프라이빗 블록체인 기반 i-PIN 중복가입확인정보 변조 방지 시스템 구현

정권영, 박동준, 정재웅, 이광재*

*상명대학교

{201821255, 201821234, 201821256}@sangmyung.kr, *begleam@smu.ac.kr

An Implementation of a Private Blockchain-based Anti-Tampering System for i-PIN Duplicated Information

Kwon-Young Jung, Dong-Jun Park, Jae-Woong Jeong, Kwangjae Lee*

*Sangmyung Univ.

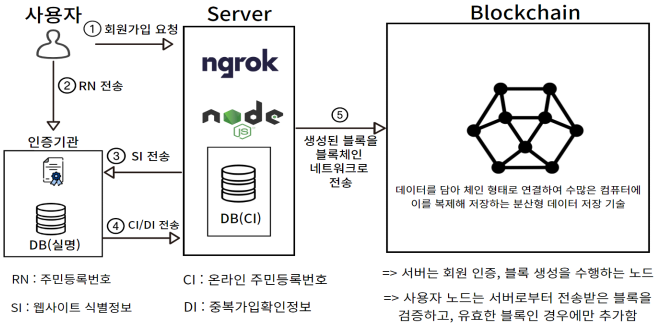
요 약

온라인 이용자 식별 수단중 하나인 i-PIN은 온라인 주민등록번호 CI와 중복가입확인정보 DI로 구성된다. 그 중, DI는 웹사이트에서의 사용자 중복가입을 막는 역할을 하는데 만약 이 정보가 변조된다면 무한적으로 가입되는 문제를 가진다. 본 논문에서는 DI 변조를 방지하기 위해 프라이빗 블록체인 시스템을 제안한다. 이 시스템은 인증기관에서 사용자의 정보를 통해 만들어낸 DI를 웹 서버를 거쳐 블록체인 네트워크에 전송하여 공유하는 방식으로 구현되었다. 만일, 한 사용자의 DI가 해킹으로 값이 변조될 시, 다른 사용자의 노드들이 해당 DI를 실시간으로 검증하므로 변조 공격을 막을 수 있다.

Ⅰ. 서론

2014년 8월부터 모든 공공기관 및 민간사업자에게 주민등록번호를 수집하는 행위가 원칙적으로 금지되었다[1]. 따라서 온라인에서 사용하는 새로운 이용자 식별 수단이 필요했는데 가장 보편화된 수단이 인터넷 개인식별 번호(i-PIN)이다[2]. i-PIN은 인터넷 사용자에게 이용자의 중복가입을 확인할 수 있는 중복가입확인정보(Duplicated Information; DI)와 동일 사용자를 식별할 수 있도록 확인하는 연계정보(Connecting Information; CI)로 구성된다. 이 중에서 DI는 웹사이트에서 사용자의 중복가입을 방지하는 기능을 수행하는데 데이터베이스에 저장되는 DI의 경우, 공격자들에 의해 값이 변조된다면 해당 사용자의 정보로 제약 없이 가입할 수 있게 된다[3].

본 논문은 DI 변조 방지를 위해 하이퍼레저 패브릭 기반 블록체인 네트워크를 제안한다. 제안하는 시스템은 인증기관에서 사용자의 정보를 통해 만들어낸 DI를 웹 서버를 거쳐 블록체인 네트워크에 전송하여 공격자의 DI 변조 방지를 보여준다. 피어 노드 장부의 데이터를 변조할 때 절반 이상의 장부를 모두 변조해야 한다는 블록체인의 특성을 이용하여, 한 사용자의 DI가 해킹으로 변조가 시도되더라도 다른 사용자 노드에 저장된 DI로 공격을 막을 수 있다.



[그림 1] 제안하는 DI 변조 방지 시스템 구조

Ⅱ. 본론

본 논문에서 제안하는 시스템의 구조는 그림 1과 같이 인증기관, 웹 서버, 블록체인 네트워크로 이루어져 있으며 인증기관에서 만들어낸 CI와 DI를 웹 서버를 거쳐 블록체인 네트워크에 전달한다. 생성된 DI는 블록체인의 피어 노드 장부에 저장된다. 이때, 피어 노드를 동적으로 생성하여 실시간으로 대응할 수 있도록 설계해 시스템의 완성도를 높였다.

인증기관은 크게 두 가지 기능을 수행한다. 하나는 서버와 클라이언트 간 암호화 통신을 위한 인증서를 발급하는 기능이고, 다른 하나는 웹사이트 식별정보를 이용하여 CI와 DI를 생성하는 기능이다. 첫째, 인증서 발급은 대칭키를 안전하게 전달하고 공유하는 목적으로 공개 키와 계산된 서명 정보가 담겨있다. 발급된 인증서를 통해서 공유 비밀정보를 계산할 수 있다. 둘째, CI와 DI 생성은 웹 서버에서 사용자가 회원 가입 중 본인확인을 시도하였을 때 수행한다. 사용자의 주민등록번호(RN)와 웹사이트 식별정보(SI)를 받아 CI와 DI 값을 계산하여 웹 서버로 전달한다. CI 계산은 입력 개인정보와 비밀정보를 이용해 xor 연산을 수행하고, HMAC 방식으로 도출한다. 이때, S_A 및 SK는 인증기관과 웹 서버가 공유하는 비밀정보이다. DI 계산은 입력 개인정보 및 서버 식별 정보를 해시 함수로 축약하며, HMAC 방식으로 도출한다. CI와 DI의 생성 계산식은 각각 식(1)과 식(2)이다.

$$Temp = (RN \| Padding) \oplus S_A \quad (1)$$
$$CI = HMAC_{SK}(Temp)$$

$$Temp = H(RN \| SI) \quad (2)$$
$$DI = HMAC_{SK}(Temp)$$

웹 서버는 중복가입이 방지됨을 확인할 수 있는 기능인 로그인, 회원 가입, 회원 탈퇴로 웹사이트를 구현하였다. 사용자는 웹사이트에서 회원 가입을 통해 해당하는 정보를 모두 입력하게 되면 웹 서버는 사용자의 중복 여부를 확인한다. 이상이 없을 시에는 본인인증 버튼을 통해 인증기관이

제작한 사이트로 넘어가 인증을 시행한다. 인증기관의 확인을 통해 본인인증이 완료되었다면 회원 가입이 정상적으로 이루어지고 사용자 정보는 데이터베이스에 저장되며, 인증기관의 제작과정을 통해 만들어진 CI와 DI를 전달받아 CI는 데이터베이스에 저장하고 DI는 블록체인 네트워크로 전달하게 된다.

본 논문에서 제안하는 블록체인 네트워크는 DI를 저장하고 중복 여부를 검증하는 기능을 수행한다. DI는 온라인에서 사용하는 이용자 식별 수단이므로 보안성을 추가한 프라이빗 블록체인의 개념을 가진 하이퍼레저 패브릭 네트워크로 구현하였다. 그리고 자체 API를 개발하여 웹 서버에서 새로운 DI를 전송하면 새로운 조직을 생성할 수 있도록 설정하였다.

하이퍼레저 패브릭은 스마트 계약을 체인코드 함수로 구현하고, 트랜잭션 플로우에 따라 조직 간 합의를 통해 블록을 생성한다[4]. 하이퍼레저 패브릭에서 저장되는 데이터는 자산(Asset)으로 지칭되며, 자산의 형식과 자산을 핸들링하는 함수는 체인코드에 정의된다. 여기서 체인코드는 하이퍼레저 패브릭이 정의하는 스마트 계약을 의미한다. 하이퍼레저 패브릭의 트랜잭션 플로우는 표 1과 같이 수행되며, 원장이 갱신된 후에는 월드 스테이트 데이터베이스에 체인 코드에서 지정한 데이터를 키로 가지는 로그가 저장되고 이는 블록 조회 시 사용된다[4].

[표 1] 하이퍼레저 패브릭의 트랜잭션 플로우

순서	설명
1	클라이언트가 트랜잭션을 채널에 가입된 모든 피어 노드에게 제안
2	피어 노드는 클라이언트의 서명을 확인하고 제안된 트랜잭션을 실행
3	피어 노드는 트랜잭션 실행 시, 에러가 발생하면 허용 응답을 거부 에러가 발생하지 않으면 허용의 의미로 트랜잭션에 서명 전송
4	클라이언트는 허용 응답이 2 / 3을 초과하면 서명된 응답을 오더러 노드에게 전송 오더러 노드는 트랜잭션 순서를 지정한 후에 이를 블록으로 생성
5	생성한 블록이 채널에 가입된 모든 피어 노드에게 전달
6	원장이 갱신

패브릭 애플리케이션은 웹 서버로부터 새로운 DI 생성 요청을 받았을 때 트랜잭션 플로우에 따라 합의를 진행하게 된다. 이때 중복되는 DI가 없다면, 새로운 DI가 추가되고, 새로운 노드가 생성되며 회원 가입 절차가 완료된다. 이 경우, 웹 서버에게 성공 메시지를 전송한다. 그러나 중복되는 DI가 있는 경우에는 웹 서버에게 실패 메시지를 전송하여 회원 가입 절차를 중단시킨다. 이러한 패브릭 애플리케이션 명세는 표 2와 같다.

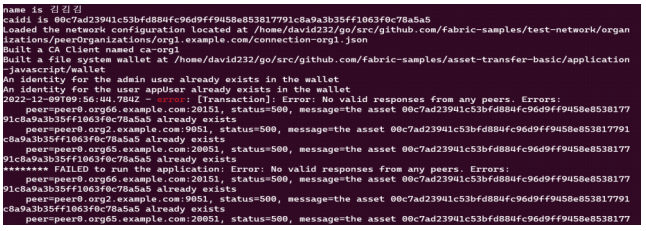
[표 2] 패브릭 애플리케이션 명세

요청	기능	반환값
자산 생성 (회원 가입)	전송된 CaiDi와 Name을 사용하여 자산을 생성하는 트랜잭션 제안 자산 생성 성공 시, 새로운 조직 (새로운 사용자 노드) 생성	조건에 따라 성공 'Success' 반환 / 실패 'Fail' 반환
자산의 소유자 변경	전송된 CaiDi에 해당하는 자산의 소유자를 전송된 Name으로 변경하는 트랜잭션 제안	
자산 삭제 (회원 탈퇴)	전송된 CaiDi에 해당하는 자산을 삭제하는 트랜잭션 제안 자산 삭제 성공 시, 해당 사용자 노드 삭제	

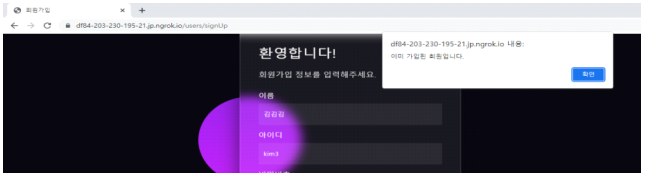
Ⅲ. DI 변조 방지 실험

제안한 시스템이 블록체인 네트워크를 통한 DI 변조 방지가 됨을 확인하기 위해서 그림 2와 같이 인증기관, 블록체인 네트워크, 웹 서버가 TLS를 이용해 통신하는 실험을 준비하였다. 그림 2(a)와 같이 사용자가 회원 가입을 통해 인증기관에 넘어와 본인인증을 수행한다. 하지만 이미 가입한 사용자이므로 그림 2(b)에서 보듯이 블록체인 네트워크에서 already exists의 오류를 발생시키며 웹 서버로 fail의 메시지를 전달한다. 웹 서버는 이 메시지를 토대로 그림 2(c)와 같이 "이미 가입된 회원입니다" 의 메시지를 사용자에게 보여주며 중복가입이 되지 않음을 확인할 수 있다.

(a)



(b)



(c)

[그림 2] 블록체인 네트워크를 통한 DI 변조 방지 실험 결과 화면
(a) 인증기관, (b) 블록체인 네트워크 로그, (c) 웹 서버 (변조 실패)

Ⅳ. 결론

본 논문에서는 인증기관, 웹 서버, 블록체인 네트워크로 구성된 DI 변조 방지 시스템을 설계했다. 이 시스템은 변조 시도가 있더라도 각각의 사용자가 가지고 있는 DI 정보를 통해 중복가입이 방지되므로 사용자의 정보를 안전하게 관리할 수 있다. 하지만 블록체인의 특성으로 다수의 노드가 존재하면 느린 속도를 개선해야 하는 문제점이 있다. 그러나 인터넷 시장의 규모가 확대됨에 따라 그에 다른 악의적인 공격 등의 사례가 증가할 것으로 판단되므로, 본 논문에서 제안하는 DI 변조 방지 시스템의 연구 및 개발을 통해 사용자의 중복가입을 막고 웹사이트 운용에 도움이 될 것으로 판단한다.

참 고 문 헌

[1] K.-Y. Kim. "Resident registration number, no longer collected carelessly." inews24.com. https://www.inews24.com/view/798327 (accessed Jan. 5, 2009).

[2] Connecting Information for internet-Personal Identification Number Service Conformity, KS X 3228-3:2012, Korea, Sep. 2012.

[3] Duplicated Joining Verification Information for internet-Personal Identification Number Service, KS X 3226:2012, Korea, Sep. 2012.

[4] "A Blockchain Platform for the Enterprise:HYPERLEDGER FABRIC v2.2," USA, Linux Foundation, 2020. [Online]. Available: https://hlf.readthedocs.io/en/v2.2.1/index.html