https://kiisc.or.kr

2022년 한국정보보호학회 동계학술대회

CISC-W'22

Conference on Information Security and Cryptography-Winter 2022

2022년 11월 26일 (토) | 국민대학교

- 학술대회 등록대: 미래관 자율주행 스튜디오 (4층)
- 개회식/정기총회: 본부관 (1층)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KMU 국민대학교 KOOKMIN UNIVERSITY

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 지란지교시큐리티, PILAB

한국정보보호학회
Korea Institute of Information Security & Cryptology

클라우드 환경에서의 보안 사고 분석 및 발전 방향 제시

유광민*, 김홍현*, 이은진*, 권혁우*, 지찬영*, 이세한[1], 박기웅†

, † 세종대학교 정보보호학과 (학부생, 교수†)
[1]세종대학교 시스템보안연구실 (지능형드론 융합전공) (대학원생)

Suggestion of Development for Cloud Environment through Analysis of Security Incidents

Kwang-Min Yoo*, Hong-Hyeon Kim*, Eun-Jin Lee*, Hyeok-Woo Kwon*, Chan-Young Ji*, Se-Han Lee[1], Ki-Woong Park†

, † Dept. of Computer and Information Security, Sejong University (Undergraduate Student, Professor†)
[1]SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University (Graduate Student)

요 약

최근 COVID-19로 인해 비대면 시대로 전면 전환되어 업무와 서비스 환경이 클라우드 환경으로 이전되고 있다. 아마존 社의 클라우드 지원 등 정책적인 변화와 여러 IT 그룹들의 클라우드 환경 이전에 따라 클라우드 시장이 점차 확대되고 있으며 이로 인한 사이버 공격의 위협 또한 증가하고 있다. 이에 본 논문에서는 클라우드 보안 위협에 대응하기 위해 클라우드 환경의 보안 사고 사례에 대한 조사 및 보안 위협 요소를 세 가지 관점으로 분석하여 클라우드 환경의 보안성 발전 방향에 대해 제시한다.

I. 서론

최근 아마존 社에서 보안 인증 등급제로 나누어진 클라우드 컴퓨팅 환경 서비스를 美 정부와 국방부에 제공하였다. 美 정부가 클라우드 시스템을 사용함에 따라, 전 세계적으로 클라우드 시장이 커지고 있다. 또한 최근 COVID-19 사태로 인한 비대면 시대로의 빠른 전환으로 기업 내 업무, 서비스 환경이 클라우드 환경으로 전환되고 네트워크 사용량이 폭발적으로 증가하고 있다[1].

클라우드 환경의 동적이고 분산적인 특성은 클라우드의 시장이 커짐에 따라 네트워크 공격 표면이 광범위하게 확산하고 있다. 이에 사이버 공격 등의 보안 위협에 노출될 확률 또한 급격하게 늘어나고, 기존보다 더욱 다양하고 복잡한 새로운 보안 위협 요소를 증가시켰다[2]. 이를 해결하기 위한 클라우드 환경에서의 증가한 사이버 보안 위협 요소 대비 및 새로운 보안 체계 수립을 위해서는 클라우드 환경 시스템의 장점 및 단점, 그리고 이에 따른 보안 위협 요소를 파악하는 것이 중요하다.

이에 본 논문에서는 클라우드 환경의 장점 및 단점, 그리고 문제점을 행위 주체에 따라서 분석하여 파악한다. 또한 클라우드 환경에 대한 사이버 공격 행위의 주체를 제공자, 이용자, 제3자, 총 세 가지 관점으로 분류하여 현재 클라우드 환경 시스템의 문제점과 단점을 자세히 분석하고, 이전에 해결된 문제들의 사례(요소)들과 접목하여 결과적으로 클라우드 시스템의 발전 방향성을 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 국내 및 국외에서 발생한 클라우드 컴퓨팅 환경에서의 보안 사고 조사 및 분석 내용에 대하여 설명하고, 3장에서는 클라우드 환경 보안 발

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)

본 논문은 과학기술정보통신부의 재원으로 정보보호국제공동연구(No. RS-2022-00165794, 80%), 한국연구재단 중견연계연구지원사업(No. NRF-2020R1A2C4002737, 20%)의 지원으로 수행된 연구임.

전 방향에 대하여 설명한다. 4장에서는 결론 및 향후 연구 계획에 관해 설명한다.

II. 클라우드 환경에서의 보안 사고 분석

2.1 국내의 클라우드 환경 보안 사고 분석

국내 클라우드 관련 보안 사고 사례로는 야놀자 社와 스타일 공유 사업자 간의 개인정보 보호조치와 개인정보 파기 위반 사고가 발생했으며 집 꾸미기 사업자는 개인정보 유출통지 및 신고 위반으로 서비스를 이용하는 고객들의 개인정보가 대량으로 유출되는 사고가 발생하였다. 이와 관련해서는 관리자 접근 권한을 충분히 제한하지 않거나, 장기 미 이용자의 개인정보를 파기 또는 분리 보관하지 않는 등 보안 취약점을 방치한 것이 원인이었다고 밝혔다[3].

2.2 국외의 클라우드 환경 보안 사고 분석

국외 클라우드 관련 보안 사고 사례로는 Capital One 社의 개인정보 유출 사고로 1억 600만 명의 개인정보 유출 피해가 발생하였다. 특별한 보안 인증 절차를 설정하지 않은 AWS 인스턴스의 방화벽 취약점을 이용해서 공격자가 쉽게 접근할 수 있었던 것이 가장 큰 원인이었다. AWS 측은 인스턴스가 설계된 대로 동작한 것이기 때문에 해당 서비스를 사용하는 기업의 문제라고 결론지었다. 이처럼 보안 설정을 제대로 하지 않고 클라우드 서비스를 이용하게 되면 보안 취약점이 발생하게 된다[1].

2.3 세 가지 관점에 따른 클라우드 환경 보안 위협 분석

본 논문에서는 클라우드 환경 보안 위협을 총 세 가지 관점(제공자, 이용자, 제3자)으로 구분하여 분석을 진행하였으며, 그 내용은 [표 1]과 같다.

제공자 관점에서는 관리자의 잘못된 습관과 내부자의 위협으로 발생하는 위협 요소를 확인하였고, 이용자 관점에서는 SW 취약점 및 클라우드 시스템 사용에 대한 보안 설정 부재 등으로 인한 위협 요소가 존재하는 것을 확인하였다. 마지막으로 제 3자 관점에서는 계정입력 또는 서비스 사용 시에 네트워크 트래픽 하이재킹 공격으로 인한 위협 요소와 사이버 공격자의 사용자 계정 탈취로 인한 위협 요소를 확인하였다.

분류	보안 위협 요소[2]
제공자	• 관리자의 잘못된 설정으로 기인한 부적절한 변경 제어 및 잘못된 구성 • 내부자가 악의적으로 보안 정보 유출 • 클라우드 보안 아키텍처 및 전략 부족 • 스토리지 공유로 발생하는 보안 취약점
이용자	• 클라우드 시스템의 보안 요소 설정 부족 • 권한을 가진 이용자의 접근 • SW 취약점을 이용한 부당한 이용 • 클라우드 서비스 업체의 계정 보안 부족
제3자	• 계정입력 또는 서비스 사용 시 네트워크 트래픽 하이재킹 • 해커가 불법적으로 획득한 사용자 계정으로 클라우드 시스템 제어

표 1. 세 가지 관점으로 분석한 클라우드 환경 보안 위협

III. 클라우드 환경 보안 발전 방향

클라우드 환경 보안 발전 방향성을 분석하기 위해 우선 클라우드 환경에서의 세 가지 관점에서 보안 위협 및 대응 방안에 대해 분석하였다. 세 가지 관점은 제공자, 이용자, 제 3자로 구분하였으며 클라우드 환경 보안 위협 대응 방안을 분석하였으며 그 내용은 [표 2]와 같다.

분류	보안 위협	대응 방안[4]
제공자	원격 액세스 관리 부재	• 네트워크 흐름 모니터링 및 적절한 차단
이용자	애플리케이션 보호 부재	• 웹 애플리케이션 방화벽 사용 • Microsoft Defender App Guard의 퍼블릭 프리뷰 검토 사용
제3자	계정보안을 위한 SMS 문자 메시지 MFA 미사용	• Google이나 Authy의 사용자 계정 인증 앱을 사용 • Microsoft Azure의 액티브 디렉토리 글로벌 관리자 역할 변경사항 모니터링

표 2. 세 가지 관점의 클라우드 환경 보안 위협 대응 방안

본 논문에서는 클라우드 환경 보안 발전 방향을 이용자(기업) 측면과 서비스 제공자 측면에서 제안한다.

이용자(기업) 측면에서는 사용하고 있는 클라우드 인프라에 대해 자체 보안 인력 할당 혹은 외부 보안업체에 수주 등의 수단을 통해 보안 정책을 안전하고 구체적으로 확립하는 방식으로 나아가야 한다. 즉 클라우드 서비스 보안 업체를 너무 맹신하지 말고 자체적으로 보안 규정을 확립해야 한다.

클라우드 서비스 제공자 측면에서는 정보보안에 대한 이해도가 낮은 고객을 고려하여 인프라 이외에도 충분한 보안 서비스를 제공해주는 방향으로 서비스를 확대해야 한다. 다양한 고객층을 수용할 수 있는 클라우드 컴퓨팅 환경 안전망을 강화해야 하며, 클라우드 환경 내 계정 로그인 시 다양한 요소를 활용한 인증 체계 강제 방안을 제공해야 한다. 또한 평소에 대비하여 클라우드 환경 사용량이 급격히 상승했을 경우, 클라우드 환경을 자동으로 차단하는 대책도 참고해야 한다. 이러한 인프라의 정확한 보안 수준을 서비스 이용자에게 고지를 해야 한다[5]. 추가로 중앙집중형의 데이터 센터에 집중된 보안 서비스와 별개로 사용자와 개별 장치에 집중되어 통합 클라우드 제공 보안 접근 서비스가 필요하다[6].

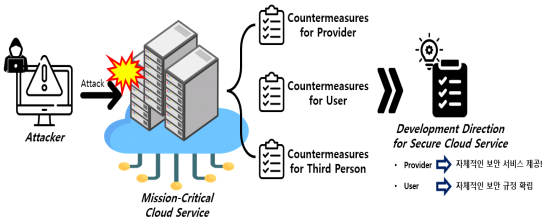

그림 1. 세 가지 관점의 클라우드 환경 보안 발전 방향

IV. 결론

최근 전 세계적으로 클라우드 시스템을 도입하여 클라우드의 역할이 점점 커짐에 따라 위험성 또한 커지고 있다. 본 논문에서는 주체를 제공자, 이용자, 제3자로 분류하여 현재 클라우드 컴퓨팅 환경의 문제점 및 보안 위협 요소를 분석하였다. 분석한 문제점과 위협 요소를 기반으로 클라우드 컴퓨팅 환경의 발전 방향성을 도출하였으며, 이러한 연구를 통해 보안 위협 재발을 방지할 수 있는 예방 효과를 기대할 수 있다.

향후 클라우드 시스템의 취약점에 대한 구체적인 위협 및 대응 방안과 이와 관련된 실험을 통해 개선책을 마련하여, 클라우드 컴퓨팅 환경을 사용 및 활용하고자 하는 모든 이용자에게 정보보안에 있어 도움을 주고자 한다.

[참고문헌]

[1] IT DAILY, “인프라닉스, ‘인터넷 기반 육군 민간 클라우드 인프라 확보 사업’ 수주,“ 2022.10.,http://www.itdaily.kr/news/articleView.html?idxno=210423

[2] 양주호, 박기웅, 클라우드 보안 분류체계 설계를 위한 요구사항 도출, 한국정보보호학회 하계학술대회 논문집, 제31권 제1호, pp.619-623, 2021.06.

[3] ZDNet Korea, “빗발치는 '클라우드' 보안 사고…정부, 대응책 준비”, 2021.10., https://zdnet.co.kr/view/?no=20211028170157

[4] 우성희, 이효정, 조영복, 클라우드 보안사고와 대응방안, 한국정보통신학회 종합학술대회 논문집, 제24권 제2호, pp.343-345, 2020.10.

[5] IT DAILY, “해킹으로 이틀 만에 1억 원 피해… 클라우드 보안 대책은?”, 2022.05., http://www.itdaily.kr/news/articleView.html?idxno=207832

[6] 구동영, 클라우드 컴퓨팅 보안 기술 동향, 정보보호학회지, 제30권 제6호, pp.101-106, 2020.12.