다중 사이버 보안 AI 모델을 이용한 침해위협 탐지와 ELK 기반 대응 시각화에 대한 연구

이인재[1], 박찬웅[1], 권오준[1], 정재윤[2], 김채은[3], 한영우[4]
[1]부경대학교 정보통신공학과 학부생
[2]부경대학교 고분자공학과 학부생
[3]한국해양대학교 데이터정보학과 학부생
[4]한국예탁결제원
lhkgg7548@gmail.com, cksdnddlek99@gmail.com, kwonoj999@gmail.com,
rhdfyd128@gmail.com, chaeeung478@gmail.com, ywhan6@gmail.com

A Study on the Detection of Infringement Threats Using Multiple Cybersecurity AI Models and Visualization of Response Based on ELK

In-Jae Lee[1], Chan-Woong Park[1], Oh-Jun Kwon[1],
Jae-Yoon Jung[2],Chae-Eun Kim[3]
[1]Dept. of Information and Communication Engineering, Pukyong National University
[2]Dept. of Polymer Engineering, Pukyong National University
[3]Dept. of Data Information, Korea Maritime and Ocean University
[4]Korea Securities Depository

요 약

최근 많은 기업체들은 점점 고도화되고 있는 사이버 공격 위협에 대응하기 위해 다양한 보안 솔루션 도입 및 종합적인 네트워크 보안 분석을 수행하고 있다. 하지만 보안 영역에 많은 자원과 예산을 투입할 여력이 없는 중소형 업체들은 특히 침해위협 탐지와 대응 결과 시각화에 대한 어려움을 겪고 있다. 이에 따라 본 연구에서는 다중 사이버 보안 AI 모델 구현을 통해 다각도의 사이버 침해위협 발생 가능성을 예측하고, 추가적으로 오픈소스 기반의 ELK 플랫폼을 통한 대응 결과 시각화를 구현하고자 한다.

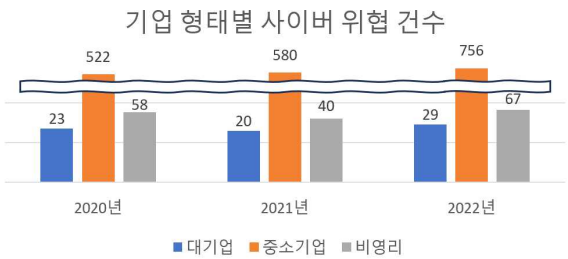
1. 서론

급속한 인터넷의 발달과 함께 사이버 공격이 증가하고 있으며, 이로 인해 현재 비즈니스 환경은 과거보다 더 큰 사이버 보안 위협을 받고 있다. <그림 1>에 따르면 매년 공격 건수가 증가하는 추세이며, 특히 중소기업이 사이버 공격에 가장 취약함을 알 수 있다. 이때 공격 유형은 '랜섬웨어', 'DDoS', '악성코드 유포' 순서대로 높게 나타났다.

본 연구에서는 이를 해결하기 위한 방법 중 하나로 다수의 사이버 보안 AI 모델을 이용해 DDoS와 악성 코드를 탐지하고, 탐지 결과를 분석할 수 있는 ELK 플랫폼을 구축하였다.

ELK는 분석 및 저장 기능을 담당하는 ElasticSearch, 수집 기능을 하는 Logstash, 이를 시각화하는 도구인 Kibana로 구성된 빅데이터 분석 프레임워크이다. 실시간 로그 분석과 확장성, 효과적인 시각화 및 대시보드, 다양한 데이터 유형을 지원하기에 ELK를 선택하여 플랫폼을 구축했다.

<그림 1> 기업 형태별 사이버 위협 건수
(출처: 한국인터넷진흥원)



DDoS는 Distributed Denial of Service의 약어로 사이트에 과도한 트래픽을 보내 마비시키는 사이버 공격이다. DDoS는 특정 탐지 장비로 처리가 가능하나, 장비의 가격대로 인해 다수의 중소기업은 처리 환경을 구축하지 못하고 있는 실정이다. 그래서 수집한 네트워크 트래픽으로 머신러닝 훈련을 진행하여 손쉽게 DDoS를 탐지할 수 있게 했다.

악성코드 탐지는 현장에서 주로 쓰이는 전자 문서인 PDF 내에 포함되는 악성코드를 대상으로 했으며, 여러 악성코드의 트리거가 될 수 있는 자바스크립트의 난독화 여부를 탐지하는 기능도 추가했다.

2. 본론

2.1 이상징후 DDoS 탐지 및 정적 악성코드 탐지 모델

본 프로젝트에 사용된 데이터셋은 다음과 같다. DDoS 데이터 세트는 CIC-DDoS-2019를 이용했다. 해당 데이터셋은 네트워크 트래픽들의 패턴과 레이블(DDoS or 정상)을 제공한다.

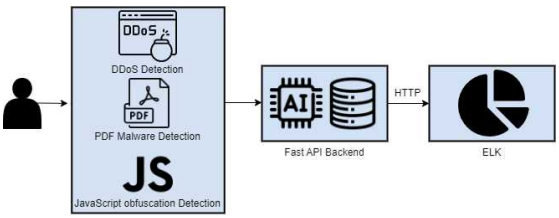
PDF 파일 특성화 데이터셋은 CIC-Evasive-PDFMal 2022를 이용했으며 PDF 파일들의 해시값과 헤더 특성, 악성 코드 유형들로 구성된다.

난독화된 자바스크립트 데이터셋은 정상과 난독화 자바스크립트로 이루어져 있으며, 자연어 처리를 통해 난독화의 특징을 추출했다. 위 데이터셋들을 전처리 후 GridSearch 모듈을 사용하여 Decision Tree, Random Forest, XGBoost, AdaBoost, LightGBM 모형에 대한 학습과 튜닝을 수행하였고 pkl 파일로 결과를 저장했다.

2.2 ELK 시각화 플랫폼 연결

pkl파일들을 FastAPI 서버에 저장한 다음 HTTP 통신으로 모델 추론 결과를 ELK서버에 저장했다. 이를 kibana에서 그래프로 시각화하였으며, 각 모델마다 따로 테이블을 만들어 대시보드를 구현하였다.

<그림 2> 다중 AI 탐지 모델과 ELK 시각화 구성도



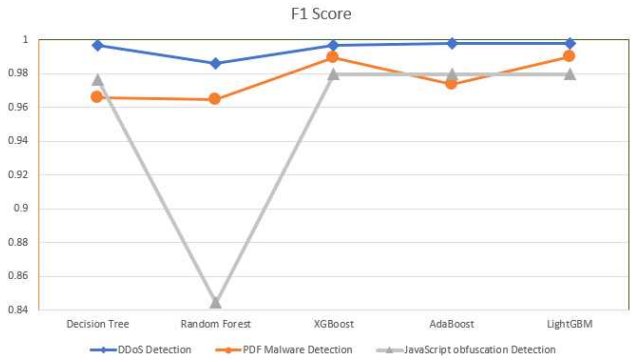
3. 결과 및 결론

본 연구에서는 DDoS탐지, PDF악성코드 탐지 및 자바스크립트 난독화 탐지의 세 가지 다른 사이버 보안 탐지 모델을 구현 및 성능 평가했다. <그림 3>의 DDoS 탐지에서는 AdaBoost 모델의 F1-Score가 0.998로 가장 우수한 성능을 보였다. 랜덤 포레스트와 XGBoost 모델도 좋은 성능을 보였지만, 0.9861과 0.9967로 약간 낮은 F1-Score를 보였다.

PDF 악성 코드 탐지 작업에서는, LightGBM의 F1-Score가 0.9902로 가장 뛰어난 성능을 보였으며, XGBoost도 0.9893의 높은 F1-Score를 기록하여 효과적인 악성 코드 탐지성능을 보였다. AdaBoost와 의사 결정 트리 모델은 어느 정도 성능을 보였지만 랜덤 포레스트 모델의 F1-Score는 약간 낮았다.

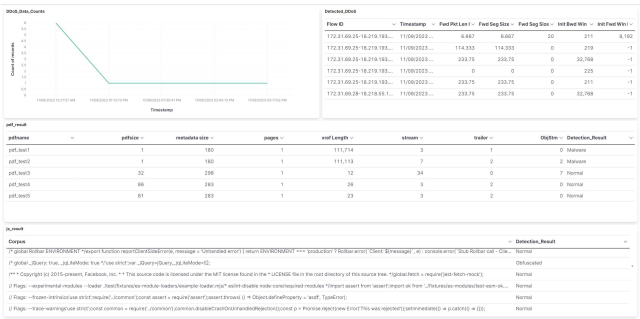
JavaScript 난독화 탐지에서는 랜덤 포레스트가 0.8444로 가장 낮은 F1-Score를 기록했으며, XGBoost와 AdaBoost, LightGBM이 모두 0.9797로 높은 성능을 나타냈다.

<그림 3> 3가지 탐지 모델별 F1-Score 비교



대응 시각화 플랫폼은 <그림4>과 같이 구성된다. DDoS와 PDF, 자바스크립트 관련 데이터를 각각 테이블로 제공해 특성을 살펴볼 수 있고 Detection_Result 열에서 해당 행의 데이터가 정상인지 아닌지 예측 결과를 확인 할 수 있다. 그리고 DDoS의 경우 해당 시간에 들어온 데이터의 수를 확인할 수 있는 그래프를 구현했다.

<그림 4> ELK 대시보드 화면



본 모델들은 설명하기 어려운 복잡한 기존 모델에 비해 단순한 알고리즘을 사용하므로 설명하기 용이하다. 또한 모델의 이상 탐지 속도가 빨라 보안 인프라가 부족한 기업도 빠르게 대응할 수 있다.

향후 실제 환경에서의 데이터를 활용한 현장 테스트와 탐지 모델 개선 과정이 필요하며 이를 기반으로 본 논문이 중소기업들의 사이버 보안 실무 능력 향상에 도움이 될 것으로 기대한다.

※ 본 프로젝트는 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT멘토링 프로젝트 결과물입니다.

참고문헌

[1] 이용필, 국내 사이버 침해사고의 경제적 피해 금액 산정, Korea Business Review, 24권, 2호, pp.143-164,2020.
[2] 김종민, 엘라스틱 스택에 기반한 실시간 웹서비스 관제 시스템의 설계와 구현, 한국정보과학회, 개최지, 2018, pp.1901-1903.
[3] Emmanuel Tsukerman, 사이버 보안을 위한 머신러닝 쿡북, 서울, 에이콘 출판사, 2021.
[4]서준석, 인공지능, 보안을 배우다, 서울, BJ퍼블릭, 2019.