클라우드 환경에서의 머신러닝 기반 웹 공격 탐지 성능 비교

김건민[1] 김예진[2], 김태림[3], 김경백[1]
전남대학교 인공지능융합학과[1]
전남대학교 소프트웨어공학과[2]
전남대학교 인공지능학부[3]
ye031010@jnu.ac.kr, ktr0706@jnu.ac.kr, geonminkim@jnu.ac.kr,
kyungbaekkim@jnu.ac.kr

Comparative Anlaysis of Machine Learning Models for Web Attack Detection in Clouds

Geonmin Kim[1], Yejin Kim[2], Taerim Kim[3], Kyungbaek Kim[1]
Dept. of AI Convergence, Chonnam National University[1]
Dept. of Software Engineering, Chonnam National University[2]
Dept. of Artificial Intelligence, Chonnam National University[3]

요 약

클라우드 컴퓨팅으로의 전환은 IT 인프라에 유연성과 확장성을 부여했지만, 동시에 동적이고 분산된 환경으로 인해 새로운 보안 패러다임을 요구한다. 기존의 경계 기반 모델은 수시로 변하는 클라우드 환경에서 한계를 드러내며, 방대한 양의 로그 데이터 속에서 정교한 위협을 탐지하기 위해 머신러닝 및 인공지능 기술이 도입되고 있다. 본 연구는 이러한 흐름 속에서, 웹 애플리케이션을 보호하는 핵심 요소인 지능형 공격 탐지 시스템 구축을 목표로, 클라우드 환경에서 수집된 웹 로그 데이터를 활용하여 네 가지 머신러닝 모델(RandomForest, XGBoost, LightGBM, HistGradientBoosting)의 성능을 비교 평가한다. 실험 결과, HistGradientBoosting이 높은 탐지 정확도를 보여주었으며, 이는 대규모 클라우드 환경의 자동화된 실시간 위협 대응 시스템 구축의 높은 잠재력을 시사한다.

1. 서 론

클라우드 환경의 확산과 함께 웹 기반 사이버 공격은 점점 더 복잡하고 동적으로 변화하고 있다. 특히 하이브리드 클라우드 환경은 온프레미스 환경과 클라우드의 결합으로 네트워크 경계가 모호해져 기존의 경계 기반의 보안 모델은 한계를 드러낸다[1]. 이에 최근에는 머신러닝과 AI를 활용한 지능형 위협 탐지 시스템에 대한 연구가 활발히 진행되고 있다[2-4]. 특히, 웹 로그나 URL의 텍스트 패턴을 분석하여 악성 행위를 판별하는 접근법은 높은 탐지 정확도를 보이며 그 가능성을 입증해왔으며, 머신러닝 모델을 특징 선택 도구로 사용하고, 온라인에서는 추출된 핵심 특징 기반의 간단한 규칙으로 탐지하는 방식이 주목받고 있다[5]. 이에 본 연구는 특징 선택기로서 배깅 기법의 RandomForest, 부스팅 계열의 XGBoost와 LightGBM, HistGradientBoosting의 성능을 비교하여 최적의 모델을 도출한다. 각 모델이 식별하는 핵심 특징 차이가 최종 규칙의 탐지 성능에 미치는 영향을 정량적으로 비교 분석함으로써, 효과적인 동적 규칙 생성 프레임워크를 제안한다.

2. 관련 연구

클라우드 환경의 확산과 함께, 대규모 로그 데이터를 분석하여 이상 행위를 탐지하는 연구가 활발히 진행되고 있다[2-5]. 특히, 하이브리드 및 멀티 클라우드 환경은 이질적인 인프라와 분산된 서비스 간의 상호작용으로 인해 새로운 형태의 위협을 초래하고 있으며, 이러한 복합적 공격 벡터를 실시간으로 식별하기 위한 머신러닝 및 인공지능 기반 위협 탐지 기술이 주목 받고 있다. 본 연구는 머신러닝 모델별 웹 로그 기반 위협 탐지 성능을 비교 분석함으로써 보안 시스템의 실효성을 높이고자 한다.

3. AI 기반 위협 탐지 방법론

3.1 데이터 수집 및 전처리

대규모 원시 로그 데이터를 머신러닝 모델이 학습할 수 있는 형태로 가공한다. 로그는 734576건의 정상 로그, 81798건의 Malware, 43348건의 Phishing, 30371건의 Spam으로 구성되어 있다. Elasticsearch에 수집된 웹 로그에서 DNS 도메인과 URI 정보, Protocol 등을 추출한 뒤, 텍스트를 토큰 단위로 분리한다. 이렇게 생성된 토큰들은 CountVectorizer를 통해 각 로그를 단어 등장 빈도 기반의 고차원 희소 행렬로 변환하였다. 최대 피처 수는 5000으로 제한하여 과적합을 방지하였다. 또한, 변동성이 거의 없는 상수형 특징을 제거하기 위해 VarianceThreshold를 적용하였으며, Dense 모델 학습에 적합한 형태로 변환하기 위해 TruncatedSVD를 활용하였다. 이를 통해 로그의 구조적 복잡도를 줄이면서 주요 특징만을 남겨 모델 학습 효율성을 확보하였다.

3.2 모델 학습 및 평가

가공된 훈련 데이터를 특징 선택기로서의 앙상블 모델들을 각각 학습시킨다. 모델의 안정성을 검증하기 위해 데이터를 무작위로 샘플링하여 총 3회에 걸쳐 훈련(80%) 및 테스트(20%)를 반복하는 방식으로 실험을 진행하였다. 본 연구에서는 배깅 기법의 RandomForest와 부스팅 기법의 XGBoost, LightGBM, HistGradientBoosting을 비교 대상으로 선정하였다. 또한, 각 모델의 상위 중요 토큰 300개를 선정하여, 이 토큰들은 정규표현식 기반 패턴으로 변환되어 공격 탐지 정책으로 활용되었다. 이를 통해 모델이 학습한 패턴이 실제 정책 수준에서 얼마나 유효한지 검증함으로써, 모델 기반 동적 정책 생성의 가능성을 실험적으로 평가하였다. 이러한 절차를 통해 각 모델의 탐지 성능을 비교 분석하였으며, 모델 간 일관된 평가를 위해 동일한 피처 파이프라인을 유지하였다.

4. 실험 결과

Model	Round	Accuracy
RandomForest	1	0.8531
	2	0.8661
	3	0.8719
	Avg	0.8637
XGBoost	1	0.8366
	2	0.8382
	3	0.8412
	Avg	0.8387
LightGBM	1	0.8254
	2	0.8271
	3	0.8321
	Avg	0.8252
HistGradientBoosting	1	0.8768
	2	0.8683
	3	0.8801
	Avg	0.8751

(표 1) 머신러닝 및 딥러닝 모델 성능 비교

실험 결과 HistGradientBoosting 모델과 RandomForest가 일관되고 높은 탐지 성능을 기록하였다. 특히, HistGradientBoosting은 88%를 상회하는 탐지 정확도(Accuracy)를 달성하기도 하였다. 본 실험은 정확도에 초점을 맞추어 진행되었으나, 실제 클라우드 환경에 모델을 배포할 경우에는 운영 효율성 또한 중요한 고려사항이다. HistGradientBoosting과 같은 최신 부스팅 알고리즘은 대규모 데이터셋에 대한 학습 속도와 자원 사용량 측면에서 이점을 갖는다. 따라서 본 실험에서 입증된 높은 정확도와 함께 이러한 효율성을 고려할 시 HistGradientBoosting 모델이 클라우드 네이티브 보안 환경을 위한 균형잡힌 모델로 평가할 수 있다.

5. 결론

본 연구는 현대 클라우드 환경이 직면한 복합적인 보안 과제를 조명하고, 이를 해결하기 위한 머신러닝 기반 위협 탐지 프레임워크를 제안하였다. 머신러닝 모델을 선정하기 위한 성능 비교 분석을 통해, HistGradientBoosting과 RandomForest가 웹 공격 탐지 시나리오에서 뛰어난 성능을 보임을 확인했다. 향후 연구에서는 본 연구에서 도출된 모델별 특징을 활용하여, 경량 정책 집합을 자동으로 생성하고, 이를 온라인 정책 평가 시스템에 연동하여 실시간 위협 차단 능력을 검증할 예정이다. 이를 통해 클라우드 네이티브 보안 시스템에서 모델 기반 정책 자동화의 실현 가능성을 높일 수 있다.

감 사 의 글

본 연구는 2025년도 과학기술정보통신부 및 정보통신기획평가원의 소프트웨어중심대학사업의 연구결과로 수행되었습니다.(2021-0-01409)(50%). 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임(IITP-2025-RS-2022-00156287)(50%).

참 고 문 헌

[1] S. B. Mallisetty, G. A. Tripuramallu, K. Kamada, P. Devineni, S. Kavitha and A. V. P. Krishna, "A Review on Cloud Security and Its Challenges," 2023 International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2023, pp. 798-804

[2] C. Anjani, R. M. Balajee, G. Divya, Y. S. Sree, K. Padmanabham and S. S. Srithar, "Evolving Threats and AI Solutions for Modern Hybrid Cloud Architectures," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 478-484

[3] S. J, K. Kanagasabapathi, K. Mahajan, S. Ahamad, E. Soumya and S. Barthwal, "AI-Enhanced Multi-Cloud Security Management: Ensuring Robust Cybersecurity in Hybrid Cloud Environments," 2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2023, pp. 1-6

[4] D. K. Seth, K. K. Ratra and A. P. Sundareswaran, "AI and Generative AI-Driven Automation for Multi-Cloud and Hybrid Cloud Architectures: Enhancing Security, Performance, and Operational Efficiency," 2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2025, pp. 00784-00793

[5] G. Kim, Y. Kim, E. Lee, H. Jang and K. Kim, "Edge-Based Policy Caching for Low Latency Security Enforcement in Hybrid Clouds," 2025 25th Asia-Pacific Network Operations and Management Symposium (APNOMS), Kaohsiung, Taiwan, 2025, pp. 1-6