과도한 권한이 부여된 클라우드 Access Key 유출에 따른 스토리지 스냅샷 기반 침해사고 시나리오 연구

김미연, 최상훈, 박기웅*

세종대학교 SysCore Lab., *세종대학교 정보보호학과

miyeon2002@naver.com, csh0052@gmail.com, *woongbak@sejong.ac.kr

A Study on Storage Snapshot-Based Breach Scenarios Resulting from the Leakage of Cloud Access Key with Excessive Privileges

Mi-Yeon Kim, Sang-Hoon Choi, Ki-Woong Park*

SysCore Lab., Sejong University, *Dept. of Computer and Information Security, Sejong University

요 약

최근 디지털 전환이 가속화되고 있으며, 클라우드는 디지털 전환 시대의 핵심 기술이 되었다. 클라우드 서비스 제공업체에서는 접근성과 개발 편의성을 위해 Access Key를 제공하지만, 소스코드에 하드코딩되어 있던 자격증명이 공개 저장소에 노출되면서 공격자에 의해 악용되는 사례가 지속적으로 발생하고 있다. 본 논문에서는 과도한 권한이 부여된 Access Key가 유출되었음을 전제로 하여 침해사고 시나리오를 구성하고, 이를 국내 클라우드 환경에 적용하여 침해사고 발생 여부를 확인한다.

Ⅰ. 서 론

전 세계적으로 디지털 전환이 가속화되고 있으며, 클라우드는 디지털 전환을 위한 핵심 기술이 되었다 [1]. 클라우드는 자원 사용량만큼의 비용만 지불하므로 비용 절감의 효과가 있고, 유연성, 확장성 등을 보장하여 서비스의 성능을 효율적으로 향상시킬 수 있다 [2-3]. 클라우드 서비스 제공업체에서는 사용자의 접근성과 개발 편의성을 위해 Access Key를 제공하고 있으며, Access Key는 API 호출이나 클라우드 자원 접근 시에 사용할 수 있는 자격증명을 의미한다.

그러나 서비스 개발을 위해 소스코드에 하드코딩되어 있던 자격증명이 공개 저장소(Github, Docker Hub 등)에 그대로 노출되면서 공격자에 의해 악용되는 사례가 빈번하게 발생하고 있다 [4]. 특히, 유출된 자격증명에 최소 권한 원칙이 적용되어 있지 않다면, 피해 정도는 더욱 심각해질 수 있다. 국외에서는 클라우드 환경에서의 보안 위협을 사전에 식별하고 이해하기 위해 침해사고 시나리오 연구를 활발하게 진행하고 있지만, 국내 클라우드 환경을 대상으로 한 연구는 상대적으로 부족한 실정이다.

따라서 본 논문에서는 최소 권한 원칙이 미적용된 Access Key가 유출되었다는 가정을 전제로 하여 서버 내부 정보를 열람하기 위한 침해사고 시나리오를 구성한다. 또한, KT 클라우드와 Naver 클라우드 환경에 시나리오를 적용하여 침해사고 발생 여부를 확인한다.

Ⅱ. 실험 설정

<표 1> 실험 요구사항 및 제공업체별 차이점

구분	KT클라우드	Naver클라우드
자격증명	인증 토큰	Access Key
서버 접속 방식	SSH Key 기반	관리자 비밀번호 기반
스냅샷 연결 방식	스냅샷을 서버 이미지로 변환하여 새로운 서버를 생성	스냅샷을 서버에 연결한 후, 서버 내부에서 마운트 수행

우리는 실험을 위해 KT 클라우드와 NAVER 클라우드 환경에 가상 머신을 생성한 후, (그림 1) 및 (그림 2)와 같은 테스트 데이터를 각각의 환경에 저장하였다. 이후, 서버 및 VPC에 대한 권한이 과도하게 부여된 Naver 클라우드 서브 계정의 Access Key를 조회하였고, KT 클라우드에서는 API 호출에 사용할 수 있는 인증 토큰을 발급받았다. 본 연구에서는 이 두 가지 자격증명이 유출되었음을 전제로 하며, 실험을 위한 주요 요구사항과 제공업체별 차이점은 <표 1>과 같이 정리할 수 있다.

```
mysql> select name, age, phone from user;
+------------+-----+---------------+
| name       | age | phone         |
+------------+-----+---------------+
| Kim minsoo |   20| 010-1234-5678 |
+------------+-----+---------------+
```

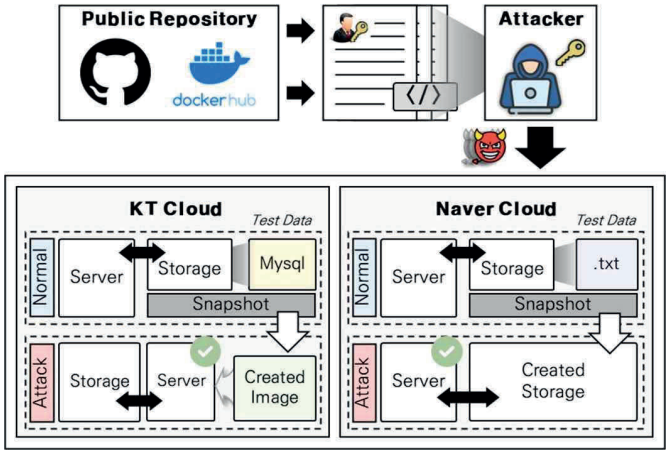
(그림 1) KT 클라우드 환경에 저장된 테스트 데이터

```
ncloud@syscore-db:~$ sudo vim important.txt
ncloud@syscore-db:~$ cat important.txt
very important file!
```

(그림 2) Naver 클라우드 환경에 저장된 테스트 데이터

Ⅲ. 시나리오 구성 및 적용

최소 권한 원칙이 미적용된 서버나 VPC 권한은 가상 머신 생성, 인증키(Key Pair) 생성, 스냅샷 생성 등 다양한 작업을 가능하게 한다. 본 연구에서는 (그림 3)과 같은 시나리오를 클라우드 환경에 적용하여 과도한 권한이 부여된 Access Key를 통해 서버 내부의 정보를 열람할 수 있는지 확인한다. 먼저, 각 환경에서 테스트 데이터가 저장된 서버 볼륨의 스냅샷을 생성하였다. 이후, KT 클라우드에서는 생성된 스냅샷을 서버 이미지로 전환하여 이를 기반으로 가상 머신을 생성하였고, Naver 클라우드에서는 새로운 서버를 생성하여 해당 서버에 스냅샷 기반 스토리지를 연결하였다. 이때, 공격자가 Access Key를 확보하였다고 하더라도 기존 사용자의 인증키 정보는 알 수 없기 때문에 실행 중인 기존 서버에는 접속할 수 없다.



(그림 3) 시나리오 개요

또한, 기존의 인증키를 자신이 생성한 새로운 서버에 적용할 수도 없다. 그러나 이미 서버에 대한 대부분의 권한을 보유한 공격자는 새로운 인증키를 생성할 수 있으며, 자신이 생성한 서버에 이를 적용하면 기존의 인증키 없이도 서버 내부로 접속할 수 있다.

우리는 침해사고 발생 여부를 확인하기 위해 KT 클라우드 환경에 접속하여 새로 생성한 서버에서 데이터베이스를 조회하였으며, (그림 4)와 같이 별도의 설치 과정 없이도 mysql을 실행할 수 있었다. 또한, 2장에서 저장했던 테이블과 정보를 모두 열람할 수 있었다. Naver 클라우드 환경에서는 서버 내부에서 스토리지 마운트를 한 번 더 수행해야 한다. 이후, 2장에서 테스트 데이터를 저장했던 경로로 이동하여 파일의 목록을 조회한 결과, (그림 5)와 같이 테스트 데이터의 내용과 동일한 내용이 출력되는 것을 확인할 수 있었다. 우리는 주요 정보의 외부 유출을 시뮬레이션하기 위해 (그림 6) 및 (그림 7)과 같이 scp(secure copy) 명령어를 활용하여 각 환경에 저장된 테스트 데이터를 외부 서버로 전송하였다. (그림 8)과 (그림 9)는 테스트 데이터가 전송된 외부 서버에서 테스트 데이터를 조회한 결과이며, 이는 2차 피해로 이어질 수 있음을 시사한다.

```
mysql> SELECT * FROM user;
+------------+-----+---------------+
| name       | age | phone         |
+------------+-----+---------------+
| Kim minsoo |  20 | 010-1234-5678 |
+------------+-----+---------------+
```

(그림 4) KT 클라우드 스냅샷 스토리지에서 확인한 테스트 데이터

```
ncloud@sju-attack-snap:~$ cd /mnt/a/home1/ncloud
ncloud@sju-attack-snap:/mnt/a/home1/ncloud$ ls
filebeat-oss-8.15.0-amd64.deb.1  filebeat-oss-8.15.0-
amd64.deb.sha512.1  important.txt
ncloud@sju-attack-snap:/mnt/a/home1/ncloud$ cat important.txt
very important file!
```

(그림 5) Naver 클라우드 스냅샷 스토리지에서 확인한 테스트 데이터

```
ubuntu@sju-attack-snap-test:~$ sudo mysql D info e "SELECT * FROM user;" >
./important.txt
ubuntu@sju-attack-snap-test:~$ sudo scp important.txt
root@223.130.xxx.xxx:/root/importantDB/important.txt
The authenticity of host '223.130.xxx.xxx (223.130.xxx.xxx)' can't be established.

                                    . . .

root@223.130.xxx.xxx's password:
important.txt                                 100%   43    28.1KB/s   00:00
```

(그림 6) KT 클라우드 환경에서 외부 서버로 전송된 테스트 데이터

```
ncloud@sju-attack-snap-test:/mnt/a/home1/ncloud$ scp important.txt
root@110.165.xxx.xxx:/root/important.txt
The authenticity of host '110.165.xxx.xxx (110.165.xxx.xxx)' can't be established.

                                    . . .

root@110.165.xxx.xxx's password:
important.txt
```

(그림 7) Naver 클라우드 환경에서 외부 서버로 전송된 테스트 데이터

```
root@login-test:~/importantDB# ls
important.txt
root@login-test:~/importantDB# cat important.txt
name     age     phone
Kim minsoo      20      010-1234-5678
```

(그림 8) 외부 서버에서 조회한 KT 클라우드의 테스트 데이터

```
root@s19a3071bf45:~# pwd
/root
root@s19a3071bf45:~# ls
important.txt
root@s19a3071bf45:~# cat important.txt
very important file!
```

(그림 9) 외부 서버에서 조회한 Naver 클라우드의 테스트 데이터

Ⅳ. 결론 및 향후 연구

본 논문에서는 최소 권한 원칙이 적용되지 않은 클라우드 Access Key 유출을 전제로 하여 스토리지 스냅샷 기반의 내부 정보 열람 시나리오를 구성하였다. 또한, 국내 클라우드 환경에 해당 시나리오를 적용하여 침해사고 발생 여부를 확인하였다.

확인 결과, 과도한 권한이 부여된 Access Key를 확보한 공격자는 새로운 인증키와 서버를 생성할 수 있고, 기존 스토리지의 스냅샷을 서버에 연결하면 기존 서버 내부에 저장된 정보를 열람할 수 있었다. 우리는 해당 시나리오를 통해 공격자가 인증키나 관리자 비밀번호로 구성된 서버 자체의 보안도 우회할 수 있음을 확인하였다. 이러한 침해사고를 방지하기 위해서는 서브 계정에 최소 권한 원칙을 반드시 적용하고, 공개 저장소에 소스코드를 업로드하기 전, 자격증명과 같은 주요 정보가 코드에 포함되지 않았는지 검토하는 것이 매우 중요하다.

향후 연구에서는 더욱 다양한 유형의 클라우드 침해사고 시나리오를 정립하여 국내 클라우드 환경에서 검증을 수행하고, 이를 완화할 수 있는 방안을 연구하고자 한다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보보호핵심원천기술개발(Project No. RS-2026-25519773, 30%; RS-2024-00438551, 10%), 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 20%), 대학ICT연구센터(ITRC) (Project No. IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431, 30%)의 지원을 받아 수행된 연구임.

참 고 문 헌

[1] Atencio, G. S. "Cloud adoption in emerging economies: A Costa Rican RBV-SAM Analysis," LACCEI 2.13, 2025.

[2] Qazi, F., Kwak, D., Khan, F. G., Ali, F., and Khan, S. U. "Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges,." Internet of Things, vol. 25:101126, 2024.

[3] Nascimento, B., Santos, R., Henriques, J., Bernardo, M. V., and Caldeira, F. "Availability, scalability, and security in the migration from container-based to cloud-native applications," Computers, vol. 13, no. 8:192, 2024.

[4] Demir, N., Vekaria, Y., Smaragdakis, G., and Durumeric, Z. "Keys on Doormats: Exposed API Credentials on the Web," arXiv preprint arXiv:2603.12498, 2026.