사물인터넷융복합논문지 Vol. 11, No. 1, pp. 107-114, 2025 https://doi.org/10.20465/KIOTS.2025.11.1.107

MS-Office 계열 파일 내 매크로 정보 기반 악성 정보 자동 검출 메커니즘 설계 및 구현

이형우*
한신대학교 AISW대학 교수

Design and Implementation of an Automatic Detection Mechanism for Malicious Information Based on Macro Data in MS-Office File

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

요 약 본 논문에서는 머신러닝 기법을 적용하여 MS Office 파일 내에 포함된 매크로 악성 정보를 자동으로 검출할 수 있는 시스템을 설계 및 구현하였다. MS Office 파일 내 매크로 기능을 포함할 경우 사용자 시스템에 대한 비정상 행위를 수행하고 결과적으로 시스템 내에 저장된 중요 개인 정보 등이 외부로 유출될 가능성이 있다. 따라서 MS Office 파일 내에 포함된 악성 스크립트를 자동 탐지하고, 위변조 여부를 자동 검출할 수 있는 시스템이 필요하다. 이를 위해서 본 연구에서는 MS Office 파일 내 매크로 포함 여부 자동 판별하기 위해 지도 학습 및 비지도 학습 기반 머신러닝 기반 모델을 적용한 악성 매크로 자동 검출 시스템을 설계 및 구현하였다. 실험 결과 기존 기법 보다 개선된 자동 검출 성능을 제공하여 MS Office 디지털 파일에 대해 안전한 이용 환경을 제공할 수 있다.

주제어 : MS Office 매크로 파일, 악성 코드, 머신러닝, 자동 검출 시스템, 지도/비지도 학습 모델

Abstract In this paper, we designed and implemented a system that applies machine learning techniques to automatically detect malicious macro information embedded in MS Office files. When an MS Office file contains macro functionality, it may perform abnormal actions on the user's system, potentially leading to the leakage of sensitive personal information stored within the system. Therefore, a system is needed to automatically detect malicious scripts embedded in MS Office files and verify any tampering. To achieve this, this study applies supervised and unsupervised learning-based machine learning models to design and implement an automatic detection system for determining whether an MS Office file contains malicious macro data. Experimental results demonstrate that the proposed system provides improved detection performance compared to existing methods, ensuring a safer environment for the use of MS Office files.

Key Words : MS Office Macro File, Malicious Code, Machine Learning, Auto-Detection System, Supervised/Unsupervised Learning Model

이 논문은 한신대학교 학술연구비 지원에 의해 연구되었음.
*교신저자 : 이형우(hwlee@hs.ac.kr)
접수일 2025년 01월 21일 수정일 2025년 02월 11일 심사완료일 2025년 02월 17일

1. 서론

MS Office 디지털 파일 내에 악성 스크립트 등이 포함/은닉되어 있을 경우 비정상적인 행위를 수행할 수 있다. MS Office 파일인 경우 OLE VBA 매크로 객체를 포함할 경우 일반적인 백신 소프트웨어 등을 사용하더라도 검출되지 않는 등 많은 문제점이 발견되고 있다[1-4]. 특히 MS Office 파일은 ZIP 압축 형태로 저장되며 OOXML 저장 포맷 구조로 관리되고 있으나 MS Office 파일 내 OLE VBA 매크로 객체 등을 포함하고 있을 경우 사용자 시스템에 치명적인 악성 행위를 유발할 수 있다[5][6]. 따라서, MS-Office 계열의 디지털 파일에 대한 분석[7-9] 및 매크로 객체 검사 과정을 통해 디지털 파일에 대한 위변조 여부를 확인하고 비정상적인 디지털 파일 내부 구조를 식별하며 내부에 은닉된 악성 파일을 탐지할 수 있는 기술이 개발되어야 한다.

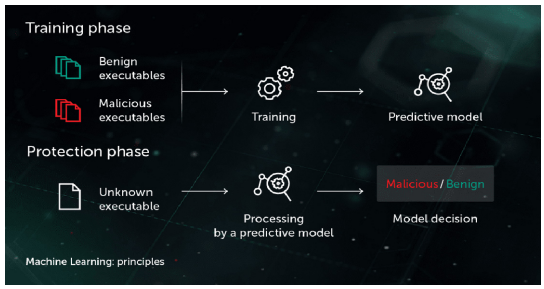
이에 본 연구에서는 머신러닝 기술을 사용하여 MS Office 파일 내에 포함된 OLE VBA 매크로 객체 등을 자동 검출하고 악성 스크립트 은닉 여부를 자동 판별할 수 있는 메커니즘을 설계 및 구현하였다. 본 연구에서 제안한 시스템을 이용할 경우 MS Office 계열의 각종 디지털 파일에 대한 위변조 여부와 악성 스크립트에 대한 은닉 여부를 효율적으로 자동 판별하여 보다 안전한 디지털 문서 편집 환경을 제공할 수 있다.

2. 머신러닝 기법 적용

2.1 머신러닝 기반 학습 및 판별 구조

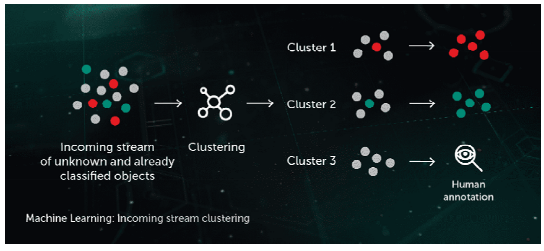
MS-Office 계열 파일 내 매크로 정보를 기반으로 악성 여부를 자동 검출하는 머신러닝 시스템[8][9]의 학습 및 판별 과정은 크게 데이터 수집, 특징 추출, 모델 학습, 판별 및 검증의 4단계를 수행하게 된다. 해당 과정의 주요 목적은 악성 매크로 코드의 패턴을 학습하고 새로운 악성 위협을 효과적으로 탐지하는 것을 목적으로 한다.

MS-Office 문서 내 매크로 정보를 기반으로 악성 여부를 판별하기 위해 머신러닝 시스템[10-12]을 적용할 경우 아래 그림 1과 같이 (1) Training Phase(훈련 단계)와 (2) Prediction Phase(예측 단계)로 구성된다[1][2][4].



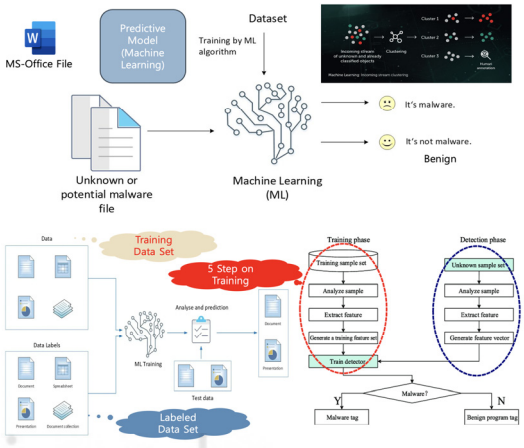
[Fig. 1] Training and Prediction Phase on ML

각 단계는 데이터 수집, 특징 추출, 모델 학습 및 평가, 실시간 예측 및 대응 등의 과정을 포함하며, 아래 그림 2와 같이 Training Phase에서는 정상 및 악성 매크로 데이터로 부터 학습과정을 수행하여 패턴을 익히는 과정을 수행하고, Prediction Phase에서는 사용자로부터 임의의 디지털 문서를 입력받은 후 기존에 학습된 모델을 사용하여 정상/악성 여부를 자동 판별하게 된다[15-17].



[Fig. 2] ML based Clustering for Classification

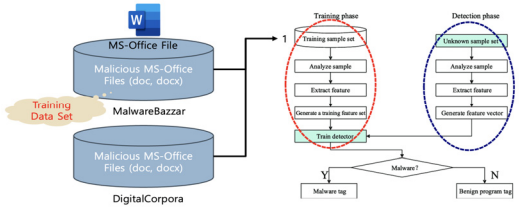
2.2 머신러닝 기반 훈련 단계



[Fig. 3] Training Phase on Machine Learing

위 그림 3과 같이 Training Phase는 머신러닝 모델이 정상 및 악성 매크로의 특징을 학습하는 과정으로, 구축하고자 하는 머신러닝 모델은 악성 매크로를 판별하는데 필요한 패턴을 학습하고, 최적의 성능을 내기 위해 반복적인 학습과 평가를 수행한다.

이를 위해서 (1단계) 데이터 수집 및 전처리 (Data Collection & Preprocessing)을 수행한다. 머신러닝 모델의 성능을 높이기 위해 정상적인 매크로 데이터, 기업 내부 문서 및 일반 사용자 문서와 MS Office 템플릿 문서 등과 같이 대량의 정상 및 악성 매크로 데이터를 확보해야 한다. 또한 공개 매크로 코드 저장소 및 악성 매크로 데이터 등을 수집한 후 전처리 과정을 거쳐 학습 가능한 형태로 변환한다. MalwareBazaar[22] 등과 같은 공개 악성 문서 데이터셋을 확보한 후 (2단계) 데이터 전처리 (Data Preprocessing) 과정을 수행한다. 문서 내부에서 매크로 코드를 분리하거나 난독화 해제(Deobfuscation), Base64 디코딩, 문자열 치환, 암호화 해제 및 불필요한 메타데이터 제거 과정을 수행한다. 전처리 과정을 마친 이후에는 (3단계) 특징 추출(Feature Extraction) 과정을 수행한다. 머신러닝 모델이 효과적으로 학습 과정을 수행할 수 있도록, 매크로 코드에서 중요한 특징(features) 정보를 추출한다. 이와 같이 3단계 과정을 수행한 후에는 (4단계) 모델 학습(Model Training) 과정을 수행한다[3].

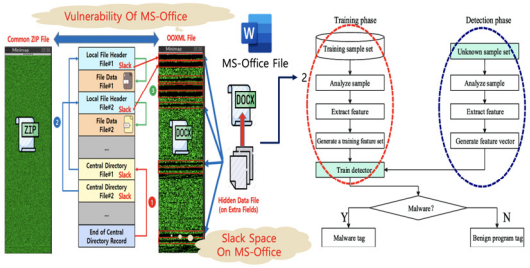


[Fig. 4] Prediction/Decision Phase on MS Office File

추출된 특징에 대해 머신러닝 알고리즘을 적용하여 최적의 머신러닝 모델을 선별하게 된다. 정상/악성 데이터 라벨링(Data Labeling) 과정을 수행한 후 머신러닝 알고리즘을 적용하며 최종 (5단계) 모델 평가 및 최적화 (Model Evaluation & Optimization) 과정을 수행하게 된다. 위 그림 4와 같이 학습된 모델이 새로운 데이터에서도 정확하게 악성 매크로를 탐지할 수 있도록 F1 Score 등을 토대로 성능을 평가하고 최적화 과정을 수행한다.

2.3 머신러닝 기반 예측 단계

머신러닝 기반 Prediction Phase에서는 훈련 단계에서 구축 및 학습된 모델을 사용하여 임의의 MS-Office 문서에 대해 악성 여부를 예측/판별하게 된다. 입력된 디지털 파일로부터 (1단계) 특징 정보를 추출 (Input & Feature Extraction)한 후에 디지털 파일 내 매크로 코드를 추출하고, 앞서 수행한 Training Phase와 동일한 방식으로 정적, 동적, 통계적 특징을 분석하여 추출된 특징을 머신러닝 모델이 이해할 수 있는 벡터(vector)로 변환하는 과정을 수행한다.



[Fig. 5] MS Office File Training & Decision Phase

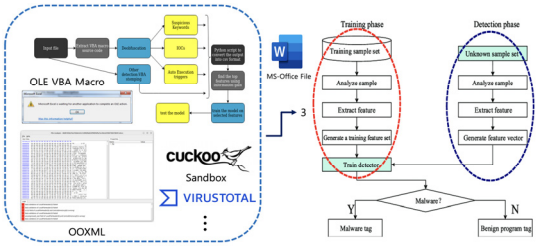
이를 토대로 (2단계) 악성 여부 예측 (Malware Detection & Classification) 과정을 수행한다. 학습된 머신러닝 모델에 입력된 특징을 전달한 후 예측 결과를 기반으로 악성 여부를 정상(Benign)/의심(Suspicious)/악성(Malicious)의 3개 형태로 판별한다. 판별된 파일에 대해서는 최종적으로 (3단계) 실시간 대응 및 보안 조치 (Real-time Response & Security Actions) 과정을 수행한다. 이메일 첨부파일 필터링, 실행 차단 의심 문서 추가 분석 등과 같은 과정을 수행하거나, 탐지된 악성 매크로 데이터를 Training Phase에 반영하는 등 새로운 악성 패턴 학습 과정을 적용한다.

결국 Training Phase에서는 머신러닝 모델이 정상 및 악성 매크로 데이터를 학습하여 탐지 패턴을 익히고, Prediction Phase에서는 실시간으로 새로운 문서를 분석하여 악성 여부를 판별하게 된다. 이와 같은 훈련/예측 단계를 효과적으로 설계하고 최적화하면, 기존 탐지 기법을 우회하는 신종 악성 매크로에 대해 효과적으로 탐지할 수 있으며, 실시간 대응 시스템과 연계하여 보안성을 강화할 수 있다.

3. 머신러닝 기반 MS Office 계열 매크로 악성 파일 자동 판별 시스템

3.1 머신러닝 기반 매크로 악성 여부 판별

본 연구에서는 머신러닝 기법[9-12]을 적용하여 그림 6과 같이 MS Office 계열 매크로 악성 파일을 자동 검출/판별하는 시스템을 설계 및 구현하였다. 임의의 MS Office 파일을 대상으로 정상/악성 여부를 판별하기 위해서는 특징 정보를 추출하고 이를 벡터화 하여 자동 분석하는 과정을 수행하였다. MS Office 파일 내부 속성 정보, 매크로 정보와 특징 정보를 추출한 후 이를 토대로 최적의 머신러닝 모델을 적용하여 악성 스크립트가 은닉된 손상 파일 여부를 정확하게 판단할 수 있다.

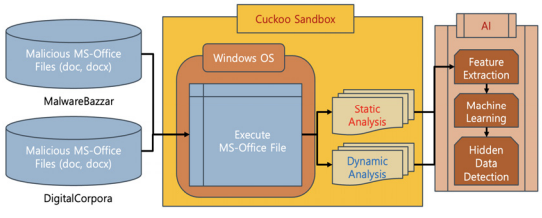


[Fig. 6] ML based Macro File Auto Detection

OLE VBA 기반 매크로 포함 여부 판별하고 비정상적 구조 분석 및 악성 스크립트 포함 여부 등을 판별하여 최적의 성능을 제시하는 머신러닝 모델을 제시하였다.

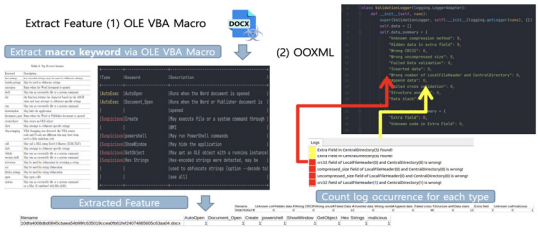
3.2 정적 특징 정보 추출 방식

MS Office 매크로 파일에 대한 머신러닝 기법 적용을 위해 아래 그림 7과 같이 정적/동적 특징 추출 및 분석 과정[7][22][23]을 수행하였다.



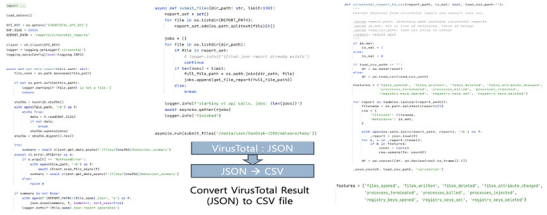
[Fig. 7] Static/Dynamic Analysis based ML

우선 정적 분석을 위해 아래 그림 8과 같이 OLE VBA 매크로 객체 포함 여부를 분석하고 이를 정적 특징 정보(Static Feature)로 추출하며, MS Office 계열 내부 구조를 토대로 OLE VBA 메타 데이터를 분석하고 디지털 파일 내부에 포함된 의심 객체를 대상으로 특징 정보를 JSON 파일로 추출/생성토록 하였다.



[Fig. 8] Static Feature Analysis

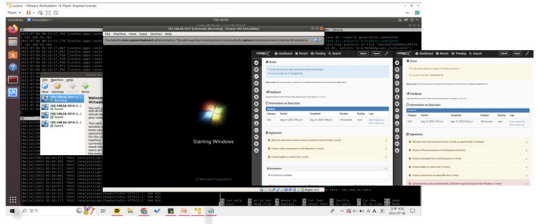
효율적인 머신러닝 과정을 수행하기 위해 아래 그림 9와 같이 특징 정보를 벡터 데이터 형태로 변환/생성하였으며, 추출된 특징 정보를 JSON 파일 형태로 변환한 후에 최종적으로 CSV 포맷으로 변환/생성하여 머신러닝 훈련 과정의 입력 데이터로 생성하였다. 이와 같이 MS Office 디지털 파일에 대한 분석 벡터 정보는 머신러닝 과정에사 사용되는 중요 입력 데이터로 사용된다.



[Fig. 9] CSV Feature File Extraction

3.3 동적 특징 정보 추출 방식

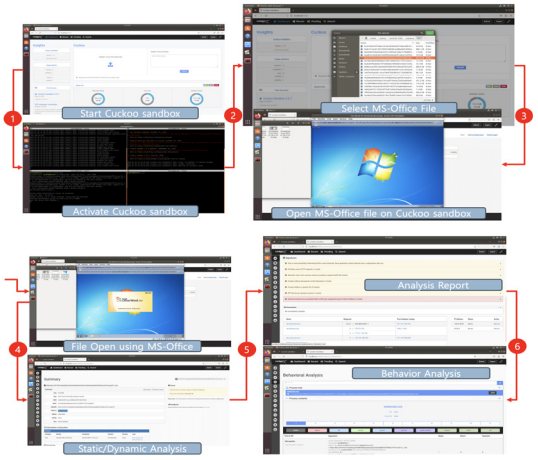
MS Office 파일이 사용자 시스템에서 구동되는 과정에서 생성되는 특징 정보를 이용할 경우 더욱 더 정확하게 정상/악성 여부를 판별할 수 있다. 따라서 본 연구에서는 아래 그림 10과 같이 동적 실행 과정을 통해 생성



[Fig. 10] Cuckoo Sandbox based Analysis

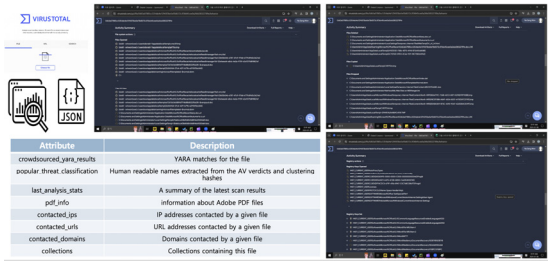
되는 특징 정보(Dynamic Feature)를 추출하였다. 우선 아래 그림과 같이 Cuckoo 샌드박스 내에 MS Windows를 설치한 후에 정상/악성 MS Office 파일을 실행하여 실시간으로 생성되는 이벤트 정보 및 네트워크 연결 정보 등을 수집하여 특징 정보로 생성하였다.

동적 특징 정보를 수집하는 과정을 단계적으로 제시하면 아래 그림 11과 같다.



[Fig. 11] Cuckoo Sandbox based Analysis Process

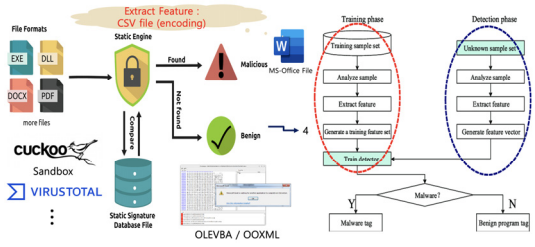
위 그림에서 제시한 내용과 같이 Cuckoo 샌드박스 내에서 MS Office 파일을 실행할 경우 동적 행위 분석 결과를 벡터 정보로 생성하여 정상/악성 파일의 특징 정보로 수집할 수 있었다. 이에 더하여 본 연구에서는 아래 그림 12와 같이 정상/악성 파일에 대한 판별 정확도를 향상시키기 위해서 VirusTotal[19] 시스템과 연계하여 동적 행위 정보 등을 추가적으로 수집/구축하였다. 파일 정보, 내부 구성 정보 및 은닉 매크로 포함 여부 등을 복합 판별하여 정상/악성 파일에 대한 판별 정확도를 향상시키도록 하였다.



[Fig. 12] VirusTotal based Dynamic Analysis Process

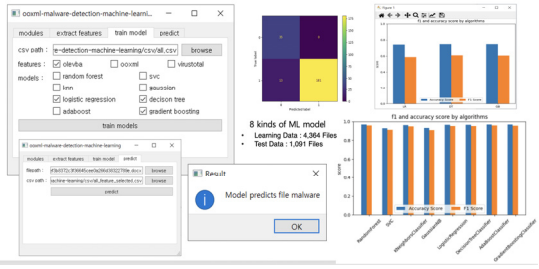
3.4 머신러닝 기반 매크로 악성 파일 자동 판별 시스템 설계 및 구현

위에 제시한 내용을 기반으로 아래 그림 13과 같이 머신러닝 기반 매크로 악성 디지털 파일에 대한 자동 판별 시스템을 설계 및 구현하였다. 임의의 MS Office 파일을 입력하면 매크로 포함 여부, 구조 분석 및 악성 DB에 대한 자동 분석 과정을 통해 높은 정확도로 정상/악성 파일을 자동 판별해 주는 머신러닝 시스템을 개발하였다.



[Fig. 13] Propose ML based Analysis Process

또한 본 연구에서는 사용된 머신러닝 기법에 따라 검출 성능을 비교 분석할 수 있도록 성능 비교 평가 시스템을 개발/적용하였다. 정적/동적 특징 정보가 포함된 특징 정보 데이터를 토대로 8개의 지도 학습(supervised learning) 및 뉴럴 네트워크 기반 비지도 학습(unsupervised learning) 방식을 적용하여 각각의 머신러닝 모델을 통해 자동 판별 과정의 성능을 비교 분석할 수 있도록 하였다. 지도 및 비지도 학습 과정을 수행한 후에는 아래 그림 14와 같이 임의의 MS Office 계열 파일에 대한 머신러닝 기반 자동 판별 성능을 표시토록 하였다.



[Fig. 14] Implementation Results

4. 실험 결과 분석

4.1 실험 환경 및 머신러닝 모델 상세

임의의 MS Office 계열의 디지털 파일에 대한 매크로 악성 코드 감염 여부 및 정상/악성 여부를 자동 판별하기 위해 파이썬[20] 기반 scikit-learn 라이브러리[21]를 이용하여 각각의 머신러닝 모델별 자동 판별 성능[13][14][18]을 비교 분석하였다. 머신러닝 모델별로 F1 스코어를 비교하여 임의의 MS Office 파일을 대상으로 매크로 악성 파일 포함 여부를 자동 판별하였으며, Random Forest, SVM, K-NN, Gausian Naive Bayes, Logistic Regression, Decision Tree, Ada Boost, Gradient Boosting 등과 같은 8개의 지도 학습 머신러닝 모델과 함께 Neural Network 기반 비지도 학습 머신러닝 모델을 적용하여 검출 성능을 비교 분석하였다.

4.2 머신러닝 모델별 성능 비교 평가

위에 제시한 내용과 같이 총 9개의 머신러닝 기법을 적용하였을 경우 각각의 머신러닝 모델별 검출 성능을 비교/평가하기 위해 F1 score를 측정하여 머신러닝 모델의 성능 비교 과정을 수행하였다.

$$Accuracy = \frac{(TP + TN)}{100} \quad (1)$$

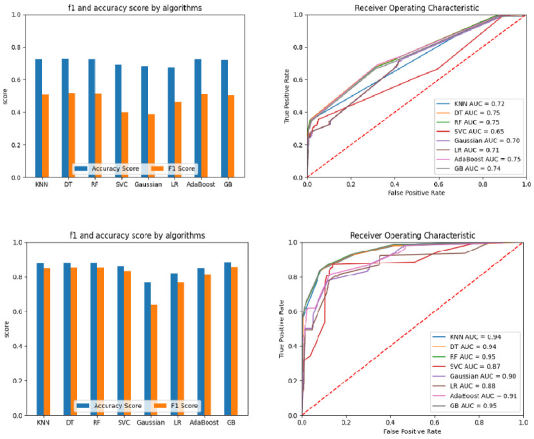
$$\mathrm{Precision} = \frac{TP}{(TP + FP)} \quad (2)$$

$$Recall = \frac{TP}{(TP + FN)} \quad (3)$$

$$F1\,score = \frac{2\,(\mathrm{Precision} * Recall)}{(\mathrm{Precision} + Recall)} \quad (4)$$

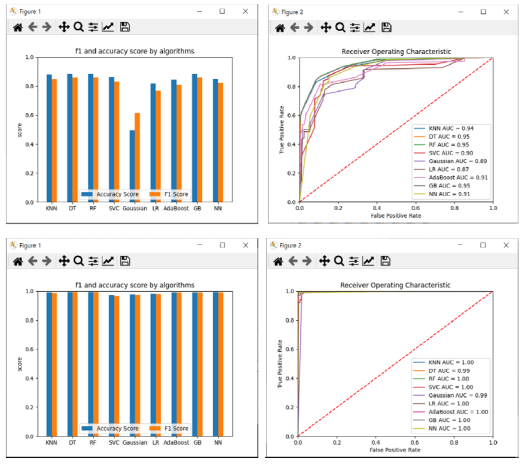
실험 데이터로는 MalwareBazzar[22], DigitalCorpora[23] 사이트에서 제공하는 MS Office 계열 데이터셋을 사용하였다. 정상 파일 250개와 악성 스크립트를 포함한 비정상 데이터 파일 250개 등 총 500개의 MS Office 파일을 대상으로 실험을 수행하였다.

지도 학습(Supervised learning) 기반 8개 머신러닝 모델을 적용하였을 경우 정상/악성 판별 정확도를 비교 분석해 보면 아래 그림 15와 같이 나타나는 것을 확인할 수 있었다. 측정 결과 Gaussian 모델이 가장 성능이 낮은 것으로 나타났으며 k-NN, Decision Tree 및 Random Forest 모델은 유사한 판별 성능을 나타냈다. 그리고 각각의 모델에서 학습 데이터가 증가할수록 False Positive Rate가 변화하는 것도 측정할 수 있었다.



[Fig. 15] Proformance Analysis : Supervised Learning

이에 추가적으로 아래 그림 16과 같이 지도 학습 8개 모델과 함께 Neural Network 기반 비지도 학습 1개 모델을 적용하였을 경우에 자동 검출 성능을 비교 분석하였다. 정상/비정상이 포함된 총 500개의 MS Office 파일을 대상으로 통합적인 형태로 자동 판별 과정을 실험한 결과 아래 그림 16과 같이 지도 학습에서 측정된 F1 Score와 비지도 학습 머신러닝 모델을 적용하였을 때를 각각 비교해 보면 비지도 학습인 경우에도 지도 학습과 비교하였을 경우 대체적으로 우수한 판별 성능을 나타냄을 확인할 수 있었다. 특히 OLE VBA 매크로, OOXML 구조 분석 및 VirusTotal 악성코드 기반 정적/동적 분석 기법을 모두 적용하였을 경우에 False Positive Rate가 안정적으로 수렴하는 것을 확인할 수 있었다.



[Fig. 16] Proformance Analysis : Unsupervised Learning

5. 결론

본 연구에서는 최근 급증하고 있는 MS Office 계열 디지털 파일 내에 매크로 악성 코드 등에 의한 감염 및 피해를 최소화하기 위해 머신러닝 기법을 적용하여 자동으로 검출/판별할 수 있는 시스템을 설계 및 구현하였다. MS Office 계열 디지털 파일에 대한 위변조 및 악성코드 포함 여부를 자동 판별하기 위해서 총 9개의 지도/비지도 학습 모델을 적용하여 자동 판별 성능을 비교 분석하였다. 실험 결과 MS Office 계열 매크로 악성 파일에 대해 기존 기법[13][14] 대비 (1) 생성된 로그 파일을 토대로 정적 분석하였을 경우 평균 78.4%의 확률로 검출하였으며, (2) 파일 확장자 정보를 추가로 포함하여 분석하였을 경우 평균 89.5%의 확률로 지도/비지도 학습 기반 판별 과정을 수행하는 것을 확인할 수 있었으며, (3) Neural Network 기반 비지도 학습 모델인 경우에도 기존 8개의 지도 학습 기반 모델과 유사하게 평균 88.4%의 검출 성능을 제공함을 확인할 수 있었다. 앞으로 본 연구에서 제시한 머신러닝 기반 검출 시스템을 더욱 발전시켜 대단위 CTI(Cyber Threat Intelligent) 시스템 환경에서 악성 파일에 대한 자동 검출 및 사이버 침해공격에 능동적으로 대응할 수 있는 시스템을 개발하고자 한다.

REFERENCES

[1] S. Rafique, M. R. Ali, and M. A. Mirza, "Macro Malware: Detection and Mitigation Techniques," Journal of Cyber Security, Vol.12, No.3, pp.45-60, 2021.

[2] S. D. l. Santos and J. Torres, "Macro malware detection using machine learning techniques - a new approach," in Proceedings of the 3rd International Conference on Information SystemsSecurity and Privacy - Volume 1: ICISSP, INSTICC. SciTePress, 2017, pp.295-302.

[3] P. Sung, M. Kim, and H. Lee, "Behavioral Analysis of Macro-based Malware," IEEE Transactions on Information Security and Forensics, Vol.17, No.2, pp.299-312, 2022.

[4] A. Patel, "Office Macro Malware: How Attackers Exploit VBA for Cybercrime," Cyber Threat Research Journal, Vol.8, No.1, pp.11-25, 2020.

[5] J. Saxe and K. Berlin, "Malware Data Science: Attack Detection and Attribution", No Starch Press, 2018.

[6] T. Schmid, "Machine Learning for Malware Detection," Proceedings of the IEEE International Conference on Machine Learning and Security (ICMLS), 2020.

[7] S. Zeltser, "Understanding Static and Dynamic Malware Analysis Techniques," SANS Institute Research Paper, 2019.

[8] C. Szegedy et al., "Intrusion Detection Using Machine Learning Techniques," ACM Conference on Cybersecurity and AI, 2019.

[9] P. Singh, "Detection of Malicious OOXML Documents Using Domain Specific Features", Master's thesis, Indian Institute of Information Technology and Management, 2017.

[10] Z. Wang, J. Wang, "Applications of Machine Learning in Public Security Informatin and Resource Management", Hindawi Scientific Programming, Vol.2021, Article ID 4734187, 2021.

[11] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Machine learning models for secure data analytics: a taxonomy and threat model," Computer Communications, Vol.153, pp.406-440, 2020.

[12] A. Cohen, N. Nissim, L. Rokach, and Y. Elovici, "Sfem: Structural feature extraction methodology for the detection of malicious office documents using machine learning methods," ExpertSystems with Applications, Vol.63, pp.324-343, 2016.

[13] H. S. Lee, H.-W. Lee, "Forgery Detection Mechanism with Abnormal Structure Analysis on Office Open XML based MS-Word File," IJASC, Vol.8, No.4, 2019.

[14] S. Na and H.-W. Lee, "Implementation of Malicious Data Analysis and Detection System Hidden in the Slack Space of Corrupted OOXML-based MS-Office Digital Files", Advanced and Applied Convergence Letters AACL 21 (9th International Joint Conference on Convergence, IJCC2023), pp.97-103, 2023.

[15] A. Catsiglione, B. D'Alessio, A. D. Santis, "Hiding Information into OOXML Documents: New Steganographic Perspectives", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol.2, No.4, pp.59-83, 2011.

[16] S. Kim, S. Hong, J. Oh, and H. Lee, "Obfuscated vba macro detection using machine learning," in 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), pp.490-501, June 2018.

[17] B. Mahesh, "Machine Learning Algorithms - A Review", International Journal of Science and Research, Vol.9, No.1, 2020.

[18] W. Richert, L. P. Coelho, "Building Machine Learning Systems with Python", Packt Publishing Ltd., ISBN 978-1-78216-140-0

[19] VirusTotal, https://www.virustotal.com/.

[20] Python, https://www.python.org/.

[21] scikit-learn, https://scikit-learn.org/.

[22] MalwareBazaar, https://bazaar.abuse.ch/.

[23] Digital Corpora, https://digitalcorpora.org/.

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