제로 트러스트 기반 AWS S3 설계 및 운영

조경현[O], 조재한[*], 김지연[*]
[O]대구대학교 컴퓨터정보공학부(컴퓨터소프트웨어전공),
[*]대구대학교 컴퓨터정보공학부(컴퓨터공학전공)
e-mail: jgh1118@daegu.ac.kr[O], {chojh0208, jyk}@daegu.ac.kr[*]

Design and Operation of AWS S3 based on Zero Trust

Kyeong-Hyun Cho[O], Jae-Han Cho[*], Jiyeon Kim[*]
[O]Dept. of Computer and Software Engineering, Daegu University,
[*]Dept. of Computer Engineering, Daegu University

● 요 약 ●

기업 및 공공기관의 클라우드 서비스 도입이 확산되면서 업무 시스템에 대한 보안 요구사항이 변화하고 있다. 기존에는 보호해야 할 정보자산이 물리적으로 외부와 분리된 내부 공간에 집중되었다면 클라우드 환경에서는 자산의 분포 범위가 넓어지면서 내부와 외부의 경계가 모호해진다. 따라서 경계 기반의 전통적인 보안 방식은 클라우드 기반 업무환경에 적합하지 않으며 정보 서비스를 이용하는 전 주기에서 암묵적인 신뢰를 배제하고 지속적으로 검증을 수행하는 제로 트러스트 기반의 업무 시스템 운영이 필요하다. 본 논문에서는 스토리지 클라우드 서비스인 아마존 웹 서비스 S3(Simple Storage Service)에 대하여 제로 트러스트 모델을 설계하고, 직접 서비스를 운영하며 제안된 제로 트러스트 모델의 안전성을 검증한다. 제로 트러스트 모델은 스토리지에 접근하는 사용자에 대한 인증 및 식별 기술, 스토리지 암호화 기술, 암호화 키 관리 기술을 활용하여 설계하였으며 제로 트러스트 기술 적용 시, 스토리지 보안성이 향상되는 것을 실제 서비스 운영을 통한 실험을 통해 확인하였다.

키워드: 제로 트러스트(Zero Trust), 아마존 웹 서비스(Amazon Web Service), S3(Simple Storage Service)

I. Introduction

제로 트러스트(Zero Trust)는 'Never trust, always verify'라는 원칙을 바탕으로 제안된 사이버 보안 모델로서 정보 서비스를 이용하는 전 주기에서 지속적으로 사용자, 단말, 서비스 등의 IT 자산을 검증하도록 한다. 2021년부터 국내에서 진행 중인 클라우드 전환 사업으로 인해 기업 및 기관의 클라우드 서비스 도입이 빠르게 확산되고 있으며 기존에는 폐쇄적인 업무환경이 점차 개방된 업무환경으로 변화하고 있다. 이와같이 개방된 업무환경을 위한 새로운 보안기술 개발의 중요성이 점점 커지면서 세분화된 IT 자산에 대해 지속적인 검증을 수행하는 제로 트러스트 보안 모델 개념이 등장하였다. 클라우드 환경에서의 제로 트러스트 기술은 접근 제어를 위한 권한 정책을 설정하고 이를 사용자, 단말, 서비스별로 세분화하여 적용하는 방법으로 구현할 수 있다.

본 논문에서는 아마존 웹 서비스(Amazon Web Service, 이하 AWS)에서 제공하는 클라우드 스토리지 서비스인 AWS S3(Simple Storage Service, 이하 S3)를 안전하게 운영하기 위한 제로 트러스트 모델을 제안하고, 실제 운영을 통해 보안성을 검증한다.

본 논문의 구성은 다음과 같다. 2장에서는 AWS S3 제로 트러스트 모델을 설계하고, 3장에서는 운영을 통한 제로 트러스트 모델의 안전성을 검증한다. 마지막으로 4장에서는 결론 및 향후 연구를 제시한다.

II. Zero Trust-based AWS S3

제로 트러스트 기반의 AWS S3 운영을 위하여 본 연구에서는 먼저 Amazon S3에 버킷을 생성하였고, 접근 제어 목록(Access Control List, 이하 ACL)을 해당 버킷에만 활성화하여 URL로 접근을 가능하도록 설정해 주었다. 버킷에 업로드한 파일은 동영상 파일로서 버킷에 업로드 시 AWS KMS(Key Management System)를 사용하여 파일을 암호화한다. AWS KMS는 사용자별로 사용 권한을 가지고

있으며 Table 1은 본 연구에서 제로 트러스트 모델 설계를 위해 설정한 사용자별 권한 시나리오를 보여준다.

Table 1. 사용자별 AWS KMS 권한 부여 시나리오

시나리오	접근 방법	다운로드 계정
1	내부 다운로드	사용자1
2	내부 다운로드	사용자2
3	객체 URL	없음

3개의 시나리오는 업로드한 동영상에 대한 다운로드 접근 방법 및 다운로드 사용 계정에 따라 구분된다. 시나리오 1은 모든 권한이 부여된 사용자 1이 AWS S3 내부에서 직접 다운로드를 하는 경우이고, 시나리오 2의 경우 권한이 부여되지 않은 사용자 2가 내부 다운로드를 실행하는 경우이다. 시나리오 3은 객체의 URL로 접근을 하는 것이기 때문에 특정 사용자가 지정되지 않은 경우이다. 추가적으로 각 사용자 및 사용자가 속한 그룹의 정책 및 자격을 관리하는 IAM(Identification and Authentication Management) 서비스를 통해 제로 트러스트 구현을 위해 필요한 IAM 권한, KMS 권한, Cloud HSM(Hardware Security Module) 권한을 사용자별로 다르게 부여하였다. 사용자 1은 키를 소유하였을 때 파일 다운로드가 되는지 확인하기 위하여 IAM 권한을 모두 부여하였으며 사용자2는 키를 소유하지 않았을 때 파일에 대한 다운로드를 확인하기 위하여 모든 권한을 부여하지 않았다.

III. Experimental Results

2장에서 설계한 제로 트러스트 모델의 안전성을 검증하기 위하여 AWS S3를 직접 운영하며 시나리오별로 관찰한 결과는 다음과 같다.

사용자 1의 경우에는 KMS와 IAM 권한을 모두 소유하고 있으므로 S3 내부에서 다운로드를 진행하였을 때 파일이 성공적으로 다운로드 되는 것을 확인할 수 있었다.

사용자 2의 경우에는 객체 파일의 복호화를 위한 KMS 키를 소유하지 않았기 때문에 파일이 다운로드 되지 않고, Fig 1과 같이 오류 화면이 나타나는 것을 확인할 수 있다.

Fig. 1. 시나리오 1, 3 운영 결과 - 파일 접근 불가

시나리오 3은 특정되지 않은 사용자가 객체 URL을 통해 접근하는 방법이므로 시나리오 2와 마찬가지로 사용자가 파일 복호화를 위한 KMS 키를 소유하고 있지 않다. 따라서 시나리오 3은 시나리오 2와 동일하게 Fig 1과 같은 오류 화면을 보이는 것을 확인할 수 있었다.

IV. Conclusion

본 논문에서는 AWS의 인증 및 식별 관리 서비스인 IAM, 암호화 및 키 관리 서비스인 KMS를 활용하여 AWS S3를 제로 트러스트 기반으로 운영하기 위한 모델을 설계하였다. 또한, 제안된 제로 트러스트 모델을 기반으로 AWS S3 서비스를 운영할 경우, 스토리지에 저장된 파일의 보안성을 향상시킬 수 있음을 세 가지 시나리오의 실험을 통해 검증하였다.

본 연구 결과는 안전한 S3 서비스 운영을 위한 제로 트러스트 참조 모델로 사용될 수 있으며 향후에는 IAM 및 KMS 권한을 더욱 세분화하여 보안성을 비교함으로써 다양한 보안 수준을 갖는 제로 트러스트 모델을 제안할 예정이다.

REFERENCES

[1] W. Song, Zero Trust Architecture, National Information Society Agency, 2022.

[2] S.H. Han and H.K Lee. “Zero Trust Technology Trend and Implementation Strategy”, Korea Convergence Security Association, 21(5), 43-50, 2021.

[3] Rodigari, Simone, et al. "Performance Analysis of Zero-Trust multi-cloud." 2021 IEEE 14th International Conference on Cloud Computing (CLOUD). IEEE, 2021.

[4] Mehraj, Saima, and M. Tariq Banday. "Establishing a zero trust strategy in cloud computing environment." 2020 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2020.