공공 클라우드 서비스 환경에서 안전한 메시지 전송을 위한 통신 프로토콜 설계

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

A Design of Communication Protocol for Secure Message Transmission in Public Cloud Environment

Jong-Soo Kyoung
Klic Co., Ltd

요 약

부처 및 공공기관에서 안정성 높은 서비스를 운영하기 위해서 운영하는 정보시스템을 클라우드 전환 및 통합작업을 수행하고 있다. 운영하는 모든 정보시스템이 클라우드 서비스로 전환되면 수요자 맞춤형 디지털 행정서비스에 대한 수행이 가능하고 향후 물리적인 측면에서 비용 절감과 생산성 향상을 기대할 수 있다. 그러나 클라우드 서비스 환경에서는 다양한 보안위협이 존재하고 있으며, 공격자가 이를 통해 서비스 장애가 발생 시 막대한 경제적인 피해가 발생할 수 있다. 그러므로 본 논문에서는 공공 클라우드 서비스 환경에서 안전한 메시지 전송을 위한 통신 프로토콜을 설계하고자 한다. 제안한 통신프로토콜에 대해서 안전성 분석과 기존 클라우드 시스템 대비 보안성 분석을 수행하였다.

1. 서론

클라우드 컴퓨팅 서비스는 직접 공유된 정보통신기기, 통신설비, 소프트웨어 등 정보자원을 활용하는 사용자에 따라서 효율적으로 이용할 수 있는 정보처리체계가 정의할 수 있다[1-2]. 클라우드 서비스 기술을 활용하면 공간적 제약, 단말기 제약을 받지 않고 업무를 처리할 수 있는 업무환경이 구축되어 안전하게 서비스를 운영할 수 있다. 그러나 다양한 서비스 클라우드 서비스 이면에는 다양한 보안위협이 존재한다. 대표적으로 클라우드 도메인을 이용한 공격, 설정이 취약한 클라우드 서비스 공격, 공개 저장소에 노출된 자격 증명 값 등이 존재한다[2]. 공격자는 이러한 공격기법을 통해 클라우드 서비스 장애가 발생 시 막대한 경제적인 피해가 발생한다[3]. 그러므로 본 논문에서는 공공 클라우드 서비스 환경에서 안전한 메시지 전송을 위한 통신 프로토콜을 설계하고자 한다. 본 논문의 구성은 다음과 같다. 2장 선행연구에서는 공공 클라우드 정의, 공공 클라우드 서비스에 대한 보안위협 요소에 대해서 서술한다. 3장 제안부에서는 안전한 통신 메시지 전송을 위한 프로토콜을 설계하도록 한다. 4장에서는 2장 선행연구에서 언급한 보안위협에 대해서 안전성 분석을 수행하고, 기존 클라우드 시스템 대비 보안성 분석을 수행한다. 5장에서는 마지막 장으로 본 논문의 결론을 맺는다.

2. 선행연구

2.1 공공 클라우드 정의

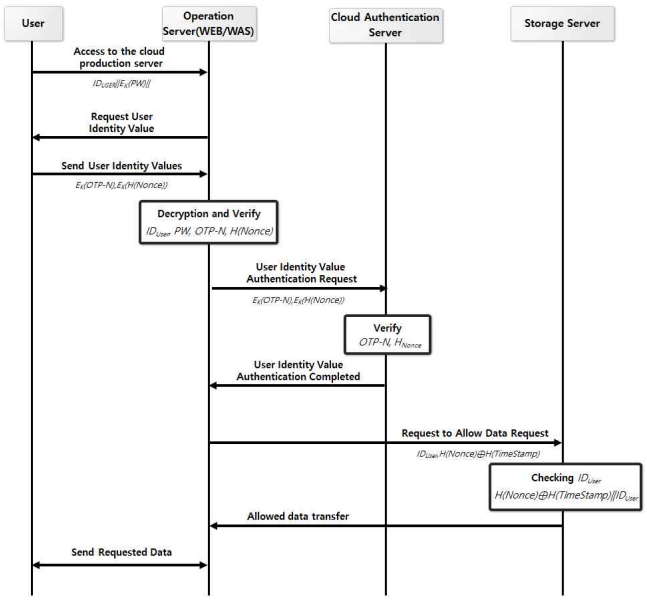
클라우드컴퓨팅법 제2조제3호의 정의에 따라 클라우드 컴퓨팅서비스는 타인에게 정보통신자원을 제공하는 서비스라 말한다. 동법 시행령(제3조)에서는 대통령령으로 정한 서비스는 서버, 저장장치, 네트워크 등을 제공하는 서비스, 응용프로그램 등 소프트웨어를 제공하는 서비스, 응용프로그램 등 소프트웨어의 개발·배포·운영·관리 등을 위한 환경을 제공하는 서비스를 중에 하나에 해당되는 서비스를 말한다[1][3]. 여기서 공공 클라우드 서비스는 행정기관이 용역발주 등을 통해 클라우드 컴퓨팅 기술을 활용하여 자체적으로 구축한 거는 클라우드 컴퓨팅 서비스라 할 수 없다. 행정 및 공공기관의 업무 효율성 향상을 위해 클라우드 기술에 대한 도입이 필요하여 전자정부법 제54조의2가 신설되었고 클라우드 컴퓨팅 서비스에 대한 이용을 우선시 하도록 정책을 강화하였다[1][4]. 신규로 정보시스템을 구축하거나 운영 및 관리하는 입장에서는 클라우드 컴퓨팅 서비스 이용을 우선적으로 검토해야하고 디지털 환경변화에 유연하게 대응해야한다[2].

2.2 공공 클라우드 서비스 보안위협 요소

공공 클라우드 서비스 환경에서는 클라우드 서비스에 대한 취약점을 이용하여 공격하는 기법이 존재한다. 우선 무결성에 대한 위협요소에서는 데이터 침해, 불충분한 아이덴티티, 자격증명, 내부자 위협 등이 있다[3-4]. 그리고 기밀성에 대한 위협요소에서는 클라우드 보안 아키텍처 및 전략 부족, 엑세스 키 관리, 계정도용, 취약한 제어 영역 등이 있다. 마지막으로 가용성에 대한 위협요소에서는 제한된 클라우드 사용 가시성, 클라우드 서비스의 남용 및 악의적인 사용이 있다. 그밖에도 메타 구조와 응용 구조 실패, 로그인 보안취약으로 인한 계정 도용이 있다[5].

3. 제안한 통신 프로토콜 설계

본 장에서는 공공 클라우드 서비스 환경에서 안전한 메시지 전송을 위한 통신 프로토콜 설계에 대한 내용을 서술한다. 제안한 공공 클라우드 서비스 환경에서는 사용자, 클라우드 인증서버, 스토리지 서버, 운영서버로 구성되어 있으며 통신 프로토콜에 대한 절차는 아래 [그림 1]과 같다.



[그림 1] 제안한 통신 프로토콜 절차

1. 사용자는 운영서버(WEB/WAS)를 통해서 클라우드 서비스에 대한 접근요청을 수행한다.

$$ID_{USER}||E_K(PW)$$

2. 운영서버는 사용자로부터 식별 값을 요청한다.

3. 사용자는 운영서버에 대한 식별값 메시지를 확인 하고 사용자 OTP Factor에 난수 값을 기반으로 식별 값에 대한 메시지를 전송한다.

$$E_K(OTP\text{-}N),\ E_K(H(Nonce))$$

3. 운영서버에서는 앞서 수신한 메시지에 대해서 복호화 및 검증을 수행한다.

4. 운영서버는 클라우드 인증서버로 사용자 식별값 인증 요청 메시지를 전송한다.

$$E_K(OTP\text{-}N),E_K(H(Nonce)$$

5. 클라우드 인증 서버에서는 인증서버에서 수신한 메시지를 검증 후 사용자로부터 인증완료 메시지를 전송한다.

6. 운영서버에서는 인증서버로부터 운영완료 메시지를 확인한 다음에 스토리지 서버로부터 허용된 데이터를 요청한다.

$$ID_{USER},\ H(Nonce)\oplus H(Timestamp)$$

7. 스토리지 서버에서는 운영 서버에 대한 데이터(사용자 ID, 운영서버에서 연접한 Timstamp값을 검증한다.

$$H(Nonce)\oplus H(Timestamp)||ID_{User})$$

8. 운영서버는 스토리지 서버로부터 서용된 데이터를 수신 후 검증한 다음 사용자로부터 요청한 데이터를 전송한다.

4. 보안성 평가

본 장에서는 제안한 통신 프로토콜에 대해 앞 장의 언급된 클라우드 서비스 보안위협 요소를 기반으로 공격기법에 따른 안전성과 보안성을 평가한다. 데이터 침해, 내부자 위협, 엑세스 키 관리, 악의적인 사용자에 따른 클라우드 서비스 남용에 대한 안전성 분석 내용은 아래와 같다.

데이터 침해 : 클라우드 서비스 환경에서 발생하는 데이터 침해에 대한 위협은 표적 공격 또는 부적절한 보안 관행, 공개되지 않은 데이터 유출로부터 위협이 된다. 데이터 침해에 대한 위협을 보완하기 위해 설계한 프로토콜의 식별값($H(Nonce)\oplus H(Timestamp)$)를 통해 안전한 통신을 수행할 수 있다.

내부자 위협 : 클라우드 서비스 환경에서 발생하는 대표적인 위협인 내부자 위협은 엑세스 권한 유무에 상관하지 않고 의도하지 않는 방식으로 악의적인 영향을 발생하는 것을 말한다. 본 논문에서는 내부자 위협을 방지하지 위해서 인증서버에 대한 사용자 식별 값(*OTP-N, H(Nonce)*)을 검증함으로써 내부자 위협에 대한 취약점 대응이 가능하다.

엑세스 키 관리 : 클라우드 서비스를 운영하는 환경에서는 중요한 리소스에 대한 엑세스 관리, 모니터링 할 수 있는 도구에 대한 정책이 미흡하다. 이에 따른 보안성을 강화하기 위해서는 클라우드 인증서버에서 Timestamp를 생성 후 사용자가 전송한 식별값(H(Nonce))를 기반으로 식별값을 저장 후 관리함으로써 안전하다.

악의적인 사용자에 따른 클라우드 서비스 남용 : 클라우드 서비스 환경을 운영하는 담당자 측면에서 사용자 조직 기타 클라우드 공급자를 대상으로 악의적인 수행행위가 발생한다. 이러한 위협요소를 보완하기 위해서 운영서버에서 인증서버로 사용자의 식별값 검증과 스토리지 서버로 사용자 식별값, 운영서버의 인자값 검증을 수행함으로써 서비스 운영에 대한 안정성을 높일 수 있다.

[표 1] 기존 클라우드 시스템 대비 보안성 분석 결과

	기존 통신 프로토콜	제안한 통신 프로토콜
데이터 침해	위협요소 존재	대응가능
내부자 위협	취약점 존재	취약점 대응가능
엑세스 키 관리	-	키 관리에 따른 보안성 강화
악의적인 사용자에 따른 클라우드 서비스 남용	-	서비스 운영이 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] 이광형, 이재승, "IoT 환경에서 해시 체인 기반 센서 상호 인증 기법", 한국산학기술학회 논문지, Vol. 11, No. 19, pp. 303-309, Nov. 2018.

[2] 행정·공공기관 클라우드 컴퓨팅 서비스 이용안내서, NIA, 행정안전부, 2022. 6.

[3] 경종수 ,공공 클라우드 환경에서 분산원장 기술을 활용한 데이터 통신 프로토콜 설계, 2022 산학기술학회 추계학술대회

[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