KIPS Trans. Softw. and Data Eng.
Vol.12, No.8 pp.355~364
ISSN: 2287-5905 (Print), ISSN: 2734-0503 (Online)

https://doi.org/10.3745/KTSDE.2023.12.8.355

Intrusion Detection Method Using Unsupervised Learning-Based Embedding and Autoencoder

Junwoo Lee† · Kangseok Kim††

ABSTRACT

As advanced cyber threats continue to increase in recent years, it is difficult to detect new types of cyber attacks with existing pattern or signature-based intrusion detection method. Therefore, research on anomaly detection methods using data learning-based artificial intelligence technology is increasing. In addition, supervised learning-based anomaly detection methods are difficult to use in real environments because they require sufficient labeled data for learning. Research on an unsupervised learning-based method that learns from normal data and detects an anomaly by finding a pattern in the data itself has been actively conducted. Therefore, this study aims to extract a latent vector that preserves useful sequence information from sequence log data and develop an anomaly detection learning model using the extracted latent vector. Word2Vec was used to create a dense vector representation corresponding to the characteristics of each sequence, and an unsupervised autoencoder was developed to extract latent vectors from sequence data expressed as dense vectors. The developed autoencoder model is a recurrent neural network GRU (Gated Recurrent Unit) based denoising autoencoder suitable for sequence data, a one-dimensional convolutional neural network-based autoencoder to solve the limited short-term memory problem that GRU can have, and an autoencoder combining GRU and one-dimensional convolution was used. The data used in the experiment is time-series-based NGIDS (Next Generation IDS Dataset) data, and as a result of the experiment, an autoencoder that combines GRU and one-dimensional convolution is better than a model using a GRU-based autoencoder or a one-dimensional convolution-based autoencoder. It was efficient in terms of learning time for extracting useful latent patterns from training data, and showed stable performance with smaller fluctuations in anomaly detection performance.

Keywords : Anomaly Detection, Unsupervised Learning, Embedding Techniques, Autoencoder, Time-series Data

비지도 학습 기반의 임베딩과 오토인코더를 사용한 침입 탐지 방법

이 준 우† · 김 강 석††

요 약

최근 지능화된 사이버 위협이 지속적으로 증가함에 따라 기존의 패턴 혹은 시그니처 기반의 침입 탐지 방식은 새로운 유형의 사이버 공격을 탐지하는데 어려움이 있다. 따라서 데이터 학습 기반 인공지능 기술을 적용한 이상 징후 탐지 방법에 관한 연구가 증가하고 있다. 또한 지도학습 기반 이상 탐지 방식은 학습을 위해 레이블 된 이용 가능한 충분한 데이터를 필요로 하기 때문에 실제 환경에서 사용하기에는 어려움이 있다. 최근에는 정상 데이터로 학습하고 데이터 자체에서 패턴을 찾아 이상 징후를 탐지하는 비지도 학습 기반의 방법에 대한 연구가 활발히 진행되고 있다. 그러므로 본 연구는 시퀀스 로그 데이터로부터 유용한 시퀀스 정보를 보존하는 잠재 벡터(Latent Vector)를 추출하고, 추출된 잠재 벡터를 사용하여 이상 탐지 학습 모델을 개발하는데 있다. 각 시퀀스의 특성들에 대응하는 밀집 벡터 표현을 생성하기 위하여 Word2Vec을 사용하였으며, 밀집 벡터로 표현된 시퀀스 데이터로부터 잠재 벡터를 추출하기 위하여 비지도 방식의 오토인코더(Autoencoder)를 사용하였다. 개발된 오토인코더 모델은 시퀀스 데이터에 적합한 순환신경망 GRU(Gated Recurrent Unit) 기반의 잡음 제거 오토인코더, GRU 네트워크의 제한적인 단기 기억문제를 해결하기 위한 1차원 합성곱 신경망 기반의 오토인코더 및 GRU와 1차원 합성곱을 결합한 오토인코더를 사용하였다. 실험에 사용된 데이터는 시계열 기반의 NGIDS(Next Generation IDS Dataset) 데이터이며, 실험 결과 GRU 기반의 오토인코더나, 1차원 합성곱 기반의 오토인코더를 사용한 모델보다 GRU와 1차원 합성곱을 결합한 오토인코더가 훈련 데이터로부터 유용한 잠재 패턴을 추출하기 위한 학습 시간적 측면에서 효율적이었고 이상 탐지 성능 변동의 폭이 더 작은 안정된 성능을 보였다.

키워드 : 이상탐지, 비지도 학습, 임베딩 기법, 오토인코더, 시계열 데이터

1. 서 론

최근 인터넷을 통한 방대한 정보 및 서비스, 시스템 및 네트워크의 사용으로 랜섬웨어와 같은 악성코드 감염, 딥페이크 기술을 활용한 해킹 등의 다양해지고 지능화된 사이버 위협이 증가하고 있다. 따라서 지능화된 사이버 위협에 대응하기 위한 침입 탐지 기술의 개발이 중요해지고 있다. 기존의

※ 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2019R1F1A1059036).
† 비 회 원 : 아주대학교 지식정보공학과 석사
†† 정 회 원 : 아주대학교 사이버보안학과 부교수
Manuscript Received : March 10, 2023
First Revision : June 12, 2023
Second Revision : July 14, 2023
Accepted : July 19, 2023
* Corresponding Author : Kangseok Kim(kangskim@ajou.ac.kr)

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/ licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

침입 및 이상 탐지 보안 시스템은 시그니처 기반의 시나리오에 기인하여, 정보 자원에 불법으로 접근하거나 자원을 고갈시키는 이상 행위(Anomaly Behavior)를 탐지 및 차단하고 있어, 새로운 유형의 사이버 공격을 탐지하고 이에 대처하기에는 어려움이 있다[1]. 이러한 한계를 극복하기 위하여 인공지능 기반의 데이터 분석 기술과 사이버보안 도구를 이상 탐지에 적용함으로써, 오탐 제거와 미탐 공격을 탐지할 수 있는 지능형 이상 징후 탐지 기술에 관한 연구가 증가하고 있다.

기존의 인공지능 기반 이상 탐지 시스템은 지도학습 기반 탐지 방법들이 사용되었으나, 일반적으로 지도학습 기반의 이상 탐지 방법은 성능은 좋지만, 학습을 위해 레이블 된 이용 가능한 충분한 데이터가 필요하고, 정상 데이터와 비정상 데이터를 분류하는 작업에 많은 자원이 소모되며, 또한 이상 데이터의 샘플 수가 정상 데이터의 샘플 수와 균형이 맞지 않는 데이터 불균형 문제도 해결해야 하므로 실제 환경에서 사용하기에는 어려움이 있다. 따라서 최근에는 딥러닝 기술의 발달에 따라 정상 데이터만으로 학습하여 데이터 자체에서 패턴을 찾아 이상 탐지를 수행하는 비지도 학습(Unsupervised Learning) 기반 딥러닝 알고리즘들이 활발하게 연구되고 있다[2].

그러므로 본 연구는 시계열 로그 데이터로부터 유용한 시퀀스 정보를 보존하는 잠재 벡터(Latent Vector)를 추출하고, 추출된 잠재 벡터를 사용하여 이상 탐지 모델을 개발하는데 있다. 일반적으로 시계열 데이터는 가변 길이이기 때문에 각 샘플을 일정 길이의 시퀀스로 만드는 것이 필요하고, 각 시퀀스의 특성들에 대응하는 임베딩 벡터(Embedding Vector)[3]를 생성하기 위하여 Word2Vec의 skip-gram[4] 방법을 사용하였으며, 임베딩 벡터로 표현된 시퀀스 데이터로부터 잠재 벡터를 추출하기 위하여 비지도 학습 기반의 오토인코더(Autoencoder)[5]를 사용하였다. 실험에 사용된 시퀀스 데이터로부터 유용한 잠재 벡터를 추출하기 위하여 3가지 방식의 오토인코더를 사용하였다. 개발된 오토인코더 모델은 중요하지 않은 세부 사항은 버리고 유용한 시퀀스 정보를 보존하도록 학습하기 위하여 시퀀스 데이터에 적합한 순환신경망 GRU 기반의 잡음 제거 오토인코더(GRU-DAE)와 일반적으로 순환신경망의 제한적인 단기 기억(short-term memory) 문제를 해결하기 위한 1차원 합성곱 신경망 기반의 오토인코더(Conv1d-AE)를 개발하였다. 또한 1차원 합성곱과 GRU를 결합하여 1차원 합성곱으로 입력 시퀀스 길이를 줄이고, GRU 은닉층이 시퀀스 패턴을 감지하도록 하여 유용한 특성 벡터를 추출하기 위한 오토인코더(Conv1d-GRU-AE)를 개발하였다. 제안된 오토인코더들에 기반 한 이상 탐지 모델의 성능을 평가하기 위하여 비지도 기계학습 기반 이상 탐지 알고리즘인 IF(Isolation Forest)[6]를 사용하여 이상 탐지 성능 평가를 수행하였으며 실험에 사용된 데이터는 시계열 기반의 NGIDS-DS(Next Generation IDS Dataset)[7]이다.

그러므로 본 논문은 이상 탐지 시 로그 시퀀스에 내재된 의미 있는 정보(semantic information)를 고려하기 위해 Word2Vec을 사용한 임베딩 기법과 입력 시퀀스의 내재된 패턴을 학습하기 위한 오토인코더를 사용하여 이상 탐지 방법을 개발하는데 있다. 또한 이상 탐지 방법의 성능 평가 시 고려사항인 탐지율을 높이고 오경보 비율을 낮추기 위한 비지도 학습 기반 이상 탐지 방법의 개발에 중점을 두고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 비지도 학습 기반 이상 탐지 방법 관련 연구를 기술하였고, 3장에서는 본 연구에서 사용한 데이터와 임베딩 방법 및 개발된 오토인코더 모델 기반 이상 탐지 방법을 기술하였으며, 4장에서는 제안 방법들에 관한 실험 결과 및 분석을 기술하였고, 5장에서는 결론 및 향후 연구에 대해 제시하였다.

2. 관련 연구

최근 인공지능 구현 기술인 기계학습 및 딥러닝을 적용한 비지도 학습 기반 이상 징후 탐지 방법에 관한 다양한 연구가 수행되고 있다. 기존의 비지도 학습을 활용하여 이상 탐지를 수행한 알고리즘은 데이터의 상대적 밀도를 고려한 LOF (Local Outlier Factor)[8], 결정 트리(Decision Tree)를 사용한 IF(Isolation Forest)[6], 데이터를 구분하는 초평면(Hyperplane)을 사용한 단일 클래스 서포트 벡터 머신(OC-SVM: One Class Support Vector Machine)[9] 등의 방법들이 사용되었다. 또한 최근에는 비선형 데이터를 다루는데 효과적인 오토인코더(Autoencoder), Deep SVDD(Deep Support Vector Data Description)[10] 등과 같은 비지도 학습 기반의 딥러닝을 활용한 이상 탐지 알고리즘들이 개발되기 시작했다.

오토인코더란 인코더(Encoder)와 디코더(Decoder)가 결합한 구조로써, 인코더에선 입력 데이터의 차원을 축소하여 잠재 벡터를 추출하고, 디코더에선 추출된 잠재 벡터를 사용하여 입력 데이터와 유사한 데이터를 재구성하기 위한 딥러닝 기반의 비지도 학습 방법이다. 오토인코더의 입력 데이터와 복원된 데이터의 재구성 오차(reconstruction error)에 임계값을 두어 복원 오차가 일정 값 이상 일 때 해당 샘플을 이상(Anomaly)으로 간주하는 방법[11, 12]도 사용되었으나, 임계값을 정할 때, 사람의 주관적인 판단이 포함되어야 하는 단점이 존재한다. 이러한 단점을 극복하기 위해 오토인코더의 인코더로부터 생성된 잠재 벡터를 활용한 이상 탐지 방법이 제시되었다[13]. 오토인코더로 추출한 잠재 벡터를 LOF 알고리즘과 결합하여 이상 탐지를 수행하거나[14], 잠재 벡터와 IF 알고리즘을 결합하여 이상 탐지를 수행하는 연구도 있다[15]. [16]은 비지도 방식으로 정상 샘플에 대한 오토인코더와 공격 샘플에 대한 오토인코더를 각각 훈련시키고, 두 오토인코더의 입력과 출력을 사용하여 지도학습 방식으로 합성곱 신경망 분류기를 학습하는 탐지 모델을 개발했다. [17]은 가변 길이의 시스템 콜들을 고정 길이 차원의 실수 벡터로 변

환하기 위해 Doc2Vec 및 순환 신경망 기반 오토인코더 및 순환 신경망 기반 잡음제거 오토인코더를 사용하여 이상 탐지 모델을 개발하였다. [18]은 이상 탐지 시 로그 시퀀스에 숨겨진 의미 정보를 고려하기 위해 듀얼 LSTM(dual-LSTM) 모델이 포함된 합성곱 신경망을 사용하여 로그 이상을 자동으로 식별하는 연구를 수행하였다. 오토인코더는 입력 데이터의 특징에 따라 다양한 오토인코더를 구성할 수 있다. 이미지 데이터엔 이미지 처리에 적합한 알고리즘인 합성곱 신경망[19]을 사용하거나, 시계열 데이터에는 순차적 특성을 처리할 수 있는 순환 신경망 기반 알고리즘을 활용하여 오토인코더를 구성하는 등 데이터의 특징을 활용한 알고리즘을 사용할 수 있다. 정보 보안 로그들은 일반적으로 시계열 데이터이므로 시퀀스 로그로부터 이상 탐지를 수행하기 위해 순환 신경망 기반 오토인코더를 활용한 연구[20]도 수행되었다. 하지만 순환 신경망들은 매우 제한적인 단기 기억을 갖기 때문에 긴 시퀀스의 장기 패턴을 학습하는 데 어려움이 있다는 한계점이 존재한다. [21]에서는 네트워크 흐름 기반 이상 탐지를 위해 두 가지 벤치마크 데이터에서 K-Means, Self Organizing Maps (SOM), deep autoencoding Gaussian mixture model (DAGMM), adversarially learned anomaly detection (ALAD) 등의 비지도 학습 알고리즘을 조사하고 기존 알고리즘과 딥러닝 알고리즘의 통합이 중요함을 기술하였다. [22]에서는 이상 탐지 시스템에서 사용되는 모델 및 최적화 알고리즘의 장단점을 기술하고 향후 이상 탐지 분야에서 사용할 수 있는 대체 알고리즘을 기술하였다. 또한 이상 탐지 모델의 개발 시 낮은 탐지율(Low Detection Rate)과 함께 오경보 비율(False Alarm Rate)이 높아지는 문제뿐만 아니라 성능 평가에 영향을 미칠 수 있는 불균형 데이터 세트(Unbalanced Dataset) 문제와 응답시간(Response Time)의 고려도 필요하다고 기술하였다. 향후 연구에서 기존 알고리즘과 딥러닝 알고리즘의 통합 및 [22]에서 기술된 알고리즘을 고려할 것이다.

3. 연구 방법

본 연구는 시계열 데이터를 벡터로 변환하는 임베딩 기법과 오토인코더 기반의 비지도 학습을 사용한 이상 징후 탐지 방법을 개발하는 것으로 3단계로 구성되어 진다. 첫 번째 단계에서는 시계열 기반의 데이터를 전처리하고, 전처리된 데이터에 대하여 Word2Vec을 사용하여 입력 데이터를 임베딩 벡터로 변환하는 작업을 수행한다. 두 번째 단계에서는 변환된 임베딩 벡터를 비지도 학습 기반의 오토인코더에 주입하여 학습 후, 잠재 벡터를 추출하는 과정이다. 세 번째 단계에서는 추출된 잠재 벡터를 비지도 기계 학습 방식의 이상 탐지 알고리즘인 IF(Isolation Forest)를 사용하여 학습된 이상 탐지 모델의 성능을 평가한다. Fig. 1은 본 연구에서 제안하는 비지도 학습 기반 이상 탐지 모델의 전체적인 작업 흐름을 나타낸다.

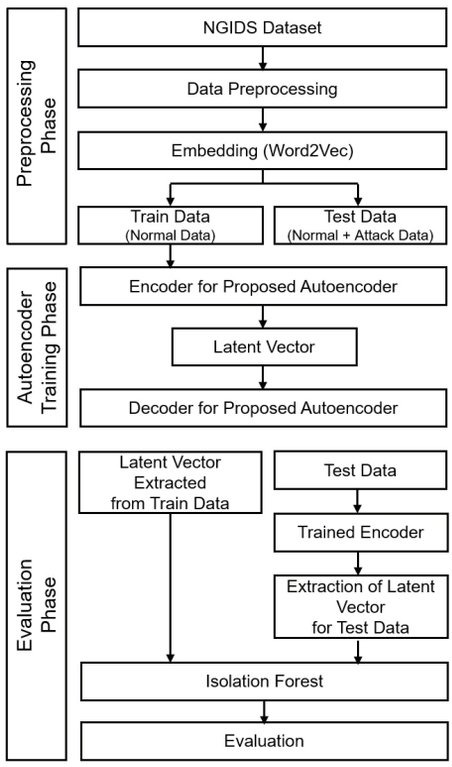

Fig. 1. Overall Workflow for the Unsupervised based Anomaly Detection Method Performed in This Study

3.1 데이터셋

실험에 사용된 NGIDS 데이터는 ADFA(Australian Defence Force Academy)에서 미가공된 리눅스 명령어 데이터로, 90,054,160개의 호스트 로그로 sequence, date_time, pro_id, path, sys_call, attack_cat, attack_subcat, label 등 8개의 속성으로 구성되어 있다. 본 연구에서 사용된 속성은 sequence, path, sys_call, label이다. path와 sys_call은 범주형 특성으로 path 속성은 100개의 범주, sys_call 속성은 122개의 범주를 가지고 있다. NGIDS 데이터를 사용하여 모델을 만들기 위하여 일정 길이(20, 30, 50 시퀀스)의 시퀀스(Sequence)를 하나의 샘플로 만드는 작업을 수행하였다. 한 샘플 당 한 개의 레이블(label)을 할당해주기 위하여 샘플 안에 레이블이 1(abnormal)인 시퀀스가 1개 이상 존재할 경우, 해당 샘플의 레이블을 1로 설정해주었고, 레이블이 1인 샘플을 이상 데이터로 취급하였다. 시퀀스 길이별 생성된 정상 샘플(normal samples)과 공격 샘플(abnormal samples) 수는 Table 1에 나타내었다.

Table 1. Number of Normal and Abnormal Samples According to Sequence Length

Sequence Length	Number of Normal Samples	Number of Abnormal Samples
20	4,434,807	67,904
30	2,954,871	46,936
50	1,770,904	30,180

Table 2. Number of Training, Validation, and Test Samples According to Sequence Length Used in the Experiment

Sequence Length	Number of Training Samples	Number of Validation Samples	Number of Test Samples
20	3,493,523	873,380	135,808
30	2,326,348	581,587	93,872
50	1,392,580	348,144	60,360

3.2 데이터 임베딩

임베딩(Embedding)이란 자연어를 산술 연산하기 위하여 단어를 벡터로 변환해주는 기법이다. 자연어의 벡터화 방식에는 희소 표현(Sparse Representation) 방식과 밀집 표현(Dense Representation) 방식이 있으며, 희소 표현은 단어를 벡터 기반으로 수치화 표현할 때 극히 일부의 인덱스만 특정 값으로, 나머지 인덱스들은 의미 없는 값으로 표현하는 방법이고, 밀집 표현은 설정한 벡터의 크기만큼 실수 인덱스들로 표현된다.

NGIDS 데이터의 path와 sys_call 속성은 각각 100개와 122개의 범주를 가진 특성이므로 벡터로 변환하는 작업을 수행하였다. path와 sys_call에 Word2Vec의 skip-gram 방법을 사용하여 path 간의 관계와 sys_call 간의 관계를 각각 밀집 표현 벡터로 변환하였다. 벡터로 변환 후, 한 시퀀스에 존재하는 변환된 path 벡터와 sys_call 벡터를 결합하여 해당 시퀀스의 벡터 표현을 생성하였다. NGIDS 데이터를 전처리와 임베딩 과정을 수행하고 나면 각 샘플은 일정 길이의 시퀀스로 만들어지고, 각 시퀀스에 대응하는 임베딩 벡터가 생성되며, 또한 각 샘플에 대응되는 레이블이 할당되어진다. 전처리된 데이터를 훈련 데이터(Training Data), 검증 데이터(Validation Data), 테스트 데이터(Test Data)로 나누었다. 테스트 데이터는 이상 샘플과 정상 샘플의 비율을 1:1로 생성하였으며, 훈련 데이터와 검증 데이터는 테스트 데이터에 사용된 정상 샘플들을 제외한 나머지 정상 샘플들을 8:2로 나누어서 사용하였다. Table 2에 실험에서 사용된 각 시퀀스 길이에 따른 훈련 데이터와 검증 데이터, 테스트 데이터의 샘플 수를 나타내었다.

3.3 비지도 방식의 딥러닝 기반 오토인코더 모델

정상 샘플들로만 구성된 입력 데이터로부터 추출된 특징 패턴 기반의 이상 탐지 모델을 개발하기 위하여 비지도 방식의 딥러닝 기반 오토인코더를 사용하였다. 순차 데이터인 NGIDS 데이터에 오토인코더를 적용하기 위하여 본 연구에서는 3가지 방식의 오토인코더를 사용하여 이상 탐지 모델을 개발하였다. 첫 번째 오토인코더 모델은 GRU 기반의 잡음 제거(Denoising) 오토인코더(GRU-DAE)로 GRU층과 드롭아웃(Dropout)층으로 구성된 인코더가 입력 시퀀스를 유용한 하나의 벡터로 압축하여 입력 시퀀스의 내재된 패턴을 학습하기 위한 오토인코더이다. 그러나 GRU는 일반적으로 제한적인 단기 기억을 가져 긴 시퀀스에서 장기(long-term) 패턴을 학습하는데 잘 작동하지 않을 수 있다. 따라서 인코더와 디코더를 1차원 합성곱 층(Conv1D)으로 구성하여 입력 시퀀스를 짧게 줄이기 위한 오토인코더를 개발하였다(Conv1d-AE). 두 번째로 개발된 Conv1d-AE 모델은 1차원 합성곱 층이 긴 입력 시퀀스에 대해 몇 개의 커널이 시퀀스 위를 슬라이딩하여 커널마다 짧은 하나의 시퀀스 패턴을 감지하도록 학습하고 압축된 특성 벡터로부터 입력 시퀀스의 잠재표현을 추출하기 위한 오토인코더이다. 세 번째로 개발된 오토인코더 모델은 GRU와 Conv1d를 결합한 오토인코더 (Conv1d-GRU-AE)이다. Conv1d-GRU-AE는 1차원 합성곱 층으로 입력 시퀀스 길이를 줄이고, 다음 GRU 은닉층이 더 긴 시퀀스 패턴을 감지하도록 하여 압축된 유용한 특성 벡터를 추출하기 위한 오토인코더 모델이다. 개발된 오토인코더 모델의 아키텍처는 다음과 같다.

1) GRU-DAE 오토인코더

GRU[23]는 LSTM(Long Short-Term Memory)[24]과 같은 순환 신경망의 한 종류로 LSTM과 유사한 성능을 보이면서 구조를 단순화시켜 학습 속도를 향상시킨 모델이다. 본 연구에서는 적은 파라미터로 모델의 학습 속도를 개선할 수 있는 GRU 층을 활용하여 Fig. 2와 같이 GRU-DAE(GRU-Denoising AE) 모델을 구성하였다. 인코더에는 2개의 GRU 층을 사용하였다. GRU 층 사이에 드롭아웃(Dropout) 층을 사용하여 잡음 제거 오토인코더(Denoising Autoencoder)의 특징이 결합된 모델을 만들고 과대 적합을 방지하였다. GRU 층 이후 선형 변환 층을 두어 잠재 벡터를 추출하였다. 디코더에도 인코더와 마찬가지로 2개의 GRU 층과 과대 적합 방지를 위한 드롭아웃 층을 사용하였다. GRU 층 이후에 선형 변환 층을 두어 입력 데이터와 유사한 재구성 데이터가 생성되도록 학습을 수행하였다.

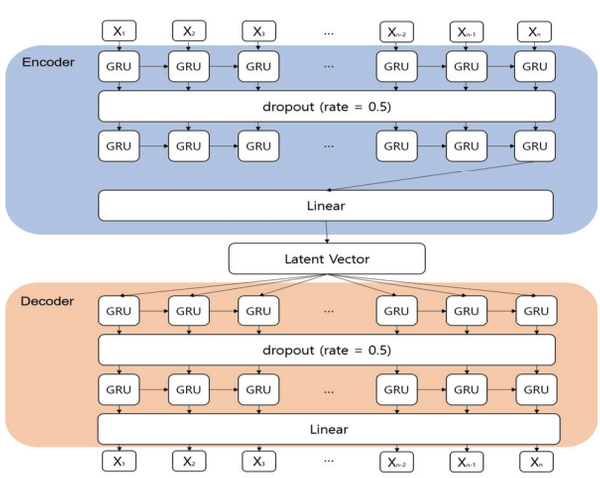

Fig. 2. GRU-DAE Model

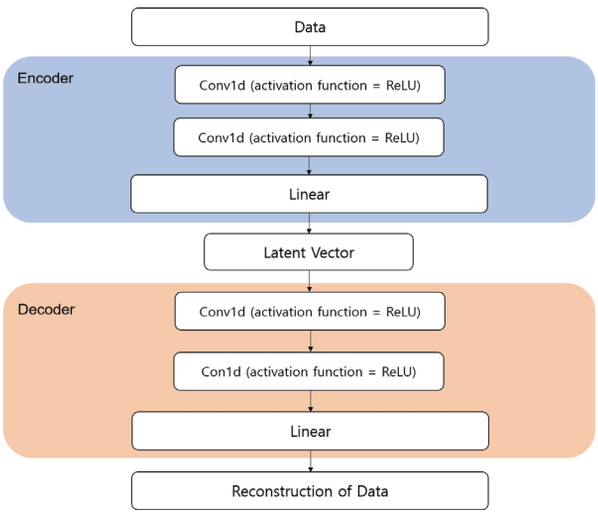

Fig. 3. Conv1d-AE Model

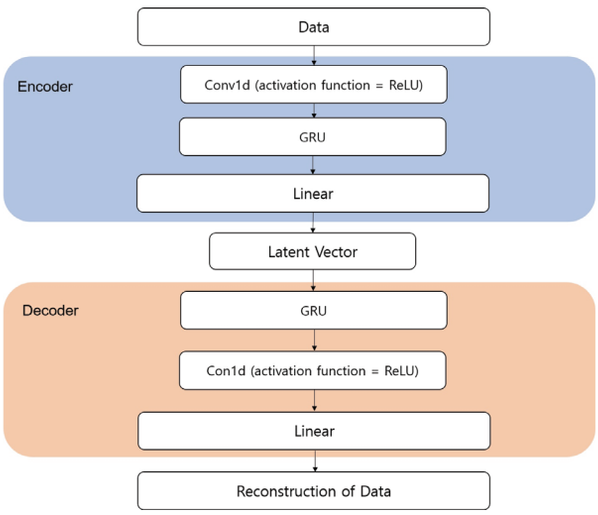

Fig. 4. Conv1d-GRU-AE Model

2) Conv1d-AE 오토인코더

1차원 합성곱(Conv1d)은 순차 정보를 효율적으로 학습할 수 있는 시계열 데이터 분석에 적합한 합성곱 신경망 모델이다. 순차 데이터 분석을 수행할 수 있는 시간적 차원 합성곱 층을 사용하여 Fig. 3과 같이 모델을 구성하였다. 인코더와 디코더에 사용되는 모든 1차원 합성곱 층에는 ReLU(Rectified Linear Unit) 활성화 함수를 사용하였다. 인코더는 2개의 1차원 합성곱 층과 잠재 벡터의 추출을 위한 선형 변환 층으로 구성하였다. 디코더도 마찬가지로 2개의 1차원 합성곱 층과 재구성 데이터의 생성을 위한 선형 변환 층으로 구성하였다.

3) Conv1d-GRU-AE 오토인코더

Conv1d-GRU-AE는 GRU와 Conv1d를 결합한 오토인코더이다. 일반적으로 시계열 데이터에 적합한 순환 신경망 기반인 GRU 알고리즘은 입력 데이터의 시퀀스 길이가 길어질수록 기울기 소실 문제가 발생하여 긴 시퀀스를 가진 데이터의 사용에는 제약이 따른다. 따라서 1차원 합성곱 신경망은 이러한 시퀀스 길이를 줄이는 연산이 가능하므로, GRU와 Conv1d를 결합한 오토인코더 모델을 구성하였다.

본 연구에서는 1차원 합성곱 층과 GRU 층을 사용하여 Fig. 4와 같이 오토인코더를 구성하였다. 인코더와 디코더에 사용되는 모든 1차원 합성곱 층에는 ReLU 활성화 함수를 사용하였다. 인코더에는 1차원 합성곱 층 이후 GRU 층을 구성하고 인코더의 출력층에서 선형 변환 층을 사용하여 잠재 벡터를 추출하도록 구성하였다. 디코더는 잠재 벡터를 입력으로 사용하여 GRU 층을 거친 뒤 1차원 합성곱 층을 거쳐 입력 데이터와 유사한 시퀀스의 데이터가 될 수 있도록 구성하였다. 1차원 합성곱 층 이후 선형 변환 층을 두어 재구성 데이터를 생성하였다.

4) 제안된 이상 탐지 모델의 성능 평가 지표

일반적으로 비지도 학습 기반 이상 탐지는 입력 데이터의 차원 축소(유용한 특성 추출) 과정을 거친 뒤, 이상 탐지 알고리즘에 주입하는 것으로 동작한다. 본 연구에서 사용된 시계열 데이터(NGIDS)의 잠재 벡터를 추출하기 위하여, 3.3절에서 제시한 3가지 방법의 오토인코더 모델을 사용하였다.

입력 데이터로부터 변환된 임베딩 벡터를 각 오토인코더 모델에 주입하여 학습시킨 후 추출한 잠재 벡터를 가지고 비지도 학습 기반 이상 탐지 알고리즘인 IF(Isolation Forest)를 사용하여 이상 탐지 성능 평가를 수행하였다. 본 연구에서는 정밀도, 재현율, F1-Score, 및 AUROC(Area Under Receiver Operating Characteristic) Score를 중심으로 모델의 성능을 평가하였다.

4. 실험 결과 및 분석

3장에서 제안한 오토인코더 기반의 모델들을 사용하여 이상 탐지 실험 및 성능 평가를 수행하였다. 실험 환경은 Table 3과 같다. Table 4에 기술된 하이퍼파라미터(Hyperparameter)에 따라 학습된 GRU-DAE 기반의 모델, Conv1d-AE 기반의 모델, Conv1d-GRU-AE 기반의 모델 각 54개씩, 총 162개 모델의 성능을 비교 분석하였다. 제안된 모델들에 대한 성능 비교의 간결성을 위해 각 오토인코더 모델들의 탐지 성능 결과들을 평균값, 분산 및 최대값을 사용하여 비교하였다. 또한 F1-Score와 AUROC가 가장 높을 모델들의 하이퍼파라미터를 기술하였다.

Table 3. Experimental Environment

OS	Window 10 21H2
CPU	Intel(R) Core(TM) i9-10900KF
RAM	64GB
GPU	NVIDIA Geforce RTX 3070
Python	3.9.7
PyTorch	1.10.2

Table 4. Hyperparameters Used in the Experiment

Input Data	Sequence Length	20, 30, 50
Word2Vec	Window Size	1, 2, 3
	Vector Dimension	8, 10
Encoder of Autoencoder	Number of Nodes in 1st-Hidden Layer	8
	Number of Nodes in 2nd-Hidden Layer	8, 6
	Latent Vector Dimension	6, 4
Isolation Forest	Number of Estimators (n_estimators)	100
	Max of Samples (max_samples)	32

4.1 GRU-DAE 모델과 Conv1d-AE 모델의 이상 탐지 성능 비교

GRU-DAE와 Conv1d-AE 오토인코더의 인코더는 입력층에서 코딩 층으로 갈수록 입력 벡터의 차원을 감소시켜 각 샘플의 잠재 벡터를 추출하였다. 디코더는 코딩 층에서 출력층으로 갈수록 벡터의 차원을 증가시켜 입력 데이터와 유사하도록 잠재벡터를 재구성하였다. 정상 데이터에서만 추출된 잠재 벡터로 IF 알고리즘을 사용하여 학습시키고 정상 데이터와 이상 데이터가 1:1로 구성된 테스트 데이터를 사용하여 이상 탐지 성능 평가를 수행하였다.

Table 5에 나타낸 것처럼, 이상 탐지 성능 평가 지표로 사용된 F1-Score가 GRU-DAE 모델이 Conv1d-AE 모델 보다 성능의 변동 폭이 약간 컸으나 Table 6에 나타낸 것처럼 가장 높은 F1-Score는 GRU-DAE 에서 도출되었다. 따라서 모델 성능의 고점을 높이고, 모델을 좀 더 안정적으로 만들기 위하여 Conv1d 와 GRU를 결합한 모델을 실험하였다.

4.2 Conv1d-GRU-AE 기반의 이상 탐지 성능 결과

일반적으로 시계열 데이터에 사용되는 GRU 기반 오토인코더는 불안정하다는 단점이 있었으나, 앞에서 언급한 두 모델의 비교에서 좀 더 좋은 성능을 보여주었다. 반면 1차원 합성곱 오토인코더 모델(Conv1d-AE)은 상대적으로 안정되나, GRU 기반 오토인코더 모델에 비하여 좋은 성능을 보여주진 못하였다. 따라서 1차원 합성곱 모델과 GRU 모델의 장점을 살리고 단점을 보완하기 위하여 두 모델을 결합한 Conv1d-GRU-AE 모델(Fig. 4)의 성능 실험을 수행하였다. Table 7과 같이 Conv1d-GRU-AE 기반 모델들의 F1-Score에 대한 분산은 Conv1d-AE 모델들의 F1-Score에 대한 분산에 비하여 좀 더 안정된 성능을 보여주었다.

Fig. 5 ~ Fig. 9는 GRU-DAE, Conv1d-AE, Conv1d-GRU-AE 모델들의 각 샘플 시퀀스 길이별 정확도(Accuracy), F1-Score, AUROC Score, 재현율(Recall), 정밀도(Precision)의 평균을 그래프로 나타낸 것이다.

Fig. 5 ~ Fig. 7에 나타낸 것처럼 Conv1d-GRU-AE 모델이 다른 두 모델인 GRU-DAE, Conv1d-AE 모델보다 정확도, F1-Score와 AUROC Score가 전체적으로 더 높은 결과를 보였다. 그러나 Conv1d-AE의 경우 다른 두 오토인코더를 사용한 이상 탐지 모델의 경우보다 불안정한 성능을 보였으며, 이것은 1차원 합성곱층이 유용한 입력 시퀀스 패턴을 학습하기 위하여 커널이 상대적으로 더 짧은 시퀀스 패턴을 감지하도록 학습하기 때문인 것으로 보인다. 향후 좀 더 세밀한 튜닝이 필요한 것처럼 보인다. Fig. 8과 Fig. 9에서 GRU-DAE와 Conv1d-GRU-AE의 경우 입력 시퀀스 길이가 길어질수록 재현율은 감소하고 정밀도는 증가하는 경향을 보였으며, 실험을 통해 입력 시퀀스 길이가 70, 80, 90인 경우에도 유사한 경향을 보이는 것을 확인하였다. 이는 시퀀스 길이가 길어질수록 공격 레이블을 가지는 비정상으로 레이블 된 샘플 안에는 공격 패턴뿐만 아니라 정상 패턴들도 증가하여 정상 패턴이 차지하는 비율이 높아지기 때문에 발생하는 현상으로 보인다. 또한 GRU는 일반적으로 제한적인 단기 기억을 보존함에도 어느 정도의 시퀀스에서는 유용한 패턴을 학습할 수 있는 특징을 갖고 있기 때문으로 보인다. 따라서 이상 탐지에 대한 오탐(false positive)을 줄이기 위하여 좀 더 긴 입력 시퀀스에 대한 학습을 필요로 하고, 미탐(false negative)을 줄이기 위하여 좀 더 짧은 입력 시퀀스에 대한 학습을 필요로 하는 것을 확인하였다. 향후 연구를 통하여 탐지 성능의 향상뿐만 아니라 시퀀스 길이에 따른 유용한 잠재패턴을 추출하기 위한 다양한 실험을 고려할 것이다.

Table 5. Mean and Variance of F1-Scores of GRU-DAE and Conv1d-AE Models

Autoencoder Model	Average of F1-Scores	Variance of F1-Scores
GRU-DAE	0.614	0.0064
Conv1d-AE	0.6456	0.0022

Table 6. The highest F1-Score for GRU-DAE Model and Cvon1d-AE Model According to the Hyperparameters Used in the Experiment

Autoencoer Model	Highest F1-Score
GRU-DAE	0.7439
Conv1d-AE	0.7215

Table 7. Mean and Variance of F1-Scores of GRU-DAE and Conv1d-AE Models

Autoencoder Model	Average of F1-Scores	Variance of F1-Scores
GRU-DAE	0.614	0.0064
Conv1d-AE	0.6456	0.0022
Conv1d-GRU-AE	0.6599	0.0016

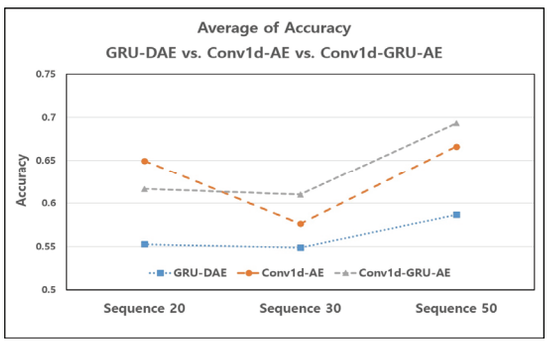

Fig. 5. Average of Accuracy for GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE Models According to Sequence Length

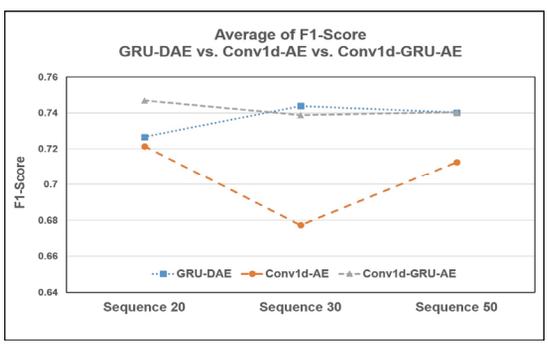

Fig. 6. Average of F1-Scores for GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE Models According to Sequence Length

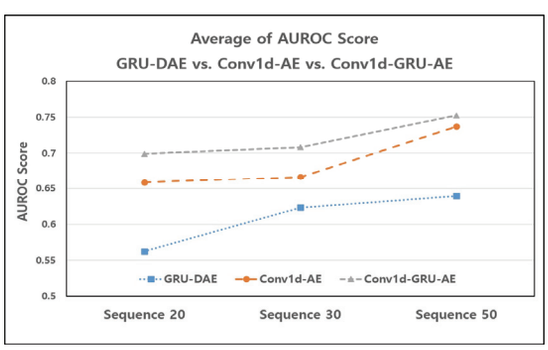

Fig. 7. Average of AUROC Scores for GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE Models According to Sequence Length

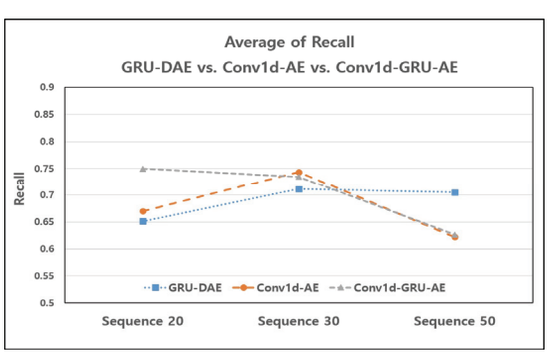

Fig. 8. Average of recalls for GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE models according to sequence length

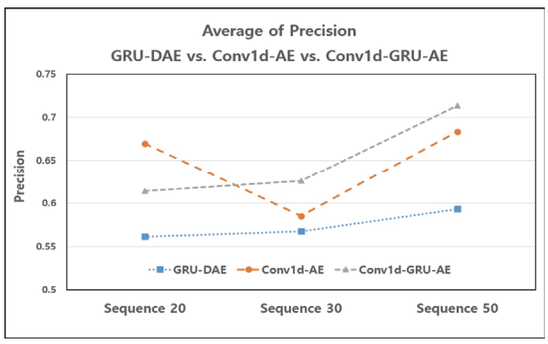

Fig. 9. Average of Precisions for GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE Models According to sequence length

4.3 시퀀스 길이에 따른 각 모델이 훈련 데이터 샘플로부터 잠재 벡터를 추출하기까지 소요되는 평균 학습 시간

Fig. 10은 각 오토인코더 모델이 훈련 데이터 샘플로부터 잠재 벡터를 추출하기까지 소요되는 평균 학습 시간을 시퀀스 길이 별로 나타낸 그래프이다. Conv1d-GRU-AE 모델의 학습 시간이 다른 두 모델의 학습 시간에 비해 짧았다. 시퀀스 길이가 20인 경우, Conv1d-GRU-AE 모델의 학습 시간은 GRU-DAE 모델 학습 시간에 비해 52% 단축되었고, Conv1d-AE 모델의 학습 시간에 비해 88% 단축되었다. 시퀀스 길이가 30인 경우, Conv1d-GRU-AE 모델의 학습 시간은 GRU-DAE 모델 학습 시간에 비해 70% 단축되었고, Conv1d-AE 모델의 학습 시간에 비해 93% 단축되었다. 시퀀스 길이가 50인 경우, Conv1d-GRU-AE 모델의 학습 시간은 GRU-DAE 모델 학습 시간에 비해 82% 단축되었고, Conv1d-AE 모델의 학습 시간에 비해 96% 단축되었다. Conv1d의 학습 시간이 오래 걸린 이유는 유용한 잠재 벡터를 추출하기 위한 재구성 오차(reconstruction error)가 일정 값으로 수렴하는 데 오래 걸렸기 때문이다.

Table 8 ~ Table 10은 GRU-DAE, Conv1d-AE, Conv1d-GRU-AE 모델들의 시퀀스 길이별 F1-Score와 AUROC가 가장 좋은 결과를 나타냈을 경우의 하이퍼파라미터를 나타낸

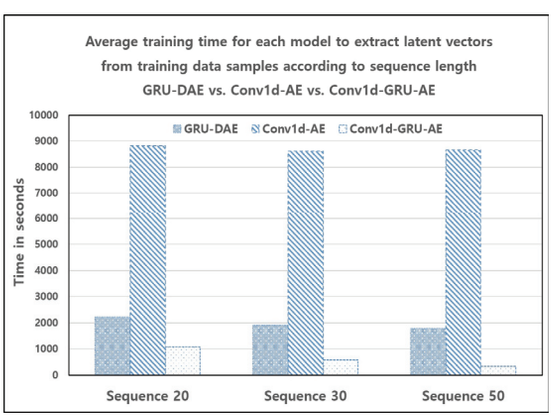

Fig. 10. Average Training Time for Each Model to Extract Latent Vectors from Training Data Samples According to Sequence Length

Table 8. Hyperparameters of Each Model When F1-Score and AUROC are Highest (sequence length = 20)

Autoencoder Model	F1-Score	AUROC
GRU-DAE	V(8, 1) AE(8, 6, 4)	V(10, 3) AE(8, 6, 4)
Conv1d-AE	V(10, 3) AE(8, 8, 6)	V(8, 2) AE(8, 8, 6)
Conv1d-GRU-AE	V(8, 1) AE(8, 8, 6)	V(8, 1) AE(8, 8, 6)

Table 9. Hyperparameters of Each Model When F1-Score and AUROC are Highest (sequence length = 30)

Autoencoder Model	F1-Score	AUROC
GRU-DAE	V(8, 3) AE(8, 6, 6)	V(8, 3) AE(8, 6, 4)
Conv1d-AE	V(8, 1) AE(8, 8, 6)	V(8, 3) AE(8, 8, 6)
Conv1d-GRU-AE	V(8, 1) AE(8, 8, 4)	V(8, 3) AE(8, 6, 4)

Table 10. Hyperparameters of Each Model When F1-Score and AUROC are Highest (sequence length = 50)

Autoencoder Model	F1-Score	AUROC
GRU-DAE	V(8, 3) AE(8, 8, 6)	V(8, 3) AE(8, 6, 4)
Conv1d-AE	V(8, 1) AE(8, 6, 4)	V(8, 1) AE(8, 6, 4)
Conv1d-GRU-AE	V(8, 3) AE(8, 6, 4)	V(8, 3) AE(8, 6, 4)

다. 실험 결과의 가시성을 위하여 두 함수 AE(a, b, c)와 W2V(x, y)를 정의하였다. AE(a, b, c)에서 a는 오토인코더의 첫 번째 층의 벡터 차원(Vector Dimension), b는 오토인코더의 두 번째 층의 벡터 차원, c는 잠재 벡터의 차원을 의미한다. 또한 W2V(x, y)에서 x는 임베딩 벡터의 차원, y는 Word2Vec 알고리즘의 하이퍼파라미터인 윈도우 사이즈(Window Size)를 의미한다. Fig. 11과 Fig. 12는 Table 8~Table 10에 나타낸 F1-Score와 AUROC Score를 그래프로 나타낸 것이다. GRU-DAE 모델이 시퀀스 길이가 30일 경우 F1-Score와 AUROC 모두 Conv1d-GRU-AE보다 높은 성능을 보였으나, 큰 차이가 없으며 Fig. 13에 나타낸 것처럼 Conv1d-GRU-AE 모델이 다른 두 모델보다 입력 데이터로부터 잠재 벡터를 추출하기까지 소요되는 학습 시간이 더 빠른 결과를 얻었으며, Table 7과 같이 Conv1d-GRU-AE 모델이 다른 두 모델보다 성능 변동의 폭이 더 작은 결과를 얻을 수 있었다. 따라서 GRU 신경망과 Conv1d 신경망의 장점을 결합한 Conv1d-GRU-AE 모델이 시계열 기반의 이상 탐지 모델에 주입하기 위한 유용한 잠재 벡터를 추출하는데 효율적이며 효과적인 비지도 방식의 모델이라고 판단된다.

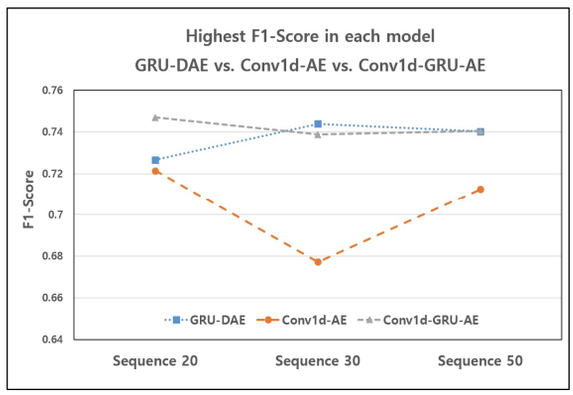

Fig. 11. Highest F1-Score in GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE Models

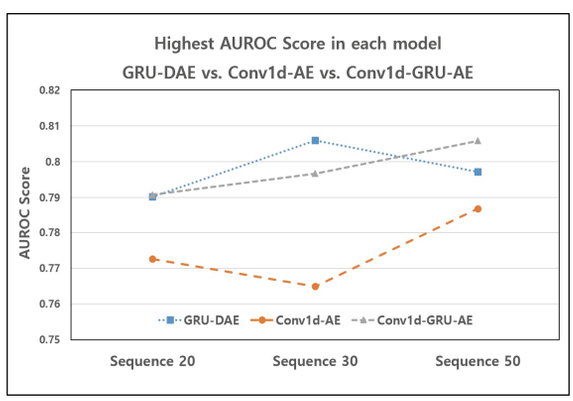

Fig. 12. Highest AUROC Score in GRU-DAE, Conv1d-AE, and Conv1d-GRU-AE Models

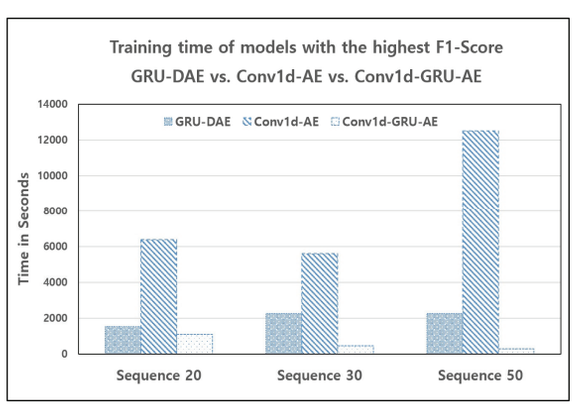

Fig. 13. Training Time of Models with the Highest F1-Score

5. 결 론

본 연구에서는 비지도 학습 기반의 임베딩 기법과 오토인코더를 활용하여 로그와 같은 시계열 데이터에 적용 가능한 이상 탐지 모델을 제안하였다. 임베딩 기법은 Word2Vec의 Skip-gram 방식을 사용하였으며, 입력 시퀀스의 특성 벡터(잠재 벡터)를 추출하기 위하여 GRU 기반의 오토인코더(GRU-DAE)와 1차원 합성곱 기반의 오토인코더(Conv1d-AE), 또

한 1차원 합성곱과 GRU를 결합한 오토인코더(Conv1d-GRU-AE)를 개발하였다. 이상 탐지 모델을 만들기 위하여 개발된 각 오토인코더 모델로부터 추출된 잠재 벡터를 기계학습 기반의 이상 탐지 알고리즘인 IF(Isolation Forest)를 사용하여 학습하였으며 개발된 모델들의 성능을 비교하였다.

비교 분석 결과 Conv1d-GRU-AE 모델은 GRU-DAE 모델과 유사한 탐지 성능을 보이지만 훈련 데이터로부터 유용한 패턴을 추출하기 위한 학습 시간적 측면에서 더 효율적이었고, 탐지 성능 변동의 폭이 적은 안정된 성능을 보였다. 그러나 비지도 학습의 한계로 인하여 모델의 성능을 높이는 데는 어려움이 있었다. 향후에 샘플들의 시퀀스 길이, 시퀀스 전후의 윈도우 길이, 임베딩 벡터 차원, 사용될 신경망 모델의 층(layer) 개수, 활성화 함수, 손실 함수 등의 다양한 하이퍼파라미터 조정(Tuning)을 통해 탐지 성능 측면에서 탐지율을 높이고 오경보율을 낮추어 더 효과적인 이상 탐지 방법을 개발할 것이다.

또한 향후 연구로 기계학습 기반의 IF외에도 딥러닝 기반의 Deep SVDD(Deep Support Vector Data Description)[10], OC-NN(One Class Neural Network)[25] 등과 같은 신경망 기반의 비지도 방식을 사용하여 이상 탐지 방법을 개발할 것이다. 또한 셀프 어텐션(Self-Attention) 기법의 경량화 된 트랜스포머(Transformer)[26]를 활용한 잠재 벡터를 추출하여 시퀀스 길이에 제약을 받지 않는 실제 활용 가능한 탐지 방법을 개발할 것이다.

References

[1] J. Song, H. Takakura, and Y. Kwon, "A generalized feature extraction scheme to detect 0-day attacks via IDS alerts," *International Symposium on Applications and the Internet*, 2008. https://doi.org/10.1109/SAINT.2008.85

[2] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo, "A geometric framework for unsupervised anomaly detection," *Applications of Data Mining in Computer Security*, Vol.6, pp.77-101, 2002. Springer, Boston, MA, https://doi.org/10.1007/978-1-4615-0953-0_4

[3] S. Selva Birunda and R. Kanniga Devi, "A review on word embedding techniques for text classification," *Innovative Data Communication Technologies and Application*, Vol. 59, pp.267-281, Springer, Singapore, 2021. https://doi.org/10.1007/978-981-15-9651-3_23

[4] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," *arXiv preprint arXiv:1301.3781v3*, 2013. https://doi.org/10.48550/arXiv.1301.3781

[5] M. A. Kramer, "Nonlinear principal component analysis using autoassociative neural networks," *AIChE Journal*, Vol.37, No.2, pp.233-243, 1991. https://doi.org/10.1002/aic.690370209

[6] F. T. Liu, K. M. Ting, and Z. Zhou, "Isolation forest," *Eighth IEEE International Conference on Data Mining*, pp.413-422, 2008. Pisa, https://doi.org/10.1109/ICDM.2008.17

[7] W. Haider, J. Hua, J. Slaya, B. P. Turnbull, and Y. Xieb, "Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling," *Journal of Network and Computer Applications*, Vol.87, No.1, pp.185-192, 2017. https://doi.org/10.1016/j.jnca.2017.03.018

[8] M. M. Breunig et al., "LOF: Identifying density-based local outliers," *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data*, Dallas Texas, USA, 2000. https://doi.org/10.1145/342009.335388

[9] Y. Chen, X. S. Zhou, and T. S. Huang, "One-class SVM for learning in image retrieval," *Proceedings of International Conference on Image Processing*, Vol.1, pp.34-37, 2001. https://doi.org/10.1109/ICIP.2001.958946

[10] L. Ruff et al., "Deep one-class classification," *Proceedings of the 35th International Conference on Machine Learning (PMLR)*, Vol.80, pp.4393-4402, 2018. https://proceedings.mlr.press/v80/ruff18a.html

[11] C. Baur et al., "Deep autoencoding models for unsupervised anomaly segmentation in brain MR images," *International MICCAI Brainlesion Workshop*, pp.161-169, Granada Spain, 2018. https://doi.org/10.1007/978-3-030-11723-8_16

[12] P. Bergmann et al., "Improving unsupervised defect segmentation by applying structural similarity to autoencoders," *arXiv preprint arXiv:1807.02011v3*, 2018. https://doi.org/10.48550/arXiv.1807.02011

[13] S. Pidhorskyi, R. Almohsen, D. A. Adjeroh, and G. Doretto, "Generative probabilistic novelty detection with adversarial autoencoders," *Proceedings of the 32nd International Conference on Neural Information Processing Systems (NeurIPS 2018)*, pp.6823-6834, Montréal Canada, Dec. 2018. https://dl.acm.org/doi/10.5555/3327757.3327787

[14] T. Kieu, B. Yang, C. Guo, and C. S. Jensen, "Outlier detection for time series with recurrent autoencoder ensembles," *Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI-19)*, pp.2725-2732, Macao China, Aug. 2019. https://doi.org/10.24963/ijcai.2019/378

[15] K. Sadaf and J. Sultana, "Intrusion detection based on autoencoder and isolation forest in fog computing," *IEEE Access*, Vol.8, pp.167059-167068, 2020. https://doi.org/10.1109/ACCESS.2020.3022855

[16] G. Andresini, A. Appice, N. D. Mauro, C. Loglisci, and D. Malerba, "Multi-channel deep feature learning for intrusion detection," *IEEE Access*, Vol.8, pp.53346-53359, 2020. https://doi.org/10.1109/ACCESS.2020.2980937

[17] C. Kim, M. Jang, S. Seo, K. Park, and P. Kang, "Intrusion detection based on sequential information preserving log embedding methods and anomaly detection algorithms," IEEE Access, Vol.9, pp.58088-58101, 2021. https://doi.org/10.1109/ACCESS.2021.3071763

[18] S. Ranga and M. N. Guptha, "Log anomaly detection using sequential convolution neural networks and Dual-LSTM model," *SN Computer Science*, Vol.4, No.3, 2023. https://doi.org/10.1007/s42979-023-01676-6

[19] W. Tang, C. M. Vian, Z. Tang, and B. Yang, "Anomaly detection of core failures in die casting X-ray inspection images using a convolutional autoencoder," Machine Vision and Application, Vol.32, No.4, pp.1-17, 2021. https://doi.org/10.1007/s00138-021-01226-1

[20] M. S. Elsayed et al., "Network anomaly detection using LSTM based autoencoder," *Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, pp.37-45, Alicante, Spain, Nov. 2020. https://doi.org/10.1145/3416013.3426457

[21] M. A. Kabir and X. Luo, "Unsupervised learning for network flow based anomaly detection in the era of deep learning," *IEEE Sixth International Conference on Big Data Computing Service and Applications (BigDataService)*, pp.165-168, Oxford, UK, 2020. https://doi.org/10.1109/BigDataService49289.2020.00032

[22] M. Aljanabi et al., "Intrusion detection systems, issues, challenges, and needs," *International Journal of Computational Intelligence Systems*, Vol.14, No.1, pp.560-571, 2021. https://doi.org/10.2991/ijcis.d.210105.001

[23] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, "Empirical evaluation of gated recurrent neural networks on sequence modeling," *Presented in NIPS 2014 Deep Learning and Representation Learning Workshop, arXiv preprint arXiv: 1412.3555*, 2014. https://doi.org/10.48550/arXiv.1412.3555

[24] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, Vol.9, No.8, pp.1735-1780, 1997. https://doi.org/10.1162/neco.1997.9.8.1735

[25] R. Chalapathy, A. K. Menon, and S. Chawla, "Anomaly detection using one-class neural networks," *arXiv preprint arXiv:1802.06360*, 2019. https://doi.org/10.48550/arXiv.1802.0636

[26] A. Vaswani et al., "Attention is all you need," *31st Conference on Neural Information Processing Systems (NIPS 2017)*, Long Beach, CA, USA, 2017. https://doi.org/10.48550/arXiv.1706.03762

이 준 우

https://orcid.org/0000-0002-8394-9662
e-mail : leejw95@ajou.ac.kr
2020년 아주대학교 사이버보안학과(학사)
2023년 아주대학교 지식정보공학과(석사)
관심분야 : 정보보안, 기계학습 및 딥러닝

김 강 석

https://orcid.org/0000-0001-8950-7577
e-mail : kangskim@ajou.ac.kr
2007년 미국 인디애나대학교(Bloomington) 컴퓨터공학(박사)
2010년 ~ 2016년 아주대학교 지식정보공학과 연구교수
2016년 ~ 현 재 아주대학교 사이버보안학과 부교수
관심분야 : 빅데이터 응용보안, 기계학습 및 딥러닝