# 클라우드 포렌식에서의 SLA 한계와 개선 방안 제안

김미연[1], 최상훈[2], 박기웅[3†]
[1]세종대학교 SysCore Lab. 석사과정
[2]세종대학교 SysCore Lab. 연구교수
[3]세종대학교 정보보호학과 교수
miyeon2002@naver.com, csh0052@gmail.com, woongbak@sejong.ac.kr

# SLA Limitations in Cloud Forensics and Suggestions for Improvement

Mi-Yeon Kim[1], Sang-Hoon Choi[2], Ki-Woong Park[3†]
[1-2] SysCore Lab., Sejong University
[3]Dept. of Computer and Information Security, Sejong University

요 약

클라우드 컴퓨팅은 적은 초기 비용만으로도 효율적인 자원 관리와 서비스를 이용할 수 있는 기술이다. 이러한 장점으로 인해 클라우드 서비스를 이용하는 개인과 기업의 비율이 갈수록 증가하고 있지만 이에 따른 보안 사고도 비례하여 증가하고 있다. 클라우드 내에서 보안 사고가 발생하면 클라우드 포렌식을 통한 조사가 신속하게 이루어져야 하는데 다양한 사용자의 자원이 공유되고 있는 멀티-테넌트 환경이 증거 수집을 지연시킨다. 또한 위치에 상관없이 접근하여 수정이 가능하다는 클라우드의 특성이 증거 변조의 위협성을 높여 클라우드 포렌식을 어렵게 한다. 따라서 본 논문에서는 클라우드 포렌식의 한계를 완화하기 위해 클라우드 서비스를 이용하기 전에 맺는 SLA(Service Level Agreement)의 한계에 대해 분석하고 그에 따른 개선 방안을 제안하고자 한다.

## 1. 서론

클라우드 컴퓨팅은 탄력성과 확장성을 갖추고 있으며 여러 테넌트가 자원을 공유하는 멀티-테넌트 환경이다. 이로 인해 개인과 기업은 적은 비용으로도 데이터 저장, 네트워크 리소스 등의 서비스를 이용할 수 있게 되었다 [1]. 물리적 위치와 관계없이 스토리지 내에 저장된 리소스를 활용할 수 있다는 점도 클라우드의 큰 장점 중 하나이다 [2]. 이러한 편리성과 경제적 이점 때문에 최근 몇 년간 클라우드 서비스 이용자 수가 크게 증가했으며, 클라우드 서비스에 대한 사용자 지출은 2024년 현재, 2023년과 비교했을 때보다 20.4% 더 증가할 것으로 예측된다 [3].

그러나 클라우드 사용자가 증가할수록 클라우드 보안 사고의 빈도 또한 비례하여 증가한다. 실제로 영국 시장조사업체인 Expert Insights의 조사 결과에 따르면 퍼블릭 클라우드 보안 사고를 경험한 기업은 2024년을 기준으로 했을 때 전년도보다 약 10% 이상 증가한 것으로 나타났다 [4]. 클라우드 내부에서 보안 위협, 침해 등의 사고가 발생하면 클라우드 포렌식(Cloud Forensics)을 통한 조사가 이루어져야 하는데 클라우드 서버에서 증거를 획득하기 위해서는 클라우드 서비스를 제공하는 CSP(Cloud Service Providers)의 협조가 필요하다.

그러나 CSP는 다른 테넌트의 정보 보호를 근거로 하여 정보 제공에 비협조적인 경우가 많기 때문에 클라우드 포렌식은 증거 수집 단계에서부터 많은 어려움이 따른다 [5]. 또한 이와 관련된 지침과 법령이 제대로 마련되어 있지 않아 클라우드 포렌식은 비교적 더 많은 시간과 혼란이 야기되는 분야이다 [6]. 본 논문에서는 이러한 클라우드 포렌식의 어려움을 완화하기 위해 클라우드 서비스를 이용하기 전에 맺는 SLA의 한계에 대해 분석하고 그에 따른 개선 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서 클라우드 포렌식의 정의와 한계에 대해 분석한 후 3장에서 SLA 항목의 한계점과 그에 따른 개선 방향을 제안한다. 4장에서는 결론 및 향후 연구를 기술한다.

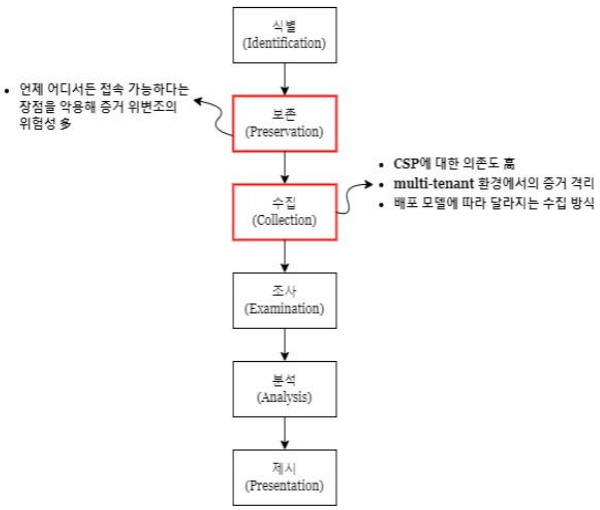
## 2. 클라우드 포렌식의 단계별 한계

클라우드 포렌식은 디지털 포렌식의 한 분야로

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

클라우드 내부에서 발생한 보안 사고를 조사하기 위해 클라우드 환경에서 증거를 수집하여 진행한다 [7]. 일반적인 디지털 포렌식과 클라우드 포렌식의 절차는 식별-보존-수집-조사-분석-제시의 단계로 동일하다 [8]. 그러나 언제 어디서든 접속하여 이용할 수 있는 클라우드 서비스의 특성상 증거 위변조에 대한 위협이 있고, 다른 테넌트 정보의 기밀성은 보장하되 대상이 되는 사용자의 데이터만을 잘 격리해서 수집해야 한다는 어려움이 있다 [9, 10].

또한 클라우드에 저장된 데이터는 대부분 CSP가 엔터프라이즈의 외부에서 보유하고 있다. 따라서 조사관이 클라우드 포렌식에 이용할 증거를 수집하기 위해서는 CSP에 대한 의존도가 높아질 수밖에 없고 클라우드 서비스의 배포 모델이나 유형에 따라 수집 방식을 달리해야 한다는 차이점이 있다 [8]. 즉, 전반적인 절차는 같지만, 보존과 수집의 단계적 측면에서 고려했을 때 기존의 포렌식과 클라우드 포렌식 간의 차이가 명확하게 나타난다. 다음 그림 1은 포렌식의 전반적인 절차와 클라우드 포렌식의 보존, 수집 단계에서의 한계를 정리하여 나타낸 도식이다.




(그림 1) 포렌식 절차와 클라우드 포렌식의 단계별 한계

앞서 언급했던 바와 같이 보존단계에서는 높은 가용성을 가진 클라우드의 특성이 악용되어 증거 수집이 진행되기 전에 위변조가 발생할 수 있다.

수집 단계에서는 클라우드 자원이 CSP에 의해 공유 및 관리되기 때문에 증거 획득을 위해서는 CSP의 협조가 필요하다. 또한 클라우드 환경이 멀티-테넌트 환경이라는 점과 배포된 모델에 따라 달라져야 하는 방식도 증거의 수집을 지연시키는 한계가 될 수 있다.

## 3. Cloud SLA의 한계점과 개선 방향

SLA는 서비스를 제공하는 공급자와 이를 이용하는 고객 간의 서비스 수준 계약으로 서비스 목록이나 비용 등의 내용을 문서화하여 법적 구속력을 갖춘 것이다 [11]. 이때 클라우드에서의 SLA는 클라우드 서비스를 제공하는 CSP와 클라우드 서비스 이용자인 CSC(Cloud Service Customer) 사이에서 이루어지는 계약을 일컫는다. 클라우드 SLA 작성을 위해 마련된 표준화나 지침은 따로 없지만, 보편적으로는 서비스에 대한 보증과 기간, 비용에 관한 내용이 상세하게 포함된다 [12, 13]. 그러나 대다수의 CSP는 포렌식과 관련된 SLA 조항을 간과하고 있으며, CSC도 클라우드 포렌식의 필요성이나 조사 과정 중 발생하는 문제에 대해 인지하지 못하고 있는 경우가 많다 [14].

2020년 Fernandes 외 3명이 발표한 논문에 따르면 최신 SLA 항목에는 클라우드 포렌식에 관한 조항이 포함되어 있지 않다고 언급하고 있다 [15]. 또한 법과 정책 시스템이 기술의 발전 속도를 따라가지 못해 클라우드 포렌식에 관한 표준이 미흡하다는 견해도 있다 [16]. 클라우드는 멀티-테넌트 환경이기 때문에 여러 명의 사용자가 물리적으로 같은 리소스를 사용하게 되는데 이러한 환경에서 증거를 수집해야 한다면 다른 테넌트의 동의를 구하는 것이 불가피하다. 그러나 표준화 미흡과 SLA 상에서의 포렌식 조항이 누락된 현 상황에서는 신속한 대응을 하기 어렵고 나아가 CSP에 대한 신뢰성과 안전성에 대한 문제까지 제기될 수 있으며, 포렌식을 수행하는 조사관에게도 매우 큰 부담과 어려움을 안겨주는 일이다 [17].

따라서 이러한 한계를 해결하기 위해 CSP는 사전에 법을 집행하는 기관과 CSC의 동의를 구한 후 SLA 상에 클라우드 포렌식에 관련된 사항들을 명확하게 기재해야 한다 [14, 18]. 특히 2020년 Akbar 외 3명이 발표한 논문에서는 SLA의 투명성을 위해 국제적 차원에서의 법 개정이 필요하다고 언급하고 있다 [14]. Omollo, R. & Aketch, S. (2024).이 발표한 문서에서도 클라우드 포렌식과 관련한 조항을 추가하여 SLA의 내용을 개선해야 하고 이를 국제법 표준으로 개정하는 데 중점을 두어야 한다고 강조한다 [19].

2011년 Ruan 외 3명이 발표한 논문에서는 SLA 상에 (1) 제공 서비스, 지원 기술, 포렌식 조사에 대하여 CSP가 고객에게 부여한 접근 권한 (2) 포렌식

수행 시 CSP와 고객 간의 역할 및 책임 (3) 포렌식 수행 시 법적인 규제와 테넌트 기밀성 측면에서 여러 관할권 환경의 보안 유지 방법 (4) 멀티-테넌트 환경에서 포렌식을 수행할 때의 보안 유지 방법과 같은 4가지 조항을 명시해야 한다고 언급하고 있다 [20].

## 4. 결론

클라우드 컴퓨팅은 비용 효율성과 확장성, 물리적 위치와 무관한 접근성을 제공하며, 이에 대한 사용자 수와 지출이 지속적으로 증가하고 있다. 클라우드의 사용률이 증가할수록 보안 사고의 빈도도 증가하며, 이를 해결하기 위해서는 클라우드 포렌식을 통한 조사가 필요하다. 그러나 클라우드 서버에서 증거를 확보하려면 CSP의 협조가 필수적인데 다른 사용자 정보의 기밀성을 근거로 CSP가 협조하지 않을 수 있고 명확한 표준화나 지침이 마련되어 있지 않아 클라우드 포렌식 시 다양한 어려움이 따르게 된다. 이러한 한계를 완화하기 위해서는 CSP가 SLA 상에 클라우드 포렌식에 관한 조항을 반드시 포함해야 한다. 또한 클라우드 도입, 관리, 유지보수 등의 업무를 수행하는 MSP(Managed Service Providers)는 SLA 체결 시에 CSC가 해당 조항을 인지할 수 있도록 지속적으로 강조해야 한다. 체결된 SLA를 근거로 CSP는 조사 기관과 협력할 수 있으며 빠른 대응을 통해 서비스의 안정성과 신뢰성을 확보할 수 있다. 또한 CSC도 SLA 항목에 대해 면밀하게 검토해야 하며, 포렌식 조사 시 발생할 수 있는 문제에 대해 인지하고 있어야 한다. 나아가 클라우드 포렌식에 관한 국가적, 국제적 차원에서의 법안과 표준안이 마련된다면 더 원활하고 발전된 클라우드 포렌식이 진행될 수 있을 것이다.

향후 연구에서는 멀티-테넌트 환경에서의 증거 격리와 높은 가용성으로 인한 증거 위변조를 완화하기 위해 연구를 수행할 예정이다.

## Acknowledge

본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원(IITP)의 정보통신방송혁신인재양성사업 (Project No. 2021-0-01816, 50%), 국방ICT융합연구 (Project No. 2022-11220701, 20%), 한국연구재단(NRF) 중견후속연구사업(Project No. RS-2023-00208460, 30%)의 지원을 받아 수행된 연구임.

## 참고문헌

[1] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M., “Cloud Forensics”, Advances in Digital Forensics VII: 7th IFIP WG 11.9 International Conference on Digital Forensics, Orlando, FL, USA, 2011, pp. 35 - 46.

[2] Mistry, H. K., Mavani, C., Goswami, A., & Patel, R., “The Impact Of Cloud Computing And Ai On Industry Dynamics And Competition”, Educational Administration: Theory and Practice, 30, 7, pp. 797-804, 2024.

[3] LoDolce, M., & Howely, C., “Gartner Forecasts Worldwide Public Cloud End-User Spending to Surpass $675 Billion in 2024”, Gartner, 2024. https://www.gartner.com/en/newsroom/press-releases/2024-05-20-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-surpass-675-billion-in-2024

[4] Harris, C., “50 Cloud Security Stats You Should Know In 2024”, Expert Insights, 2024. https://expertinsights.com/insights/50-cloud-security-stats-you-should-know/

[5] Umamaheswari, K., & Sujatha, S., “INSPECT-An Intelligent and Reliable Forensic Investigation through Virtual Machine Snapshots”, International Journal of Modern Education and Computer Science (IJMECS), 10, 3, pp. 17 - 28, 2024.

[6] Akter, S. S., & Rahman, M. S., “Cloud Forensic: Issues, Challenges, and Solution Models”, A Practical Guide on Security and Privacy in Cyber-Physical Systems: Foundations, Applications and Limitations, pp. 113-152, 2024.

[7] Al-mugern, R., Othman, S. H., Al-Dhaqm, A., & Ali, A., “A Cloud Forensics Framework to Identify, Gather, and Analyze Cloud Computing Incidents”, Engineering, Technology & Applied Science Research, 14(3), pp. 14483-14491, 2024.

[8] Sanda, P., Pawar, D., & Radha, V., “An insight into cloud forensic readiness by leading cloud service providers: a survey”, Computing, 104, 9, pp. 2005 - 2030, 2022.

[10] Egho-Promise, E., Idahosa, S., Asante, G., & Okungbowa, A., “Digital Forensic Investigation Standards in Cloud Computing”, Universal Journal of Computer Sciences and Communications, 3, 1, p

p. 23 - 45, 2024.
[11] Cinar, B., & Bharadiya, J. P., “Cloud computing forensics; challenges and future perspectives: A review”, Asian Journal of Research in Computer Science, 16, 1, pp. 1-14, 2023.
[12] Wazir, U., Khan, F. G., & shah, S., “Service Level Agreement in Cloud Computing: A Survey”, International Journal of Computer Science and Information Security (IJCSIS), 14, 6, pp. 324 - 330, 2016.
[13] Baset, S., “Cloud SLAs: Present and Future”, SIGOPS Oper. Syst. Rev., 46, 2, pp. 57 - 66, 2012.
[14] Akbar, M., Suaib, M., Husain, M. S., & Shukla, S., “A Compendium of Cloud Forensics”, Critical Concepts, Standards, and Techniques in Cyber Forensics, pp. 215-227, 2020.
[15] Fernandes, R., Colaco, R. M., Shetty, S., & Moorthy, R., “A new era of digital forensics in the form of cloud forensics: A review”, 2020 second international conference on inventive research in computing applications (ICIRCA). IEEE, pp. 422-427, 2020.
[16] Marshall, K., & Rea, A., “Legal Challenges in Cloud Forensics”, AMCIS, 2021.
[17] Ashawa, M., Mansour, A., Riley, J., Osamor, J., & Owoh, N. P., “Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation”, Cloud Computing and Data Science, 5, 1, pp. 140-156, 2024.
[18] Alqahtany, S., Clarke, N., Furnell, S., & Reich, C., “Cloud forensics: a review of challenges, solutions and open problems”, 2015 international conference on cloud computing (ICCC). IEEE, pp. 1-9, 2015.
[19] Omollo, R., & Aketch, S., “A MODEL APPROACH TO ADDRESSING CLOUD FORENSICS CHALLENGES”, Global Scientific JOURNALS, 12, 3, pp. 1637-1650, 2024.
[20] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M., “Cloud forensics: An Overview”, ResearchGate, 2011. https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview?enrichId=rgreq-1e98da1a2f52b5af438ecf849bdb197d-XXX&enrichSource=Y292ZXJQYWdlOzIyOTAyMTMzOTtBUzo5OTA3MTY4NzY1OTUyMEAxNDAwNjMxOTM5MjA5&el=1_x_2