국내 클라우드 감사 로그 기반 공격 경로 역추적 프레임워크 설계

표자연[1], 박주원[1], 이은진[1], 권수빈[1], 박기웅[2†]
[1]세종대학교 정보보호학과 학부생
[2]세종대학교 정보보호학과 교수
23011727@sju.ac.kr, park21@sju.ac.kr, 22011760@sju.ac.kr, 22011775@sju.ac.kr,
woongbak@sejong.ac.kr

Design of an Attack Path Reconstruction Framework Based on Domestic Cloud Audit Logs

Ja-Yeon Pyo[1], Joo-Won Park[1], Eun-Jin Lee[1], Soo-Bin Kwon[1],
Ki-Woong Park[2†]
[1,2]Dept. of Computer and Information Security, Sejong University

요 약

클라우드 환경에서 발생하는 침해사고의 복잡성이 증가함에 따라, 방대한 감사 로그를 기반으로 공격 경로를 자동으로 재구성하는 기술의 필요성이 높아지고 있다. 기존 보안 도구들은 로그들을 개별적으로 나열하는 수준에 머물러, 다단계 공격 흐름 전체를 직관적으로 파악하기 어렵다. 따라서 본 논문에서는 국내 클라우드 NHN Cloud, Naver Cloud 두 플랫폼의 API 감사 로그를 수집 및 정규화하고, Rule-based 탐지와 Isolation Forest를 결합한 하이브리드 탐지를 수행한 후, 로그 간 공통 식별자를 활용하여 공격 경로를 그래프 형태로 재구성하는 TRACE(Traceability-based Retrospective Attack & Cloud Explorer) 프레임워크를 제안한다.

1. 서론

국내 클라우드 시장은 빠르게 성장하고 있으며, 공공, 금융, 제조 등 다양한 산업에서 하이브리드 멀티 클라우드 전환이 가속화되면서 기업이 관리해야 할 보안 자산의 범위도 급수적으로 넓어지고 있다.

클라우드 보안 침해사고 역시 빠르게 증가하고 있다. Splunk CISO Report 2026에 따르면 전 세계 보안 책임자의 92%가 위협 탐지 및 대응 역량 강화를 최우선 과제로 꼽고 있으며[1], 2023년 기준 평균 데이터 침해 비용은 USD 4.45 million으로 3년 전 대비 15% 증가하였다[2]. 국내에서도 2023년 통신사 고객정보 유출 사고와 Toyota Motor 클라우드 설정 오류로 인한 대규모 정보 노출 등 클라우드 API 자격증명 탈취를 통한 다단계 공격이 반복되고 있다.

클라우드 환경에서는 매일 수십억 건 이상의 API 호출 이벤트 로그가 생성되며, 이를 수동으로 분석하여 공격 경로를 파악하기까지 수 시간에서 수 일이 소요된다. 더 근본적인 문제는 기존 로그 분석 도구가 이벤트를 테이블 형태로 나열하는 수준에 그쳐, 이벤트 간 인과관계를 연결하여 공격 흐름 전체를 파악하는 것이 어렵다는 점이다.

본 논문에서는 이러한 한계를 극복하기 위해 국내 클라우드 NHN Cloud, Naver Cloud 두 플랫폼의 감사 로그를 수집 및 정규화하고, 하이브리드 이상 탐지와 그래프 기반 공격 경로 재구성을 결합한 TRACE(Traceability-based Retrospective Attack & Cloud Explorer) 프레임워크를 설계하여 제안한다.

2. 관련 연구

2.1 클라우드 로그 기반 이상 탐지

클라우드 감사 로그를 활용한 이상 탐지 연구는 다양한 방향으로 발전해 왔다. BERT와 Llama를 결합한 LogLLM 접근법은 로그의 의미적 특성까지 분석할 수 있어 주목받고 있다[3]. 라벨이 부족한 실제 보안 환경에서는 Isolation Forest와 같은 비지도 학습 기법이 현실적인 대안으로 활용된다. RAG(Retrieval-Augmented Generation)를 활용하여 ATT&CK 기법에 자동 매칭하는 연구에서는 baseline 대비 70% 이상의 매핑 정확도 향상이 보고

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

되었다[4].

2.2 보안 그래프 기반 공격 경로 분석

클라우드 자산, 계정, 권한, API 호출 간의 관계를 노드와 엣지를 표현하는 Security Graph 기반 접근은 공격 경로 분석의 핵심 방법론으로 자리잡고 있다. GNN(Graph Neural Network)을 활용한 공격 경로 예측 연구[5]는 복잡한 클라우드 환경의 잠재적 공격 경로를 시뮬레이션하는 데 적합하다. 그러나 기존 연구들은 네트워크 패킷이나 시스템 이벤트 수준에 초점을 맞추고 있어, 클라우드 제어 플레인(API) 수준의 공격 경로 재구성에는 한계가 있다.

2.3 MITRE ATT&CK 프레임워크 적용

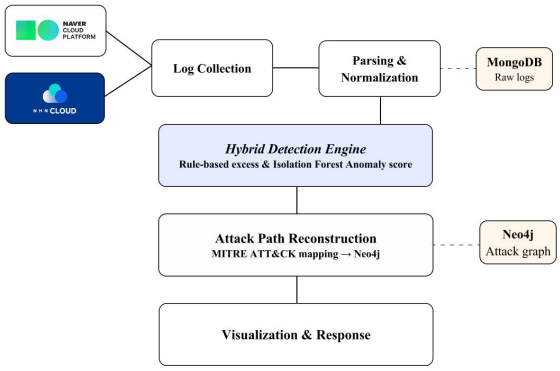
MITRE ATT&CK는 실제 사례 기반 전술·기술 분류 표준으로, IaaS Matrix를 통해 IMDS(Instance Metadata Service) 악용, 권한 상승, 방어 회피 등 클라우드 고유 공격 기법을 체계적으로 분류한다[6]. 이를 활용한 연구들은 개별 이벤트 단위 매핑에 머무르고 있어, 연속 API 호출 흐름을 하나의 공격 시나리오로 연결하는 기능에는 여전히 한계가 존재한다. TRACE는 공통 식별자 기반 추적 가능성 개념으로 이 간극을 해소한다.

3. 프레임워크 설계

3.1 전체 구조

TRACE는 그림1과 같이 로그 수집, 파싱 및 정규화, 공격 탐지, 경로 재구성, 시각화 및 대응의 다섯 모듈로 구성된다.

로그 수집은 NHN Cloud(Cloud Activity Log), Naver Cloud(Cloud Activity Tracer) 두 플랫폼을 대상으로 일단위 배치 방식으로 수행한다. 이는 NHN·Naver 로그가 Object Storage에 일 단위로 적재되는 특성을 반영한 설계로, 현재는 사후 침해사고 조사 및 포렌식 분석에 최적화되어 있으며, 향후 스트리밍 처리 방식으로의 전환을 통해 실시간 탐지와 MTTR(Mean Time To Respond) 단축 효과를 극대화할 계획이다.



(그림 1) TRACE 시스템 아키텍처

3.2 Traceability 기반 경로 재구성

본 프레임워크의 핵심 개념은 Traceability, 즉 로그 간 공통 식별자를 통해 흩어진 이벤트를 연결하여 하나의 공격 흐름(Trace)으로 구성하는 것이다. 표1과 같이 네 가지 공통 키를 활용하여 API 호출을 그룹화하고 시계열로 연결한다.

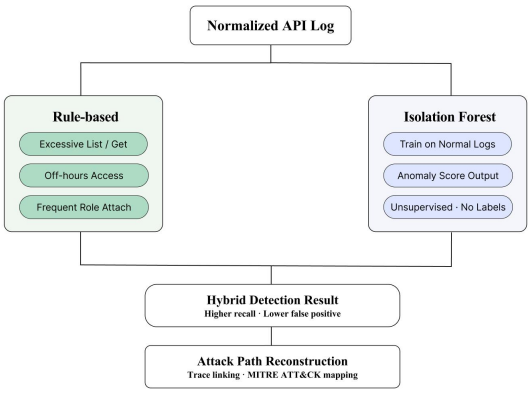
3.3 하이브리드 탐지 엔진

탐지 엔진은 두단계로 구성된다. 1차 탐지는 Rule-based 방식으로 과도한 List/Get 요청(임계값: 분당 100회 초과), 새벽 시간대 이상 접근(00:00 - 05:00), 빈번한 권한 부여(10분 내 3회 이상) 등 사전 정의 규칙을 적용하여 의심 로그를 선별한다. 2차 탐지는 Isolation Forest 알고리즘을 활용하여 정상 로그만으로 학습한 후 이상 점수를 산출한다. Isolation Forest는 레이블이 없는 클라우드 로그 환경에서 고차원 희소 데이터에 강점을 보이며, LOF(Local Outlier Factor) 등 대안 대비 학습·추론 속도가 빠르고 하이퍼파라미터에 덜 민감한 특성이 있어 선택하였다.[7] 두 결과를 결합한 하이브리드 탐지를 통해 탐지율을 높이고 오탐을 줄인다.

탐지된 이상 로그는 Matrix에 자동 매핑된다. 매핑은 API 이름, 리소스 유형, 에러 코드 등 정규화된 로그 필드에서 키워드를 추출하여 사전 정의된 기법 ID(예: T1078 Valid Accounts, T1530 Data from Cloud Storage Object)와 규칙 기반으로 대응시키는

<표 1> Traceability 공통 식별자

공통 식별자	로그 필드명 (예시)	연결 목적
Access Key ID	NHN: access_key_id	동일 자격증명으로 발생한 API 호출 시퀀스 연결
Source IP	Naver: sourceip	동일 출처의 행위 흐름 그룹화
Timestamp	GCP: timestamp	시계열 공격 흐름 재구성 기준
Resource ID	NHN: resource_id	공격 대상 자산 식별 및 엣지(Edge) 연결



(그림 2) MITRE ATT&CK Cloud Matrix 자동 매핑 흐름

방식을 채택한다. 이를 통해 탐색(Discovery) → 권한 상승(Privilege Escalation) → 자원 생성(Resource Creation) → 데이터 접근(Data Access) 등의 공격 단계로 분류된다[5].

4. 결론

본 논문에서는 국내 클라우드 플랫폼 NHN Cloud와 Naver Cloud의 API 감사 로그를 기반으로 공격 경로를 자동으로 역추적하는 TRACE 프레임워크를 설계하여 제안하였다. 본 프레임워크의 주요 기여는 다음과 같다. 첫째, Traceability 개념을 도입하여 Access Key ID, Source IP, Timestamp, Resource ID 등 공통 식별자를 통해 단편적인 로그 이벤트를 하나의 공격 흐름으로 재구성하였다. 둘째, Rule-based 탐지와 Isolation Forest를 결합한 하이브리드 이상 탐지를 통해 탐지율과 오탐률의 균형을 도모하였다. 셋째, MITRE ATT&CK Cloud Matrix와의 자동 매핑 및 Neo4j 기반 그래프 시각화를 통해 기존 SIEM 도구의 이벤트 단위 분석 한계를 보완할 수 있을 것으로 기대된다.

다만 본 연구는 설계 단계로서, 실제 침해사고 로그를 활용한 탐지 성능의 정량적 평가가 수행되지 않았으며, 현재 일 단위 배치 처리 방식은 실시간 대응에 한계가 있다. 향후 연구에서는 실 운영 환경 로그 적용을 통한 탐지 정확도 정량 평가와 스트리밍 처리 방식 도입을 통한 실시간 탐지 및 MTTR 단축을 목표로 한다.

Acknowledgement

본 연구은 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. ,10% IITP-2026-RS-2021-II211816, 10%), 한국연구재단(NRF) 핵심연구사업(Project No. RS-2026-25481431 30%)의 지원을 받아 수행된 연구임. 교신저자 박기웅 교수.

참고문헌

[1] Splunk, “The CISO Report: From Risk to Resilience in the AI Era,” Cisco, Feb. 2026. [Online]. Available: https://www.splunk.com/en_us/campaigns/ciso-report.html

[2] IBM Security, “Cost of a Data Breach Report 2023,” Ponemon Institute, Jul. 2023. [Online]. Available:https://www.ibm.com/reports/data-breach

[3] W. Guan, J. Cao, S. Qian, J. Gao, and C. Ouyang, “LogLLM: Log-based Anomaly Detection Using Large Language Models,” arXiv preprint arXiv:2411.08561, 2024.

[4] H. Chen et al., “Retrieval-Augmented Large Language Model for AWS Cloud Threat Detection and Modelling: Cloudtrail Mitre ATT&CK Mapping,” Computers, Materials & Continua, 2026. doi: 10.32604/cmc.2026.077606

[5] M. François, P. E. Arduin, and M. Merad, “Physics-Informed Graph Neural Networks for Attack Path Prediction,” J. Cybersecur. Priv., vol. 5, no. 2, article 15, 2025.

[6] MITRE Corporation, “MITRE ATT&CK for Cloud Matrix v14,” 2024. [Online]. Available: https://attack.mitre.org/matrices/enterprise/cloud/

[7] F. T. Liu, K. M. Ting, and Z. H. Zhou, “Isolation Forest,” in Proc. IEEE Int. Conf. Data Mining (ICDM), Pisa, Italy, 2008, pp. 413 - 422.