The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 1, pp.211-218, Feb. 29, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.1.211
JIIBC 2020-1-30

블록체인 기반 시스템 인증 방법에 대한 연구

A Study on the Blockchain-based System Authentication Method

김성환*, 김영곤**

Sunghwan Kim*, Younggon Kim**

요 약 최근 블록체인 기술의 등장으로 이 기술을 적용하여 기존의 시스템에 적용하고자 하는 시도가 증가하는 추세이다. 블록체인 기술의 합의원장과 스마트 컨트렉트를 이용하여 문서, 증명, 인증, 검증 등의 과정이 필요한 다양한 분야에 분산처리를 기반으로 하여 보안 성능과 신뢰성을 향상하기 위해 민간 분야에서 인증서, 암호화, 해쉬연산, 블록체인 등을 활용한 방법들을 연구하고 있으나, 아직까지 실용화 단계에는 이르지 못하고 있어 기술 확산에 어려움이 있는 상황이다. 본 논문에서는 블록체인 기반 업무 플랫폼 환경에서 적용이 용이하고 사용자 편의성과 강력한 보안 환경을 제공하기 위하여 사용자 장치 등록 인증 알고리즘, 블록체인 기반 질의응답 인증 알고리즘, 인증서 발급, 검증 프로세스와 암호화 알고리즘, 서버사이드 인증 알고리즘의 4가지 방법으로 블록체인 기반 시스템 인증방법에 대해 제안하였다.

Abstract Recently, with the advent of blockchain technology, attempts to apply this technology to existing systems are increasing. By using the blockchain technology consensus ledger and smart contract, it is necessary to distribute certificates to various fields that require documents, attestation, authentication, verification, etc. We are studying methods using hash operation, blockchain, etc., but it is difficult to spread the technology as it has not yet reached the stage of commercialization. In this paper, user device registration authentication algorithm, blockchain-based question and answer authentication algorithm, certificate issuance, verification process and encryption algorithm, and server-side authentication for easy application in blockchain based business platform environment We proposed a blockchain-based system authentication method using four algorithms.

Key Words : Authentication, , PKI SEEDWORD, Blockchain, Device,

Ⅰ. 서 론

최근 블록체인 기술의 등장으로 이 기술을 적용하여 기존의 시스템에 적용하고자 하는 시도가 증가하는 추세이다. 블록체인 기술의 합의원장과 스마트 컨트렉트를 이용하여 문서, 증명, 인증, 검증 등의 과정이 필요한 다양한 분야에 분산처리를 기반으로 하여 보안 성능과 신뢰성을 향상하기 위해 공공기관 및 민간 분야에서 인증서, 암호화, 해쉬연산, 블록체인 등을 활용하여 인증과정에 적용하기 위한 방법이 지속적으로 연구되고 있으나, 실제

*김성환, 한국산업기술대학교 컴퓨터공학과 linne@kpu.ac.kr
접수일자: 2019년 10월 25일, 수정완료: 2020년 1월 5일
게재확정일자: 2020년 2월 7일

Received: 25 October, 2019 / Revised: 5 January, 2020 / Accepted: 7 February, 2020
*Corresponding Author: ykkim@kpu.ac.kr
Dept. of Computer Engineering, Korea Polytechnic University, Korea

로 이를 활용한 인증 방법들에 대해서 제안하는 단계에 있으며, 사용자 환경에서 활용되고 있는 업무 시스템이나 서비스형 소프트웨어 적용한 사례가 없어 기술 확산에 어려움이 있는 상황이다. 따라서 본 논문에서는 블록체인 기반 업무 플랫폼 환경에서 적용이 용이하고 사용자 편의성과 강력한 보안 환경을 제공하기 위하여 사용자 장치 등록 인증 알고리즘, 블록체인 기반 질의응답 인증 알고리즘, 인증서 발급, 검증 프로세스와 암호화 알고리즘, 서버사이드 인증 알고리즘의 4가지 방법으로 블록체인 기반 시스템 인증방법에 대해 제안하였다.

II. 관련 연구

다수가 이용하는 서비스를 제공하는 플랫폼의 특성상 사용자를 구분하고 시스템의 보안을 강화하기 위한 인증 절차가 필수적으로 요구되고 있다. 다양한 서비스 및 시스템 환경에서 사용되는 인증 방식 구현을 위해 아래와 같이 연구되고 있다.

1. 블록체인 기술

블록체인은 '비트코인'을 유지하는 기반 보안 기술이다. 비트코인에서 블록체인은 주기적으로 발행하는 화폐인 비트코인의 이동 이력을 저장하는 일종의 분산된 디지털 장부라고 할 수 있다. 이 장부는 위변조할 수 없는 암호학적 기술로 만들어지며 비트코인의 소유권 이동을 위해 비트코인의 거래(Transaction) 과정과, 발생한 거래를 모아 시간이 매우 오래 걸리는 특정 조건의 해시 값을 갖게 하는 난수(Nonce) 찾기 문제로 거래 내용의 위변조를 방지할 수 있는 작업증명(Proof of Work) 단계 등으로 구성된다[1].

분산장부 시스템을 통한 투명한 거래로 보안, 감독, 규제 비용 절감 가능하며 P2P 네트워크 방식을 기반으로 참여자간 직접 거래가 이루어지기 때문에 중개기관 수수료가 발생하지 않는 장점과 탈 중앙화 구조이기 때문에 참여자의 인프라를 공유하여 사용하므로 대규모의 인프라 구축이 없이 사용할 수 있는 장점이 있으나, 분산 익명 시스템의 구조상 직접적인 통제가 필요한 시스템에 적용하기 어려운 문제와 거래와 관련된 모든 데이터가 참여자들에게 공개되는 특성상 정보 공개를 원하지 않거나 법 제도상 공개되지 않아야 하는 정보를 가지고 있는 환경에는 적용할 수 없기에 실제 기업에서 블록체인 도입을 결정하지 못하게 되는 요인이 되고 있다. 따라서 네트워크에서 지정한 제한된 참여자에게만 원장을 공유하는 방식의 프라이빗 블록체인 기술을 활용할 수 있는 대안이 연구되고 있으며, 블록체인 합의 인증 프로세스는 다음 그림 1과 같다[2],[3].

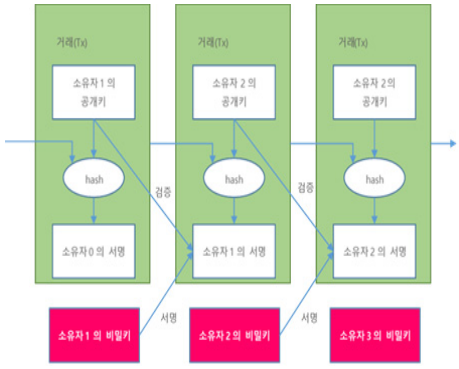

그림 1. 블록체인 인증 프로세스

Fig. 1. Blockchain authentication process

2. PKI 기반 인증서 기술

PKI는 공개키 암호시스템을 안전하게 사용하고 관리하기 위한 정보보호 표준 방식으로 인터넷상의 전자상거래와 같이 지역적으로 떨어져 있는 이용자 간의 전자서명과 암호화에 의한 보안기술이다. 즉, 통신을 하 고자 하는 쌍방이 모두 신뢰할 수 있는 기관(공인인증 기관)에서 생성한 공개키와 개인키를 사용하여 안전한 전자상거래를 할 수 있도록 지원한다. PKI 인증시스템은 사용자 정보에 따라 랜덤하게 생성된 공개키 정보를 저장한 인증서를 발급하고 관리하는 인증기관(CA), 사용자의 인증서 발급요청에 따라 사용자 정보를 등록하는 등록 대행기관(RA), 인증서와 폐지된 인증서 목록을 사용자에게 제공하는 디렉터리 시스템(DS) 등으로 구성되며, 각 구성요소 간 관계 PKI 프로세스 개요는 그림 2와 같다.

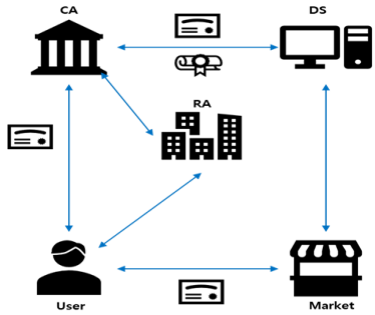

그림 2. PKI 프로세스 개요

Fig. 2. PKI Process Overview

PKI 인증시스템의 동작 절차는 사용자가 등록 대행기관에서 자신의 신원정보를 확인받고 인증서 발급 요청한다. 요청을 받은 등록대행 기관은 사용자 신원정보를 전송하면서 인증기관에 인증서 발급요청을 한다. 사용자 인증서 발급요청을 수신한 인증기관은 사용자에게 인증서를 발급해주면서 발급된 인증서와 인증서 폐지목록을 디렉터리 시스템에 게시한다. 사용자가 인터넷 상점(Market)에 접속하여 전자상거래 시 상점에서는 디렉터리 시스템에 접속하여 사용자 인증서와 인증서 폐지목록을 받아 사용자의 인증서의 유효성을 검사 후 인증서가 유효한 사용자에게만 해당 서비스를 제공한다. PKI 인증시스템은 암·복호화 및 전자서명 기술을 이용한 데이터의 위·변조 검증 절차를 가지고 있어 인터넷 서비스나 전자상거래를 안전하게 할 수 있도록 지원한다. 전자상거래 시 ID/PW, 보안토큰 등과 비교 시 PKI 기반의 기술이 암호학적으로 더 안전한 장점을 가지고 있으며, X.509 공인인증서 구성 파일은 표 1과 같다[4],[5],[6].

표 1. X.509 공인인증서 구성파일
Table 1. X.509 public certificate configuration file

파일명	용 도
signCert.der	인증서의 버전, 인증서 소유자 정보, 유효기간, 인증서 발급자 정보 등이 X.509 형식에 맞춰서 저장된 공개키 파일
signPri.key	PKCS#8 구조에 따라 저장한 개인키 파일
CaPubs	인증서의 유효성 검증을 위한 인증서 체인(발급기관 정보) 파일

3. 디바이스 등록 인증방법

사전에 등록된 Device의 고유정보를 활용하여 인증하는 방법은 과정이 간단하면서도 보안성이 환경을 제공할 수 있으며, Device의 고유 값을 보안 설정에 필드로 추가하여 구현이 가능하다. 장치가 게이트웨이에 접속을 시도할 경우 게이트웨이에서 사전 입력된 Device의 고유 정보를 대조 후 일치 여부에 따라 인증을 완료하는 과정을 가지고 있어 간편하게 시스템 보안성을 확보할 수 있는 장점이 있다. 그러나 사전에 등록된 정보가 유출될 경우 침해 위협에 노출될 수 있어 보안 취약성이 발생하게 되는 문제점이 있어 이에 대한 개선이 필요하며, Device 사전 등록 인증 프로세스는 다음 그림3과 같다[7].

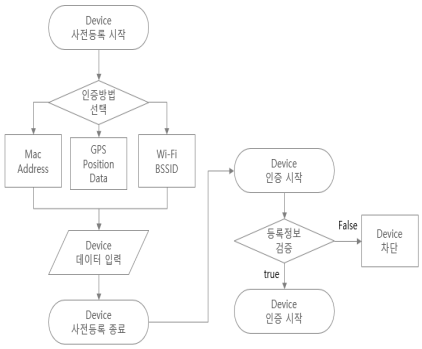

그림 3. Device 사전 등록 인증 프로세스
Fig. 3. Device preregistration authentication process

4. 질의 응답형 인증방식

질의 응답형 인증 방식은 Device의 사전 등록을 위한 인증 프로세스가 종료된 이후 사용자 장치가 인증 요청을 하는 과정에서 Challenge and Response 방식으로 수행하는 일련의 과정이 포함되어 있다. 장치가 서버에 OTP 번호를 전송하면 서버는 난수를 생성하여 challenge로 사용자 장치에 전달한다. 이와 동시에 사용자 장치 식별 번호에 해당하는 Seed Words 키를 데이터베이스에서 추출하고 추출된 키를 이용하여 난수의 암호화를 시작한다. challenge를 받은 사용자 장치는 내장되어 있는 Seed Words 값을 반환하며. 서버는 서버에서 계산한 값과 수신한 값이 일치할 경우 권한을 부여하는 인증하는 절차를 가지며, Challenge and Response 방식 인증 프로세스는 다음 그림 4와 같다.

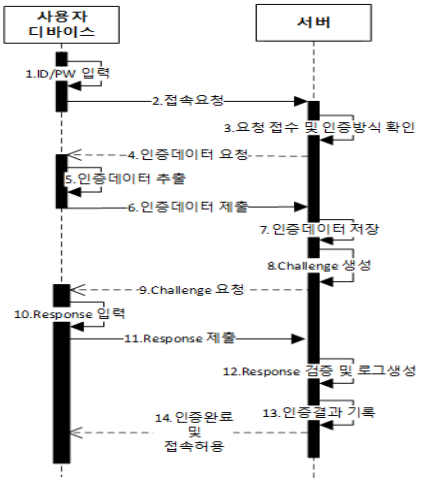

그림 4. 질의응답 방식 인증 프로세스
Fig. 4. Challenge and Response authentication process

Seed Words는 숫자, 알파벳 소문자, 알파벳 대문자를 조합하여 6자리로 4개의 조합된 단어를 생성하는 기법을 적용하였다. 제안되는 기법은 기존에 널리 사용되는 난수표에서 생성되는 코드와 비교했을 때 무작위 생성된 단어의 조합되어 있어 유추 또는 연산을 통한 해킹이 어렵고, 코드 생성 과정에서 복잡한 연산처리를 요구하지 않는 특성을 가지고 있어 시스템에서 요구하는 기본적인 보안 성능의 저하 없이 장치의 성능에 대한 영향을 최소화하여 저 사양의 사용자 장치에도 적용할 수 있다. 제안되는 인증방법은 다음 그림5 질의 응답형 인증 알고리즘과 같다[8].

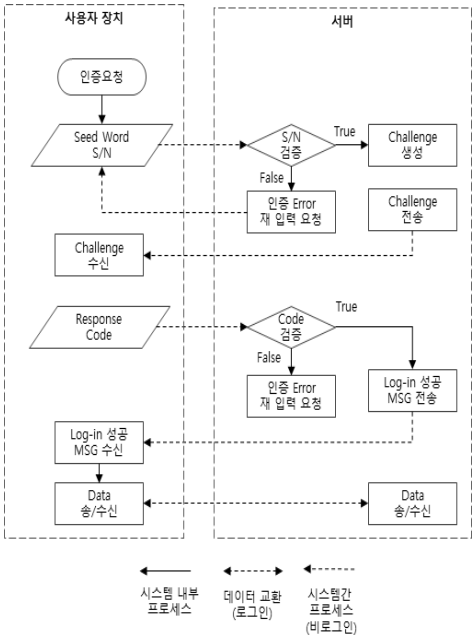

그림 5. 질의응답형 인증 알고리즘
Fig. 5. Challenge and Response Algorithm

Ⅲ. 제안한 프로세스와 알고리즘

본 논문에서는 블록체인 기반 계약관리 플랫폼 환경에서 요구되는 사용자 인증 방식의 복잡성과 보안 취약성을 개선하여 편의성을 강화하고, 암호화 알고리즘을 적용하여 보안 위협으로부터 안전한 사용 환경을 제공하기 위한 방법과 계약 체결에 기반이 되는 전자서명 과정에서 발생하는 취약성 및 복잡성을 개선하여 신뢰할 수 있고 보안성을 강화할 수 있는 인증서 발급에 대한 프로세스 및 알고리즘에 대해 제안하고자 한다.

1. 사용자 장치 등록 인증 알고리즘

이 방식은 블록체인 기반 시스템에 참여하는 사용자가 회원 가입 과정에서 접속할 장치를 등록하도록 하여, 등록되지 않은 장치로 부터의 접속을 차단하는 방법으로 허가받지 않은 사용자로 부터의 침해 요인을 최소화 하여 보안 성능을 강화하는 방법이다.

사용자 등록 과정에서 장치의 등록을 위해 사용자는 자신의 환경에 최적화된 인증 방식을 선택하고, 인증 과정에서 요구되는 데이터를 입력하는 절차를 통해 장치를 등록할 수 있다. 블록체인 기반 시스템은 시스템 사용을 위해 로그인을 시도할 경우 등록되어 있는 장치 유무를 검증하기 위해 장치가 가진 고유 정보 값과 OTP 코드를 비교 검증하는 과정을 통해 등록된 값과 사용자의 장치의 값이 일치할 경우 인증을 완료하는 과정을 가진다. 사용자 장치 등록 알고리즘 의사코드는 다음 표2와 같고, 시스템에 접속을 요청할 때 장치 인증 알고리즘 의사코드는 표3과 같다.

표 2. 사용자 장치 등록 알고리즘 의사코드
Table 2. User Device Registration Algorithm Pseudocode

```
1   authentication Select
2   IF select THEN
3   authentication sequence 1
4   ELSE
5   authentication sequence 2
6   ELSE
7   authentication sequence 3
8   ENDIF
9   sequence-name 1
10  IF Input Data = R1
11  comment="pass"
12  ELSE
13  Display "Error, authentication Fail!"
14  ENDIF
15  sequence-name 2
16  IF Input Data = R2
17  ELSE
18  Display "Error, authentication Fail!"
19  ENDIF
20  sequence-name 3
21  IF Input Data = R3
22  comment="pass"
23  ELSE
24  Display "Error, authentication Fail!“
25  ENDIF
26  IF sequence comment=”pass”
27  Comment=” authentication success!”
28  ELSE
29  Display “authentication Fail!”
30  ENDIF
```

표 3. 장치 인증 알고리즘 의사코드
Table 3. Device Authentication Algorithm Pseudocode

```
1   /*Device Seed word Data Fail!, Retry Please.*/
2   IF Input Data C1= S1
3   Else
4   Display "Seed word Data Fail!, Retry Please."
5   End IF
6   IF Build data=true
7   Send Challenge Code
8   Else
9   Rebuild data
10  End IF
11  IF receive Data=true
12  comment="authentication Success!"
13  system log-in
14  Else
15  Response send "Challenge Data Fail!, Retry Please."
16  End IF
17  IF System Connect=true
18  Data I/O Process Start
19  Else
20  Display "System Connect Fail!, Retry Please."
21  End IF
```

2. 블록체인 기반 질의응답 인증 알고리즘

본 논문에서 제안하는 질의응답 기반 블록체인 합의 인증방법은 시스템 접속을 위해 사용자가 ID/PW를 이용하여 인증을 완료하게 되면 서버는 사전에 사용자가 지정한 방식으로 사용자 장치에서 제공한 고유의 데이터 값을 수집하는 절차를 통해 블록체인에 Hash 값과 UTXO(unspent transaction output)를 생성한다. 서버는 생성된 Hash 값을 이용하여 난수 값을 생성한 후 생성된 난수 값 정보를 이용하여 Challenge를 생성한 후 사용자 장치에 Challenge를 요청한다. Challenge를 받은 사용자는 Challenge 값에 대응하는 Response 값을 Seedword 생성 애플리케이션에서 제공되는 값을 입력하여 제출한다. 제출된 Response 값은 블록체인 네트워크를 통해 검증 과정을 가지며, 검증이 완료되면 발급된 키의 UTXO 상태가 소멸되고, 검증 결과가 기록되며, 인증이 완료된다. 인증을 위한 생성된 키는 인증 과정에서만 일시적으로 사용자 장치에 보관되며, 인증 절차 완료 후 소멸되어 사용할 수 없는 상태로 변경된다. 제안된 블록체인 기반 질의응답 인증 프로세스는 다음 그림 6과 같고 블록체인 기반 질의응답 인증 알고리즘은 다음 그림 7과 같다.

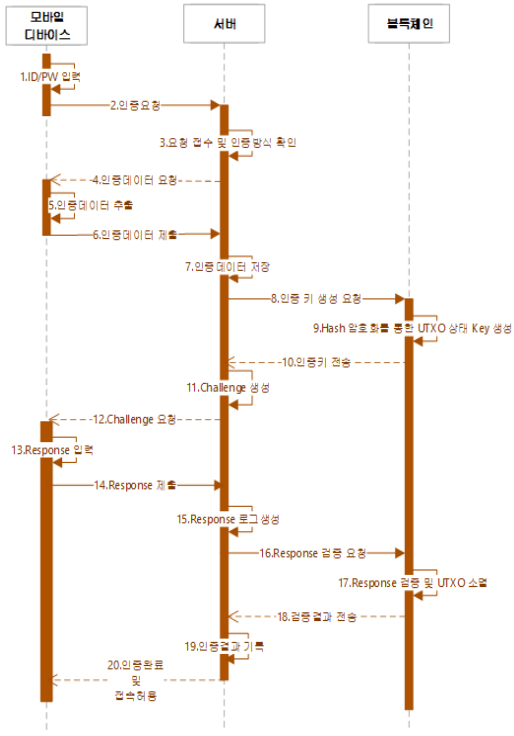

그림 6. 블록체인 기반 질의응답 인증 프로세스
Fig. 6. blockchain based Challenge and Response authentication process

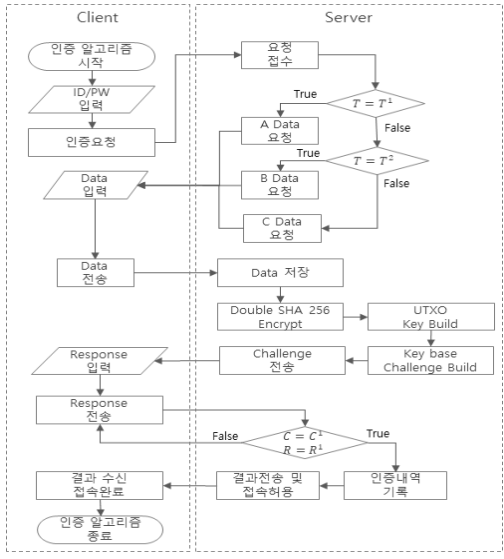

그림 7. 블록체인 기반 질의응답 인증 알고리즘
Fig. 7. blockchain based Challenge and Response authentication Algorithm

3. 인증서 발급 및 검증 알고리즘

인증서의 발급을 위해 사용자가 필수 데이터를 입력하여 요청하는 절차를 가진다. 요청은 노드를 통해 플랫폼의 계정관리 서비스를 통해 사용자에게 발급되며, 발급된 이력과 퍼블릭 키의 해시값 정보는 블록체인에 저장한다. 다른 참여자가 제출받은 전자서명의 유효성을 확인을 위해 검증 요청을 받으면 노드를 통해 진위 여부를 확인하는 절차를 가지며, 인증서 발급 및 검증 프로세스는 다음 그림8과 같다.

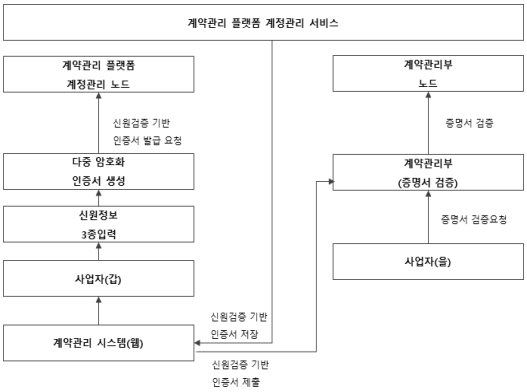

그림 8. 인증서 발급 및 검증 프로세스
Fig. 8. Certificate issuance and verification process

사용자가 시스템에 로그인 하는 과정에서 서버는 사용자의 장치에 정보 전송을 요청하게 된다, 사용자 장치에서 서버에 장치 정보를 제출하면 서버는 사용자의 장치가 제출한 데이터를 무작위 SHA 256 암호화를 통해 1차 암호화를 수행하여 해쉬 값을 생성한다. 생성된 해쉬 데이터의 복호화를 위해 해쉬 데이터에 버전을 확인할 수 있도록 식별코드와 복호화 코드를 추가한 후 Base58 인코딩 과정을 통해 비밀키를 생성한다. 생성된 비밀 키를 타원곡선 SECP256K1 알고리즘을 이용하여 공개키를 생성한다. 생성된 공개키에 이중 SHA256 암호화를 통해 해쉬 값을 생성한다. 생성된 해쉬 데이터에 복호화를 위한 식별코드와 복호화 코드를 추가하고 다시 Base58 인코딩을 통해 최종적으로 공개키를 생성하는 절차를 제안하였다. 제안되는 인증서 암호화 프로세스는 다음 그림 9와 같다.

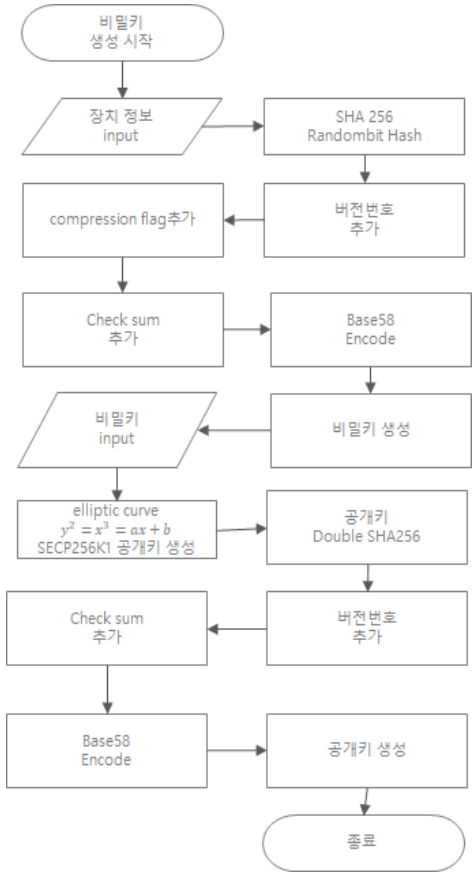

그림 9. 인증서 암호화 알고리즘
Fig. 9. Certificate Encryption Algorithm

4. Sever-Side 인증 알고리즘

서버는 모바일 디바이스의 운영체제에서 인증서를 안전하게 보관하기 위해 제공하는 IOS(Keychain), 안드로이드(Keystore)의 API를 이용하여 사용자의 암호화 키 저장을 요청한다. 이러한 방법을 통해 인증시스템이 아닌 다른 애플리케이션이나 인가되지 않은 악성코드 및 침해요인을 차단할 수 있다. 사용자의 암호키는 제공된 디바이스 정보의 해쉬 값과 함께 별도로 랜덤 어레이를 사용하여 발생된 난수를 적용하여 서버사이드(Server-Side) 암호화를 수행한 후 보관한다. 보관된 암호는 서버에 보관되고, 인증서의 갱신, 신규생성, 서명과정에서 서버에서 새로운 인증을 받아야 하므로 무작위 입력을 반복하는 브루투 포스 공격을 차단할 수 있어 사용자의 인증서와 비밀번호가 유출될 경우라도 서버에서 진위여부를 최종적으로 검증하게 되므로 안전한 보안환경을 제공할 수 있다. Server-Side 인증 알고리즘은 다음 그림 10과 같다.

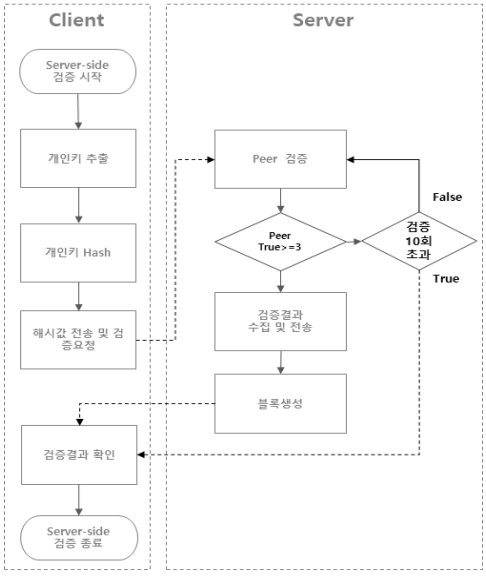

그림 10. Server-Side 인증 알고리즘
Fig. 10. Server-Side Authentication Algorithm

5. 제안한 알고리즘의 장점

제안한 블록체인 기반 시스템 인증 방법은 개선된 알고리즘과 프로세스들을 제안하여 적용하였다. 제안된 알고리즘은 첫째, 사용자 장치 등록 알고리즘, 둘째 블록체인 기반 질의응답 인증 알고리즘, 셋째 인증서 발급 및 검증 알고리즘, 넷째 Server-Side 인증 알고리즘으로 구성되어 있다. 제안된 알고리즘이 적용된 인증 시스템은 사용성을 유지하면서 보안 성능은 강화하고, 암호화 관리, 인증서 관리 부분을 개선하여 침해 사고 발생 요인을 최소화 하였고, 중앙화 시스템을 탈중앙화 한 분산처리 환경 기반으로 구현되어 편리하고 보안성 높은 환경을 제공한다. 제안된 블록체인 기반 질의응답 알고리즘의 장점은 표 4와 같다.

표 4. 블록체인 기반 인증 알고리즘의 장점
Table 4. Advantages of Blockchain-based Authentication Algorithms

구분	기존 인증방식	블록체인 기반 알고리즘 인증방식
저장위치	클라이언트 일반 저장장치	운영체제 내부의 암호화 공간
시스템 구조	중앙화	탈 중앙화
인증키 유효	일정 기간 또는 영구	1회
인증 단계	2 Factor	3 Factor
사용자 입력횟수	2회	2회
패스워드 생성방식	사용자 지정	1회용 생성
암호화	SHA25	이중SHA256 타워곡선
보안성능	안전	매우 안전

Ⅳ. 결 론

본 논문에서는 다양한 장치에서의 호환성을 확보하기 위한 사용자 장치 등록 알고리즘, 사용자 편의성과 시스템 복잡성 개선을 위해 인증 프로세스를 단순화한 질의응답 기반 합의인증 알고리즘, 보안성 강화를 위해 암호화와 복합인증 알고리즘과 인증서 발급 프로세스, Server-side 인증 알고리즘을 고안하여 적용한 블록체인 기반 시스템 인증 방법을 제안하였다.

본 논문에서 제안한 블록체인 기반 시스템 인증 방법을 활용한다면 일반적인 고성능의 디바이스 뿐만 아니라 저 사양의 사용자 장치들과 다양한 운영체제 환경 기반의 기기들로 구성되는 블록체인 기반 시스템 네트워크를 쉽게 구축할 수 있어 사용자의 편의성과 보안성이 요구되는 블록체인 기반 시스템 환경에서 널리 사용될 수 있을 것으로 기대한다.

향후 과제로는 블록체인 기반 시스템 인증 방법을 적용한 블록체인 기반 어플리케이션 플랫폼을 구현하는 방법에 대한 연구를 통해 어플리케이션을 가지고 있는 개발자들이 별도로 시스템 구성이나 설치 없이 어플리케이션을 API 형태로 플랫폼과 연동하여 활용할 수 있도록 보완할 계획이다.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer to Peer Electronic Cash System”, Oct 2008.

[2] Chul-Jin Kim, “A Static and Dynamic Design Technique of Smart Contract based on Block Chain”, Journal of the Korea Academia-Industrial, Vol. 19, No. 6 pp. 110-119, March, 2018.
DOI: https://doi.org/10.5762/KAIS.2018.19.6.110

[3] Yoo Soon-duck, Kim Ki-heung. A Study on Improvement for Service Proliferation Based on Blockchain. The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), Vol. 18, No. 1, pp.185-194, Feb 2018.
DOI:https://doi.org/10.7236/JIIBC.2018.18.1.185

[4] Kim Seon-Joo, Joe In-June, "Management Method to

Secure Private Key of PKI using One Time Password", The Journal of the Korea Contents Association, Vol.14.No. 12, pp565-573, 2014.10
DOI: https://doi.org/10.5392/JKCA.2014.14.12.565

[5] B. Kaliski, PKCS #5: Private-Password Based Cryptography Standard V2.1, RSA Laboratories, 2000.

[6] B. Kaliski, PKCS #8: Private-Key Information Syntax Standard V1.2, RSA Laboratories, 2008.

[7] Kim, Sung-hwan, Kim Young-gon,."A Study on Light Weight Authentication Method of Distributed Cluster-based IoT Devices", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 19, No. 2, pp.103-109, 2019.04. DOI: 10.7236/JIIBC.2019.19.2.103

[8] Kim Sung-hwan, Kim Young-gon, "A Study on Contract Management Platform Based on Blockchain", The Journal of The Institute of Internet, Broadcasting and Communication, vol. 19, No. 3, pp.103-109, 2019.06.
DOI:10.7236/ JIIBC.2019.19.3.97.

저 자 소 개

김 성 환(정회원)

- 2009년 2월: 열린사이버대학교 정보통신공학과(공학사)
- 2017년 8월: 한국산업기술대학교 소프트웨어융합공학과(공학석사)
- 2017년 9월~현재: 한국산업기술대학교 컴퓨터공학과 박사과정
- 관심분야 : 소프트웨어공학, 정보통신시스템, 임베디드 시스템

김 영 곤(정회원)

- 1983년 2월: 경북대학교 전자공학과(공학사)
- 1985년 2월: 연세대학교 본대학원 전자공학과(공학석사)
- 2000년 2월: 한국과학기술원 전산학과(공학박사)
- 1985년~2007년: KT 수석연구원
- 2007년~현재: 한국산업기술대학교 컴퓨터공학과 교수
- 관심분야 : 소프트웨어공학, 정보통신시스템, 객체지향 분석 및 설계