클라우드 컴퓨팅 환경에서 안전한 데이터 관리 및 전송을 위한 공공정보시스템 연구

조경모*
*(주)지오인프라
e-mail:chokm@gioinfra.co.kr

A Study of Public Information System for Secure Data Management and Transmission in Cloud Computing Environment

Kyung-Mo Cho*
*Gioinfra Co., Ltd

요 약

코로나 팬데믹 기간 클라우드 컴퓨팅 기술을 활용한 서비스 기술이 급증하고 있으며, 국내 국가기관에서도 클라우드 컴퓨팅 전환이 진행되고 있다. 클라우드 전환사항을 통해 다양하고 긴급한 행정수요에 정보서비스를 제공할 수 있도록 목표하고 있다. 그러나 공공 클라우드 컴퓨팅 전환에 따른 보안 이슈가 존재하고 있으며, 프라이버시 및 신규 및 변종 보안 이슈로 인한 문제점이 있다. 본 논문에서는 공공정보시스템을 안전하게 데이터 관리 및 통신을 위한 연구를 수행하도록 한다. 제안한 시스템의 대표적인 보안위협 및 취약점을 분석하여 보안성을 평가한다.

1. 서론

ICT기술의 발전으로 인해 과거의 클라우드 컴퓨팅 환경이 폐쇄적인 환경에서 공공성으로 전환되고 있으며 클라우드 컴퓨팅 기술이 폭넓게 활용되고 있다. 국내 범부처, 지자체, 공공기관에서도 클라우드 컴퓨팅 전환 작업을 진행하고 있으며, 전환된 작업을 기반으로 대국민으로부터 다양한 서비스를 진행하고자 한다[1][3].

하지만 클라우드 컴퓨팅 기술을 통한 비용, 기술적, 경제적인 문제가 이슈되고 있으며, 데이터 관리에 따른 취약점 및 위협사항이 존재하고 있다[2].

본 논문에서는 클라우드 컴퓨팅 환경에서 안전한 데이터 관리 및 전송을 위한 공공정보시스템 설계에 대한 연구를 수행하고자 한다.

2. 관련연구

2.1 공공 클라우드 전환사례 및 기술동향

2022년부터 국내 부처·지자체 공공기관의 1만여 개의 시스템을 2025년까지 클라우드로 전환을 목표로 하고 있다. 수요기관은 민간 클라우드와 정부가 지정한 공공 클라우드 컴퓨팅 센터를 선택하여 도입·전환한다[1].

공공부분을 클라우드 컴퓨팅 서비스 전활응 위해 클라우드서비스보안인증(CSAP)인증 제도를 거쳐서 운용하고 있으며, 여러 기관 사업에서 서비스 보안성과 안정성을 담보하고 있다.[2-4]

클라우드 컴퓨팅 기술 동향에 대해서 살펴보면 초기의 기업들은 Private 방의 클라우드를 구축하였다. 내부의 데이터 자체를 보관하고 보안성을 중시하였다. 하지만 ICT 기술의 발전과 기술 활용에 따른 미흡 사항이 발생하여 Public 클라우드 방식으로 전환하고 있다. Public 클라우드 기술은 초기 구축 비용이 상대적으로 적고 관리가 용이하다는 장점이 있다. 하지만 엄격한 보안성 검토와 활용할 수 있는 제약사항이 생겨서 도입에 따른 사항에서 고려하고 있다[2].

국내 공공부분 디지털혁신을 위해서 Public 클라우드를 전환하고 있으며, 위의 언급한 클라우드 보안인증제(CSAP)를 활용하여 서비스를 사용하는 대민으로부터 보다 안정적인 서비스를 제공하도록 연구하고 있다[3].

2.2 클라우드 컴퓨팅 환경의 보안위협

클라우드 컴퓨팅을 운영하는 환경에서는 다양한 보안 위협을 통해 사용자의 프라이버시 침해 및 경제적 피해가 발생할 수 있다. 대표적인 클라우드 컴퓨팅 환경의 보안 위협은 익명성을 이용한 공격, 클라우드 컴퓨팅의 관리적인 측면의 운영, 신규 및 변종에 따른 외부 공격, 법제도적 취약함을 이용한 공격이 있다. 아래의 [표 1]은 클라우드 컴퓨팅 환경에서 대표적인 보안 위협에 대해 서술하였다[5-6].

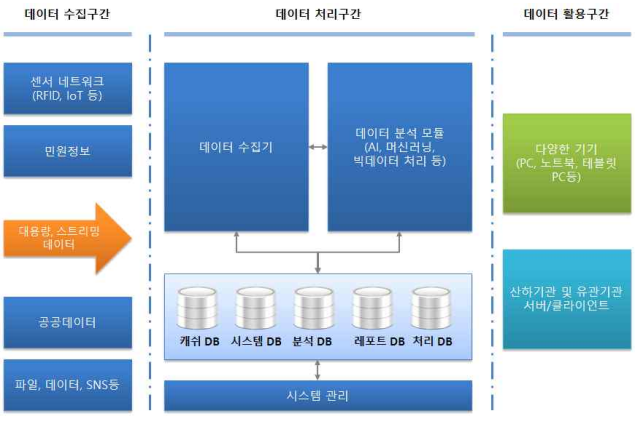
[표 1] 클라우드 컴퓨팅 환경의 대표적인 보안위협

구분	설명
익명성을 이용한 공격	▪ 외부로 수집되는 다양한 데이터 중 익명성을 이용하여 웹쉘, 악성코드 등을 유입 후 운영 중인 클라우드 컴퓨팅 시스템의 서비스를 중지할 수 있음
클라우드 컴퓨팅의 관리적인 측면의 운영	▪ 운영하는 내부자의 실수로 인한 데이터 손실 및 유출, 악의적인 의도를 가지고 데이터를 파괴하는 보안 위협이 존재
신규 및 변종에 따른 외부 공격	▪ 무선네트워크 환경에서 발생하는 공격 외로 기존의 공격방식을 변형한 변종공격과 신규 다양한 공격기법이 존재
법제도적 취약함을 이용한 공격	▪ 클라우드는 여러 국가에서 서비스를 제공할 수 있는데 각 국가의 법제도에 따른 기존이 표준화되어 있지 않아 법률의 적응속도를 노린 타겟팅 공격 기법이 존재

3. 클라우드 컴퓨팅 환경에서 안전한 데이터 관리 및 전송을 위한 공공정보시스템 설계

3.1 제안한 공공정보시스템 구성도

본 절에서는 클라우드 컴퓨팅 환경에서 안전한 데이터 관리 및 전송을 위한 공공정보시스템을 설계하고자 한다. 제안한 공공정보시스템 설계에 따른 구성도는 아래 [그림 1]과 같다.



[그림 1] 제안한 공공정보시스템 구성도

클라우드 컴퓨팅 환경을 기반으로 데이터 수집구간, 데이터 처리구간, 데이터 활용구간으로 나누어져 있다. 우선 데이터 수집구간에는 센서 네트워크 수집항목, 민원정보, 공공데이터, 파일, 데이터, SNS 등의 데이터를 수집한다. 그리고 데이터 처리구간에서는 데이터 수집기, 데이터 분석 모듈(AI, 머신러닝, 빅데이터 처리 등) 통합 DB, 시스템 관리로 구성되어 있다. 마지막으로 데이터 활용구간에서는 담당자가 활용할 수 있는 다양한 기기(PC, 노트북, 테블릿 PC 등)와 산하기관 및 유관기관 서버/클라이언트로 구성되어 있다.

3.2 제안한 데이터 통신 프로토콜 설계

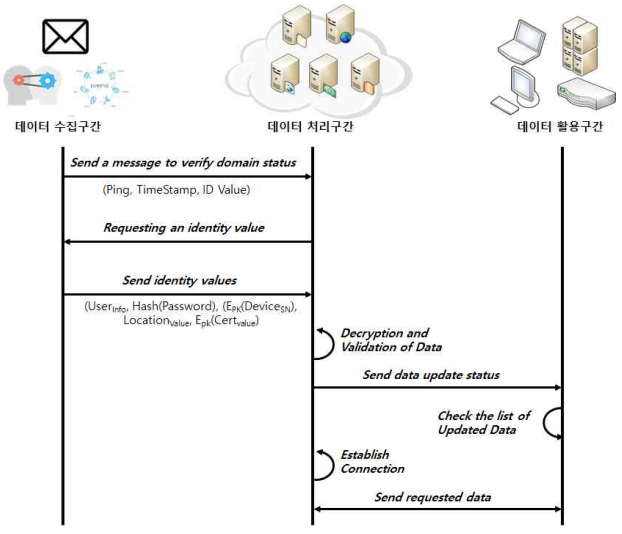
본 절에서는 각 구간 사이의 데이터를 안전하게 전송하기 위한 통신 프로토콜을 설계하고자 한다. 안전한 데이터 수집을 위해 데이터 수집구간에서는 데이터 처리구간으로 도메인 상태 관련 메시지를 전송한다. 데이터 처리구간으로 보내는 메시지 값의 항목은 아래 [식 1]과 같다.

$$<\text{Ping}||\text{TimeStamp}||\text{ID}_{\text{Value}}> \quad \text{(식 1)}$$

이후 데이터 처리구간에서는 신원 검증항목에 대한 메시지를 값을 요청한다. 데이터 수집구간에서는 신원검증값을 전송하는데, 일반적인 공개 데이터에서는 데이터 정보, 수집된 위치 값을 송부하지만, 사용자의 정보 및 검증 값을 보낼 때 접근권한과 사용하는 디바이스의 식별값을 고려하여 아래 [식 2]와 같은 메시지를 전송한다..

$$<\text{User}_{\text{Info}}, \text{HAsh(Password)}, (E_{PK}(\text{Device}_{SN}), \text{Location}_{\text{Value}}, E_{PK}(\text{Cert}_{\text{Value}})> \quad \text{(식 2)}$$

이후 데이터 처리구간에서는 수신 받은 데이터를 복호화하고 데이터 검증을 수행한다. 그리고 데이터 처리구간에서는 데이터 활용구간으로 현재 갱신된 상태에 따른 메시지(ex. Ping, Updated Status Values 등)를 전송한다. 데이터 활용구간에서는 갱신된 데이터 항목에 대한 값을 검증한 후 데이터 처리구간에서 안전하게 데이터 송신을 위해 안전한 채널 송신 설정을 수행한다. 마지막으로 데이터 송신 설정이 완료되면 안전하게 데이터를 전송한다.



[그림 2] 제안한 통신 프로토콜

4. 보안성 평가

본 장에서는 클라우드 환경기반으로 안전한 데이터 송신을 수행하기 위한 대표적인 클라우드 보안 위협요소에 대해서 분석을 수행하였다. 데이터 무결성, 위장공격, 서비스 장애 공격과 같은 보안 위협에 대해서 보안성 평가를 수행하였다.

데이터 무결성에 대한 침해 : 클라우드 환경에서 데이터 송신시 발생하는 데이터 무결성에 대한 침해를 방지하기 위해 데이터 통신 프로토콜 과정에서 (식 2)와 같은 접근권한 설정을 수행하여 데이터를 안전하게 송신하도록 설계하였다. 인증이 필요한 구간에서는 별도의 $E_{PK}(Cert_{Value})$, $E_{PK}(Device_{SN})$를 검증함으로써 기존의 클라우드 기반의 공공정보시스템 보다 안전하다.

위장공격 : 클라우드 컴퓨팅 환경뿐만 아니라 기존의 유무선 네트워크 환경에서 발생하는 위장공격에 대한 위협을 방지하기 위해서 데이터를 수집, 검증할 때 식1, 식2에 해당되는 파라미터를 검증 후 이를 분석함으로써 위장공격을 실패하게 된다.

서비스 장애 공격 : 24시간 안정적으로 운영하는 대민서비스를 제공하는 공공정보시스템은 가용성에 대한 안전이 보장되어야 한다. 서비스 장애에 대한 안정적인 데이터를 전송하기 위해서 데이터를 수신 후 전송하는 구간에 수신된 메시지를 복호화 후 송신 설정구간을 설계함으로써 데이터 서비스 전송에 대한 보안성을 향상시킬 수 있다.

[표 3] 기존 시스템과 제안한 시스템 비교

	기존 시스템	제안한 시스템
데이터 무결성에 대한 침해	Enable	Disable
위장공격	부분적 접근제어 설정 후 데이터 수집	데이터 수집 시 접근제어 설정 기반에 따른 사용자 분석
서비스 장애 공격	–	○

5. 결론

본 논문에서는 클라우드 컴퓨팅 환경에서 안전한 데이터 관리 및 전송을 위한 공공정보시스템 설계에 대해서 연구를 수행하였다. 공공정보시스템을 구성하여 통신프로토콜을 제안하였으며, 이를 안전하게 수행하기 위해서 접근제어 관련한 파라미터를 설계하였다.

제안한 논문의 보안성을 평가하기 위해 대표적인 보안 위협 요소 데이터 무결성에 대한 침해, 위장공격, 서비스 장애 공격에 대해서 보안성을 분석하였다.

현재 공공정보시스템은 물리적인 서버 환경에서 클라우드 환경으로 전환되는 만큼 신규 및 변종공격에 대한 대응방안 및 보안정책이 연구되어야 한다. 그리고 운영하는 시스템의 보안성 향상과 서비스 제공에 따른 효율성 증대에 따른 메시지 처리 개선방안에 대한 연구가 필요하다.

참고문헌

[1] 전자신문, https://www.etnews.com/20220629000043, “[기획] 공공 클라우드 전환, 정부 서비스 혁신 '단비' 내렸다”
[2] 안보경영연구소(SMI), “국방 클라우드컴퓨팅 운영환경 구축방안 연구”, 2016.
[3] 박준규, 전우진, 이상훈, 박기웅, “민간 클라우드 도입 장애요인 분석을 통한 국방 클라우드 도입 전략 도출” 한국정보보호학회, 2018.
[4] 이은정, “국방 클라우드 보안성 향상을 위한 엣지컴퓨팅 적용방안”, 한양대학교, 2020.
[5] 전자신문, https://www.etnews.com/20211105000161, 제4회 디지털 혁신포럼
[6] 안성원, 유호석, 김다혜클라우드 보안의 핵심이슈와 대응책, 2017. 12. 제2017-006호, 소프트웨어정책연구소