여 공인인증서를 구성한다.

2.2 DID(Decentralized Identifier)

DID(Decentralized Identifier)는 블록체인에서 ID를 보호하기 위한 소프트웨어 스키마이다. 기본적으로 DID는 ID를 분산화한 후 사용자의 제어 하에 둔다. 다시 말해 신원 관리 지갑에서 공개 키와 개인 키를 기반으로 신뢰성 있는 기관에 신원 증명을 신청한 후, 개인에게 발행된 디지털 ID가 분산 원장에 쓰임으로써 생성된다. 이 DID의 가장 큰 특징은 자기 주권형 신원 증명이라는 것이다. 이용자 개인의 지갑에서 분산 ID를 신청하고 블록에 기록되면 DID의 고유성을 통해 자신의 ID가 신뢰성을 갖고 있다는 사실이 모든 사람에게 공개된다. 따라서 외부인들은 지갑보유자에게 일단 공개키 정보가 포함된 DID의 확인을 요구할 수 있고, 지갑보유자는 개인키를 이용해 자신을 증명할 수 있다. 요약하면 DID의 특징은 외부환경의 변화와 관계없이 개인의 지갑을 기반으로, 언제든지 선택적으로 자신의 개인정보를 스스로 관리하고, 제공할 수 있고, 보호할 수 있다는 것이다.

2.3 블록체인

블록체인 기술은 네트워크 내 모든 참여자가 거래 정보를 공유, 검증 기록할 수 있는 기술이며, 거래 정보가 기록되는 거래 장부는 네트워크에 참여하는 모든 참여자에게 분산 저장되기 때문에 참여자가 모두 해킹되지 않는 이상 조작이 불가능하다. 공유되는 거래 정보의 유형도 일반적인 데이터 형식과 특정한 기능을 수행하도록 프로그래밍된 스마트 컨트랙트(Smart contract)가 있다. 스마트 컨트랙트는 블록체인 네트워크 참여자가 동시에 동일한 코드를 실행하고 결과를 검증하여 모두 동일한 경우에만 그 결과를 블록체인의 장부에 기록하거나 수정할 수 있도록 설계할 수 있는 프로그램이다. 공인된 제3의 기관을 이용하지 않아도 블록체인 네트워크에 참여하는 모든 참여자가 스마트 컨트랙트를 통해서 기록되는 정보를 신뢰할 수 있다. 이러한 블록체인 특성을 이용하여 지문정보를 클라이언트들 간에 공유를 할 수있다면 비밀번호 분실시 기관을 찾아가 비밀번호를 복구하지 않고도 사용자 지문을 이용하여 안전하게 비밀번호를 복구할 수 있다. 이로인하여 사용자는 기관을 찾아가 인증서를 재발급 받고 재설정 해야되는 번거로움이 사라지게 된다.

2.4 생체인식

FIDO 인증 기술은 현재 사용자가 인증서 등과 같은인증 수단을 소지하고, 패스워드와 같은 암호를 외우는데서 발생하는 보안상의 문제점을 극복하고자 개발되었다. FIDO 인증 기술은 UAF 방식과 U2F방식을 제공한다. UAF 인증 방식은 기존의 ID/Password 인증 방식보다 보안이 강화된 개인의 생체 정보를 활용하는 표준이며, U2F는 ID/Password 인증 방식에 별도의 인증 장치를 추가적으로 사용하는 방식이다. UAF 프로토콜은 사용자가 가지고 있는 디바이스에서온라인 서비스와 연동하여 인증하는 기술이다. FIDOUAF 프로토콜에서는 사용자 디바이스를 이용하여 생체정보를 인식하게 되면 FIDO 서버에 접근할 수 있다. 그리고 사용자 디바이스에서 제공하는 보안 키를 입력하는처리 절차를 가지고 있다. UAF 프로토콜 표준에서는 웹서버, FIDO 서버, 사용자 디바이스 간에 연동되는 UAF메시지를 정의하는 UAF Protocol Specification 등의 문서로 구성되어 있다. U2F 프로토콜은 기존 인증 방법인 ID/Password 기반인증 방식으로 1차 인증 한 후, 1회용 보안키를 저장한USB 동글 또는 스마트 카드와 같은 별도의 디바이스를이용하여 2차 인증하는 기술이다.

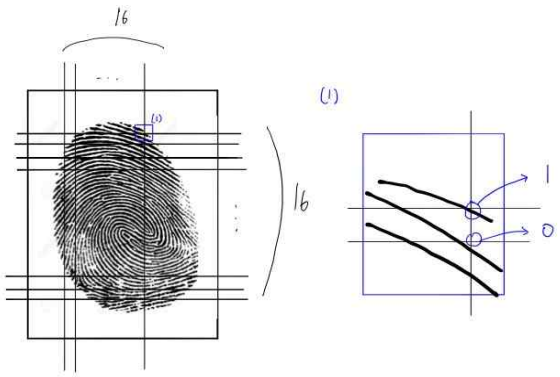
Ⅲ. 복구 기법

비밀번호를 보호함에 가장 큰 요구사항은 그 비밀번호를 훔칠 수 없게 하는 것이다. 기억을 잃지 않아야 사용 가능하다는 요구사항과 더불어 정리하자면 비밀번호는 잊을 수 있지 않아야 하며 어딘가에 적어둔 것을 공격자가 훔칠 수 없어야 한다. 이에 가장 부합하는 것은 바로 생체 인식이다. 본 논문은 생체 인식을 활용한 DID를 제안한다.

3.1 지문 등록절차

생체 인식은 본인이 아닐 경우 위조하기에 가장 까다로운 보안 방법의 하나다. 사용자의 지문 혹은 홍채의 패턴을 이용하면 보안에 위협을 받을 확률이 현저히 줄게 되며 사용자가 개인 키를 기억할 필요조차 없어지게 된다.

3.2 패스워드 분산 과정



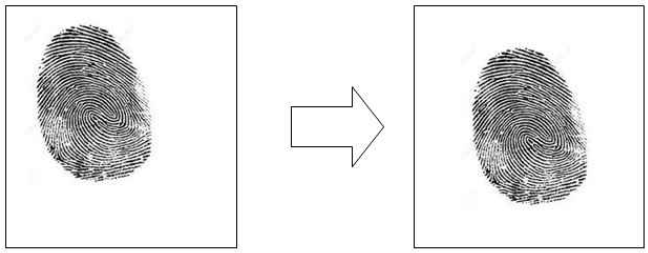
[그림 1]지문 등록절차

사용자의 지문을 스캔하여 그것을 256개의 교차점이 생기도록 한다. 이때, 교차점에 지문 정보가 위치하고 있으면 1, 없으면 0을 대입한다. 이 정보를 순서대로 나열하여 나오는 256자리의 수에서 0과 1이 연속되어

있는 수 만큼 더한 길이로 나누어 분산하여 저장하도록 한다. 예를 들어 100111011과 같은 패턴의 수가 나왔다고 가정하자. 연속된 숫자의 길이는 앞에서부터 1이 한 개, 0이 2개, 1이 3개, 0이 1개, 1이 두 개다. 개인키는 대체로 256비트로 이루어져 있고 연속된 숫자의 개수대로 나누어 랜덤한 노드에 분산시켜 저장한다.

3.2.1 지문 위치 재정렬

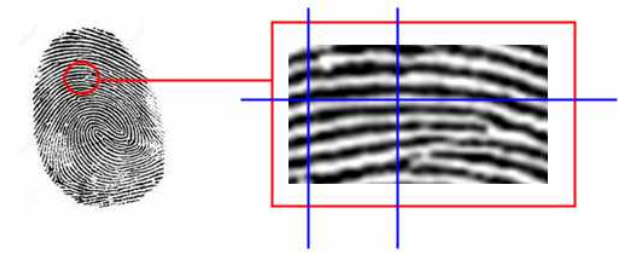
지문이 스캔 되어 찍힌 위치를 조정하여 중앙으로 이미지를 이동한다. 이는 지문이 스캐너 어느 곳에 찍혀있어도 일정 이상의 정확도를 얻기 위함이다.



[그림 2] 지문 위치 정렬

3.2.2 데이터 정렬

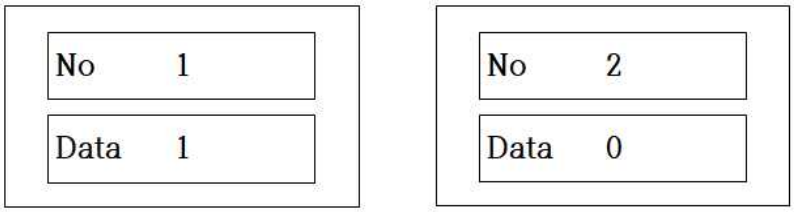
읽어온 지문 데이터를 가로, 세로 각각 16개의 간격이 일정한 선들을 교차시켜 교차점을 만든다. 이후 해당되는 교차점에 지문 데이터가 존재한다면 1을, 존재하지 않는다면 0의 데이터를 추출한다. 이렇게 총 256개의 0과 1로 구성된 데이터를 얻는다. 각 숫자 데이터는 순서대로 번호를 받는다. 그림을 예시로 들자면 파란색 선이 교차된 두 지점 중 왼쪽 데이터에 1번을 부여하는 식이다.



[그림 3]지문 데이터 추출

3.2.3 데이터 정렬

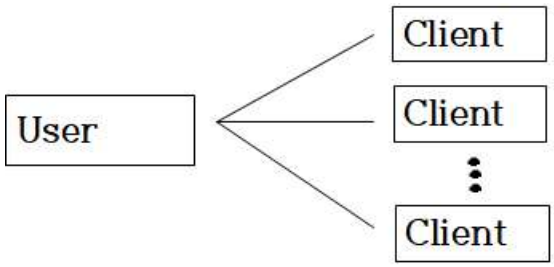
이와 같이 지문이 찍혔다면 지문의 원본데이터는 사용자 서버에서 보관한다. 지문이 찍힌 것을 토대로 지문데이터가 찍혔으면 data 1을 가지고 블록으로 저장되고 지문데이터가 찍히지 않았다면 data 0을 저장하게된다.



[그림 4] 블록 구조

3.2.4 배분

생성된 블록을 기반으로 사용자와 연결된 노드들에게 지문 블록데이터를 배분하게 된다.



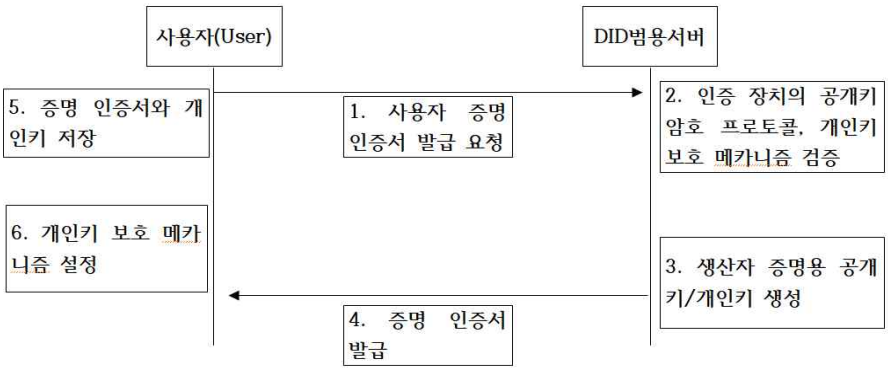
[그림 5] 데이터 분산

3.3 적합성 분석

이 단계는 사용자(User)가 지문인식을 이용하여 DID범용 서버에 정당한 사용자 임을 증명하기 위한 과정이다. 사용자는 자신의 생체인식정보 즉, 지문인식을 통해 분산시켜 저장해 놓은 노드의 값을 이용하여 DID범용 서버에서 사용자 인증을 진행한다.

3.3.1 인증서 발급 절차

사용자는 서버에 사용자 증명 인증서(attestation certificate) 발급을 요청한다. 클라이언트 서버는 지문의 공개키 암호 프로토콜, 개인키 보호 메카니즘 등을 검증하고, 안정성, 호환성, 편의성 등의 측면에서 그 기준에 부합하면 사용자 증명용 공개키/개인키를 생성한 다음 증명 인증서를 발급한다. 증명 인증서를 발급 받은 사용자는 자신이 생산하는 인증장치 즉, 지문이 등록된 장치에 증명 인증서와 개인키를 안전하게 저장하고, 인증서 발급 과정에서 증명된 개인키 보호 메카니즘을 설정한다.



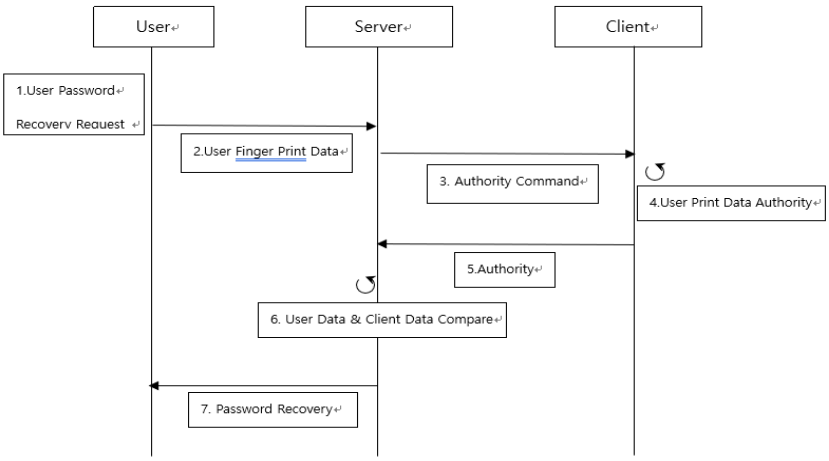
[그림 6] 인증서 발급 절차

3.3.2 인증 절차

(1) 사용자(User)는 사용자 인증을 위해 클라이언트에게 인증을 진행 준비를 위한 인증요청 메시지를 전송한다.
(2) 클라이언트는 DID범용 서버에게 인증을 위한 인증 요청 메시지를 전송한다.
(3) User는 클라이언트의 요청에 따라 실제 User의 생체인식 즉, 지문인식을 통해 생체 인증을 한다.
(4) User는 생체인증을 통해 랜덤한 노드의 값을 저장되어 있는 개인키를 생성하고 이 개인키를 Response를 생성하여 DID범용 서버에 전송한다.

(5) DID범용 서버는 User의 공개키를 이용하여 User의 Response를 검증하고, 이상이 없다면 User와 클라이언트간의 대칭키를 암호화 하고 인증결과 메시지(Auth Result)를 클라이언트에게 보낸다.
(6) 클라이언트는 전송 받은 Auth Result를 받아 Auth Info의 진위를 확인을 하고 User에게 Auth Result를 전송한다.

3.4 적합성 분석



[그림 7] 비밀번호 복구 절차

1. 인증서 비밀번호 분실시 사용자는 서버에 패스워드 복구 요청을 보낸다.
2. 사용자 지문데이터를 서버가 전달받는다.
3. 서버는 클라이언트에게 인증명령을 전달한다.
4. 사용자 지문데이터를 가지고있는 클라이언트들이 사용자 지문정보를 토대로 인증절차를 진행한다.
5. 클라이언트들의 인증이 성공했다면 분산된 데이터를 취합하여 지문데이터를 서버에 전달한다.
6. 사용자 지문데이터와 클라이언트 지문데이터를 비교대조 한다.
7. 서버에서 인증서 비밀번호를 사용자에게 전달한다.

IV. 결 론

본 연구에서는 블록체인 기술의 DID를 이용하여 생체 지문데이터를 분산 저장하는 방식을 제안하였다. 비밀번호는 잊을 수 있지 않아야 하며 어딘가에 적어둔 것을 공격자가 훔칠 수 없어야 한다. 지문 데이터는 개인이 가지고있는 데이터중 중복될수 없는 데이터이며 DID를 사용하여 지문 데이터를 분산 보관한다. 사용자는 인증을 위해서 클라이언트에게 인증요청메세지를 전다랗고 DID범용 서버에 인증을 위한 인 증요청 메시지를 전송한다 그리고 지문인식을 통해 생체 인증을 시작하며 사용자 지문데이터를 랜덤한 노드 값이 저장되어 있는 개인키를 생성하고 이 개인키를 DID범용 서버에 전송한다. DID범용 서버는 사용자의 공개키를 이용하여 사용자를 검증하고 사용자와 서버간의 대칭키를 암호화하고 인증결과 메시지를 클라이언트에게 전송하는 방법으로써 인증메시지의 진위를 확인하고 사용자에게 결과를 전송한다. 인증서 비밀번호 분실시 사용자는 서버에 패스워드 복구 요청을 보냄으로써 지문데이터를 서버가 전달 받음으로써 기존에 저장되어있던 사용자의 지문데이터를 취합하여 사용자 진위여부를 판별한다. 위와 같은방식으로 데이터를 저장하고 복구를 진행할 시 공격자가 비밀

번호 탈취시도를 하더라도 공격자는 사용자가 가지고 있는 지문데이터는 분산되어 각노드들에 저장되어있기 때문에 비밀번호를 탈취하기 어렵게된다.

REFERENCE

Kim, H,U., B. Y. Kim, and S. J. Moon(2016), “A design of user authentication protocol using biometric in mobile-cloud environments,” KAIS, 18(1), 2017, pp 32-39

Authentication Method using Multiple Biometric Information in FIDO Environment. pp.159-164

A Comparative Analysis of PKI Authentication and FIDO Authentication

FIDO UniversalAuthentication System Based on Blockchain. 2018 ETRI

Encryption of Biometrics data for Security Improvement in the User Authentication System.

Development of Integrated Preservation System for Fingerprint Recognition. 2008

Wi, Y. Y., and J. Kwak(2013), “OpenID based user authentication scheme for multi-clouds environment,” The Journal of Digital Policy & Management, 11(7), 2017, pp 215-223.

Rolf Lindemann, Davit Baghdasaryan, Eric Tiffany, "FIDO UAF Protocol Specification v1.0", FIDO Alliance Proposed Standard, 2014.

Sampath Srinivas, Dirk Balfanz, Eric Tiffany, "Universal 2nd factor (U2F) overview", FIDO Alliance Proposed Standard, 2015.

Lee, J. K., J. G. Son, H. M. Kim, and H. K. Oh(2013), “An authentication scheme for providing to user service transparency in multicloud environment,” Journal of The Korea Institute of Information Security & Cryptology, 23(6), pp 1131-1141.

Passwordless Authentication Technology-FIDO 2014 ETRI

A Design of Certificate Password Recovery Using Decentralized Identifier

Kim, Hyeong-uk[1)]
Kim, Sang-jin[2)]
Kim, Tae-jin[3)]
Yu, Hyeong-geun[4)]

Abstract

In the public certificate technology commonly used in Korea, users have a cumbersome problem of always resetting when they forget their password. In this paper, as a solution to this problem, we propose a secure authentication certificate password recovery protocol using blockchain, PKI, and DID for distributed storage. DID is a schema for protecting block ID in blockchain system. The private key used in the PKI is configured as a user's biometric, for example, a fingerprint, so that it can completely replace the memory of the complex private key.

To this end, based on the FIDO authentication technology that most users currently use on their smartphones, the process of authenticating a user to access data inside the block minimizes the risk of an attacker taking over the data.

Keywords: *Block-chain, DID(Decentralized Identifier), PKI, FIDO*

1)Author, Korea Electronic Certification Authroity, do3196@naver.com
2)Co-author, Undergraduate of Chungwoon University, kespanate@gmail.com
3)Co-author, Undergraduate of Chungwoon University, kimtj319@naver.com
4)Co-author, Undergraduate of Chungwoon University, kjhgfd6702@naver.com

저 자 소 개

■김 형 욱(Kim, Hyung-uk)
■한국전자인증, 수석연구원
■청운대학교 멀티미디어학과 겸임교수
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI

공 동 저 자 소 개

■김 상 진(Kim, Sang-jin)
■청운대학교 학부생
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI

공 동 저 자 소 개

■김 태 진 (Kim, Tae-Jin)
■청운대학교 학부생
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI

공 동 저 자 소 개

■유 형 근 (Yu, Hyeong-geun)
■청운대학교 학부생
<관심분야>:정보보안, 블록체인, 빅데이타, IoT, 생체인증, PKI