논문 22-47-01-08 The Journal of Korean Institute of Communications and Information Sciences '22-01 Vol.47 No.01
https://doi.org/10.7840/kics.2022.47.1.58

로그인 로그를 활용한 이상 탐지 성능 향상을 위한 기능화 방법

임 선 영◆, 김 상 수°, 심 신 우*, 구 성 모**, 조 병 모*, 김 광 수*, 김 태 규*

A Featurization Method to Improve Anomaly Detection Performance Using Login Logs

Sun-Young Im◆, Sang-soo Kim°, Shinwoo Shim*, Sung-mo Koo**,
Byoungmo Cho*, Kwangsoo Kim*, Taekyu Kim*

요 약

이상 로그인 탐지는 기업들의 데이터를 보호하고 안전한 시스템을 구축하기 위한 필수 요소이다. 공격자가 올바른 암호를 입력하고 성공적으로 서버에 로그인을 하면 시스템에서 유의미한 정보를 찾기 시작한다. 이때 계정의 이상 로그인 행위를 탐지하여 해당 계정의 권한을 제한하거나 취소시키면 시스템의 손실을 감소시킬 수 있다. 본 연구에서는 로그인 로그를 활용하여 이상 로그인 탐지 성능 향상을 위한 데이터 전처리 방법을 연구하였다. 출발지 사용자, 출발지 도메인, 출발지 컴퓨터, 도착지 사용자, 도착지 도메인, 도착지 컴퓨터, 인증 유형, 로그온 유형, 로그온/로그오프 상태, 로그인 성공/실패 여부를 기준으로 동일한 이벤트가 반복되는 횟수를 산출하여 각 이벤트마다 빈도수(frequency) 헤더를 생성하였다. 그리고 출발지 사용자, 도착지 사용자, 인증 유형, 로그온 유형, 빈도수 헤더의 데이터에 대해 원-핫 인코딩을 수행하였다. 인코딩을 수행한 후 6개의 이상 탐지 알고리즘(ABOD, HBOS, IForest, KNN, LOF, OCSVM)을 적용하여 제안 방법 적용 전과 후를 비교하여 AUC가 43% 이상(최대 50%), TPR이 86% 이상(최대 93%) 성능이 향상된 것을 확인할 수 있었다.

Key Words : Login Log, Anomaly Detection, Los Alamos, PyOD, ABOD, HBOS, IForest, KNN, LOF, OCSVM

ABSTRACT

Anomaly login detection is an essential element for protecting corporate data and building a secure system. When an attacker enters the correct password and successfully logs in to the server, the attacker begins looking for meaningful information in the system. At this time, by detecting anomaly login behavior of the account and restricting or revoking the privileges of the account, system loss can be reduced. In this study, a data preprocessing method was studied to improve the anomaly login detection performance by using the login log. We generated frequency headers for each event by calculating the number of times the same event repeats based on the source user, source domain, source computer, destination user, destination domain, destination computer, authentication type, logon type, authentication_orientation, and login success/failure. And one-hot encoding was performed on the data of the source user, destination user, authentication type, logon type, and

◆ First Author : LIG Nex1 Co., sunyoung.im@lignex1.com, 정회원
° Corresponding Author : Agency for Defense Development, wisdory@naver.com, 정회원
* LIG Nex1 Co., {shimshinwoo, byoungmo.cho, kwangsoo.kim, taekyu.kim}@lignex1.com
** Agency for Defense Development, smkoo12@add.re.kr, 정회원
논문번호 : 202108-199-B-RN, Received August 12, 2021; Revised October 6, 2021; Accepted October 10, 2021

frequency header. After encoding, 6 anomaly detection algorithms (ABOD, HBOS, IForest, KNN, LOF, OCSVM) were applied to compare before and after applying the proposed method, and the AUC was 43% or more (up to 50%), and the TPR was 86% or more. (up to 93%) performance was improved.

Ⅰ. 서 론

이상 로그인 탐지는 기업들의 데이터를 보호하고 안전한 시스템을 구축하기 위한 필수 요소이다. 공격자가 올바른 암호를 입력하고 성공적으로 서버에 로그인을 하면 시스템에서 대상 데이터 또는 민감한 파일의 위치를 찾기 시작 한다[1]. 이때 계정의 비정상적 로그인 행위를 탐지하여 해당 계정의 권한을 제한하거나 취소시키면 시스템의 손실을 감소시킬 수 있다[2]. 이처럼 이상 로그인을 탐지할 수 있다면 데이터가 유출되기 전에 공격자를 식별하여 조치를 취하고 데이터를 보호할 수 있다.

본 연구에서는 일반적인 컴퓨팅 환경에서 수집할 수 있는 로그인 로그를 가지고 이상 탐지를 효과적으로 수행하기 위한 데이터 전처리 방법을 연구하였다. 이를 위해 공개 데이터 셋인 로스 알라모스 연구소(Los Alamos National Laboratory)의 “Comprehensive, Multi-Source Cybersecurity Events[3]” 데이터 셋을 사용하였다. 논문의 구성은 다음과 같다. 2장에서는 관련 연구와 사용된 이상 탐지 알고리즘에 대해 살펴보고, 3장에서는 제안 방법을 설명한다. 4장에서는 실험 결과를 분석하고, 5장에서 결론을 맺는다.

Ⅱ. 관련 연구 및 배경

기존 연구[4]에서는 로그인 패턴을 추출하여 로그인 구조를 모델링하고, 해당 로그인 구조와 일치하지 않는 이상 로그인을 탐지하였다. 해당 연구는 정탐율(TPR, True Positive Rate) 82%의 성능을 보여주었다.

이상 탐지 알고리즘으로는 PyOD(Python Outlier Detection) 라이브러리[5]의 6개 알고리즘을 사용하였다. 사용한 알고리즘은 다음과 같다.

첫 번째로 ABOD(Angle-Based Outlier Detection) 알고리즘[6]은 한 데이터 포인트의 차이 벡터와 포인트의 거리에 의해 가중치가 부여된 집합의 다른 모든 포인트들의 쌍 사이의 각도에 대한 분산을 계산하여 이상치를 탐지한다.

두 번째로 HBOS(Histogram-based Outlier Score) 알고리즘[7]은 독립성을 가정하고 각 단일 피처(Feature)에 대한 히스토그램을 계산하고 개별적으로 점수를 매겨 마지막에 결합하여 이상치를 탐지한다.

세 번째로 IForest(Isolation Forest) 알고리즘[8]은 인스턴스가 재귀적으로 분할되는 무작위로 생성 된 이진트리이다. 이러한 트리는 이상치가 차지하는 지역에서 발생하므로 이상치에 대해 눈에 띄게 짧은 경로를 생성한다. 즉 경로 길이가 짧으면 이상치로 분류된다.

네 번째로 KNN(K Nearest Neighbors) 알고리즘[9]은 K번째의 가장 가까운 이웃까지의 거리를 이상치 점수로 사용하여 이상치를 판별한다.

다섯 번째로 LOF(Local Outlier Factor) 알고리즘[10]은 밀도 기반 이상 탐지 알고리즘으로 포인트가 주변 이웃과 얼마나 분리되어 있는지 계산하며 밀도 차이를 고려한다.

마지막으로 OCSVM(One-Class Support Vector Machines) 알고리즘[11]은 피처(Feature) 공간 원점에서 모든 데이터 포인트를 분리하고 초평면(hyperplane)에서 원점까지의 거리를 최대화하여 이상치를 찾아낸다.

Ⅲ. 제안 방법

본 장에서는 로그인 로그로 사용될 데이터 셋과 로그인 로그 전처리 방법 및 성능 측정 지표에 대해 설명한다.

3.1 데이터 셋

데이터 셋은 공개 데이터 셋인 로스 알라모스 연구소(Los Alamos National Laboratory)의 “Comprehensive, Multi-Source Cybersecurity Events[3]” 데이터 셋을 사용하였다. 이 데이터 셋은 로스 알라모스 연구소의 기업 내부 컴퓨터 네트워크 내 5개 소스에서 수집된 58일 동안의 이벤트 데이터이다. 12,425명의 사용자 및 17,684대의 컴퓨터, 62,974개의 프로세스에 대해 총 1,648,275,307개의 이벤트로 구성되어 있다. 데이터 셋은 총 5개의 개별 파일(auth.txt, proc.txt, flows.txt, dns.txt, redteam.txt)로 구성되어 있는데 본 연구에서는 인증 로그(auth.txt)와 공격 로그인 로그(redteam.txt)를 사용하였다.

3.2 인증 로그

인증 로그는 개별 Windows 기반 데스크톱 컴퓨터 및 서버, Active Directory 서버에서 수집된 인증 이벤트를 나타낸다. 각 이벤트는 표 1에 있는 속성(Attribute)을 쉼표로 구분하여 한 줄씩 작성되어 있으며 해당 시간(time)에 발생한 인증 이벤트를 나타낸다. 유효한 값이 없는 필드는 물음표("?")로 표시된다.

time은 로그가 수집된 시각을 나타내며 1초부터 시작하여 1초 단위로 경과한 시간을 의미한다. source user@domain은 로그인을 시도하는 출발지 사용자명과 도메인명이고, destination user@domain은 도착지 사용자명과 도메인명이다. source computer와 destination computer은 출발지 컴퓨터와 도착지 컴퓨터를 나타낸다. authentication type은 Negotiate, Kerberos와 같은 인증 유형을 의미한다. logon type은 윈도우즈 로그온 유형을 나타낸다. authentication orientation은 로그온/로그오프 상태를 나타낸다. success/failure는 로그인 성공/실패 여부를 나타낸다.

표 1. 인증 로그의 속성 및 예시
Table 1. Attribute and examples of the authentication log

Attribute	Examples	
time	1	1
source user@domain	C625$@DOM1	C653$@DOM1
destination user@domain	U147@DOM1	SYSTEM@C653
source computer	C625	C653
destination computer	C625	C653
authentication type	Negotiate	Negotiate
logon type	Batch	Service
authentication orientation	LogOn	LogOn
success/failure	Success	Success

3.3 공격 로그인 로그

공격 로그인 로그는 알려진 공격자 침해 이벤트를 나타내는 인증 데이터에서 가져온 특정 이벤트들이다. 즉, 정상 사용자 및 컴퓨터의 활동과 다른 비정상적인 활동 로그만을 모아 놓은 데이터이다. 각 이벤트는 표 2에 있는 속성(Attribute)을 쉼표로 구분하여 한 줄씩 작성되어 있으며 해당 시간(time)에 발생한 공격 이벤트를 나타낸다. time은 로그가 수집된 시각을 나타내며 1초부터 시작하여 1초 단위로 경과한 시간을 의미한다. user@domain은 로그인 공격을 시도하는 사용자명과 도메인명이고, source computer와 destination computer 출발지 컴퓨터와 도착지 컴퓨터를 나타낸다.

표 2. 공격 로그인 로그의 속성 및 예시
Table 2. Attributes and examples of attack login logs

Attribute	Examples	
time	151648	151993
user@domain	U748@DOM1	U6115@DOM1
source computer	C17693	C17693
destination computer	C728	C1173

3.4 데이터 추출

인증과 공격 로그인 로그를 합쳐서 총 50,000개의 데이터를 추출하였다. 인증 로그 데이터는 49,261개를 추출하였는데 결측치가 있는 데이터와 공격 로그인 로그에 있는 데이터는 추출에서 제외하였다. 공격 로그인 데이터는 739개로 총 50,000개 데이터 중 공격 로그인 데이터의 비율은 0.01478%이다. 공격 로그인 로그 데이터 739개는 공격 로그인 로그에 기록되어 있는 모든 이벤트의 수와 동일하다.

3.5 데이터 전처리

인증 로그에서 공격 로그인 로그에 있는 이벤트는 제외하고 데이터를 추출해서 인증 로그 데이터는 정상 데이터, 공격 로그인 로그 데이터는 비정상 데이터로 판별하였다.

3.5.1 정상 데이터 전처리

정상 데이터의 헤더를 표 3과 같이 전처리를 하였다. source_user@domain, destination_user@domain 헤더를 source_user, source_domain, destination_user, destination_domain로 파싱하였다. 그리고 positive 헤더는 이상 탐지 알고리즘 적용 시 사용할 타겟 헤더로 정상/비정상을 분류하기 위해 추가하였다. 정상 데이터는 0, 비정상 데이터는 1로 기록하여서 정상 데이터의 positive 헤더의 값은 모두 0으로 설정하였다.

표 3. 정상 데이터 전처리
Table 3. Normal data preprocessing

Before	After
time	time
source_user@domain	source_user
	source_domain

Before	After
destination_user@domain	destination_user
	destination_domain
source_computer	source_computer
destination_computer	destination_computer
authentication_type	authentication_type
logon_type	logon_type
authentication_orientation	authentication_orientation
success/failure	success/failure
-	positive

표 4. 비정상 데이터 전처리
Table 4. Abnormal data preprocessing

Before	After
time	time
user@domain	source_user
	source_domain
	destination_user
	destination_domain
source_computer	source_computer
destination_computer	destination_computer
authentication_type	authentication_type
logon_type	logon_type
authentication_orientation	authentication_orientation
success/failure	success/failure
-	positive

3.5.2 비정상 데이터 전처리

비정상 데이터의 헤더를 표 4와 같이 전처리를 하였다. 공격 로그인 로그에 이벤트를 인증 로그에서 찾아본 결과 source_user와 destination_user가 동일하고, source_domain과 destination_domain이 동일한 것을 발견하였다. 그래서 user@domain 헤더를 source_user, source_domain, destination_user, destination_domain로 파싱하였다. 그리고 positive 헤더를 추가하고 값은 모두 1로 설정하였다.

3.5.3 데이터 병합 및 인코딩

동일한 헤더를 가진 데이터로 전 처리된 정상 데이터 셋과 비정상 데이터 셋을 병합한 후 frequency 헤더를 추가하였다. frequency 헤더는 빈도수를 나타낸다. 표 5의 그룹 헤더를 기준으로 동일한 이벤트가 반복되는 횟수를 산출하여 각 이벤트마다 빈도수(frequency) 값을 추가하였다. 이때 빈도수(frequency) 헤더의 값은 전체 데이터 셋에 대해서가 아닌 훈련 데이터 셋과 테스트 데이터 셋을 7:3 비율로 나눈 후 각 데이터 셋 내에서의 빈도수를 산정하였다. 훈련 데이터 셋 35,000개, 테스트 데이터 셋 15,000개로 분류되었으며 테스트 데이터 셋 15,000개 중 비정상 행위는 총 212개이다.

표 5. 그룹 헤더
Table 5. Group header

Group header
source_user
source_domain
destination_user
destination_domain
source_computer
destination_computer
authentication_type
logon_type
authentication_orientation
success/failure

정상 행위와 공격 행위를 구분하기 위한 요소로써 이벤트 발생 빈도수가 영향을 미칠 수 있다고 판단하여 통계 정보인 이벤트 발생 빈도수(frequency)를 추가하였다.

그리고 [source_user, source_domain, source_computer], [destination_user, destination_ domain, destination_ computer] 쌍은 정상 행위에서 보통 동일한 쌍인 경우가 많을 것으로 보여 source_user와 destination_user만 인코딩에 사용하였다. 결과적으로 성능 향상을 위해 중복 개념을 제거 하고 표 6과 같은 인코딩 헤더를 구성하여 해당 헤더에 대해 원-핫 인코딩(One-hot Encoding)을 수행하였다. 본 논문에서 사용하는 데이터 셋은 숫자로 이루어진 수치형 데이터가 아닌 몇 개의 범주로 나누어진 범주형 데이터여서 범주형 피쳐를 처리하는데 사용하는 원-핫 인코딩을 사용하였다. 원-핫 인코딩은 N개의 클래스를 N차원의 원-핫 벡터(One-hot Vector)로 표현되도록 변환하고, 고유값들을 피쳐로 만들어 정답에 해당하는 열은 1로 나머지 0으로 표시한다. 예를 들어, source_user가 C625, C653, SYSTEM의 세 가지 범주를 가지면 C625는 100, C653은 010, SYSTEM은 001로 변환된다.

3.6 성능 측정 지표

성능 측정 지표로는 수행 시간, 오차 행렬(Confusion Matrix), 정확도(Accuracy), 오탐율(FPR, False Positive Rate), 정탐율(TPR, True Positive

표 6. 인코딩 헤더
Table 6. Encoding header

Encoding header
source_user
destination_user
authentication_type
logon_type
frequency

Rate), AUC(Area Under the Curve)를 사용하였다.

오차 행렬은 표 7로 나타낼 수 있다. 오차 행렬은 실제(Actual Class)와 예측(Predict Class)의 오차를 확인할 수 있는 행렬이다. 본 연구에서는 테스트 데이터 중 비정상 데이터를 예측하는 것이 목적이므로 Positive를 비정상, Negative를 정상으로 설명한다. 실제와 예측이 동일하면 True, 동일하지 않으면 False로 판단한다. TP는 실제로 비정상인 것을 비정상으로 예측한 수, FP는 실제로 정상인 것을 비정상으로 예측한 수, FN은 실제로 비정상인 것을 정상으로 예측한 수, TN은 실제로 정상인 것을 정상으로 예측한 수를 나타낸다.

표 7. 오차 행렬
Table 7. Confusion Matrix

		Actual Class	
		Positive (1)	Negative (0)
Predict Class	Positive (1)	True Positive (TP)	False Positive (FP)
	Negative (0)	False Negative (FN)	True Negative (TN)

정확도는 전체 이상 탐지 결과에서 정상을 정상으로, 비정상을 비정상으로 예측한 비율을 나타내며 수식 (1)과 같이 계산한다.

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

FPR은 오탐율로 실제로 정상인 것을 비정상으로 잘못 예측한 비율을 나타내며 수식 (2)와 같이 계산한다.

$$FPR = \frac{FP}{FP + TN} \quad (2)$$

TPR은 정탐율로 정상인 것을 정상으로 맞게 예측한 비율을 나타내며 수식 (3)과 같이 계산한다.

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

AUC는 ROC curve (Receiver Operating Characteristic curve)의 아래 면적을 나타내는 수치이다. ROC curve는 FPR을 x축, TPR을 y축으로 나타낸 그래프이다. 이때 생성되는 curve의 아래 면적이 AUC로 값이 1에 가까울수록 분류 모델의 성능이 좋다는 것을 의미한다.

Ⅳ. 실 험

실험 환경은 표 8과 같으며 가상 데스크톱 PC에 CentOS 7.9 운영체제를 설치하여 진행하였다. 프로세서는 Intel(R) Xeon(R) CPU E5-2667 v4, 메모리는 20GB를 할당하였다. 그리고 사용 언어로는 Python을 사용하였다. Python 라이브러리인 Pandas를 이용하여 데이터를 처리하였고, PyOD 라이브러리의 이상 탐지 알고리즘을 활용하였다.

표 8. 실험 환경
Table 8. experimental environment

운영체제	CentOS 7.9
프로세서	Intel(R) Xeon(R) CPU E5-2667 v4
메모리	20GB
사용 언어	Python
사용 라이브러리	Pandas, PyOD

4.1 이상 탐지 수행

본 절에서는 이상 탐지 알고리즘에 사용한 파라미터 정보와 모든 헤더에 대해 원-핫 인코딩을 수행한 후 실험한 결과를 보여주는 제안 방법 적용 전 실험과 인코딩 헤더에 대해서만 원-핫 인코딩을 수행한 후 실험한 결과를 보여주는 제안 방법 적용 후 실험에 대하여 설명한다.

4.1.1 이상 탐지 알고리즘 파라미터

PyOD 라이브러리의 이상 탐지 알고리즘 중에서 ABOD, HBOS, IForest, KNN, LOF, OCSVM의 6가지 알고리즘을 사용하였다. 각 알고리즘의 파라미터 설정은 표 9와 같다. ABOD의 파라미터는 contamination, method, n_neighbors의 세 가지로 구성되어 있다. contamination은 데이터 셋의 오염 정도를 나타낸다. 즉 데이터 셋의 이상치 비율이며 실수형 (0., 0.5) 값을 가진다. 결정 함수(decision function)에

표 9. 이상 탐지 알고리즘 파라미터
Table 9. Parameters of anomaly detection algorithm

Algorithm	Parameter
ABOD	contamination=0.1, method='fast', n_neighbors=5
HBOS	alpha=0.1, contamination=0.1, n_bins=3, tol=0.5
IForest	behaviour='old', bootstrap=False, contamination=0.1, max_features=0.5, max_samples='auto', n_estimators=10, n_jobs=1, random_state=None, verbose=0
KNN	algorithm='auto', contamination=0.1, leaf_size=30, method='largest', metric='minkowski', metric_params=None, n_jobs=1, n_neighbors=100, p=2, radius=1.0)
LOF	algorithm='auto', contamination=0.1, leaf_size=30, metric='minkowski', metric_params=None, n_jobs=1, n_neighbors=300, p=2
OCSVM	cache_size=200, coef0=0.0, contamination=0.1, degree=3, gamma='auto', kernel='rbf', max_iter=-1, nu=0.5, shrinking=True, tol=0.001, verbose=False

대한 임계값을 정의하기 위해 피팅(fitting)할 때 사용된다. n_neighbors는 k neighbors 쿼리에 기본적으로 사용할 이웃 수를 나타낸다. 정수형이며 기본값으로 10을 가진다. method는 알고리즘에 사용할 메소드를 나타내며 fast와 default를 값으로 가진다. fast는 fast ABOD로 훈련 포인트의 n_neighbor만 고려한다. default는 original ABOD로 모든 훈련 포인트를 고려하여 속도가 느릴 수 있다. 나머지 5개의 알고리즘에 대한 파라미터 설명은 PyOD 모델 설명 페이지[5]에서 확인이 가능하다. 각 알고리즘의 파라미터 중 기본 값이 아닌 값을 변경한 파라미터 정보는 다음과 같다. HBOS (n_bins = 3), IForest (max_features = 0.5, n_estimators = 10), KNN (n_neighbors = 100), LOF (n_neighbors = 300)

4.1.2 제안 방법 적용 전 실험

먼저 본 연구의 제안 방법을 적용하지 않고 각 이상 탐지 알고리즘을 적용해보았다. 표 5의 그룹 헤더에 frequency 헤더를 포함하여 11개 헤더에 대해 인코딩한 데이터 셋에 각 이상 탐지 알고리즘을 적용한 결과는 표 10, 11과 같다.

6개 알고리즘 중 OCSVM 알고리즘의 TP가 30개로 가장 많았지만 수행 시간은 약 29,672초로 8시간

표 10. 제안 방법 적용 전 이상 탐지 결과 (오차 행렬)
Table 10. The result of performing an anomaly detection before applying the proposed method (confusion matrix)

	TP	FP	FN	TN
ABOD	0	0	212	14788
HBOS	16	1374	196	13414
IForest	4	1405	208	13383
KNN	14	278	198	14510
LOF	14	1738	198	13050
OCSVM	30	1384	182	13404

14분 정도가 걸려 실제 비정상 행위를 가장 많이 탐지한데 비해 매우 오랜 시간이 걸렸다.

정확도(Accuracy)는 모든 알고리즘이 87% 이상의 성능을 보여주어 나쁘지 않은 성능으로 보이지만 AUC를 보면 0.46~0.52 사이의 값이 나와 성능이 좋지 못함을 알 수 있었다. 정탐율(TPR)은 OCSVM에서 가장 높은 값을 보여주었지만 14% 수준이었다.

표 11. 제안 방법 적용 전 이상 탐지 결과 (성능 지표)
Table 11. The result of performing an anomaly detection before applying the proposed method (performance indicators)

	Execute Time (sec)	Accuracy	AUC	FPR	TPR
ABOD	15412.44	0.99	0.50	0.00	0.00
HBOS	72.51	0.90	0.49	0.09	0.08
IForest	259.51	0.89	0.46	0.10	0.02
KNN	16914.36	0.97	0.52	0.02	0.07
LOF	223.84	0.87	0.47	0.12	0.07
OCSVM	29672.17	0.90	0.52	0.09	0.14

4.1.3 제안 방법 적용 후 실험

본 연구의 제안 방법을 적용하여 표 6의 인코딩 헤더로 인코딩한 데이터 셋에 각 이상 탐지 알고리즘을 적용한 결과는 표 12, 13과 같다.

HBOS와 LOF, OCSVM에서 TP가 212개로 실제 비정상 행위를 모두 탐지하였다.

정확도(Accuracy)는 모두 89% 이상의 성능을 보여주었다. 수행 시간도 1.8배~4.6배 이상 감소하였다. AUC는 HBOS가 0.49에서 0.96, LOF가 0.47에서 0.98, OCSVM이 0.52에서 0.96으로 크게 향상된 것으로 나타났다. 정탐율(TPR)도 HBOS와 LOF, OCSVM에서 이전 실험에서는 0.08, 0.07, 0.14이었는데 제안 방법에서는 모두 1로 나와 모든 실제 비정

상 행위를 비정상 행위로 예측하는데 성공하였다.

표 12. 제안 방법 적용 후 이상 탐지 결과 (오차 행렬)
Table 12. The result of performing an anomaly detection after applying the proposed method (confusion matrix)

	TP	FP	FN	TN
ABOD	0	0	212	14788
HBOS	212	1239	0	13549
IForest	5	1448	207	13340
KNN	0	20	212	14768
LOF	212	727	0	14061
OCSVM	212	1239	0	13549

표 13. 제안 방법 적용 후 이상 탐지 결과 (성능 지표)
Table 13. The result of performing an anomaly detection after applying the proposed method (performance indicators)

	Execute Time (sec)	Accuracy	AUC	FPR	TPR
ABOD	3363.22	0.99	0.50	0.00	0.00
HBOS	37.65	0.92	0.96	0.08	1.00
IForest	142.08	0.89	0.46	0.10	0.02
KNN	4576.41	0.98	0.50	0.00	0.00
LOF	98.14	0.95	0.98	0.05	1.00
OCSVM	9675.56	0.92	0.96	0.08	1.00

V. 결 론

본 연구에서는 출발지 사용자, 도착지 사용자, 인증 유형, 로그온 유형, 빈도수 헤더에 대해 로그인 행위를 학습하고 분석하여 비정상 로그인 행위를 6개의 이상 탐지 알고리즘(ABOD, HBOS, IForest, KNN, LOF, OCSVM)을 사용하여 탐지하였다. 제안 방법 적용 전과 후를 비교하여 AUC가 43% 이상(최대 50%), TPR이 86% 이상(최대 93%) 성능이 향상된 것을 확인할 수 있었다. 특히, HBOS와 LOF, OCSVM의 AUC가 0.96, 0.98, 0.96으로 모두 96% 이상의 값을 보여주었고, TPR의 경우 모두 1.0으로 100%의 성능을 보여주어 본 연구의 데이터 전처리 방법이 효과적임을 입증하였다.

References

[1] W. Liu and D. Li, "A file protection scheme based on the transparent encryption technology," *2018 IEEE Int. Conf. Safety Produce Informatization (IICSPI)*, pp. 793-795, Chongqing, China, 2018.

[2] P. Zhezhnych and D. Tarasov, "Methods of data processing restriction in ERP systems," *2018 IEEE 13th Int. Scientific and Tech. Conf. CSIT*, pp. 274-277, Lviv, 2018.

[3] A. D. Kent, "Comprehensive, multi-source cybersecurity events," *Los Alamos National Laboratory*, http://dx.doi.org/10.17021/1179829, 2015.

[4] H. Siadati and N. Memon, "Detecting structurally anomalous logins within enterprise networks," in *Proc. 24th ACM SIGSAC Conf. Comput. and Commun. Secur.*, pp. 1273-1284, Oct. 2017.

[5] *PyOD*, https://pyod.readthedocs.io/en/latest/pyod.models.html

[6] H. P. Kriegel, et al., "Angle-based outlier detection in high-dimensional data," in *Proc. 14th ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining*, pp. 444-452, 2008.

[7] M. Goldstein and A. Dengel, "Histogram-based outlier score (hbos): A fast unsupervised anomaly detection algorithm," *KI-2012: Poster and Demo Track*, pp. 59-63, 2012.

[8] F. T. Liu, K. M. Ting, and Z. H. Zhou, "Isolation-based anomaly detection," *ACM TKDD*, vol. 6, no. 1, pp. 1-39, 2012.

[9] F. Angiulli and C. Pizzuti, "Fast outlier detection in high dimensional spaces," in *Eur. Conf. Principles of Data Mining and Knowledge Discovery*, pp. 15-27, Springer, Berlin, Heidelberg, 2002.

[10] M. M. Breunig, H. P. Kriegel, R. T. Ng, and J. Sander, "LOF: Identifying density-based local outliers," in *Proc. 2000 ACM SIGMOD Int. Conf. Manag. Data*, pp. 93-104, 2000.

[11] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural Computation*, vol. 13, no. 7, pp. 1443-1471, 2001.

임 선 영 (Sun-Young Im)

2015년 2월 : 아주대학교 컴퓨터공학 학사
2017년 2월 : 아주대학교 컴퓨터공학 석사
2017년 1월~현재 : LIG넥스원 선임연구원

<관심분야> 사이버전, 사이버 위협 피해평가, 표적 공격 분석
[ORCID:0000-0003-4385-173X]

김 상 수 (Sang-soo Kim)

1997년 7월 : 경북대학교 전자공학과 졸업
2003년 7월 : 경북대학교 컴퓨터공학과 석사
2003년 8월~현재 : 국방과학연구소 연구원

<관심분야> 사이버보안, 사이버 상황인식, 인공지능
[ORCID:0000-0001-7975-673X]

심 신 우 (Shinwoo Shim)

2007년 2월 : 포항공과대학교 컴퓨터공학 학사
2019년 2월 : 고려대학교 정보보호학 석사
2007년 1월~현재 : LIG넥스원 수석연구원

<관심분야> 사이버 지휘통제, 임무영향평가, 사이버 위협 탐지, 사이버 위협 대응
[ORCID:0000-0003-0959-9200]

구 성 모 (Sung-mo Koo)

1994년 2월 : 홍익대학교 전자계산학과 졸업
1996년 2월 : 홍익대학교 컴퓨터공학과 석사
1996년 3월~현재 : 국방과학연구소 연구원

<관심분야> 사이버보안, 사이버 상황인식, 인공지능

조 병 모 (Byoungmo Cho)

2001년 2월 : 인하대학교 컴퓨터공학과 졸업
2003년 2월 : 인하대학교 전자계산공학과 석사
2009년 9월~현재 : LIG넥스원 수석연구원

<관심분야> 사이버 보안, Modeling & Simulation
[ORCID:0000-0002-8068-6342]

김 광 수 (Kwangsoo Kim)

2009년 2월 : 아주대학교 정보및 컴퓨터공학부 (공학사)
2017년 2월 : 아주대학교 대학원 컴퓨터공학과 (공학박사)
2017년 1월~현재 : LIG넥스원 수석연구원

<관심분야> 사이버전 훈련 기술, 네트워크 보안, 네트워크 M&S, 가상화 기술
[ORCID:0000-0003-0112-1464]

김 태 규 (Taekyu Kim)

2000년 2월 : 중앙대학교 컴퓨터공학 학사
2006년 5월 : the University of Arizona 컴퓨터공학 석사
2008년 5월 : the University of Arizona 컴퓨터공학 박사
2010년 2월~현재 : LIG넥스원 수석연구원

<관심분야> Cybersecurity Killchain and TTP (Tactics, Techniques, and procedures), 임베디드 시스템 보안, System Modeling and Simulation