클라우드 환경에서의 제로 트러스트 한계 분석

김미연*, 최상훈[1], 박기웅†

세종대학교 SysCore Lab. (대학원생, 연구교수[1])

**세종대학교 정보보호학과 교수(박기웅†)

Analyzing Zero Trust Limitations in Cloud Environments

Mi-Yeon Kim*, Sang-Hoon Choi[1], Ki-woong Park†

*SysCore Lab., Sejong University
(Graduate student*, Research professor[1])

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

요 약

클라우드의 다양한 이점으로 인해 클라우드 환경으로의 마이그레이션 비율이 갈수록 증가하는 추세이지만, 이는 보안적 측면에서의 우려를 증가시킨다. 이를 완화하기 위한 대안으로 제로 트러스트가 언급되고 있지만 단순히 제로 트러스트의 도입을 추진했다고 해서 이상적인 클라우드 보안을 수행할 수 있는 것은 아니다. 즉, 클라우드 환경에서 제로 트러스트를 구현할 때도 다양한 한계와 어려움이 존재한다. 따라서 본 논문에서는 클라우드에서 발생할 수 있는 위협과 클라우드 환경에서의 제로 트러스트 한계에 대해 분석하고 그 결과를 바탕으로 결론을 도출하고자 한다.

I. 서론

최근 전 세계의 많은 기업과 조직이 클라우드 환경으로의 마이그레이션을 추진하고 있다. 이는 많은 장점을 제공하지만 데이터 보안에 대한 우려를 증가시킨다 [1]. 즉, CSP(Cloud Service Provider)가 수요에 맞는 다양한 유형의 서비스를 제공할 수 있게 된 반면에 공격자는 새롭게 발생한 보안 취약점을 악용할 수 있게 되었다 [2]. 가상화된 서버/환경에서 구동되는 클라우드는 다양한 유저, 기기 및 네트워크와 상호 연결되며, 데이터 센터가 전 세계 여러 지역에 분산되어 있어서 데이터의 이동이 광범위하게 발생한다 [3]. 기존의 침입탐지시스템, 방화벽 등과 같은 경계 기반 보안 모델은 온프레미스(On-premise) 환경을 대상으로 한 공격에는 효과적으로 대응할 수 있었지만, 경계가 모호해진 현재 상황에서는 한계와 제약이 따른다 [4]. 다양한 학문·실무 분야에서는 이를 완화할 수 있는 방안으로 제로 트러스트를 언급하는 경우가 많지만, 제로 트러스트에도 한계가 존재한다. 본 논문에서는 클라우드에서 발생할 수 있는 위협과 이에 대한 방안으로 언급되는 제로 트러스트의 한계에 대해 분석한 뒤 조직이 클라우드 환경에 제로 트러스트를 도입하고자 할 때 고려해야 할 사항을 도출하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드에서 발생할 수 있는 위협을 나열하고, 3장에서 클라우드 환경에서의 제로 트러스트 한계에 대해 분석한다. 4장에서는 결론 및 향후 연구를 기술한다.

† 교신저자 : 박기웅(세종대학교 정보보호학과 교수)

본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 실감콘텐츠핵심기술개발(Project No. RS-2023-00228996, 50%), 정보통신방송기술 국제공동연구(Project No. RS-2022-00165794, 30%), 국방ICT융합연구(Project No. 2022-11220701, 20%)의 지원을 받아 수행된 연구임.

II. 클라우드에서 발생할 수 있는 위협

2.1 데이터 유출

J. Guffey 등[5]에 따르면 클라우드의 설정 오류는 데이터 유출 사고의 상당 부분을 차지하며, 매년 수십억 개에 해당하는 데이터가 유출되는 근본적 원인이라고 언급했다. 클라우드 컴퓨팅에서의 데이터 유출은 데이터 프라이버시를 위협하는 가장 중요한 요인 중 하나이며, 단순히 조직의 평판, 재정적 손해를 넘어 조직의 생존 가능성까지 좌우할 수 있는 심각한 보안 사고이다 [6, 7].

2.2 Dos/DDoS

S. Naiem 등[8]은 DoS/DDoS 공격이 클라우드의 보안을 위협한다고 언급했다. 특히, 애플리케이션 레이어에서의 공격은 많은 트랜잭션과 프로세스를 생성하여 단시간에 자원을 고갈시키고 탐지/대응이 어려우며, 리소스에 대한 사용률이 무분별하게 높아지면 막대한 금전적 손실이 초래되기도 한다 [9, 10].

2.3 계정 탈취

클라우드 보안을 위협하는 또 다른 공격은 계정 탈취 공격이다. 계정 탈취 공격은 해커가 계정 소유자의 자격과 권한을 취득하여 계정을 제어하는 공격을 의미한다 [1]. 공격자는 클라우드 계정을 탈취하여 악의적인 활동을 수행할 수 있으며, 규제가 잘 되어있는 조직이나 기업은 이로 인해 법적인 영향을 받게 될 수도 있다 [11].

2.4 멀웨어 공격

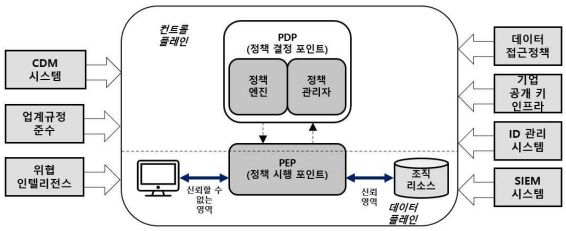
D. Tian 등[12]은 클라우드 애플리케이션의 수요가 증가함에 따라 클라우드에 대한 멀웨어 공격 위협이 점차 심화되고 있다고 언급했다. L. Zheng 등[13]에 따르면 클라우드 컴퓨팅의 발전에 따라 멀웨어는 클라우드 보안의 중요 과제가 되었지만 대부분의 연구는 악성코드 탐지 정확도에만 중점을 두고 사용자의 프라이버시는 충분히 고려하지 않는다.

2.5 기타

그 밖에도 장시간에 걸쳐 정교하게 이루어지는 APT(Advanced Persistent Threat) 공격은 클라우드 인프라의 새로운 취약점을 도출하고 있으며, 시간이 지날수록 정교해지고 조직화되고 있다 [14]. 또한 갈수록 증가하는 내부자 위협과 API 공격도 클라우드 보안을 위협하는 주요 요소가 될 수 있다.

이러한 복합적인 문제를 완화하기 위해 다양한 분야에서는 제로 트러스트에 대한 관심을 보이고 있다 [15].

III. 클라우드 환경에서 제로 트러스트의 한계



(그림 1) 제로 트러스트 아키텍처(재구성)

클라우드 환경에서 제로 트러스트가 이상적으로 구현된다면 보다 강화된 보안을 제공할 수 있지만, 다양한 한계와 단점으로 인해 생각보다 쉽지 않은 실정이다. 제로 트러스트는 정책을 기반으로 PEP-PDP 간의 통신을 통해 리소스에 대한 접근을 엄격하게 제어한다. 미국 국립표준기술연구소인 NIST에서 발간한 'SP: 800-207'에 따르면 제로 트러스트 아키텍처는 (그림 1)과 같다 [16].

최근 여러 CSP 서비스의 장점을 한 번에 활용할 수 있는 멀티 클라우드 모델로의 마이그레이션이 추진되고 있다 [17]. 그러나 각각의 업체마다 추구하는 정책이나 규정이 상이하기 때문에 이를 통합할 수 있는 정책을 마련하는 것은 어려운 일이다. 또한 클라우드 환경에서의 데이터는 광범위하게 이동하며, 전 세계 여러 곳에 걸쳐 분산되어 있다 [3]. 제로 트러스트로 조직의 리소스를 보호하기 위해서는 지속적인

모니터링이 수행되어야 하는데 광범위한 데이터 분산과 이동으로 인해 모든 데이터에 대한 추적과 파악이 어려워진다 [16]. 게다가 원격/재택근무 방식의 전환으로 인해 BYOD(Bring Your Own Device) 형태로 클라우드에 접근하는 사례가 증가했으며, 개인 클라우드를 업무에 사용하는 BYOC(Bring Your Own Cloud)로까지 확대되었다 [18]. 하지만 여러 지역에서 여러 대의 기기나 계정으로 클라우드에 접근하게 되면 네트워크 트래픽에 대한 가시성이 감소할 수밖에 없다. B. Dash가 작성한 논문에 따르면 [19] 클라우드 시스템은 최적화된 속도, 낮은 대기 시간, 높은 가용성을 유지해야 한다. 그러나 이러한 요구사항은 제로 트러스트 구현 및 설계 시에 상당한 부담을 안길 수 있다고 언급했다.

결론적으로, 제로 트러스트가 2장에서 나열된 위협에 대한 대응책이 될 수는 있지만, 이를 클라우드 환경에 구현하기 위해서는 많은 제약이 따른다. 또한 구현된 이후에도 모니터링과 가시성 확보 등의 어려움이 발생할 수 있다.

IV. 결론 및 향후 연구

본 논문에서는 선행 연구 분석을 통해 클라우드 환경에서 발생할 수 있는 위협과 이에 대한 대응책으로 제시되고 있는 제로 트러스트의 한계에 대하여 기술한다. 분석 결과에 따르면 제로 트러스트는 여러 위협에 대하여 상당한 보안성을 제공하지만, 제로 트러스트 도입 자체가 완벽한 클라우드 보안을 의미하는 것은 아니다. 이는 제로 트러스트를 클라우드 환경에 도입할 때 다양한 제약이 발생할 수 있고 도입된 이후에도 모니터링과 가시성을 확보하는 데 어려움이 따르기 때문이다.

향후 연구에서는 클라우드 환경에 대한 제로 트러스트의 한계를 완화하기 위해 방대한 양의 데이터와 네트워크를 효율적으로 추적할 수 있는 연구를 진행하고자 한다.

[참고문헌]

[1] A. V. Kumar, Y. Woinshet, M. N. Kemal, N. Woldeyohanes, A. Shah and D. Ameha, “A novel approach to prevent hijacking of accounts in the cloud,” 2023 International Conference on Computer Science and Emerging Technologies (CSET), pp. 1~5, Oct. 2023.

[2] P. Mishra, A. Gupta, P. Aggarwal, P and E. S. Pilli, “vServiceInspector: Introspection-assisted evolutionary bag-of-ngram approach to detect malware in cloud servers,” Ad Hoc Networks, Vol. 131, Jun. 2022.

[3] C. V. Suresh Babu, S. Subhash, M. Vignesh, T. Jeyavasan and V. Muthumanikavel, “Securing the Cloud: Understanding and Mitigating Data Breaches and Insider Attacks in Cloud Computing Environments,” Analyzing and Mitigating Security Risks in Cloud Computing, pp. 1~23, Feb. 2024.

[4] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi and J. Read, “Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture,” Ieee Access, Vol. 10, pp. 89270~89288, Aug. 2022.

[5] J. Guffey and Y. Li, "Cloud Service Misconfigurations: Emerging Threats, Enterprise Data Breaches and Solutions," 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0806~0812, Mar. 2023.

[6] J. Abrera, "Data Privacy and Security in Cloud Computing: A Comprehensive Review," Journal of Computer Science and Information Technology, vol. 1, no. 1, pp. 01~09, Mar. 2024.

[7] D. Molitor, A. Saharia, V. Raghupathi and W. Raghupathi, “Exploring the Characteris

tics of Data Breaches: A Descriptive Analytic Study," Journal of Information Security, vol. 15, No. 2, pp.168~195, Apr. 2024.

[8] S. Naiem, A. E. Khedr, A. M. Idrees and M. I. Maire, "Enhancing the efficiency of gaussian naïve bayes machine learning classifier in the detection of ddos in cloud computing," IEEE Access, Vol. 11, pp. 124597~124608, Oct. 2023.

[9] Z. R. Alashhab, M. Anbar, M. M. Singh, I. H. Hasbullah, P. Jain and T. A. Al-Amiedy, "Distributed denial of service attacks against cloud computing environment: survey, issues, challenges and coherent taxonomy," Applied Sciences, Vol. 12, No. 23, pp. 12441, Dec. 2022.

[10] S. Q. Ali Shah, F. Z. Khan and M. Ahmad, "Mitigating TCP SYN flooding based EDOS attack in cloud computing environment using binomial distribution in SDN," Computer Communications, Vol. 182, pp. 198~211, Jan. 2022.

[11] A. Karmakar, A. Raghuthaman, O. S. Kote and N. Jayapandian, "Cloud computing application: Research challenges and opportunity," 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1284~1289, Apr. 2022.

[12] D. Tian, R. Zhao, R. Ma, X. Jia, Q. Shen, C. Hu and W. Liu, "MDCD: A malware detection approach in cloud using deep learning," Transactions on Emerging Telecommunications Technologies, Vol. 33, No. 11, pp. e4584, Jun. 2022.

[13] L. Zheng and J. Zhang, "A new malware detection method based on VMCADR in cloud environments," Security and Communication Networks, Vol. 2022, No. 1, pp. 1~13, Mar. 2022.

[14] G. van der Merwe, C. Muller, W. van der Merwe, and D. Blaauw, "Identifying adversaries' signatures using knowledge representations of cyberattack techniques on cloud infrastructure," International Conference on Cyber Warfare and Security, Vol. 17, No. 1, pp.333~339, Mar. 2022.

[15] Y. He, D. Huang, L. Chen, Y. Ni and X. Ma, "A survey on zero trust architecture: Challenges and future trends," Wireless Communications and Mobile Computing, Vol. 2022, No. 1, Jun. 2022.

[16] S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Special Publication 800-207 : Zero Trust Arichitecture", Aug. 2020.

[17] M. Iqbal, M. I. Khan, A. Zaman, M. Shahjahan, M. Farhan, R. Ullah, M. Mustafa and A. Khalil, "Challenges in Multi-Cloud and Benefits from Leveraging Cloud Native Strategy to Digital Transformation of Business,", International Journal of Computational Intelligence in Control, Vol. 14, No. 1, Jun. 2024.

[18] 라인하트, "23. BYOD가 기업의 솔루션 표준화를 무력화한다", brunch story, Jul. 2019.

[19] B. Dash, "Zero-Trust Architecture (ZTA): Designing an AI-Powered Cloud Security Framework for LLMs' Black Box Problems," Current Trends in Engineering Science, Vol. 4, No. 2, pp. 1~5, Mar. 2024.