# 클라우드 로그 기반 이상 행위 탐지 프레임워크

강대현* 김주영* 김학범** 박선하***

*한국외국어대학교 (학부생)

**홍익대학교 (학부생)

***아주대학교 (학부생)

# A Behavior-Based Anomaly Detection Framework Using Cloud Service Logs

Dae-hyun Kang* Ju-young Kim*, Hak-beom Kim**, Seon-ha Park***

*Hankuk University of Foreign Studies(Undergraduate student)

**Hongik University(Undergraduate student)

***Ajou University(Undergraduate student)

**요 약**

제안한 프레임워크는 로그 수집, 전처리, 베이스라인 구축, 이상 탐지, 대응 및 베이스라인 조정의 5단계로 구성된다. 클라우드 로그를 기반으로 EventName, PrincipalARN, SourceIPAddress, 시간 특성을 다차원 벡터로 변환하여 정상 행위의 분포를 베이스라인으로 구축한다. 코사인 유사도 기반으로 이상 여부를 판단한다. 또한 관리자의 피드백을 반영하여 베이스라인을 지속적으로 갱신함으로써, 클라우드 환경 변화에 적응하고 오탐을 최소화한다.

## I. 서론

클라우드 서비스의 도입이 빠르게 확산되고 있으며, 기업과 기관의 IT 인프라가 점차 클라우드 중심으로 전환되고 있다. CloudZero의 보고서에 따르면 응답 기업의 약 48%가 향후 1년 내에 절반 이상의 애플리케이션을 클라우드로 이전할 계획이며, 약 20%는 전면 이전을 계획하고 있다 [1].

하지만 클라우드 환경의 보편화에 따라 이를 대상으로 한 공격 또한 증가하고 있다. 기존 이상 행위 탐지 보안 솔루션에서 사용하는 정책 기반 이상 탐지는 사전에 정의된 정책에 따라 위반 여부를 판별하는 방식이다. 그러나 이러한 방식은 정책의 갱신 속도가 실제 공격 기법의 변화 속도를 따라가지 못하면 변형된 공격이나 알려지지 않은 공격을 탐지하지 못하는 한계가 있다. 이에 따라 최근에는 동적 베이스라인이나 행위 패턴 학습을 통한 이상 행위 탐지 기법이 연구되고 있다. 베이스라인 기반 이상 행위 탐지는 시스템의 정상 행위 패턴을 모델링하고 해당 기준에서 벗어나는 행위를 실시간으로 식별함으로써 공격의 초기 징후를 조기에 포착할 수 있다. 즉 피해 발생 이후의 대응이 아니라 공격 시도를 사전에 차단하는 선제적 방어가 가능하다. 이를 위해 변화하는 환경과 행위 패턴에 대응하기 위해 베이스라인의 동적인 조정이 필수적이다. 따라서 효과적인 대응을 위해서는 공격 발생 이후의 기법 분석보다, 정상 행위의 베이스라인을 기반으로 한 실시간 이상 행위 탐지를 통해 사전 차단이 가능한 대응체계의 구축이 필요하다 [2].

따라서 본 연구는 클라우드 환경의 로그 데이터를 기반으로 정상 행위 베이스라인을 설정하고, 이를 통해 이상 행위를 조기에 탐지할 수 있는 프레임워크를 제안한다.

## II. 연구 방법

프레임워크의 구성은 [그림 1]과 같이 4단계로 이루어진다. 첫 번째로 로그 수집 및 정규화 과정이다. 클라우드 환경에서 사용자 행위에 관한 로그를 수집한다. 이후, 수집한 로그를 기반으로 베이스라인 모델을 구성한다. 리소스별 사용자의 접근 패턴과 빈도, 시간대 등의 특징을 수치화하여 정상 행위를 학습하도록 한다.

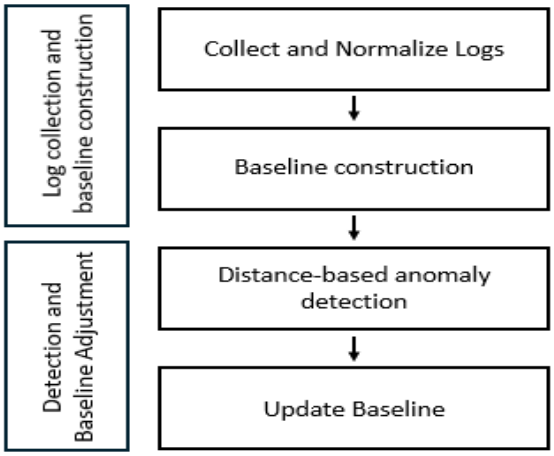


그림 1 The full framework of the proposed anomaly detection system

다음은 이상 탐지 단계이다. 실시간 로그에서 관측된 행위를 베이스라인과 비교하여 거리를 계산한다. 임계값 이상일 경우, 비정상 행위로 판단하여 관리자에게 알림을 준다. 관리자는 이벤트를 검토하고 정상 여부를 피드백한다. 이후 관리자의 피드백 결과를 반영하여 베이스라인을 조정한다. 이를 통해 시스템이 환경 변화나 신규 사용자의 패턴에 자동으로 적응할 수 있도록 하며 오탐을 최소화한다.

### 2.1 데이터 수집 및 전처리

본 연구에서는 AWS의 CloudTrail 로그를 수집하여 정상 행위에 대한 베이스라인을 구축하였다. CloudTrail은 시스템의 내외부에서 발생하는 모든 API 호출을 포괄적으로 기록하여 사용자의 상호작용에 관한 데이터를 제공한다. 또한 EventTime, SourceIPAddress, AwsRegion 등의 시간적·맥락적 정보에 관한 필드를 포함하여 언제, 어디에서 행위가 발생했는지 명확히 분석할 수 있다. 이를 기반으로 특정 리소스에 대한 사용자들의 정상 행위 로그를 수집하여 베이스라인 구축의 기반 데이터로 사용한다. 이러한 행위 정규화 과정에서 특정 리소스를 기준으로 사용자 행위 패턴을 구분하여 분석하였다.

### 2.2 행위 벡터화 및 베이스라인 구축

본 연구에서는 AWS CloudTrail 로그를 기반으로 EventName, PrincipalARN, SourceIP, 시간 특성을 총 33차원 벡터로 변환하였다. EventName은 수행 행위의 유형을 나타내며 원-핫(One-hot) 인코딩 방법을 사용하여 고유한 행위로 취급하였다. 각 리소스를 대상으로 수행할 수 있는 API 명세는 약 100개 내외의 제한된 수로 구성되어 있기 때문에 각 이벤트를 고유한 행위로 취급하여 정상 행위와의 직접적인 비교를 수행할 수 있게 하였다. PrincipalARN은 CloudTrail 로그에서 이벤트를 수행한 주체를 식별하는 고유 식별자로 사용자 유형과 계정 ID, 역할 이름, 세션 ID 등으로 구성된다. 이를 구조적으로 파싱하여 각 구성요소를 고정 차원의 임베딩 벡터로 변환하였다.

주체 유형은 root, iam_user, assume_role, federated_user, aws_service, unknown의 6가지 유형을 정의하여 각각 원-핫 벡터로 표현하였다. 계정 ID는 문자열을 MD5 해시로 변환한 뒤 sin·cos 함수를 적용하여 2차원 임베딩으로 표현하였다. 역할명 및 사용자명에 대해서도 동일하게 해시 기반 임베딩을 적용하였다. 세션 정보는 유형이 assume_role에 해당하는 경우에만 존재하며 동일한 방식으로 해시 변환 후 2차원에 임베딩하였다. 최종적으로 ARN 임베딩 벡터는 다음과 같이 구성된다.

SourceIPAddress는 이벤트의 요청이 발생한 네트워크 출처를 나타내며 사용자의 행위가 내부망에서 수행되었는지, 외부에서 접근한 것인지, AWS 서비스 내부 호출인지를 구분하기 위한 지표로 활용하였다. IP 주소를 네트워크 영역 기준으로 사내 전용망, AWS 내부 서비스 간 호출, 외부 네트워크의 접근, Missing으로 구분하였다. 사내 전용망의 경우 IP 대역을 기준으로 다시 class를 구분하였다. 각 이벤트는 6개의 카테고리 중 하나에 매핑되며 이를 기반으로 6차원의 원-핫 벡터로 변환하여 네트워크 영역의 특성을 표현하였다.

시간 특성은 EventTime 필드로부터 추출하여 8차원 벡터로 임베딩하였다. 시간과 요일은 각각 주기를 가지므로 시간 특성을 sin·cos 함수를 이용한 주기형 임베딩으로 변환하여 모델이 시간의 순환성을 학습할 수 있도록 하였다. 이외에도 시간대의 의미적 구분을 반영하기 위해 업무 시간, 주말, 심야, 주말 심야 접근으로 특징을 추가하였다. 이러한 시간 임베딩은 행위의 발생 시점을 맥락적으로 반영하여 업무 외 시간대에서 발생한 비정상 접근 행위를 구분할 수 있게 한다.

최종적으로 각 벡터를 정규화한 뒤 Concatenation 방식으로 하나의 통합 벡터로 결합한다. 이렇게 생성된 행위 벡터는 단일 이벤트를 설명하는 고정 차원의 벡터 표현으로 특정 리소스에 대한 행위에 대해 일관된 벡터화를 가능하게 한다. 모든 로그 이벤트는 위의 과정을 거쳐 벡터 공간 상의 점으로 표현되며 특정 사용자, 리소스, 역할에 따라 군집을 형성한다. 정상적인 업무 주기 내에서 발생하는 이벤트들은 벡터 공간 상에서 밀집된 분포를 이

루며 이를 베이스라인으로 정의한다.

2.3 이상 탐지 알고리즘 설계

$$D_{\cos}(v_{new}, v_{base}) = 1 - Sim_{\cos}(v_{new}, v_{base})$$

수식 1 Cosine Distance Calculation

새로운 행위 벡터와 정상 행위 벡터 간의 유사도는 코사인 거리(Cosine Distance)를 통해 계산한다. 코사인 유사도를 바탕으로 두 벡터의 방향적 유사성을 고려하고, 이를 거리 기반으로 전환하여 코사인 거리를 계산한다. 또한 시간 경과에 따라 정상 행위의 가중치를 동적으로 조정하기 위해 지수 감쇠 함수를 적용하여 오래된 행위의 영향이 점진적으로 감소하도록 한다. 최종적으로 새로운 행위 벡터와 베이스라인으로 저장된 각 행위 벡터 간의 코사인 거리를 계산하여 최소 거리를 기준으로 임계값을 초과하는 경우를 이상 행위로 탐지한다. 이때, 임계값은 정상 행위 벡터 간의 Cosine Distance 분포를 기반으로 설정한다. 정상 데이터의 평균 거리와 표준편차를 산출하고 μ + kσ 수준을 초과하는 경우를 이상으로 판단한다. 이때, k 값은 환경에 맞춰 경험적으로 설정할 수 있다.

## III. 방법론 적용 결과

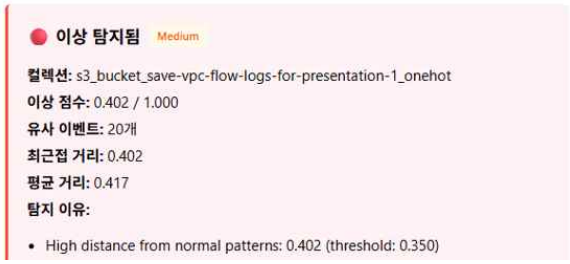


그림 2 Detection of Anomalous Behavior

이상 탐지 방법론을 검증하기 위해 AWS S3 기반의 테스트베드를 구축하였다. 서비스 환경에서 발생하는 로그를 저장하는 S3 버킷에 대한 CloudTrail 로그를 수집하였으며, 총 10만 건의 로그 이벤트를 확보하였다. 행위는 로그 저장, S3 버킷 생성, 쿼리를 전송하여 로그 조회 등의 이벤트로 구성되었고, 스크립트를 통해 사용자의 행위를 모사하여 수행될 수 있도록 하였다. 검증 과정에서는 비인가 사용자에 의한 로그 삭제 행위를 수행하여 이상 행위로 탐지되는지 확인해보았다. 검증 결과 [그림 2]와 같이 시스템에서 로그 삭제 행위를 이상 행위로 탐지하는 것을 확인할 수 있었다.

탐지된 이상 행위는 관리자에게 알림으로 전달되며, 관리자는 해당 행위를 정상 행위로 승인할지, 혹은 이상 행위로 유지할지를 판단한다. 관리자가 정상으로 승인한 행위는 베이스라인에 반영되어 이후 발생한 동일한 행위는 정상으로 처리되고, 이상으로 판단된 행위는 베이스라인에 포함되지 않아 이후에도 이상 행위로 탐지된다. 이러한 과정을 통해 베이스라인은 지속적으로 갱신되며, 시스템은 사용자의 정상 행위를 보다 더 정확하게 학습하고 정의할 수 있다. 검증에 사용된 행위는 정상 행위로 승인되지 않아 베이스라인에 포함되지 않지만, 정상 행위로 판단될 경우에는 베이스라인에 추가되어 이후에는 정상 행위로 간주된다. T-SNE로 시각화한 [그림 3]을 통해 벡터 공간 상에 새로운 행위 벡터 군집이 생성된 것을 확인할 수 있다.

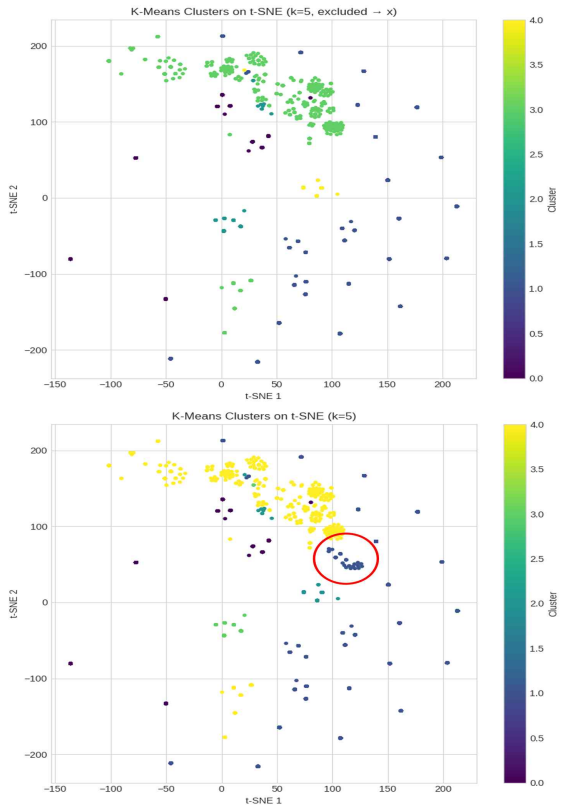


그림 3 Evolution of Baseline Clusters During Anomaly Feedback Update

## IV. 결론

클라우드 기반 기업 운영 형태가 보편화됨에 따라, 클라우드를 대상으로 하는 공격 또한 증가하고 있으며 기존의 정책 기반 보안 체계는 공격자의 이상 행위를 식별하는 것에 한계가 있다. 이에 본 논문에서는 클라우드에서 발생하는 사용자의 행위 로그를 활용하여 이상 행위를 선제적으로 탐지할 수 있는 프레임워크를 제안하였다. 제안된 프레임워크는 로그 수집 및 전처리, 베이스라인 구축, 이상 탐지, 대응 및 피드백의 단계로 구성되며, 행위 로그의 벡터 변환 및 코사인 유사도 기반의 이상 탐지를 수

행함으로써 정의된 정상 행위에서 벗어난 이상 행위를 실시간으로 식별할 수 있다. 특히, 사용자 피드백 메커니즘을 통해 베이스라인을 지속적으로 조정할 수 있어 오탐을 줄이고 정확도를 향상시킬 수 있다는 점에서 기존 연구와의 차별성을 가진다.

다만, 본 연구에서는 단일 로그를 기반으로 유사도를 산정하여 행위의 맥락을 충분히 고려하지 못하며, 행위의 빈도 증가, 연결된 시퀀스의 이상 행위 등을 탐지하기 어렵다는 한계가 있다. 또한 현재 프레임워크는 단일 클라우드 환경을 대상으로 설계되어 멀티 클라우드 및 하이브리드 환경에서의 적용 가능성에 대해서는 검증하지 않았다. 따라서 향후 연구에서는 행위 주체를 중심으로 맥락을 고려하여 행위를 해석하고, 멀티 클라우드 및 하이브리드 환경을 위한 로그 정규화 방안에 대한 추가적인 연구가 필요하다.

## [참고문헌]


[1] C. Slingerland, “90+ Cloud Computing Statistics: A 2025 Market Snapshot,” CloudZero

[2] 박문형, 김대협, 한현상, 이용준, “클라우드 환경의 서버 워크로드 보안 동향,” 정보보호학회지, 제31권 제3호, pp. 21-30, 2021년 6월.

[3] 김대협, 한현상, 박문형, 장항배, “퍼블릭 클라우드에서 자동화 IR(Incident Response)를 통한 보안 향상 기술,” 정보보호학회지, 제31권 제3호, pp. 45-50 , 2021년 6월.