KIPS Trans. Softw. and Data Eng.
Vol.10, No.3 pp.91~98
ISSN: 2287-5905 (Print), ISSN: 2734-0503 (Online)

https://doi.org/10.3745/KTSDE.2021.10.3.91

A Comparative Study of Machine Learning Algorithms Using LID-DS DataSet

Park DaeKyeong[†] · Ryu KyungJoon[††] · Shin DongIl[†††] · Shin DongKyoo[†††] · Park JeongChan[††††] · Kim JinGoog[†††††]

ABSTRACT

Today's information and communication technology is rapidly developing, the security of IT infrastructure is becoming more important, and at the same time, cyber attacks of various forms are becoming more advanced and sophisticated like intelligent persistent attacks (Advanced Persistent Threat). Early defense or prediction of increasingly sophisticated cyber attacks is extremely important, and in many cases, the analysis of network-based intrusion detection systems (NIDS) related data alone cannot prevent rapidly changing cyber attacks. Therefore, we are currently using data generated by intrusion detection systems to protect against cyber attacks described above through Host-based Intrusion Detection System (HIDS) data analysis. In this paper, we conducted a comparative study on machine learning algorithms using LID-DS (Leipzig Intrusion Detection-Data Set) host-based intrusion detection data including thread information, metadata, and buffer data missing from previously used data sets. The algorithms used were Decision Tree, Naive Bayes, MLP (Multi-Layer Perceptron), Logistic Regression, LSTM (Long Short-Term Memory model), and RNN (Recurrent Neural Network). Accuracy, accuracy, recall, F1-Score indicators and error rates were measured for evaluation. As a result, the LSTM algorithm had the highest accuracy.

Keywords : Machine Learning, HIDS, NIDS, LID-DS

LID-DS 데이터 세트를 사용한 기계학습 알고리즘 비교 연구

박 대 경[†] · 류 경 준[††] · 신 동 일[†††] · 신 동 규[†††] · 박 정 찬[††††] · 김 진 국[†††††]

요 약

오늘날 정보통신 기술이 급격하게 발달하면서 IT 인프라에서 보안의 중요성이 높아졌고 동시에 지능형 지속 공격(Advanced Persistent Threat)처럼 고도화되고 다양한 형태의 사이버 공격이 증가하고 있다. 점점 더 고도화되는 사이버 공격을 조기에 방어하거나 예측하는 것은 매우 중요한 사안으로, NIDS(Network-based Intrusion Detection System) 관련 데이터 분석만으로는 빠르게 변형하는 사이버 공격을 방어하지 못하는 경우가 많이 보고되고 있다. 따라서 현재는 HIDS(Host-based Intrusion Detection System) 데이터 분석을 통해서 위와 같은 사이버 공격을 방어하는데 침입 탐지 시스템에서 생성된 데이터를 이용하고 있다. 본 논문에서는 기존에 사용되었던 데이터 세트에서 결여된 스레드 정보, 메타 데이터 및 버퍼 데이터를 포함한 LID-DS(Leipzig Intrusion Detection-Data Set) 호스트 기반 침입 탐지 데이터를 이용하여 기계학습 알고리즘에 관한 비교 연구를 진행했다. 사용한 알고리즘은 Decision Tree, Naive Bayes, MLP(Multi-Layer Perceptron), Logistic Regression, LSTM(Long Short-Term Memory model), RNN(Recurrent Neural Network)을 사용했다. 평가를 위해 Accuracy, Precision, Recall, F1-Score 지표와 오류율을 측정했다. 그 결과 LSTM 알고리즘의 정확성이 가장 높았다.

키워드 : 기계학습, 호스트 기반 침입 탐지 시스템, 네트워크 기반 침입 탐지 시스템, LID-DS

※ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다 (UD1 90016ED).
※ 이 논문은 2020년 한국정보처리학회 춘계학술발표대회에서 "호스트 기반 침입 탐지 데이터 분석 비교"의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 세종대학교 컴퓨터공학과 지능형드론 융합전공 석사과정
†† 준 회 원 : 세종대학교 컴퓨터공학과 석사
††† 종신회원 : 세종대학교 컴퓨터공학과 지능형드론 융합전공 교수
†††† 비 회 원 : 국방과학연구소 책임연구원
††††† 비 회 원 : 국방과학연구소 선임연구원
Manuscript Received : July 22, 2020
First Revision : August 26, 2020
Accepted : August 27, 2020
* Corresponding Author : Shin DongIl(dshin@sejong.ac.kr)

1. 서 론

오늘날 정보통신 기술이 급격하게 발달하면서 IT 인프라에서 보안의 중요성이 높아졌고 동시에 사이버 공격은 지능형 지속 공격처럼 고도화되고 지능적으로 다양해지고 있다. 점점 더 고도화되는 사이버 공격을 방어하는 것은 매우 중요한 사안인데, IDS(Intrusion Detection System) 기술의 발달 속도가 빠르게 변형되는 사이버 공격을 완벽하게 탐지하

지 못한다. 따라서 현재는 HIDS 데이터 분석을 통해서 위와 같은 사이버 공격을 방어하는데 침입 탐지 시스템에서 생성된 데이터를 이용하고 있다[1]. 침입 탐지 시스템은 네트워크 기반인 NIDS, 호스트 기반인 HIDS 두 가지 방식으로 나눌 수 있다. 네트워크 기반 침입 탐지 시스템과 달리 호스트 기반 침입 탐지 시스템은 시스템 내부와 외부를 전체적으로 모니터링을 해야 하는 어려움이 있다. 그에 따라, 연구가 많이 부족하고 침입 탐지 시스템은 새로운 사이버 공격 및 내부 사이버 공격에 대한 방어 대책이 미흡하고 오경보가 증가하는 문제점이 있다. 호스트 기반 침입 탐지 시스템 방식은 오용탐지와 이상 탐지 2가지 방법으로 나눌 수 있다[2]. 오용탐지 방법은 시그니처 기반으로 사이버 공격을 탐지하기 때문에 기존의 사이버 공격을 탐지하는 것은 효과적이지만 반면에 새로운 사이버 공격에 대한 탐지는 부적합하다. 이상 탐지 방법은 오용탐지 방법과 반대로 정상적인 동작 및 행위로 정의된 상태가 아닌 것에 대한 모든 상황을 이상 행위로 판단하여 탐지하게 된다. 즉 오용탐지 방법과 달리 이상 탐지 방법은 제로 데이 공격에 대한 탐지에는 적합하지만, 정상 동작 및 이상 행위를 판단할 수 있는 많은 데이터가 요구되거나 데이터가 너무 부족하여 기계학습에 적용하기에는 어려움이 있다[3].

시그니처 기반 탐지 기술에서 IDS는 공격 시그니처가 포함된 데이터베이스를 사용하여 데이터의 침입을 탐지하므로 탐지율이 우수하다[4]. 하지만 탐지 체계의 문제점은 새로운 사이버 공격에 대한 데이터가 없어서 새로운 사이버 공격을 탐지할 수 없다[5]. 최근 호스트 기반 침입 탐지 연구는 기계학습 기술을 사용하여 변칙에 기반한 탐지 기술은 비정상적인 행동을 찾아 새로운 공격을 탐지하고 이상을 탐지하기 위해 기계학습 알고리즘이 사용되고 있다[6,7].

본 논문에서는 LID-DS 데이터 세트를 사용하여 기계학습 알고리즘에 관한 비교 연구를 진행한다.

실험에 사용한 알고리즘은 크게 데이터의 시퀀스(sequence)를 고려하지 아니하고 학습하는 알고리즘 4개와 시퀀스를 고려하여 학습하는 알고리즘 2개로 실험하였다. LID-DS 데이터 세트에서 가장 특징적인 부분이라고 할 수 있는 공격 유형에 따른 연속적인 시스템 콜을 어떠한 기계학습 알고리즘이 가장 잘 찾아낼 수 있는지에 대한 최종 결과를 서술하였다.

2. 관련 연구

침입 탐지 시스템은 공격 패턴에 대한 매칭을 이용하여 위협을 탐지하고 차단하는 시스템이다[8,9]. 이 시스템은 룰(rule) 기반으로 침입을 탐지하기 때문에 상대적으로 오경보가 높은 편이다. 이전 침입 탐지 연구에서는 KDD 및 UNM 데이터의 공격 패턴을 다양한 기계학습 기술로 분석하고 오경보를 개선한 연구가 대부분이다.

KDD 및 UNM 데이터 세트는 공개적으로 사용이 가능한 데이터이며 침입 탐지 시스템의 검증 기초가 되고 성능 테스트의 기준이 되어 많은 연구가 진행되고 있다. 하지만 일부 네트워크 정보 중에서 시스템 호출을 통해 프로세스와 커널 간에 전달되는 데이터 형식으로 호스트에서 수집된 추적을 제공하는데 기존의 데이터들은 더는 현대적인 특징을 가지고 있지 않기 때문에 최신 컴퓨터 시스템의 다양한 특징들과 사이버 공격 특징들이 반영되지 않아 새로운 데이터가 필요하다[10-12].

여러 프로세스 활동을 갖는 사이버 공격은 프로세스의 활동을 특정 프로그램이 아닌 여러 프로그램에서 무작위로 수집해야 한다. 시스템 호출 기반으로 구성된 ADFA 데이터 세트는 정상 데이터와 비정상 데이터를 분리하는 기준이 명확하지 않다는 문제점이 있다. 문제를 해결하기 위해 ADFA 데이터 세트에 전통적인 기계학습 알고리즘인 SVM(Support Vector Machine)을 적용 후, 중복된 엔트리는 짧은 시퀀스를 통해 제거하여 정상 데이터와 비정상 데이터 사이의 기준을 명확하게 구분했다. 또한, 시스템 호출 기반으로 구성된 호스트 기반 침입 탐지 시스템 방식을 평가하기 위한 여러 시스템 특징을 반영하고 있으며 리눅스와 윈도우 운영체제의 사이버 공격 패턴을 포함하고 있어 해당 데이터 세트를 이용한 여러 연구가 진행됐다[10,11,13,14].

Laskov 등[15]은 의사결정 트리, k-근접 이웃 알고리즘, 다중 계층 퍼셉트론, k-평균 클러스터링, SVM 등 여러 전통적인 기계학습 알고리즘을 침입 탐지에 적용했고, 각 알고리즘을 ROC(Receiver Operator Characteristic) 곡선을 통해 비교했다.

Kim 등[16]은 침입 탐지 시스템에서 높은 오경보율을 보이는 기존의 SVM과 k-NN 같은 기계학습 알고리즘의 문제점을 해결하기 위하여 딥러닝 알고리즘을 사용한 연구를 했다.

Kim 등[17]은 비정상 행위 기반의 호스트 침입 탐지 시스템을 설계하는 데 있어, LSTM 기반의 시스템 콜 언어 모델링(system-calllanguage-modeling) 방법을 제안하였다. 기존 방법들에서 흔하게 발생하는 높은 오탐율(false-alarm rates) 이슈를 해결하기 위해서, 저자는 새로운 앙상블(ensemble) 방법을 사용했다.

LID-DS 데이터 세트의 특징과 가장 유사한 KDD-99 데이터 세트를 이용한 Ravipati 등[18]은 8가지의 기계학습 알고리즘을 실험한 결과로 성능 평가 및 오류율 수치를 보여주었다.

본 논문에서는 기존에 사용되었던 데이터 세트에서 결여된 스레드 정보, 메타 데이터 및 버퍼 데이터를 포함하고, 데이터가 부족하여 기계학습에 적용하지 못했던 문제를 해결하기 위해서 LID-DS(Leipzig Intrusion Detection-Data Set) 데이터를 사용했다. LID-DS 데이터를 사용하여 기계학습 알고리즘에 관한 비교 연구를 통해 호스트 기반 침입 탐지 시스템이 나아갈 새로운 연구 방향을 제시한다.

3. 데이터 세트 및 실험 방법

3.1 LID-DS Dataset

본 논문에서 사용한 LID-DS 데이터 세트의 연구가 필요한 이유는 다음과 같다. 1990년대 후반, 호스트 기반 침입 탐

지 시스템을 연구하기 위해 처음 만들어진 KDD 데이터는 현재까지도 많은 연구자가 이용하고 있다. 하지만 오래된 컴퓨터 시스템의 특징과 사이버 공격 패턴으로 구성된 KDD 데이터를 이용하여 연구하기에는 적합하지 않다. 2018년 Leipzig University에서 호스트 기반 침입 탐지 시스템의 이상 탐지 연구를 위한 LID-DS 데이터 세트를 공개했다.

LID-DS 데이터 세트는 기존에 공개되었던 데이터들과 다르게 현재 공개된 데이터 세트들보다 최신 컴퓨터 시스템의 다양한 특징들과 사이버 공격 방법 및 시나리오로 구성되어 있다. LID-DS 데이터를 통해 기존에 데이터 세트들의 데이터가 부족하여 기계학습에 적용하기 어려웠던 부분을 해결하고 기계학습 방법을 이용하여 새로운 이상 행동들을 더 정확하게 탐지하여 차단할 수 있다. 이를 통해 침입 탐지 시스템의 문제점인 오경보율을 줄일 수 있다[8,11,12,19].

LID-DS 데이터 세트는 시스템 호출과 관련된 다양한 데이터가 포함되어 있으며 소프트웨어와 다양한 사이버 공격이 기록된다. LID-DS 데이터 세트는 Table 1과 같이 사이버 공격 방법과 여러 시나리오로 구성되며 시나리오를 통해 정상적인 데이터, 비정상적인 데이터를 생성하고 기록하는 프로세스를 구성할 수 있다.

Fig. 1은 Table 1의 사이버 공격 시나리오를 이용하여 데이터를 생성하는 과정이다. LID-DS 데이터 세트의 결과 시스템 호출 추적을 기록하기 위해 공격 대상은 초기 상태를 정의하고 각 공격 후 초기 상태로 되돌리기 위해 Docker 10

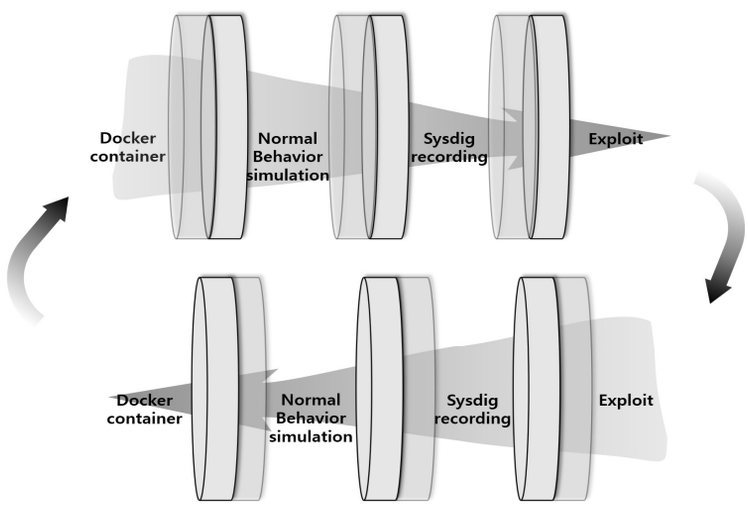

Fig. 1. Attack Simulation Procedure of LID-DS Data Set

Table 1. LID-DS Attack Method Stored in LID-DS Data

Cyber attack types	Explanation
CVE-2012-2122	Allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password.
CVE-2014-0160	Allows remote attackers to obtain sensitive information from process memory by reading private keys.
Heartbleed	
CWE-307	Improper Restriction of Excessive Authentication Attempts.
CWE-89 SQL Injection	Improper Neutralization of Special Elements used in an SQL Command.
CWE-434 (PHP, EPS)	Unrestricted Upload of File with Dangerous Type.
CVE-2014-3120	Allows remote attackers to execute arbitrary MVEL expressions and Java code via the source parameter to search.
CVE-2015-1427	Allows remote attackers to bypass the sandbox protection mechanism and execute arbitrary shell commands via a crafted script.
CVE-2017-7529	Vulnerable to integer overflow vulnerability range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
CVE-2018-3760	Specially crafted requests can be used to access files that exists on the filesystem that is outside an application's root directory.
CVE-2019-5418	Specially crafted accept headers can cause contents of arbitrary files on the target system's filesystem to be exposed.
Zip slip	Arbitrary file overwrite vulnerability that triggers from a directory traversal attack.

Table 2. LID-DS Saved Data Format

8 13:16:35.219910910 1 33 apache2 21486 〈 epoll_wait res=1
9 13:16:35.219919842 1 33 apache2 21486 〉 accept flags=0

컨테이너 가상화 소프트웨어 내에서 실행된다. 기록을 위해 LID-DS 프레임 워크를 이용하여 먼저 공격 대상을 호스팅하는 Docker 컨테이너를 시작한다. 그다음 시나리오에 따라 초기화 작업이 실행되며 정상 동작의 시뮬레이션이 시작된다. 그 후 공격 대상 소프트웨어의 시작 효과를 기록하지 않기 위해서 Sysdig가 활성화되기 전에 짧은 시간 동안 기다린다. 공격 동작을 기록하는 경우 임의의 시간이 지나면 공격이 시작되는데 원하는 시간 동안 녹화가 실행된 후 제어 스크립트에 의해 녹화가 중지된다. 또한, 정상적인 동작 및 사용된 Docker 컨테이너의 시뮬레이션을 중지하고 제거한다.

ADFA 데이터 세트는 일련의 시스템 호출 ID만 포함하고 현대의 사이버 공격 패턴을 포함하지 않기 때문에 ADFA 데이터 세트를 이용하여 이상 탐지 테스트를 하기에는 적절하지 않다[20].

LID-DS의 데이터 파일 자체의 형식은 Table 2와 같다. ADFA와 다르게 LID-DS 데이터에는 시스템 호출의 인수, 반환 값, 고정밀 타임 스탬프, 해당 프로세스 이름 및 데이터 버퍼의 내용이 포함되어 있다[21].

3.2 데이터 전처리

LID-DS 데이터 세트는 Table 3과 같이 10개의 사이버 공격 방법에 따라 데이터가 분류되어 있으며 각 사이버 공격 방법은 7개의 Feature로 구성되어 있다. 데이터를 기계학습 알고리즘에 사용하기 위해 원본 크기가 큰 일부 데이터를 제외하고 CSV 형식으로 구성했다.

Fig. 2의 3.2 파트와같이 모든 데이터에 대해 Argument Feature와 결측값은 삭제하였고 event_time Feature는 콜론(:)을 제거했다. event_direction과 event_type은 LabelEncoder

Table 3. Data Type and Attack Type

Feature	event_num
	event_time
	cpu
	user_uid
	process
	process_id
	event_direction
	event_type
Attack Type	Bruteforce
	CVE-2012-2122
	CVE-2014-0160
	CVE-2017-7529
	CVE-2018-3760
	CVE-2019-5418
	EPS_CWE-434
	PHP_CWE-434
	SQL_Injection_CWE-89
	ZipSlip

를 사용했다.

Process 카테고리는 총 16개로 구성되어 있으며 각 공격 방법마다 Process의 개수는 다르다. 그에 따라, 각 사이버 공격 방법에 사용된 Process들은 하나의 Process로 통합했다. 그 결과 총 10개의 Process로 구성된 라벨들은 LabelEncoder를 사용하여 각 Process에 라벨을 붙여 사용했다.

OneHotEncoder를 사용하지 않은 이유는 event_type의 카테고리가 99개로 구성되어 있기 때문이다. 즉 차원의 저주(Curse of Dimensionality)가 발생할 수 있는 위험이 있으므로 LabelEncoder만을 사용했다. 정규화(Normalization)는 데이터가 가진 Feature의 스케일이 심하게 차이가 나는 문제를 해결하기 위해서 최소-최대 정규화(Min-Max Normalization)를 사용하여 Feature에 대해 각각의 최솟값 0, 최댓값 1로 다른 값들은 0과 1 사이의 값으로 변환했다.

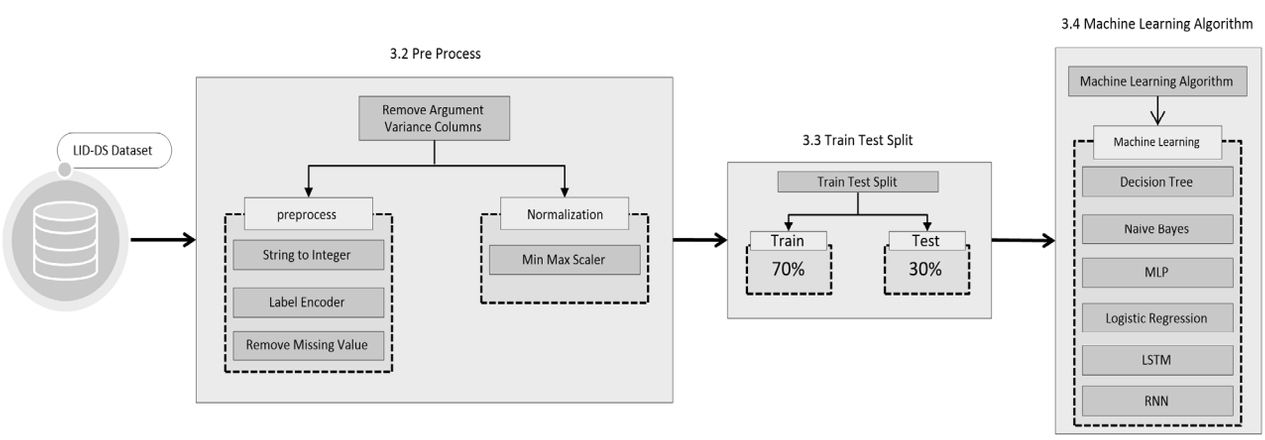

Fig. 2. Proposed LID-DS Data Set Performance Comparison Model Structure

3.3 Train Test Split

훈련 데이터는 10개의 사이버 공격 방법 데이터를 하나의 CSV 파일로 합쳐서 사용했다. 기계학습에 사용할 훈련 데이터와 테스트 데이터는 train_test_split 모듈을 사용하여 일반적으로 많이 사용하는 8:2 비율로 나누어 사용했다. 하지만 훈련 데이터를 학습시킨 후 테스트 데이터에 모델을 적용했지만, 과적합(Overfitting) 현상을 발견했다. 과적합이란 모델이 너무 과적합 되도록 학습한 나머지, 예측률이 현저히 떨어지는 현상을 말한다. 과적합을 방지하기 위하여 다른 비율로 나누어진 데이터를 포함하여 Cross-validation으로 모델평가를 진행했다. 그 결과 7:3 비율로 나누어진 데이터 세트의 모델 성능이 가장 높았다. 따라서 본 논문에서는 Fig. 2의 3.3 파트와같이 훈련 데이터와 테스트 데이터를 7:3 비율로 나누어 사용했다.

3.4 Machine Learning Algorithm

Fig. 2의 3.4 파트와 같이 실험에 사용된 알고리즘은 Decision Tree, Naive Bayes, MLP, Logistic Regression, LSTM, RNN의 6가지 기계학습 알고리즘들이다.

4. 실 험

4.1 실험 설정

실험에 사용된 알고리즘의 Hyper Parameter는 Table 4와 같다.

실험은 LID-DS의 앞서 설명 방법으로 전처리 과정을 수행한 사이버 공격 데이터를 사용했다. LabelEncoder를 사용하여 라벨을 부여한 Process 카테고리 10개의 데이터를 통하여 LID-DS 데이터 세트의 침입 탐지 정확성을 비교하는 실험을 진행했다.

학습된 모델의 성능 평가는 Precision, Recall, F1 Score를 사용했다. 그 이유는 데이터에 대해서 Accuracy만을 가지고 평가하는 것은 부적합하기 때문이다.

Table 4. Hyper Parameter used in the Algorithm

Algorithm	Hyper Parameter
Decision Tree	criterion='entropy', max_depth=3, random_state=0
Naive Bayes	default
MLP	max_iter=1000, alpha=1, random_state=0
Logistic Regression	max_iter=500, solver='liblinear'
LSTM	Activation='softmax', optimizer=adam, loss='categorical_crossentropy'
RNN	

또한, 보안에서 중요한 문제점인 오류율을 확인하기 위해 FAR(False Alarm Rate) 및 ERR(Error Rate)의 수치를 확인했다.

4.2 실험 결과

본 논문에서는 학습된 모델의 성능 평가 결과는 Table 5, 7과 같으며 각 모델의 정확성 및 오류율은 Table 6, 8과 같다. Fig. 3은 Decision Tree, Naive Bayes, MLP, Logistic Regression, LSTM, RNN 알고리즘을 이용하여 LID-DS 데이터 세트의 침입 탐지를 예측한 정확성이다.

Fig. 4는 Decision Tree, Naive Bayes, MLP, Logistic Regression, LSTM, RNN 알고리즘을 이용하여 LID-DS 데이터 세트의 오류율이다.

실험 결과로 아래의 표에서 나타내듯이 시퀀스를 고려하지 않는 학습 알고리즘 4개 중에서 가장 우수한 결과를 보여준 것은 Naive Bayes 알고리즘이었다. 이 경우에는 공격 데이터의 특징들이 각각 독립적으로 작용함을 알 수 있다. 즉, 각각

Table 5. Performance Evaluation of Learning Algorithms without Considering Sequences

Algorithm	Precision	Recall	F1-Score
Naive Bayes	81%	82%	81%
Decision Tree	81%	80%	78%
Logistic Regression	72%	75%	72%
MLP	69%	68%	65%

Table 6. Accuracy and False Alarm Rate and Error Rate of Learning Algorithms without Considering Sequences

Algorithm	Accuracy	FAR	ERR
Naive Bayes	82%	1.9%	1.8%
Decision Tree	79%	2.4%	2.3%
Logistic Regression	75%	3%	2.8%
MLP	68%	3.9%	3.8%

Table 7. Performance Evaluation of Learning Algorithms Considering Sequence

Algorithm	Precision	Recall	F1-Score
LSTM	91%	88%	88%
RNN	88%	85%	86%

Table 8. Accuracy and False Alarm Rate and Error Rate of Learning Algorithms Considering Sequences

Algorithm	Accuracy	FAR	ERR
LSTM	88%	1.5%	1.4%
RNN	85%	1.8%	1.8%

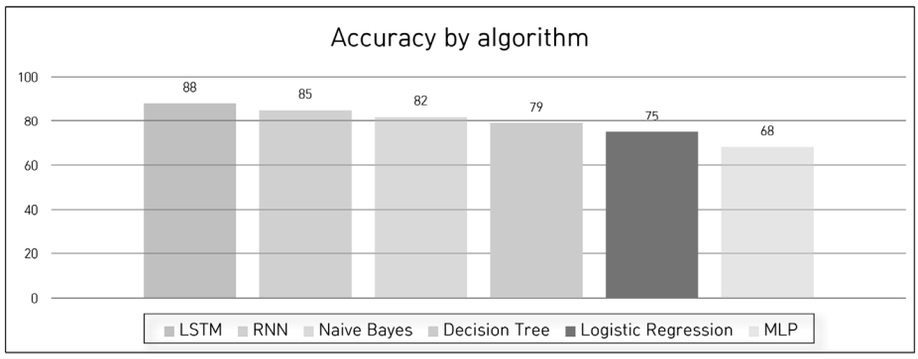

Fig. 3. Cyber Attack Data Prediction Accuracy by Algorithm

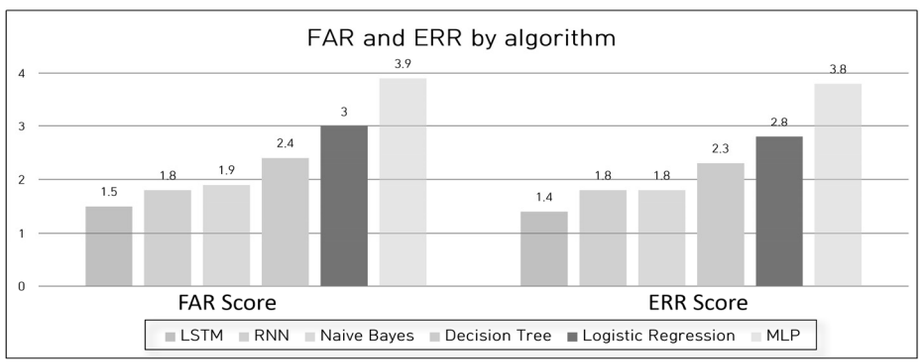

Fig. 4. FAR and ERR of Supervised Machine Learning Algorithms on LID-DS

의 특징의 독립성을 가장 정확하게 학습하고 판단하는데 최적화된 Naive Bayes 알고리즘의 우수한 성능이 이를 증명한다.

본 연구에서 사용한 LID-DS의 데이터는 연속적인 시스템 호출을 공격 유형과 연관시킨 데이터이므로, 실험 결과 시퀀스를 고려한 학습 알고리즘이 전반적으로 우월한 성능을 보여주었다.

5. 결론 및 추후 연구

본 논문에서 사용한 LID-DS 데이터 세트의 알고리즘 성능 분석 실험 결과로 LSTM 알고리즘이 가장 우수한 성능을 보여주었다. 특히 LSTM의 경우에는 Naive Bayes와 비교하여 정확도는 12.5%가 증가하였으며, 오류율은 22.2%가 향상되었다. 따라서, 연속적으로 기록된 데이터의 패턴을 알아내는데 특화된 LSTM 알고리즘이 가장 우수한 성능을 보여주었다. LID-DS 데이터의 경우 사이버 공격 데이터를 직접 만들 수 있어서 데이터의 양이 많으므로 기존에 데이터가 부족하여 기계학습을 진행하지 못하는 부분을 해결했다.

LID-DS 데이터에 더욱 효과적인 전처리 방법을 이용하여 실험을 진행한다면 앞서 나온 결과보다 높은 정확성을 나타낼 것이다. LID-DS 데이터 세트는 기존에 데이터 세트에서 부족 하였던 특징을 보완한 사이버 공격 데이터라는 점과 사이버 공격 데이터를 직접 생성할 수 있다는 점에서 관련 연구가 많이 진행되어야 할 것이다.

추후 연구로는 LID-DS 데이터를 활용하여 다양한 사이버 공격에 대한 침입 탐지하는 연구를 진행할 것이다. LID-DS 데이터에 적합한 전처리 방법과 각 알고리즘에 사용하는 Hyper Parameter 값을 최적화하여 정확성을 높이고 LID-DS 데이터 세트와 같은 최근에 생성되고 있는 데이터들을 활용하여 호스트 기반 침입 탐지 시스템의 새로운 사이버 공격 및 내부 사이버 공격에 대한 침입 탐지 정확성을 더욱 높이는 연구를 진행할 것이다.

References

[1] Y. Su, M. Li, C. Tang, and R. Shen, “A framework of apt detection based on dynamic analysis,” *2015 4th National Conference on Electrical, Electronics and Computer Engineering*, Atlantis Press, 2015.

[2] Y. G. Choi and S. S. Park, “Reinforcement Mining Method for Anomaly Detection and Misuse Detection using Post‐processing and Training Method,” *Proceedings of the Korean Information Science Society Conference*, pp.238-240, 2006.

[3] S. O. Choi and W. N. Kim, "Control system intrusion detection system technology research trend," *Review of Korea Institute of Information Security and Cryptology*, Vol.24, No.5, pp.7-14, 2014.

[4] J. JP. Tsai and S. Y. Philip, "Machine learning in cyber trust: Security privacy and reliability," Springer Science & Business Media, 2009.

[5] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," *Applied Soft Computing*, Vol.10, No.1, pp.1-35, 2010.

[6] M. S. Iftikhar and M. R. Fraz, "A Survey on Application of Swarm Intelligence in Network Security," *Transactions on Machine Learning and Artificial Intelligence*, Vol.1, No.1, pp.1-15, 2013.

[7] T. Mehmood and HBM. Rais, "Machine learning algorithms in context of intrusion detection," *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)*, Kuala Lumpur, pp.369-373, 2016.

[8] L. N. Tidjon, M. Frappier, and A. Mammar, "Intrusion detection systems: A cross-domain overview," *IEEE Communications Surveys & Tutorials*, Vol.21, No.4, pp.3639-3681, 2019.

[9] H. Kwon, Y. C. Kim, H. S. Yoon, and D. S. Choi, "Optimal cluster expansion-based intrusion tolerant system to prevent denial of service attacks," *Applied Sciences*, Vol.7, No.11, pp.1186, 2017.

[10] T. Mouttaqi, T. Rachidi, and N. Assem, "Re-evaluation of combined Markov-Bayes models for host intrusion detection on the ADFA dataset," *2017 Intelligent Systems Conference (IntelliSys)*, IEEE, 2017.

[11] O. Yavanoglu and M. Aydos, "A review on cyber security datasets for machine learning algorithms," *2017 IEEE International Conference on Big Data (Big Data)*, Boston, MA, pp.2186-2193, 2017.

[12] M. Pendleton and S. Xu, "A dataset generator for next generation system call host intrusion detection systems," M*ILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017.

[13] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns," *IEEE Transactions on Computers*, Vol.63, No.4, pp.807-819, 2013.

[14] M. Xie and J. Hu, "Evaluating host-based anomaly detection systems: A preliminary analysis of adfa-ld," *Image and Signal Processing (CISP), 2013 6th International Congress on*. Vol.3. IEEE, 2013.

[15] P. Laskov, P. Düsse, C. Schäfer, and K. Rieck, "Learning intrusion detection: supervised or unsupervised?," *International Conference on Image Analysis and Processing*. Springer, Berlin, Heidelberg, 2005.

[16] J. H. Kim and H. W. Kim, "An effective intrusion detection classifier using long short-term memory with gradient descent optimization," *2017 International Conference on Platform Technology and Service (PlatCon)*. IEEE, 2017.

[17] G. W. Kim, H. Y. Yi, J. H. Lee, Y. H. Paek, and S. R. Yoon, "LSTM-based system-call language modeling and robust ensemble method for designing host-based intrusion detection systems," arXiv preprint arXiv:1611.01726 (2016).

[18] R. D. Ravipati and M. Abualkibash, "Intrusion Detection System Classification Using Different Machine Learning Algorithms on KDD-99 and NSL-KDD Datasets-A Review Paper," *International Journal of Computer Science & Information Technology (IJCSIT)*, Vol.11, 2019.

[19] M. M. Röhling, M. Grimmer, D. Kreubel, J. Hoffmann, and B. Franczyk, "Standardized container virtualization approach for collecting host intrusion detection data," *2019 Federated Conference on Computer Science and Information Systems (FedCSIS)*, IEEE, 2019.

[20] A. Khraisat, I. Gondal, P. Vamplew and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, Vol.2, No.1, pp.1-22, 2019.

[21] M. Grimmer, MM. Röhling, D. Kreubel and S. Ganz, "A modern and sophisticated host based intrusion detection data set," *IT-Sicherheit als Voraussetzung Für Eine Erfolgreiche Digitalisierung*, pp.135-145, 2019.

박 대 경

https://orcid.org/0000-0003-1195-9017
e-mail : dkpark@sju.ac.kr
2020년 ~ 현 재 세종대학교 컴퓨터공학과 지능형드론 융합전공 석사과정
관심분야 : 디지털 포렌식, 기계학습, 정보보안

류 경 준

https://orcid.org/0000-0002-0714-2779
e-mail : rkj6663@sju.ac.kr
2021년 세종대학교 컴퓨터공학과(석사)
관심분야 : 정보보안, 기계학습, 데이터 마이닝

신 동 일

https://orcid.org/0000-0002-8621-715X
e-mail : dshin@sejong.ac.kr
1988년 연세대학교 컴퓨터과학과(학사)
1993년 Washington State University 컴퓨터과학과(석사)
1997년 North Texas University 컴퓨터과학과(박사)
1998년 ~ 현 재 세종대학교 컴퓨터공학과 지능형드론 융합전공 교수
관심분야 : 정보보안, 기계학습, 데이터 마이닝, 생체신호 데이터처리

신 동 규

https://orcid.org/0000-0002-2665-3339
e-mail : shindk@sejong.ac.kr
1986년 서울대학교 계산통계학과(학사)
1992년 Illinois Institute of Technology 컴퓨터과학과(석사)
1997년 Texas A&M University 컴퓨터과학과(박사)
1998년 ~ 현 재 세종대학교 컴퓨터공학과 지능형드론 융합전공 교수
관심분야 : 정보보안, 기계학습, 유비쿼터스 컴퓨팅, 생체신호 데이터처리

박 정 찬

https://orcid.org/0000-0001-6192-0685
e-mail : jcpark@add.re.kr
1996년 광운대학교 컴퓨터공학과(석사)
2015년 고려대학교 사이버국방학과 (박사수료)
1996년 ~ 현 재 국방과학연구소 책임연구원
관심분야 : 디지털 포렌식, 정보보안

김 진 국

https://orcid.org/0000-0001-8508-5784
e-mail : jingoog78@gmail.com
2006년 KAIST 전기전자공학과(석사)
2010년 KAIST 전기전자공학과(박사)
2010년 ~ 2011년 SKB/SKT 네트워크 부문 매니저
2011년 ~ 현 재 국방과학연구소 선임연구원
관심분야 : 무선 통신, 임베디드 시스템 보안