공공 클라우드 환경에서 분산원장 기술을 활용한 데이터 통신 프로토콜 설계

경종수*
케이엘정보통신(주)
e-mail:jskyoung@klic.co.kr

A Design of Data Communication Protocol using Distributed Ledger Technique in Public Cloud Environment

Jong-Soo Kyoung*
Klic Co., Ltd

요 약

부처 및 공공기관에서 운영중인 대민·행정시스템을 효율성있고 안전하게 운영하기 위해 모든 정보시스템을 클라우드로 전면 전환 및 통합한다고 정부에서 발표하였다. 클라우드 서비스로 전환되면 수요자 중심의 디지털 행정서비스를 수행이 가능하고, 향후 보안성과 안정성을 강화할 수 있다. 그러나 클라우드 서비스 환경에서는 신규 및 변종공격에 따른 공격위험과 취약점이 존재하여 메시지 통신 프로토콜에 대한 보완이 필요하다. 그러므로 본 논문에서는 공공 클라우드 환경에서 분산원장 기술을 활용한 데이터 통신 프로토콜을 설계하고자 한다. 제안한 통신 프로토콜의 대표적인 공격위협에 대해서 보안성을 평가하였다.

1. 서론

행전안전부에서는 행정·공공기관 정보시스템의 클라우드 전환을 위해 2021년 7월 27일날 “행정·공공기관 정보자원 클라우드 전환·통합 추진계획” 발표하였고 모든 정보시스템(10,009개)를 클라우드로 전환·통합한다고 밝혔다. 클라우드 서비스 전환으로 대민으로부터 다양한 서비스를 제공할 수 있으며, 담당자 측면에서는 효율성 있는 업무를 위한 대응체계를 구축한다고 했다[1][4]. 그러나 클라우드 서비스 환경에서 신규·변종에 따른 공격위협이 존재하고 있으며, 이에 대한 피해가 발생 시 경제적인 손해가 막대하다[2]. 그러므로 본 논문에서는 공공 클라우드 환경에서 분산원장 기술을 활용한 데이터 통신 프로토콜을 설계하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 블록체인 개요, 클라우드 서비스 운영환경의 보안요구사항에 대해 선행연구를 수행한다. 3장에서는 사용자 ID 발급 및 등록 단계, 데이터 통신 프로토콜을 설계한다. 4장에서는 기존 클라우드 서비스 환경에 발생하는 대표적인 위협에 대해서 보안성을 분석한다. 5장에서는 본 논문의 결론을 맺는다.

2. 선행연구

2.1 블록체인 개요

블록체인 기술을 기반하는 비트코인은 2008년 사토시 나카모토의 “A Peer-to-Peer Electronic Cash System”논문으로 탈중앙화 기반의 새로운 전자 화폐 시스템을 제안하였다. 블록체인은 P2P 방식으로 분산 네트워크 환경에서 참여 가능한 사용자가 거래내역을 기록 및 저장하고 각 참여자들이 새로운 블록 시스템을 검증하도록 한 시스템이다. 특징은 중앙에서 관리하는 서버 없이 안전하게 거래가 된다는 장점이 있다.

블록체인은 참여하는 네트워크 환경 및 범위, 성격에 따라서 퍼블릭 블록체인과 프라이빗 블록체인으로 나누워져 있으며, 대표적인 예는 비트코인, 이더리움 등이 있다[2-3].

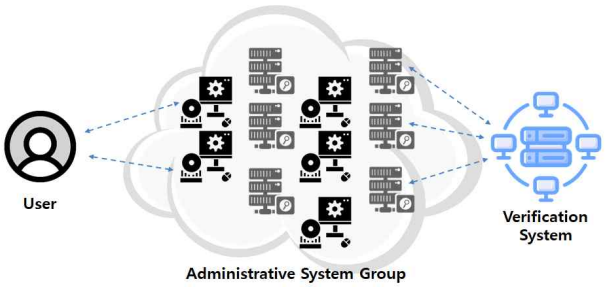
퍼블릭 블록체인과 프라이빗 블록체인은 우선 작성권한에서 차이가 있다. 퍼블릭 블록체인은 모든 참여 대상이 가능하며, 프라이빗 블록체인은 허가된 기능이 가능하다. 전송속도 측면에서 다수의 블록체인을 참여하는 퍼블릭 블록체인은 프라이빗 블록체인 대비 속도가 느리다는 특징이 있으며, 누구나 참여가 가능하다. 마지막으로 권한에서는 퍼블릭 블록체인은 누구나 블록체인 값을 통해 관리가 가능하지만, 프라이빗 블록체인은 개별적인 권한 관리가 가능하다[4].

2.2 클라우드 서비스 운영환경의 보안요구사항

클라우드 서비스 환경에서 안전하게 운영하기 위해 고려해야 할 보안사항은 기술적, 조직적, 정책적으로 보안 고려사항을 숙지해야 한다. 우선 기술적 보안요구사항에서는 데이터 보안과 암호화, 접근 제어 관리, 인프라 보안 사고대응 관리범위와 비즈니스 연속성이 있다. 그리고 조직적 보안요구사항에서는 접근 제어 관리, 어플리케이션 보안, 인프라 보안, 정보 거버넌스, 사고 대응, 컴플라이언스와 감사관리, 관리 범위와 비즈니스 연속성이 있다. 마지막 정책적 보안고려사항에서는 계약 및 E-디스커버리가 있다. 앞서 언급한 보안 요구사항을 충족 후 클라우드 서비스 환경에서 시스템을 운영해야만 사고 발생의 따른 원인추적 및 사후 대응관리가 가능하다 [2][5].

3. 공공 클라우드 환경에서 분산원장 기술을 활용한 데이터 통신 프로토콜 설계

본 장에서는 공공 클라우드 환경에서 분산원장 기술을 활용하여 데이터 통신 프로토콜을 설계하고자 한다. 데이터 통신을 수행하기 앞서 사용자의 ID 발급 및 등록 단계를 진행한다. 이후 데이터 통신 단계에서는 사용자 인증 후 데이터 통신 절차를 진행한다. 본 논문에서 제안한 데이터 통신 구성도는 아래 [그림 1]과 같다.



[그림 1] 데이터 통신 구성도

3.1 사용자 ID 발급 및 등록 단계

① User Registration Request

사용자는 행정시스템A로부터 사용자 등록 요청 메시지를 전송한다. 송신되는 메시지에서는 사용자의 ID, 사용자의 인증값, 사용자의 비밀값이 포함되어 있다. 그리고 행정시스템에서는 블록의 해쉬값을 생성한다.

$$USER_{ID},\ E_{PK\_U}(User_{Cert}||H(User_{PW}) \quad (식\ 1)$$

$$\text{Previous Hash} \quad (식\ 2)$$
$$= \text{Administrative System A(Nonce)}$$
$$\oplus H(USER_{Cert}||H(USER_{PW})||TIMESTAMP$$

② Send Verification Value

행정시스템A는 검증시스템으로부터 검증값요청 메시지를 전송한다. 전송한 메시지는 앞서 수신 받은 값과 생성한 블록의 해쉬값이 포함되어 있다. 메시지를 수신한 검증시스템은 메시지를 검증한다. 이후 블록체인 등록을 사용자 식별값과 블록체인값을 생성한다. 생성한 값을 기반으로 사용자 식별값과 블록체인값을 저장한다.

$$User_{IV-i} = \text{Verification System}(_{Nonce})\oplus USER_{ID} \quad (식\ 3)$$
$$||\text{Administrative System A(Info)}$$

$$\text{Block Chain}_{UserIV-i}= \quad (식\ 4)$$
$$USER_{ID}||\text{Administrative System A(Info)}$$

③ Send Validation and Registration Completion Messages

검증시스템에서는 행정시스템A로 검증 및 등록 완료 메시지를 전송한다. 전송한 메시지에서는 앞서 생성한 사용자 식별값이 포함되어 있다. 행정시스템A는 수신받은 메시지를 검증 후 블록체인값을 계산한다. 이후 행정시스템은 사용자 식별값과 블록체인값을 저장한다.

$$E_{PK\_V}(USER_{IV}) \quad (식\ 5)$$

④ Send Subscriber Add Notification Message

검증시스템에서는 행정시스템A로 검증 및 등록 완료 메시지를 전송하면서, 행정시스템B로 등록자가 추가되었다는 메시지를 전송한다. 전송한 메시지에서는 사용자의 식별값과 알려진 신원정보값이 포함되어 있다. 이후 사용자의 식별값과 블록체인값을 저장한다.

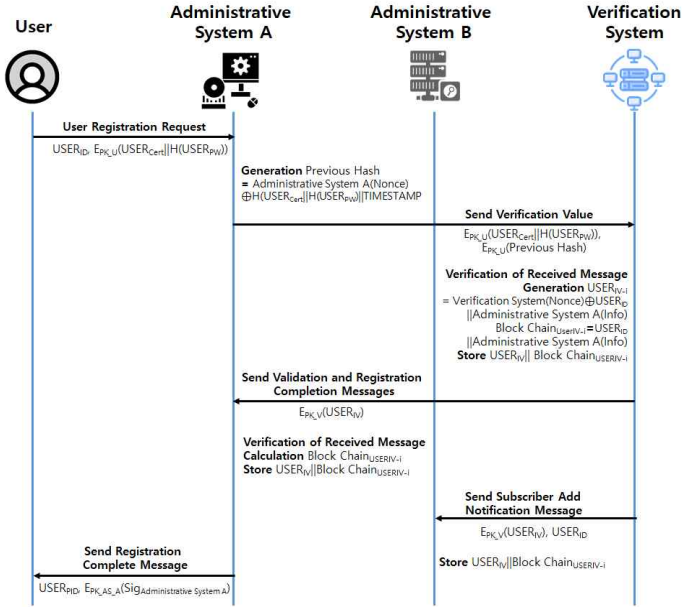
$$E_{PK\_V}(USER_{IV}),\ USER_{ID} \quad (식\ 6)$$

⑤ Send Registration Complete Message

행정시스템A는 사용자로부터 등록완료메시지를 전송한다. 송신한 메시지에서는 사용자의 참여아이디와 행정시스템A의

서명값이 포함되어 있다. 앞서 발송한 메시지를 종결로 사용자 ID 발급 및 등록 절차를 마무리한다.

$$USER_{PID},\ E_{PK\_AS\_A}(Sig_{Administrative\ System\ A}) \quad (식\ 7)$$



[그림 1] 사용자 ID 발급 및 등록 단계 절차

3.2 데이터 통신 프로토콜 설계

① Send an Access Request Message

사용자는 행정시스템B로 접근을 하기 위해 접근요청 메시지를 전송한다. 송신되는 메시지에서는 앞 절에서 수신받은 참여아이디와 서명값이 포함되어 있다.

$$USER_{PID},\ E_{PK\_AS\_A}(Sig_{Administrative\ System\ A}) \quad (식\ 8)$$

② User Verification Request

행정시스템B는 수신한 메시지를 확인하고 행정시스템A로부터 서명값 검증 요청메시지를 전송한다. 송신되는 메시지는 서명값이 포함되어 있다.

$$E_{PK\_AS\_A}(Sig_{Administrative\ System\ A}) \quad (식\ 9)$$

③ User Verification Response

행정시스템A는 수신받은 메시지를 확인 후 개인키로 암호화하여 응답메시지를 전송한다. 응답메시지에서는 타임스탬프값과 난수값이 포함되어 있다.

$$E_{PRK\_AS\_A}(TIMESTAMP) \oplus H(Nonce) \quad (식\ 10)$$

④ Send Requested Data after Access

행정시스템B는 사용자로부터 요청한 데이터 전송메시지를 송신한다. 송신한 메시지에서는 세션키로 암호화된 데이터가 포함되어 있다. 여기서 세션키는 사용자의 인증값과 참여아이디를 결합하여 생성한 값이다.

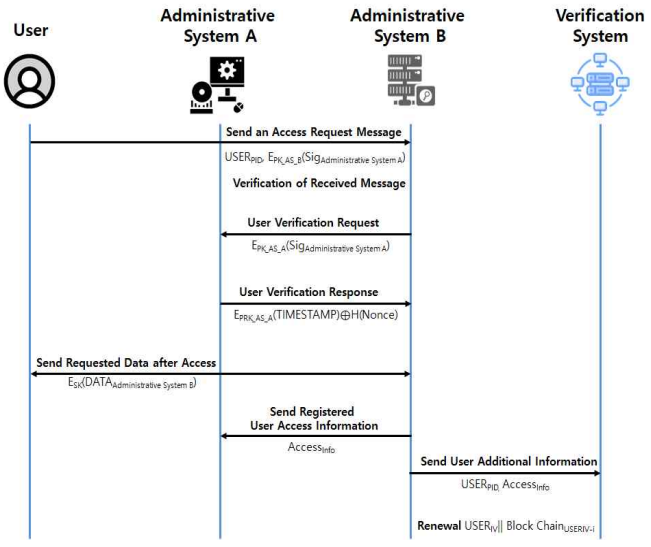
$$E_{SK}(DATA_{Administrative\ System\ B}) \quad (식\ 11)$$

⑤ Send Registered User Access Information

행정시스템B는 행정시스템A로 사용자가 접근했다는 메시지를 전송한다.

⑥ Send User Additional Information

그리고 행정시스템B는 검증시스템으로부터 사용자 접근에 따른 추가정보가 포함된 메시지를 전송한다. 검증시스템은 해당되는 메시지를 수신 후 기존의 등록된 블록체인 메시지 값을 갱신한다. 수신받은 메시지를 종결로 데이터 통신 프로토콜을 마무리한다.



[그림 3] 제안한 데이터 통신 프로토콜 설계

4. 보안성 평가

본 장에서는 앞서 제안한 통신프로토콜에 대해서 보안성

평가를 수행한다. 대표적인 공격기법인 이중 지불 공격에 대한 위협, 위장 공격에 대한 위협, 중간자 공격, 데이터 무결성 공격에 대해서 보안성을 분석하도록 한다.

이중 공격에 대한 위협 : 이중 공격은 블록체인 환경에서 발생하는 대표적인 공격이다. 이중공격은 중앙화 인증기관이 설계되지 않은 환경에서 이중 장부를 기록하게 만들어 각 도메인의 혼란을 주는 공격방법이다. 그러나 검증시스템에서는 $USER_{IV}$|| Block $Chain_{USERIV-i}$을 갱신 후 다른 도메인으로부터 실시간으로 전송함으로써 이중공격에 대한 위협을 대응할 수 있다.

위장 공격에 대한 위협 : 외부의 해커가 악의적인 목적을 가지고 사용자로 위장하여 운영하고 있는 시스템 환경으로 침투하려는 시도를 가정했을 때, 제안한 프로토콜의 인증과정과 $USER_{PID}$, 암호화된 데이터 $USER_{IV}$를 검증함으로써 위장공격이 실패하게 된다.

중간자 공격에 대한 위협 : 중간자 공격은 클라우드 환경에서 발생하는 대표적인 공격기법으로 데이터 탈취, 위조, 와 같은 위협이 발생하고 있다. 이러한 공격을 대응하기 위해 검증시스템에서 블록체인 기반의 $USER_{IV}$, Block $Chain_{USERIV-i}$ 생성하였다. 생성된 $USER_{IV}$, Block $Chain_{USERIV-i}$ 값을 활용하여 데이터 검증을 수행함으로써 기존대비 보안성을 향상 시킬 수 있다.

데이터 무결성 위협 : 네트워크 환경에서 데이터 전송에 따른 데이터 무결성에 대한 위협이 발생한다. 이를 보완하기 위해서 사용자 ID발급 및 등록단계에서 생성된 값을 $USER_{PID}$, $E_{PK_AS_A}(Sig_{Administrative\ System\ A})$을 기반으로 검증 후 데이터를 안전하게 송신하도록 설계하였다.

[표 1] 기존 클라우드 시스템 대비 보안성 분석 결과

	기존 클라우드 시스템	제안한 통신 프로토콜
이중 공격에 대한 위협	위협요소 존재	대응가능
위장 공격에 대한 위협	안전하지 않음	안전함
중간자 공격에 대한 위협	-	대응가능
데이터 무결성 위협	안전하지 않음	안전함

5. 결론

본 논문에서는 공공 클라우드 환경에서 분산원장 기술을 활용한 데이터 통신 프로토콜을 설계하였다. 제안한 통신 프로토콜 과정에서는 사용자 ID 발급 및 등록 단계, 데이터 통신 프로토콜을 설계하여 데이터를 안전하게 전송하도록 설계하였다.

제안한 통신 프로토콜의 보안성 평가를 수행하기 위해서 기존 공공 클라우드 환경에서 발생하는 위장공격, 중간자 공격, 데이터 무결성과 블록체인 환경에서 발생하는 신규 공격기법인 이중 지불공격에 대해서 보안성을 분석하였다.

공공 클라우드 환경은 점차 개방적인 환경으로 전환하게 이를 사용하는 대민으로부터 다양한 서비스를 제공하고 있어, 신규 및 변종공격기법에 대해서 꾸준히 연구를 수행해야 한다. 그리고 이를 안전하게 활용할 수 있는 보안정책에 대한 수립도 필요하다. 향후 연구로써는 다양한 행정시스템에서 적용할 수 인증시스템을 확장할 계획이다.

참고문헌

[1] Chul-Jin Kim, "A Static and Dynamic Design Technique of Smart Contract based on BlockChain", Korea Academy Industria Cooperation Society, Vol. 19, No. 6, pp. 110-119, Jun. 2018.

[2] 김정호, 허재욱, 전문석. "스마트 홈 환경에서 C-PBFT 기반의 디바이스 인증 프로토콜 설계", 한국산학기술학회 논문지, Vol. 5, No. 20,

[3] 이광형, 이재승, "IoT 환경에서 해시 체인 기반 센서 상호 인증 기법", 한국산학기술학회 논문지, Vol. 11, No. 19, pp. 303-309, Nov. 2018.

[4] KDI 경제정보센터 , 2025년까지 모든 행정·공공기관 정보시스템 클라우드로 전환, https://eiec.kdi.re.kr/policy/materialView.do?num=216446&cat=epic1&source=newsletter&utm_campaign=9_KDI_Letter_Send&utm_source=newsletter&utm_medium=email

[5] 정보통신단체표준(TTAS), 클라우드 보안 사고 조사 참조 모델 및 고려 사항, TTAK.KO-10.1041, 2017-12-13