사물인터넷융복합논문지 Vol. 12, No. 4, pp. 93-102, 2026 https://doi.org/10.20465/KIOTS.2026.12.4.093

세션 문맥 인식 정보를 이용한 BERT 기반 보안 로그 이상탐지 메커니즘

이형우*
한신대학교 AISW대학 교수

Security Log Anomaly Detection Mechanism using Session Context-Aware BERT Framework

Hyung-Woo Lee*
Professor, School of Computing and Artificial Intelligence, Hanshin University

요 약 최근 사물인터넷 환경에서는 단말, 서비스, 네트워크 프로토콜, 운영 주체가 복합적으로 연결됨에 따라 네트워크 등 보안 로그 데이터의 규모 뿐만아니라 생성되는 정보의 이질성이 점차 증가하고 있다. 이러한 환경에서 기존의 규칙 기반 이상탐지 방식이나 단일 이벤트 중심 분석 방식은 다단계 공격의 연속성과 세션 수준의 행위 맥락을 충분히 반영하지 못한다는 한계점이 있다. 특히 포트 스캔, 계정 탈취 시도, 명령제어, 데이터 유출과 같은 공격은 개별 로그 이벤트 자체보다 인접 이벤트의 흐름과 세션 단위에서 반복적으로 나타나는 행위 패턴을 비교 분석할 경우 더욱 명확히 식별될 수 있다. 이에 본 논문에서는 기존 BERT 기반으로 의미 표현, 문맥 윈도우 분석 및 세션 단위 행위 집계 방식을 결합한 Session Context-Aware BERT 구조를 제안한다. 제안 기법은 현재 이벤트를 중심으로 반경 1, 2, 3 범위내의 인접 문맥을 함께 분석하고, 세션별 평균 판정 마진, 비정상 이벤트 비율, 목적지 다양성 및 의심 패턴 밀도 등의 지표를 통합하여 최종 이상 여부를 자동 판정한다. 또한 기존의 라벨 추정 방식이 갖는 한계를 보완하기 위해 명시적 파일 단위 및 라인 단위 라벨을 구축하여 검출 성능을 비교 분석하였다. 실험 결과는 문맥 인식 정보를 이용할 경우 네트워크 이벤트 분류 성능을 향상시켰으며, 세션 정보를 사용하여 네트워크 이상 행위를 효과적으로 식별하는 것을 확인하였다.

주제어 : 세션 문맥 인식, 이상탐지, 네트워크 보안 로그 분석, 사물인터넷 보안, 다단계 공격 탐지, BERT

Abstract In recent Internet of Things (IoT) environments, the increasing interconnection of devices, services, network protocols, and operational entities has significantly increased both the volume and heterogeneity of security log data. In such environments, conventional rule-based anomaly detection and single-event-oriented analysis are limited in their ability to capture the continuity of multi-stage attacks and the behavioral context at the session level. In particular, attacks such as port scanning, account takeover attempts, command-and-control activities, and data exfiltration can be more effectively identified by analyzing adjacent event flows and recurrent behavioral patterns within a session rather than individual log events in isolation. To address this challenge, this paper proposes a Session Context-Aware BERT architecture that combines semantic representation, contextual window analysis, and session-level behavior aggregation within a BERT-based framework. The proposed method analyzes neighboring contexts within ranges of 1, 2, and 3 centered on the current event and automatically determines anomaly status by integrating Session Context-Aware indicators such as average decision margin, anomalous event ratio, destination diversity, and suspicious pattern density. In addition, explicit file-level and line-level labels are constructed to complement the limitations of conventional label estimation methods and to enable a comparative evaluation of detection performance. Experimental results show that the incorporation of contextual information improves network event classification performance and that session-level information contributes effectively to the identification of anomalous network behaviors.

Key Words : Session Context Awareness, Anomaly Detection, Network Security Log Analysis, Internet of Things Security, Multi-stage Attack Detection, BERT

이 논문은 한신대학교 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2026년 07월 06일 수정일 2026년 08월 01일 심사완료일 2026년 08월 20일

1. 서론

사물인터넷(IoT) 환경에서는 센서, 게이트웨이, 서버, 모바일 단말, 산업제어 장비 등 다양한 구성 요소가 동시에 연결되어 상호작용하므로 인증, 제어, 데이터 전송, 외부 통신과 관련된 다양한 이벤트가 연속적으로 발생한다. 이러한 이벤트는 대부분 로그의 형태로 축적되며, 시스템 운영 및 보안 관제의 핵심 자료로 활용된다. 그러나 IoT 환경에서 생성되는 보안 로그는 전통적인 정보시스템 로그에 비해 장비의 이질성이 크고, 사용되는 프로토콜의 종류가 다양하며, 동일한 시간대 또는 동일한 파일 내에 정상 행위와 비정상 행위가 혼재하는 경우가 빈번하다는 특징을 가진다. 따라서 네트워크 운영자는 단순히 대량의 로그를 처리하는 수준을 넘어, 서로 다른 의미적 특성을 갖는 이벤트를 신속하고 정확하게 구분해야 하는 문제에 직면하게 된다.

기존 보안 관제 환경에서는 룰(rule) 기반 탐지와 키워드 기반 탐지 방식이 오랫동안 널리 활용되어 왔다. 이러한 접근법은 이미 알려진 공격 시나리오에 대해서는 높은 설명 가능성과 빠른 적용성을 제공한다는 장점이 있으나, 공격자가 메시지 표현을 변형하거나 여러 단계를 결합한 복합 공격 흐름을 사용할 경우에 탐지 성능이 급격히 저하된다는 문제점이 있다. 예를 들어, 단일 로그인 실패 이벤트는 정상 사용자의 단순 실수일 가능성이 있으므로 이를 즉시 이상 행위로 판단하기 어렵다. 반면, 짧은 시간 내 동일 계정 또는 동일 출발지에서 반복적으로 발생하는 로그인 실패 패턴은 계정 탈취 시도로 해석될 가능성이 높다. 마찬가지로 단일 DNS 요청은 정상 행위일 수 있으나, 동일 세션에서 반복적으로 나타나는 장문 질의와 외부 목적지로의 확산 패턴은 DNS 터널링 또는 명령제어(Command and Control : C&C) 통신의 징후일 수 있다. 이와 같이 보안 로그 기반 이상탐지는 개별 이벤트 자체만으로 판단하기보다는 이벤트 간의 관계와 순서, 반복성, 그리고 세션 수준에서의 지속성을 함께 고려할 때 보다 효과적으로 이루어질 수 있다.

이에 최근 이러한 한계점을 보완하기 위한 방안으로 자연어처리 기반 보안 분석 기법이 활발히 연구되고 있다. 특히 Transformer[1]와 BERT(Bidirectional Encoder Representations from Transformer)[2]는 텍스트 시퀀스 내의 양방향 문맥 정보를 반영하여 의미 표현을 학습할 수 있기 때문에, 사람이 사전에 정의한 규칙을 모두 열거하지 않더라도 로그 메시지에 내재된 잠재적 의미 단서를 효율적으로 분석할 수 있는 가능성을 제시하였다. 실제로 네트워크 로그 이상탐지 분야에서 시퀀스 모델 기반의 DeepLog[4], BERT 기반의 LogBERT[5], Sentence-BERT를 활용한 접근[6], 그리고 BERT-CNN 융합 모델[7] 등 다양한 연구가 제안되었다. 그러나 다수의 선행연구는 시스템 로그 또는 템플릿 로그를 중심으로 수행되었으며, 네트워크 보안 로그와 같이 하나의 파일 내에 서로 다른 공격 유형과 정상 행위가 혼재하고, 세션 경계가 복잡하며, 동일 세션 내에서 행위 맥락이 축적되는 환경을 충분히 반영하지 못한 한계가 있다.

이에 본 연구에서는 네트워크 중심의 보안 로그 분석 과정에 다음과 같은 내용을 중심으로 실제 시스템 운영 환경에 적합한 이상탐지 구조를 설계하고자 한다. 첫째, 이벤트 단위의 분류 정확도가 높더라도 실제 보안 운영에서는 공격 세션 전체를 놓치지 않고 식별하는 것이 더욱 중요하다. 둘째, 혼합(mixed) 로그 환경에서는 정상 이벤트와 비정상 이벤트가 짧은 구간 내에 교차하여 발생하므로 기존의 단순 BERT 기반 문맥 확장 방법은 성능 저하를 유발할 가능성도 존재한다. 셋째, 라벨링 기반 추정 방식은 데이터의 실제 이상 여부를 충분히 반영하지 못하여 성능을 과대평가할 위험이 있으므로 명시적 라벨 기반 성능 평가 방식이 필요하다. 넷째, 네트워크 보안 로그는 개별 이벤트의 의미뿐만 아니라 세션 단위에서 누적되는 행위 특성이 있으므로 이벤트 수준과 세션 수준의 분석을 통합적으로 수행할 수 있는 탐지 구조가 필요하다.

따라서 본 논문에서는 BERT 기반 의미 표현과 규칙 기반 보조 특징, 인접 문맥 윈도우, 세션 단위 행위 집계를 통합한 Session Context-Aware BERT 방식을 제안한다. 제안 모델은 단일 이벤트 수준의 의미 분석에 머무르지 않고, 현재 이벤트를 중심으로 한 인접 문맥 정보를 함께 반영하며, 나아가 동일 세션에서 관찰되는 행위 통계를 종합하여 최종 이상 여부를 판단하도록 설계되었다. 구체적으로 제안 방식은 반경 1, 2, 3 범위의 문맥 윈도우를 적용하여 인접 이벤트의 영향을 단계적으로 반영하고, 세션별 비정상 이벤트 비율, 평균 판정 마진, 목적지 다양성, 의심 패턴 밀도와 같은 지표를 통합적으로 활용함으로써 보다 신뢰도 높은 이상탐지를 수행한다. 또한 본 연구에서는 전체 로그뿐 아니라 정상 및 비정상 이벤트가 혼재된 로그를 별도로 분석함으로써, 문맥 활용이 갖는 실질적 이점과 함께 한계점까지도 고찰해 보고자 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 로그 이상탐지 및 BERT 기반 보안 분석과 관련된 선행연구를 정

리하고, 3장에서는 제안하는 Session Context-Aware BERT의 구조와 기존 접근법과의 차별성을 설명한다. 4장에서는 실험 환경, 데이터셋, 평가 방법 및 성능 결과를 제시하며, 성능 비교 분석을 토대로 연구 결과의 의미를 고찰하였다. 그리고 5장에서는 최종적으로 결론과 향후 연구 방향을 제시하였다.

2. 관련연구

2.1 Transformer와 BERT 기반 문맥 표현

Transformer[1]는 self-attention 메커니즘을 중심으로 입력 시퀀스의 각 위치 간 관계를 직접적으로 모델링하는 구조로 제안되었으며, 순환신경망이나 합성곱 기반 구조에 비해 장거리 의존성을 보다 효과적으로 반영할 수 있다는 점에서 자연어처리 분야에서 중요한 전환점을 제시하였다. 이후 BERT[2]는 Transformer 인코더 구조를 기반으로 좌우 문맥을 동시에 반영하는 양방향 사전학습 언어모델로 발전하였으며, 질의응답, 문장 분류, 자연어 추론 등 다양한 과제에서 우수한 성능을 보였다. BERT의 장점은 개별 단어 또는 토큰의 의미를 독립적으로 해석하는 것이 아니라, 주변 문맥과의 관계 속에서 동적으로 해석한다는 점에 있다. 이러한 특성은 일반 자연어뿐만 아니라 짧고 불규칙하며 표현 변형이 잦은 로그 메시지 분석에도 유의미한 장점을 제공한다.

보안 로그 분석에서 Transformer 및 BERT 기반 접근이 중요한 이유는 로그가 단순한 수치의 집합이 아니라 행위 주체, 대상, 상태 변화, 결과 코드, 경고 신호 등이 혼합된 반정형 텍스트의 성격을 가지기 때문이다. 특히 네트워크 및 보안 로그에서는 동일한 이벤트 키워드가 사용되더라도 주변 시점의 이벤트 흐름이나 세션 내 반복 패턴에 따라 정상과 비정상의 경계가 달라질 수 있다. 따라서 문맥 정보를 함께 학습할 수 있는 BERT 기반 표현은 정적 규칙 중심 탐지보다 풍부한 의미 정보를 제공할 수 있으며, 보안 로그 이상탐지 연구에 적용 가능하다.

2.2 보안 로그 이상탐지

로그 이상탐지 연구는 전반적으로 로그 파싱 기반 접근, 시퀀스 예측 기반 접근, 그리고 사전학습 언어모델 기반 접근 방법으로 발전해 왔다. 먼저 로그 파싱 기반 연구는 비정형 로그를 템플릿과 변수로 분해하여 구조화된 이벤트로 변환한 뒤 이를 탐지에 활용하는 방식으로 전개되었다. 대표적으로 Drain[3]은 고정 깊이 트리를 이용하여 온라인 환경에서 로그 템플릿을 빠르고 정확하게 추출하는 방법을 제안하였으며, 대규모 로그를 스트리밍 방식으로 처리할 수 있는 가능성을 보여주었다. 그러나 이러한 방식은 템플릿 품질과 파싱 정확도에 성능이 크게 의존하므로, 자유도가 높은 문장형 로그나 표현 변형이 많은 보안 로그 환경에서는 일반화에 한계가 있다.

시퀀스 예측 기반 연구로 DeepLog[4]는 시스템 로그를 자연어 시퀀스와 유사한 형태로 간주하고, LSTM을 이용하여 다음 이벤트를 예측한 뒤 예측 오차를 바탕으로 이상 여부를 판단하지만, 주로 이벤트 ID 또는 템플릿 시퀀스에 의존하기 때문에 로그 메시지 자체의 의미적 다양성을 직접 반영하는 데에는 제약이 있다. 이후 BERT 기반 연구인 LogBERT[5]는 정상 로그 시퀀스의 패턴을 자기지도 방식으로 학습하기 위해 masked log key prediction과 hypersphere minimization을 결합한 구조를 토대로 정상 패턴에서 벗어나는 경우를 이상으로 판단한다. 또한 최근에는 다중 시스템 로그를 함께 다루는 MLAD[6]는 Sentence-BERT 기반 의미 벡터와 attention 구조를 결합하여 다중 로그 원천에 대한 이상탐지를 수행하였다. 한편 LogCSS[7]는 BERT 임베딩, CNN, 통계 정보를 함께 결합하여 의미적 특징, 시간적 특징, 상관 특징을 동시에 반영하는 하이브리드 구조를 제안하였다. 더 나아가 LLM을 로그 파싱에 활용하고 BERT 기반 이상탐지와 결합하는 연구[8]도 등장하여, 의미 기반 로그 해석과 이상탐지의 결합 가능성을 한층 확장되고 있다.

2.3 네트워크 및 IoT 보안 로그 분석

네트워크 및 IoT 보안 분야에서도 이상 행위를 단순 패킷 통계나 단일 특징으로만 분석하기보다, 시퀀스와 문맥을 반영하여 해석하려는 시도가 점차 확대되고 있다. 예를 들어 네트워크 플로우를 시간적으로 인접한 시퀀스로 구성한 후 이를 자연어와 유사한 순차 데이터로 간주하여 BERT 기반 특징추출을 수행하고, 침입탐지의 도메인 적응 성능을 향상시키고자 하였다[9]. 이러한 접근은 전통적인 분류 기반 IDS가 가지는 일반화 한계를 완화하려는 시도로 볼 수 있다.

특히 IoT 환경에서는 장비 종류와 데이터 형식의 이질성이 매우 크기 때문에, 단일 모델 또는 단일 특징만으로 이상탐지를 수행하는 데 한계가 있다. Lai 등은 IoT 환경의 이질적 특성을 토대로 다양한 모델의 예측력을 결합하는 ensemble learning이 높은 예측력을 제공할

수 있음을 제시하였다[10]. 이러한 연구들은 IoT 및 네트워크 보안 분석에서 단일 이벤트 또는 단일 특징 중심 접근보다는 다중 정보의 결합이 중요하다는 점을 보여준다. 하지만, 실제 네트워크 보안 로그에서 자주 나타나는 mixed 파일 구조, 세션 경계 문제, 동일 세션 내 반복 행위 누적 효과, 그리고 명시적 행 단위 라벨 기반 검증은 상대적으로 충분히 다루어지지 않았다고 볼 수 있다. 이는 기존 로그 이상탐지 연구가 이벤트 수준 성능에는 강점을 보이지만 실제 운영 환경에서 요구되는 세션 수준 해석과 판단으로 확장되는 데에는 한계가 있다는 것을 의미한다.

2.4 선행연구의 문제점 및 해결방안

앞에서 살펴본 선행연구는 로그의 의미 표현과 순차적 특성을 자동으로 학습하는 방향으로 발전해 왔으며, 특히 Transformer와 BERT 계열 모델의 도입 이후 로그 이상탐지의 정확도와 확장성은 크게 향상되었다. 그럼에도 불구하고 기존 연구에는 (1) 많은 연구가 이벤트 단위 또는 시퀀스 단위 분류 성능에 초점을 두고 있으며, 실제 보안 운영에서 중요한 세션 단위 탐지 성능을 별도로 평가하지 않는 경우가 많으며, (2) 정상 및 비정상 이벤트가 많지 않은 상태에서 혼합(mixed) 교차하는 상황에서 문맥 확장이 오히려 오분류를 증가시키는 경우가 발생한다. 또한 (3) 일부 연구는 템플릿 기반 라벨이나 자동 추정 라벨에 의존하므로, 실제 라인 단위 이상 여부와 불일치할 가능성이 있고, (4) 문맥 윈도우의 크기 변화와 세션 집계 효과를 체계적으로 비교함으로써 탐지 구조의 실효성을 검증한 연구는 상대적으로 제한적이다. 이에 본 연구는 기존 BERT 기반 로그 이상탐지 연구를 네트워크 보안 로그와 세션 중심 분석 관점으로 확장한 방식을 제시한다.

3. 제안 기법

3.1 제안 메커니즘 구조 설계

본 연구에서 제안하는 Session Context-Aware BERT의 목적은 네트워크 보안 로그를 단순히 개별 이벤트 단위로 판정하는 것을 넘어, 이벤트 주변의 문맥 정보와 동일 세션 내 반복 행위를 함께 반영함으로써 실제 공격 흐름을 보다 안정적으로 식별하는 데 있다. 기존의 이벤트 중심 탐지 방식은 각 로그 라인을 독립적으로 해석하므로, 단일 이벤트만으로는 명확히 드러나지 않는 다단계 공격이나 반복적 이상 행위를 충분히 반영하기 어렵다. 반면 실제 보안 공격은 특정 로그 한 줄이 아니라, 시간적으로 인접한 이벤트들의 흐름과 동일 주체에 의해 반복되는 세션 수준의 행위 패턴 속에서 보다 뚜렷하게 나타난다. 이를 반영하기 위해 본 논문은 전체 로그 집합을 다음과 같이 정의한다.

$$\varepsilon = \{e_1, e_2, \cdots, e_N\} \quad \text{식 (1)}$$

여기서 e_i는 i번째 보안 로그 이벤트를 의미하며 제안 기법은 각 이벤트 e_i에 대하여 먼저 이벤트 자체의 의미 점수를 계산하고, 다음으로 반경 1, 2, 3의 문맥 윈도우 점수를 산출한 뒤, 마지막으로 세션 단위 요약 정보를 결합하여 최종 이상 여부를 판단한다. 즉, 제안 방식은 이벤트 수준, 문맥 수준, 세션 수준의 증거를 계층적으로 통합하는 구조를 갖는다. 이를 함수 형태로 요약하면 다음과 같다.

$$\hat{y}_i = f(e_i, N_i^{(1)}, N_i^{(2)}, N_i^{(3)}, S(e_i)) \quad \text{식 (2)}$$

이때 $N_i^{(k)}$는 이벤트 e_i를 중심으로 한 반경 k의 인접 문맥 집합을 의미하며, $S(e_i)$는 이벤트 e_i가 속한 세션을 의미한다. 이와 같은 구조는 기존의 단일 이벤트 기반 탐지와 달리, 현재 로그의 의미뿐 아니라 이웃 이벤트의 분포와 세션 전체의 누적 행위를 함께 고려한다.

3.2 이벤트 대상 의미 판정

제안 기법의 첫 단계는 개별 이벤트의 의미를 BERT 기반으로 해석하여 기본 이상 점수를 산출하는 것이다. 로그 이벤트 e_i의 텍스트 표현을 BERT 인코더에 입력하여 임베딩 벡터를 생성하고, 이를 정상 프로파일과 이상 프로파일에 각각 비교함으로써 의미적 유사도를 계산한다. 이때 이벤트가 이상 행위에 얼마나 가까운지를 나타내는 기본 마진은 이상(Abnormal) 점수와 정상(Normal) 점수의 차로 정의할 수 있다.

$$M_B^{(i)} = \delta_A^{(i)} - \delta_N^{(i)} \quad \text{식 (3)}$$

여기서 $\delta_A^{(i)}$는 이벤트 e_i가 이상(Abnormal) 프로파일과의 최대 유사도(Similarity)이고, $\delta_N^{(i)}$는 정상(Normal) 프로파일과의 최대 유사도이다. 따라서 기본 마진값 $M_B^{(i)}$가 클수록 해당 이벤트는 정상보다는 이상 행위에 더 가깝다고 해석할 수 있다. 그러나 실제 네트워크 보안 로그에서는 BERT 기반 의미 점수만으로 충분하지 않은 경우가 존재한다. 예를 들어 인증 실패, 외부 목적지 연

결, 특정 관리 포트 접근, 장문 DNS 질의 등은 보안적으로 중요한 단서가 되므로, 본 연구에서는 키워드 기반 힌트와 포트·프로토콜 기반 보조 특징을 함께 반영하였다. 이를 포함한 이벤트 수준 최종 점수는 다음과 같이 표현할 수 있다.

$$\Omega_{event}(e_i) = \alpha M_B^{(i)} + \beta H_i + \gamma P_i \quad \text{식 (4)}$$

여기서 H_i는 의심 키워드 및 정상 힌트 기반 점수, P_i는 포트·프로토콜 기반 가중치이며, α, β, γ는 각 특징의 반영 비중을 조절하는 계수이다. 결국 제안 기법은 단순한 의미 임베딩 모델이 아니라, 로그 메시지의 의미와 보안 도메인 지식을 함께 결합하는 구조임을 의미한다.

3.3 문맥 윈도우 기반 보정

이벤트 단위 방식의 이상탐지는 개별 로그 한 줄의 의미를 반영하는 데 효과적이지만, 인접 이벤트와의 관계를 충분히 설명하지는 못한다. 이에 본 연구에서는 현재 이벤트 주변의 문맥 정보를 함께 고려하여, 국소적인 행위 흐름이 이상 행위와 얼마나 일치하는지를 추가적으로 평가하도록 하였다. 이벤트 e_i에 대한 반경 k의 문맥 집합은 현재 이벤트를 중심으로 앞뒤 k개의 이웃 이벤트를 포함하는 형태로 정의된다.

문맥 반영의 핵심은 단순히 여러 로그를 이어 붙이는 것이 아니라, 현재 이벤트의 의미 점수, 문맥 전체의 의미 점수, 그리고 이웃 이벤트들의 이상 분포를 함께 결합하는 데 있다. 이를 반영한 문맥 윈도우 점수는 다음과 같이 정의한다.

$$M_{window}^{(i,k)} = \omega_1 M_B^{(i)} + \omega_2 M_{CTX}^{(i,k)} + \omega_3 R_{abn}^{(i,k)} - \omega_4 R_{norm}^{(i,k)} + \omega_4 C_{aux}^{(i,k)} \quad \text{식 (5)}$$

즉, 문맥 윈도우 점수 $M_{window}^{(i,k)}$는 현재 이벤트의 기본 의미 마진값 $M_B^{(i)}$, 반경 k 문맥 텍스트 전체로부터 얻은 문맥 마진 $M_{CTX}^{(i,k)}$, 이웃 이벤트들 중 비정상 및 정상 판정 비율에 해당하는 $R_{abn}^{(i,k)}$ 및 $R_{norm}^{(i,k)}$, 반복 엔티티 수, 라벨 합의 수준, 의심 신호 다양성 등 부가 문맥 특징을 통합한 $C_{aux}^{(i,k)}$ 값으로 구성된다. 따라서 식 (5)는 현재 이벤트가 다소 모호하더라도 주변 이벤트 다수가 유사한 이상 경향을 보인다면 문맥 점수는 증가하며, 반대로 주변 이벤트 다수가 정상으로 해석되면 문맥 점수는 감소한다. 즉, 문맥 윈도우는 개별 이벤트의 즉시적 해석을 인접 행위 흐름에 의해 보정하는 역할을 수행한다.

물론 문맥이 항상 성능 향상을 가져온다고 가정하지 않는다. 정상 이벤트와 비정상 이벤트가 짧은 구간에 혼재(mixed) 교차하여 발생하므로, 문맥 반경이 지나치게 커질 경우 오히려 잡음이 증가할 수 있다. 따라서 본 논문에서는 반경 $k=1,2,3$에 대해 각각 독립적인 실험을 수행하여 문맥 범위에 따른 효과를 비교 분석하였다.

3.4 세션 프로파일링 및 최종 이상탐지 판별 과정

실제 보안 운영에서 중요한 것은 특정 로그 한 줄의 분류 정확도만이 아니라, 공격 세션 전체를 놓치지 않고 식별하는 것이다. 예를 들어 단일 로그인 실패는 정상 사용자의 오입력일 수 있지만, 동일 사용자 또는 동일 출발지에서 반복적으로 실패가 누적되고 이후 외부 접속 또는 권한 상승 시도가 이어진다면 전체 세션은 명백한 이상 행위일 가능성이 높다. 이러한 이유로 본 연구에서는 이벤트 수준 및 문맥 수준 판정 결과를 세션 단위로 다시 집계하여 최종 판정을 수행한다.

세션 s는 동일 행위 주체와 통신 채널의 조합으로 정의하며, 그 안에 포함된 이벤트 집합을 ε_s라고 할 경우 세션에 대해서 평균 마진, 비정상 이벤트 비율, 정상 이벤트 비율, 목적지 다양성, 의심 패턴 밀도 등의 특징을 계산한다. 이를 반영한 세션 수준 점수는 다음과 같이 표현할 수 있다.

$$\Omega_{Session}(s) = \lambda_1 \overline{M}_s + \lambda_2 r_s^{abm} + \lambda_3 r_s^{norm} + \lambda_4 u_s + \lambda_5 d_s + \lambda_6 b_s \quad \text{식 (6)}$$

$\overline{M}_s$는 세션 평균 마진, r_s^{abn}은 세션 내 비정상 이벤트 비율, r_s^{norm}은 정상 이벤트 비율, u_s는 세션 내 목적지 다양성, d_s는 의심 패턴 밀도, b_s는 brute-force, port scan, lateral movement, C&C beacon, data exfiltration 등 특정 공격 유형에 대한 패턴 부스트 값을 나타내며, 이를 통해서 최종적으로 이벤트 e_i의 이상 여부는 단일 이벤트 점수, 세 가지 문맥 윈도우 점수, 그리고 해당 세션의 세션 수준 점수를 결합하여 다음과 같은 수식으로 최종 판정식을 도출할 수 있다.

$$M_{final}^{(i)} = \mu_0 \Omega_{event}(e_i) + \mu_1 M_{Window}^{(i,1)} + \mu_2 M_{Window}^{(i,2)} + \mu_3 M_{Window}^{(i,3)} + \mu_4 \Omega_{Session}(s(i)) \quad \text{식 (7)}$$

위 식에서 $s(i)$는 이벤트 e_i가 속한 세션을 의미하며, $\mu_0, \mu_1, \mu_2, \mu_3, \mu_4$는 각 수준의 증거에 대한 결합 가중치이다. 최종 분류는 다음 식 (8)과 같다.

$$\hat{y}_i = \begin{cases} 1, \text{if } M_{final}^{(i)} > \tau \\ 0, otherwise \end{cases} \quad \text{식 (8)}$$

τ는 최종 판정을 위한 임계값으로, 최종 판정은 단일 이벤트의 의미 해석만으로 이루어지지 않으며 서로 다른 반경의 문맥 정보와 세션 수준의 누적 행위 증거를 함께 통합하였다. 기존의 이벤트 중심 탐지나 단순 시퀀스 모델과 달리, 이벤트–문맥–세션의 계층적 결합 방식이다.

3.5 제안 메커니즘의 차별성

제안하는 Session Context-Aware BERT 메커니즘은 다음 그림 1과 같이 의사코드 기반 알고리즘으로 간략히 추상화하여 표현 가능하다.

Proposed Session Context-Aware BERT Algorithm

Input: Event Set E*, Window Size* $W = \{1,2,3\}$
Output: Final anomaly detection result $\hat{y}$

From Event Set E
for each Event $e_i \in E$*:*
  Compute event-level score $\Omega_{event}(e_i)$
  for each window $k \in W$*:*
    Compute context score $M_{window}^{(i,k)}$
Group Event Set E *into Session Set* S
for each Session $s_j \in S$*:*
  Compute session score $\Omega_{session}(s_j)$
  for each event $e_i \in E$*:*
    Compute final score $M_{final}^{(i)}$ *based on* $\Omega_{session}(s_j)$
    Assign anomaly label $\hat{y}$ *based on* $M_{final}^{(i)}$
return $\hat{y}$

[Fig. 1] Proposed Session Context-Aware BERT Algorithm

본 연구에서 제안한 기법의 차별성은 다음과 같이 요약할 수 있다. 첫째, 로그를 독립 이벤트로만 보지 않고, 이벤트 주변의 국소 문맥과 세션 전체의 누적 패턴을 함께 반영한다는 점에서 기존의 단일 이벤트 기반 탐지와 구별된다. 둘째, 문맥 반경을 1, 2, 3으로 분리하여 평가함으로써, 문맥이 항상 유효하다는 전제를 두지 않고 정상/비정상 정보가 혼합된 로그 환경에서의 검출 한계까지 향상시킬 수 있도록 하였다. 셋째, 최종 판정의 중심을 이벤트 단위 정확도가 아니라 세션 단위의 탐지 신뢰도 향상에 두었다는 점에서 실제 보안 운영 환경에 보다 적합한 구조를 제안하였다. 결과적으로 제안한 Session Context-Aware BERT는 단순히 BERT를 로그 분석에 적용한 모델이 아니라, 의미 기반 이벤트 판정, 문맥 기반 국소 보정, 세션 기반 누적 판정을 하나의 통합 프레임워크로 구성한 계층형 이상탐지 모델이라 할 수 있다.

4. 실험 결과 및 성능 분석

4.1 실험 데이터

본 연구에서는 총 200개의 네트워크 보안 로그 파일을 대상으로 실험을 수행하였다. 사용된 로그는 정상 웹 접근, 정상 서비스 호출, 정상 인증, 정상 파일 전송과 같은 정상 시나리오뿐 아니라 brute-force 로그인, 포트 스캔, 명령제어(Command and Control), 데이터 유출, DNS 이상, lateral movement, payload 실행, 그리고 정상 및 비정상 이벤트가 혼재된 mixed 형태의 보안 로그 정보를 포함하도록 구성하였다. 실험 구현은 .txt, .log, .csv형식의 입력을 지원하며, 각 파일은 이벤트 단위로 분리되어 분석에 사용되었다. 본 실험에서는 표 1과 같이 수집된 보안 로그 파일내에는 총 619개 이벤트 정보가 포함되어 있었으며, 젠체 세션수를 총 259개로 구성되어 있었고, 정상 및 비정상 로그 이벤트 수는 64개가 혼재되어 있는 형태의 데이터를 대상으로 분석 과정을 수행하였다.

〈Table 1〉 Experimental Dataset Composition

Category	Values
Total Number of Log	200
Total Number of Events Analyzed	619
Total Number of Sessions Analyzed	259
Number of Mixed Normal/Abnormal Log Events	64

4.2 실험 설정 및 비교 모델

구현은 Python 환경에서 수행하였으며, BERT 기반 추론에는 Transformers와 PyTorch라이브러리를 사용하였다. 기본 언어모델은 'security_bert_pretrained' 모델을 사용하였으며, 입력 시퀀스의 최대 길이는 128로 설정하였고, 실행 환경에 따라 MPS, CUDA, CPU 중 사용 가능한 연산 장치를 자동 선택하도록 하였다.

성능 비교 모델은 총 네 가지로 구성하였다. Window-1/2/3 방식을 통해 현재 이벤트를 중심으로 각각 반경 1/2/3개의 인접 문맥을 함께 반영하였다. 또한 Session Context-Aware 방식을 통해 단일 이벤트 점수와 문맥 점수에 더하여 세션 프로파일 및 패턴 부스트를 함께 결합한 최종 제안 모델이다. 이와 같은 비교 설정은 문맥 반경에 따른 효과와 세션 수준 집계의 기여도를 단계적으로 확인하기 위한 것이다.

네 가지 방식에 대해 상세 성능 평가는 세 가지 수준에서 수행하였다. 첫째, 전체 이벤트에 대한 이벤트 단위

평가를 수행하였다. 둘째, 정상과 비정상 이벤트가 동일 파일 내에 공존하는 mixed 로그만을 추출하여 mixed subset 평가를 수행하였다. 그리고 세번째로는 동일 행위 주체와 채널을 기준으로 그룹화된 세션을 대상으로 세션 단위 평가를 수행하였다. 또한 파일 수 증가에 따른 baseline과 Session Context-Aware 방식의 성능 추이도 함께 산출하여, 데이터 규모 변화에 따른 성능 안정성을 관찰하였다.

4.3 성능 평가 지표

이벤트 단위 성능 평가는 Accuracy, Precision, Recall, F1-score를 사용하였다. 실제 라벨은 normal과 abnormal의 이진 범주로 통일하였으며, 혼동행렬(confusion matrix)은 True Positive(TP), True Negative(TN), False Positive(FP), False Negative(FN)를 기준으로 계산하였다.

mixed 로그는 동일 파일 내부에 정상 및 비정상 이벤트가 동시에 존재하는 복합 상황을 반영하므로, 일반 로그보다 문맥 기반 모델의 한계를 더욱 직접적으로 드러내는 스트레스 테스트 역할을 수행한다. 따라서 본 연구에서는 전체 이벤트 성능과 별도로 mixed 로그 subset 성능을 추가적으로 제시하였다.

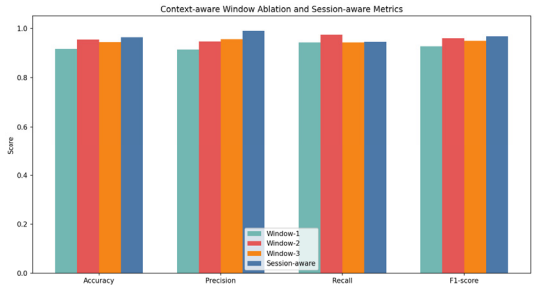
4.4 이벤트 대상 성능 평가

전체 619개 명시적 라벨 이벤트에 대한 성능 비교 결과는 표 2 및 그림 2와 같다. 실험 결과, 최종 제안 방식인 Session-Aware는 F1-score 0.9678로 Window-1/2/3 방식 보다 높은 검출 성능을 보였으며, 문맥 윈도우 기반 모델 중에서는 Window-2가 F1-score 0.9606으로 Window-1/3에 비해 안정적인 검출 성능을 보였다.

〈Table 2〉 Overall Event-Level Performance Comparison

Method	Window-1	Window-2	Window-3	Session-Aware
Accuracy	0.9176	0.9548	0.9435	**0.9645**
Precision	0.9141	0.9472	0.9565	**0.9910**
Recall	0.9429	**0.9743**	0.9429	0.9457
F1-score	0.9283	0.9606	0.9496	**0.9678**
TP	330	341	330	331
TN	238	250	254	266
FP	31	19	15	3
FN	20	9	20	19

이 결과는 단순히 인접 문맥을 추가한다고 해서 이벤트 단위 성능이 자동적으로 향상되는 것은 아님을 보여준다. 특히 Window-1은 FP가 31건으로 크게 증가하여 다섯 모델 중 가장 낮은 성능을 보였다. 이는 매우 짧은 문맥이 유효한 보조 정보를 제공하기보다 주변 잡음을 함께 포함하였기 때문으로 해석할 수 있다. 반면 Window-2는 Recall 0.9743으로 가장 높게 유지되면서도 Precision 손실을 일정 수준 통제하여, 문맥 모델 중 가장 균형 잡힌 결과를 제공하였다. 요컨대 전체 이벤트 기준에서는 단일 이벤트 자체의 의미 표현이 매우 강건하였으며, 문맥 반영은 반경의 설정에 따라 성능 향상과 성능 저하가 모두 가능함을 확인할 수 있었다.



[Fig. 2] Total Event based Detection Performance Metrics

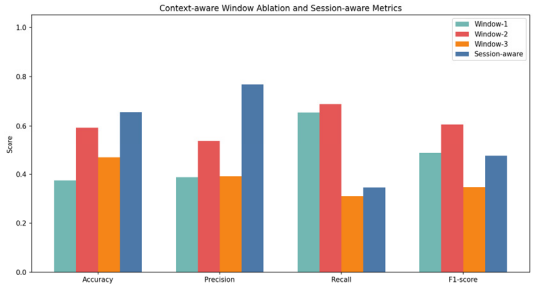
4.5 혼재(mixed) 보안 로그 이벤트 단위 성능 평가

정상과 비정상 이벤트가 한 파일 내부에서 혼재하는 mixed 로그 64개 이벤트에 대한 성능 비교 결과는 표 3 및 그림 3과 같다. 이 실험에서 문맥 기반 모델들은 전반적으로 성능이 높지 않으나, 그중에서는 Window-2가 F1-score 0.6061으로 가장 높은 값을 보였다. Session Aware는 Accuracy 0.6562, Precision 0.7692, Recall 0.3448, F1-score 0.4762를 기록하였다.

〈Table 3〉 Event-Level Performance Comparison on Mixed Security Logs

Method	Window-1	Window-2	Window-3	Session-Aware
Accuracy	0.3750	0.5938	0.4688	**0.6562**
Precision	0.3878	0.5405	0.3913	**0.7692**
Recall	0.6552	**0.6897**	0.3103	0.3448
F1-score	0.4872	**0.6061**	0.3462	0.4762
TP	19	20	9	10
TN	5	18	21	32
FP	30	17	14	3
FN	10	9	20	19

이 결과는 mixed 환경에서 문맥 결합이 오히려 과도한 평균화 효과를 유발할 수 있음을 보여준다. 즉, 현재 이벤트와 주변 이벤트가 서로 다른 의미 공간에 속할 경우, 문맥 윈도우는 공격 신호를 강화하기보다 서로 상쇄시키는 방향으로 작동할 수 있다. 특히 Window-1과 Window-3의 성능 저하는, 너무 좁거나 너무 넓은 문맥 모두 mixed 환경에서는 불안정할 수 있음을 의미한다. 이러한 결과는 제안 기법의 한계를 드러내는 동시에, 향후 연구에서 세션 경계 정교화, 이벤트 선택형 문맥 구성, 주의집중 기반 이웃 선택 메커니즘 등이 필요함을 알 수 있다.



[Fig. 3] Mixed Event based Detection Performance Metrics

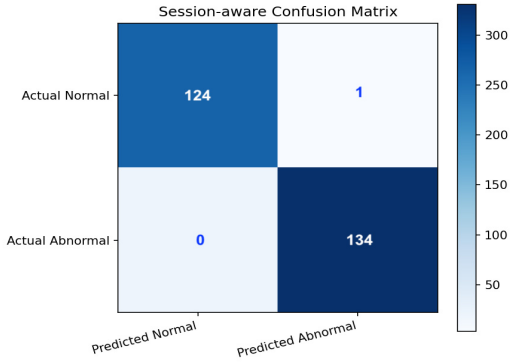
4.6 세션 이벤트 단위 성능 평가

전체 259개 세션을 대상으로 평가한 결과, 표 4와 같이 Session-Aware 모델은 Accuracy 0.9961, Precision 0.9926, Recall 1.000, F1-score 0.9963을 기록하였다. 이는 그림 4와 같이 실제 공격 세션에 대한 False Negative가 0건이었음을 의미하며, 세션 기준으로는 공격 세션을 한 건도 놓치지 않았음을 보여준다.

〈Table 4〉 Session Event-Level Performance

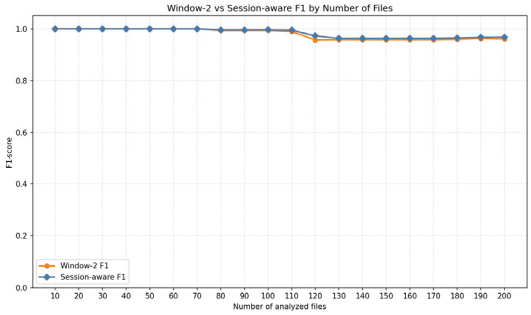
Method	Performance of Session Context-Aware BERT		
Analysis Target	Event-Oriented	Mixed-Events	Session-Oriented
Accuracy	0.9645	0.6562	0.9961
Precision	0.9910	0.7692	0.9926
Recall	0.9457	0.3448	1.000
F1-score	0.9678	0.4762	0.9963
TP	331	10	134
TN	266	32	124
FP	3	3	1
FN	19	19	0
Number of Event	619	64	259

세션 기준 오탐은 1건에 불과하였으며, 해당 사례는 정상 관리자 활동 세션이었으나 일부 비정상과 유사한 패턴을 포함하여 경계 영역에 위치한 경우로 해석될 수 있다. 중요한 점은, 이벤트 단위 F1-score만 놓고 보면 실제 운영 관점에서 더 큰 비용을 갖는 세션 단위 미탐은 Session-Aware에서 발생하지 않았다는 사실이다. 이는 본 연구가 단순한 이벤트 단위 최고 정확도 추구보다, 운영 환경에서 중요한 공격 세션 탐지 신뢰도 향상에 초점을 두고 있음을 잘 보여준다. 다시 말해 제안 방식의 핵심 장점은 이벤트 수준 분류보다 세션 수준 누적 판단에서 더욱 분명하게 드러난다.



[Fig. 4] Session-aware based Confusion Metrics

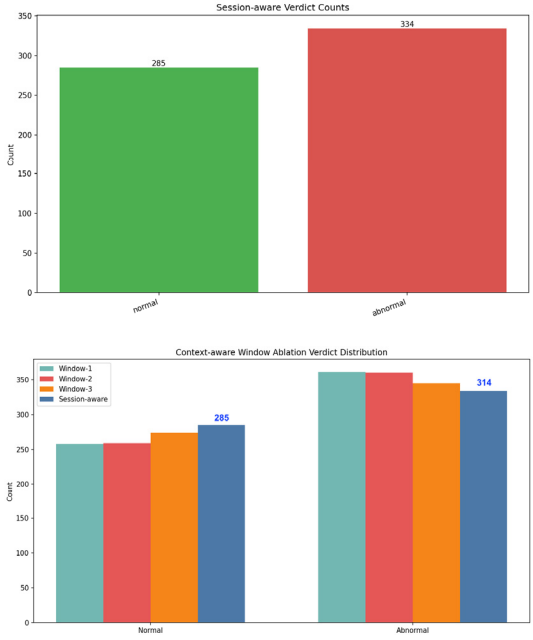
표 2와 표 3에 제시된 내용과 같이 상대적으로 우수한 성능을 보인 Window-2 모델과 Session-Aware 모델 방식에 대해 수집된 총 200개의 파일에 대해 분석 대상을 늘려가면서 F1-score 값을 비교 분석하면 다음 그림 5와 같다. 분석 결과 Session Context-Aware 모델 방식이 우수한 성능을 보이는 것을 확인할 수 있었다.



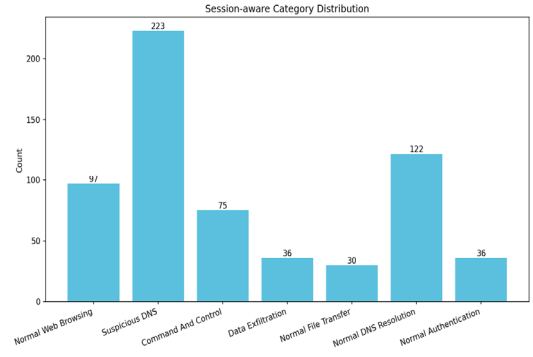
[Fig. 5] Analysis File Size based Detection Performance (F1-score)

4.7 이상탐지 결과 분석 및 고찰

제안한 Session-Aware 방식은 200개의 보안 로그 파일에 포함된 전체 분석 대상 이벤트 619개에 대해서 아래 그림 6과 같이 정상 이벤트 285개(46.04%)와 비정상 이벤트 334개(53.96%)로 판별하는 것을 확인할 수 있었다.



[Fig. 6] Session-Aware Model Verdict Counts



[Fig. 7] Session-Aware Model Detection Category Distribution

또한, Session-Aware 방식은 전체 분석 대상 이벤트 619개에 대해서 아래 그림 7과 같이 공격 패턴/유형을 자동 분류하는 기능을 제공하고 있다. 자동 분류 결과 비정상 이벤트 334개 중에서 223개의 이벤트는 Suspicious DNS(36.02%) 공격 형태로 판별하였으며, 75개의 이벤트에 대해서는 C&C(12.11%) 공격, 그리고 36개의 이벤트에 대해서는 Data Exfiltration(5.81%) 공격으로 자동 구분하여 제시함을 확인할 수 있었다.

실험 결과를 종합하면 다음과 같은 결론을 도출할 수 있다. 첫째, 전체 이벤트 단위 분류 시 문맥 윈도우 기반 모델 중 Window-2가 가장 안정적인 절충점을 제공하였다. 이는 너무 짧은 문맥은 잡음에 민감하고, 너무 넓은 문맥은 mixed 환경에서 의미 혼합을 초래할 수 있음을 의미한다. 또한, mixed 로그에서는 문맥 결합이 항상 유리하지 않았으며, 경우에 따라 오히려 성능 저하를 유발할 수 있었다. 그리고, 세션 단위 평가에서는 Session-aware가 매우 높은 성능을 보이며 공격 세션을 한 건도 놓치지 않았다. 따라서 본 연구에서 제안하는 Session Context-Aware BERT 메커니즘은 이벤트 단위 최고 정확도를 달성하는 데만 있는 것이 아니라, 실제 보안 운영에서 더욱 중요한 세션 단위 탐지 신뢰도를 향상시키는 데 있다고 할 수 있다. 특히 공격 탐지에서 미탐 비용이 오탐 비용보다 더 크게 작용하는 환경을 고려할 때, 본 연구의 세션 인식 기반 구조는 실무적 활용 가능성이 높다는 것을 알 수 있었다.

5. 결론

본 논문에서는 사물인터넷 환경에서 생성되는 네트워크 보안 로그의 이상 행위를 효과적으로 식별하기 위해 Session Context-Aware BERT를 제안하였다. 제안 기법은 기존의 이벤트 중심 탐지 방식과 달리, 개별 로그 이벤트의 의미를 BERT 기반으로 해석하는 이벤트 수준 분석, 반경 1, 2, 3의 인접 문맥을 반영하는 문맥 윈도우 분석, 그리고 동일 세션 내 반복 행위와 누적 패턴을 집계하는 세션 수준 분석을 계층적으로 결합하도록 설계되었다. 이를 통해 단일 로그 라인만으로는 명확히 드러나지 않는 다단계 공격의 연속성과 세션 수준의 행위 맥락을 보다 효과적으로 반영하고자 하였다.

실험 결과, 전체 200개 로그 파일과 619개의 명시적 라벨 이벤트, 259개의 평가 세션을 대상으로 한 실험에서 문맥 기반 모델 중에서는 Window-2가 가장 안정적인 절충점을 제공하였으나, mixed 로그 환경에서는 문맥 결합이 항상 유리하지 않았고, 경우에 따라 성능 저하를 유발할 수 있음을 확인하였다. 그리고 최종 제안하는 방식인 Context 기반의 Session-aware 모델은 실제 보안 운영 환경에서 중요한 세션 단위 탐지 신뢰도 향상

에 강점을 가진다는 것을 알 수 있었다.

향후 연구에서는 mixed 로그 환경에서 관찰된 성능 저하를 완화하기 위해 고정 반경 문맥 윈도우 대신 이벤트 중요도에 따라 문맥을 동적으로 선택하는 적응형 문맥 선택 메커니즘을 도입할 필요가 있다. 그리고 특정 도메인에 특화된 보안 로그 사전학습 모델을 적용하거나 실제 관제 환경의 대단위 장기간 수집된 로그를 대상으로 추가 학습함으로써, 보다 높은 일반화 성능과 실시간 적용 가능성을 검증한다면 제안 기법의 실무적 활용성은 더욱 높아질 것으로 기대된다.

REFERENCES

[1] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention Is All You Need," in Advances in Neural Information Processing Systems, Vol.30, 2017, pp.5998-6008.

[2] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-Training of Deep Bidirectional Transformers for Language Understanding," in Proc. 2019 Conf. of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (NAACL-HLT), Minneapolis, MN, USA, 2019, pp.4171-4186.

[3] P. He, J. Zhu, Z. Zheng, and M. R. Lyu, "Drain: An Online Log Parsing Approach with Fixed Depth Tree," in Proc. IEEE Int. Conf. on Web Services (ICWS), 2017, pp.33-40.

[4] M. Du, F. Li, G. Zheng, and V. Srikumar, "DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning," in Proc. 2017 ACM SIGSAC Conf. on Computer and Communications Security (CCS), Dallas, TX, USA, 2017, pp.1285-1298.

[5] H. Guo, S. Yuan, and X. Wu, "LogBERT: Log Anomaly Detection via BERT," in Proc. Int. Joint Conf. on Neural Networks (IJCNN), Shenzhen, China, 2021, pp.1-8.

[6] C. Hu, X. Sun, H. Dai, H. Zhang, and H. Liu, "Research on Log Anomaly Detection Based on Sentence-BERT," Electronics, Vol.12, No.17, 2023.

[7] Z. Li, X. Tu, H. Gao, S. Huang, and Z. Ma, "LogCSS: Log Anomaly Detection Based on BERT-CNN with Context-Semantics-Statistics Features," Journal of Intelligent & Fuzzy Systems, Vol.46, No.4, pp.7659-7676, 2024, doi: 10.3233/JIFS-235801.

[8] Y. Zhou, Y. Chen, X. Rao, Y. Zhou, Y. Li, and C. Hu, "Leveraging Large Language Models and BERT for Log Parsing and Anomaly Detection," Mathematics, Vol.12, No.17, 2024.

[9] Y. Yang and X. Peng, "BERT-based Network for Intrusion Detection System," EURASIP Journal on Information Security, Vol.2025, No.11, pp.1-11, 2025.

[10] T. Lai, F. Farid, A. Bello, and F. Sabrina, "Ensemble Learning Based Anomaly Detection for IoT Cybersecurity via Bayesian Hyperparameters Sensitivity Analysis," Cybersecurity, Vol.7, 2024.

[11] W. Meng, Y. Liu, Y. Zhu, S. Zhang, D. Pei, Y. Liu, Y. Chen, R. Zhang, S. Tao, P. Sun, and R. Zhou, "LogAnomaly: Unsupervised detection of sequential and quantitative anomalies in unstructured logs," in Proc. 28th Int. Joint Conf. Artificial Intelligence (IJCAI), Macao, China, 2019, pp.4739-4745.

[12] S. Chen and H. Liao, "BERT-Log: Anomaly detection for system logs based on pre-trained language model," Applied Artificial Intelligence, Vol.36, No.1, pp.1-19, 2022.

[13] C. Hu, X. Sun, H. Dai, H. Zhang, and H. Liu, "Research on log anomaly detection based on Sentence-BERT," Electronics, Vol.12, No.17, pp.1-19, 2023.

[14] V.-H. Le, H. Zhang, et al., "LightLog: A lightweight temporal convolutional network for log anomaly detection on the edge," Computer Networks, Vol.203, pp.1-14, 2022.

[15] Y. Lee, J. Kim, and P. Kang, "LAnoBERT: System log anomaly detection based on BERT masked language model," Applied Soft Computing, Vol. 145, pp. 1-16, 2023.

[16] F. Hang, W. Guo, H. Chen, L. Xie, C. Zhou, and Y. Liu, "Logformer: Cascaded transformer for system log anomaly detection,"CMES - Computer Modeling in Engineering & Sciences, Vol.136, No.1, pp.517-529, 2023.

[17] W. Niu, X. Liao, S. Huang, Y. Li, X. Zhang, and B. Li, "A robust wide & deep learning framework for log-based anomaly detection,"Applied Soft Computing, Vol.153, pp.1-17, 2024.

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 컴퓨터학과 (학사)
- 1996년 2월 : 고려대학교 컴퓨터학과 (석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 (박사)
- 1999년 3월 ~ 2003년 2월 : 백석대학교 정보통신학부 교수
- 2003년 3월 ~ 현재 : 한신대학교 AISW대학 교수

〈관심분야〉
사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식, 지능형 사이버공격 대응