클라우드 관측 가능성 환경 내 공격 분석의 한계와 시공간 식별자를 활용한 그래프 분석

박주원*, 권수빈*, 이은진*, 표자연*, 박기웅†

,† 세종대학교 정보보호학과(학부생, 교수†)

Limitations of Attack Analysis in Cloud Observability Environments and Graph-based Analysis using Spatiotemporal Identifiers

Joo-Won Park*, Soo-Bin Kwon*, Eun-Jin Lee*, Ja-Yeon Pyo*, Ki-Woong Park†

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

(Undergraduate Student*, Professor†)

요 약

최근 클라우드 네이티브 아키텍처 확산으로 Microservice Architecture(MSA) 기반 시스템이 보편화되면서, 서비스 간 상호작용의 복잡성과 데이터 파편화 문제가 심화되고 있다. 특히 방대한 텔레메트리 데이터에서 발생하는 노이즈는 기존의 단편적인 로그 분석만으로 공격 흐름을 파악하는 데 한계를 야기한다. 본 논문에서는 이를 해결하기 위해 OpenTelemetry(OTel)의 문맥 전파 원리를 응용한 시공간 ID(ST-ID) 기반 공격 흐름 재구성 및 시각화 모델을 제안한다. 제안 모델은 이질적인 데이터를 정규화하고 상관분석을 통해 파편화된 이벤트를 그래프 형태로 구조화한다. 이를 통해 클라우드 환경 내 보안 가시성 공백을 최소화하고 분석 효율성을 향상시킬 수 있다.

I. 서론

최근 MSA 및 서버리스 도입으로 인프라 복잡도가 증가하며 관측 가능성(Observability) 기술이 주목받고 있다[1]. 그러나 데이터 분산과 급격한 증폭에 따른 노이즈는 유의미한 보안 이벤트 식별을 저해한다[2]. 본 논문에서는 이를 해결하기 위해 OpenTelemetry(OTel) 개념을 응용한 ST-ID 기반 공격 흐름 가시화 모델을 제시한다.

† 교신저자: 박기웅 (세종대학교 정보보호학과 교수)

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.

II. 관련 연구

2.1 클라우드 관측 가능성 분석의 한계

클라우드 네이티브 환경의 관측 가능성은 외부 출력을 통해 시스템 내부 상태를 추론하는 능력이다. Ganesan(2022)은 데이터 이질성과 증폭이 정보 선별의 장애물이 됨을 지적했다[3]. 특히 파편화된 로그 간 상관관계(Correlation) 매핑은 분석가 피로도를 높여 대응력을 저하시킨다. 또한, 클라우드 규모에서의 비침습적 관측 가능성 확보 요구와 달리, 기존 수동 계측 방식은 제한된 권한 환경에서 가시성 공백을 야기한다. 이는 결국 은밀한 침해 사고의 탐지 지연으로 이어진다 [1, 3]

2.2 OTel과 컨텍스트 전파

OTel는 고유 ID를 통해 파편화된 이벤트를

하나의 흐름으로 연결하는 컨텍스트 전파(Context Propagation) 메커니즘을 제공한다[4]. 하지만 OTel은 주로 애플리케이션 계층에 집중되어 있어, 코드를 수정할 수 없는 클라우드 관리 영역(Control Plane) 로그를 추적하기에는 한계가 있다.

III. 문제 정의 및 분석

기존 연구를 통해 도출된 클라우드 관측 가능성의 핵심 문제는 데이터 노이즈에 따른 정보 매몰[2, 3], 이질적 데이터 분산에 따른 통합 분석의 어려움[1, 2], 그리고 시스템 복잡도 증가로 인한 분석 시간 및 비용 상승이다[1, 3]. 이로 인해 단편적인 로그·메트릭 분석만으로는 공격자의 행위 흐름을 재구성하는 데 한계가 존재한다.

이러한 문제로 인해 기존의 로그, 메트릭, 트레이스 중심의 단편적인 분석 방식만으로는 공격자의 행위 흐름을 재구성하는 데 한계가 존재한다.

IV. 제안 기법

본 장에서는 OTel의 문맥 전파(Context Propagation) 원리를 클라우드 제어 평면(Control Plane)에 이식한 Spatio-Temporal Identifier(ST-ID) 태깅 모델을 제안한다.

4.1 ST-ID의 정의 및 생성 알고리즘

ST-ID는 파편화된 개별 이벤트를 하나의 논리적 공격 시나리오로 결합하기 위한 다차원 해시 식별자이다. 본 모델은 다음과 같이 로그에 포함된 시간 및 공간 정보를 결합하여 보안 문맥을 주입한다.

$$ST-ID = Hash(PrincipalID + Action + ResourceID + Timestamp)$$

Temporal ID (시간적 선후 관계): 이벤트 발생 시점의 타임스탬프(Timestamp)와 순차적 시퀀스 번호를 결합하여 체이닝(Chaining)한다. 이를 통해 분산 환경의 수집 지연 상황에서도 행위의 인과 관계와 발생 순서를 엄밀하게 보장한다.

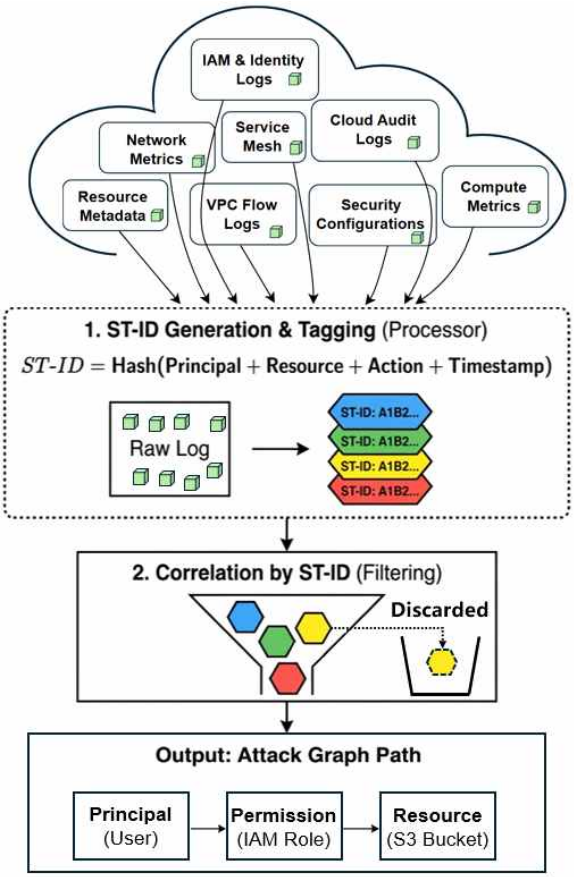
Spatial ID (공간적 위치 정보): 행위 주체(PrincipalID)와 대상 리소스(ResourceID), 그리고 해당 자원이 속한 리전 및 가용 영역(AZ) 정보를 조합한다. 이를 통해 '누가, 어디서' 발생시킨 행위인지를 논리적 공간 좌표로 고정한다.

Security Context Tagging: IAM 권한 범위, 네트워크 토폴로지, 리소스 메타데이터를 통합하여 해당 로그가 어떤 권한 체계와 경로상에서 발생했는지 나타내는 '보안 낙인(Security Stamping)' 역할을 수행한다.

4.2 단계별 데이터 처리 프로세스

4.2.1 Ingestion & Context Injection

이기종 CSP(NCP, AWS 등)로부터 로그 수집 시, 별도의 코드 수정(Instrumentation) 없이 Post-Ingestion Tagging 방식을 통해 ST-ID를 강제 주입한다. 이는 관리형 서비스의 비정형 로그를 가상의 트레이싱 스코프(Tracing Scope)로 편입시키는 과정이다.



[그림 1] ST-ID 기반 데이터 처리 프로세스

4.2.2 ST-ID 기반 상관분석 (Correlation)

대규모 데이터셋에서 동일하거나 연관된 ST-ID를 보유한 행위만을 추출함으로써 보안과 무관한 백그라운드 노이즈를 제거(De-noising)한다. 이를 통해 산재한 점(Points) 형태의 로그 데이터는 하나의 의미 있는 행위의 선(Line)으로 연결된다.

4.2.3 공격 그래프 합성 (Graph Synthesis)

추출된 상관관계를 바탕으로 [사용자-권한-자원] 간의 엣지(Edge)를 생성하여 그래프 구조로 변환한다. ST-ID 기반 인덱싱은 데이터 검색 속도를 혁신적으로 향상시키며, 공격자의 횡적 이동(Lateral Movement) 경로를 직관적으로 시각화한다.

V. 분석 및 기대 효과

5.1 기존 기법(OTel)과의 차별성

기존 OTel은 소스 코드 수정(Instrumentation)이 필수적이며 인프라 영역의 가시성 공백이 존재한다. 제안 모델은 코드 수정 없이 인프라 로그를 기반으로 보안 컨텍스트를 주입하므로, 권한 오남용 및 비정상 리소스 접근 추적에 있어 OTel보다 넓은 관측 범위를 제공한다.

5.2 실무적 가치 및 활용성

본 모델은 보안 이벤트의 상관관계를 자동으로 시각화하여 관제 인력의 알람 피로도(Alert Fatigue)를 낮추고 대응 속도를 향상시킨다. 특히 로그를 ST-ID 단위로 구조화하여 관리함으로써 핵심 보안 데이터의 가용성을 우선적으로 확보하는 전략적 데이터 관리 체계 구축이 가능하다.

VI. 결론

본 논문은 클라우드 네이티브 환경의 복잡한 공격 경로를 재구성하기 위해 OTel의 문맥 전파 개념을 응용한 ST-ID 기반 보안 관측 가능성 모델을 제안하였다.

제안된 모델은 로그의 시간(Timestamp)과 공간(Principal, Resource) 정보 등을 결합한 고유 식별자를 통해, 파편화된 이기종 클라우드 로그 간의 상관관계를 명확히 규명하였다. 이를 통해 단순한 상태 감시를 넘어 공격자의 횡적 이동을 직관적으로 시각화할 수 있는 방법론적 기틀을 마련하였다.

향후 연구에서는 제안 모델을 실제 멀티 클라우드 환경에 구현하고, AI 기반의 이상 탐지 알고리즘을 결합하여 ST-ID를 통한 실시간 위협 대응 자동화 시스템으로 확장하고자 한다.

[참고문헌]

[1] U. Faseeha, S. H. J. Samad, F. Samad, S. Zehra, and H. Ahmed, “Observability in Microservices: An In-Depth Exploration of Frameworks, Challenges, and Deployment Paradigms,” IEEE Access, vol. 13, 2025.

[2] B. Sigelman, L. A. Barroso, M. Burrows, P. Stephenson, M. Plakal, D. Beaver, and S. Jaspan, “Enjoy your observability: an industrial survey of microservice tracing and analysis,” Proceedings of the VLDB Endowment, vol. 14, no. 12, pp. 1 - 13, 2021.

[3] P. Ganesan, “Observability in Cloud-Native Environments: Challenges and Solutions,” International Journal of Core Engineering & Management (IJCEM), vol. 7, no. 4, 2022.

[4] OpenTelemetry Authors, “Context Propagation Concepts,” [Online]. Available: https://opentelemetry.io/docs/concepts/context-propagation/