Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.2, Apr. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.2.281

오토인코더 기반 IoT 디바이스 트래픽 이상징후 탐지 방법 연구*

박 승 아,[1†] 장 예 진,[1] 김 다 슬,[2] 한 미 란[3‡]
[1,2,3]고려대학교 (대학원생, 학생, 교수)

Autoencoder-Based Anomaly Detection Method for IoT Device Traffics*

Seung-A Park,[1†] Yejin Jang,[1] Da Seul Kim,[2] Mee Lan Han[3‡]
[1,2,3]Korea University (Graduate Student, Student, Professor)

요 약

6세대(6G) 이동통신 기술은 초고속과 초대역, 그리고 초연결성을 중심으로 발전하고 있다. 통신 기술의 발전으로 사물 인터넷(IoT) 기술에서 만물 인터넷(IoE) 기술로 확장되며 초연결 사회의 형성이 급속화되고 있다. 하지만 그와 동시에 IoT 디바이스를 대상으로 하는 보안 위협이 광범위해지고 무단 액세스나 정보 유출 등 침해사고에 대한 우려가 커지며 보안 강화 솔루션의 필요성이 증가하고 있다. 이에 따라, 본 논문에서는 IoT 보안 위협에 대응하기 위해 실시간으로 수집한 네트워크 트래픽을 활용하여 오토인코더 기반의 이상징후 탐지 모델을 구현한다. 실제 IoT 환경에서 각종 공격에 대한 IoT 디바이스 트래픽 데이터를 수집하기 어려운 점을 고려하여 비지도 학습 기반의 오토인코더 신경망을 사용하며, 학습 데이터의 노이즈 적용과 잠재 공간의 차원에 따라 서로 다른 6가지 오토인코더 모델을 구현한다. 실험을 통해 모델 성능을 비교하여 비정상적인 네트워크 트래픽을 탐지하는 이상징후 탐지 모델에 대한 성능 평가를 제공한다.

ABSTRACT

The sixth generation(6G) wireless communication technology is advancing toward ultra-high speed, ultra-high bandwidth, and hyper-connectivity. With the development of communication technologies, the formation of a hyper-connected society is rapidly accelerating, expanding from the IoT(Internet of Things) to the IoE(Internet of Everything). However, at the same time, security threats targeting IoT devices have become widespread, and there are concerns about security incidents such as unauthorized access and information leakage. As a result, the need for security-enhancing solutions is increasing. In this paper, we implement an autoencoder-based anomaly detection model utilizing real-time collected network traffics in respond to IoT security threats. Considering the difficulty of capturing IoT device traffic data for each attack in real IoT environments, we use an unsupervised learning-based autoencoder and implement 6 different autoencoder models based on the use of noise in the training data and the dimensions of the latent space. By comparing the model performance through experiments, we provide a performance evaluation of the anomaly detection model for detecting abnormal network traffic.

Keywords: Anomaly Detection, Autoencoder, IoT Device, Network Traffic

Received(12. 12. 2023), Modified(02. 29. 2024), Accepted(02. 29. 2024)
* 본 논문은 2023년도 한국정보보호학회 충청지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 이 논문은 고려대학교에서 지원된 연구비로 수행되었음.
또한, 이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-00252157).
† 주저자, hn8909@korea.ac.kr
‡ 교신저자, blosst@korea.ac.kr(Corresponding author)

I. 서 론

6세대(6G) 이동통신 기술은 초고속과 초대역, 그리고 초연결성을 중심으로 발전하고 있는 차세대 무선 통신 기술이다. 이러한 통신 기술의 발전으로 사람과 사물, 공간을 유기적으로 연결하는 사물 인터넷(IoT, Internet of Things) 기술을 뛰어넘어 데이터와 프로세스까지 모두 연결되어 상호작용하는 만물 인터넷(IoE, Internet of Everything) 기술로 확장되고 있다[1]. 이를 활용한 IoT 서비스 환경에서는 상시 연결된 네트워크를 통해 실시간으로 데이터를 교환함으로써 지능화된 서비스와 사용자 편의성을 제공하며 초연결 사회의 형성이 급속화되고 있다. 그러나 이기종 디바이스와 네트워크, 애플리케이션 간의 연동이 가속화되며 다양한 보안 취약성에 노출되고 있다[2][3]. 특히, IoT 서비스 환경을 구성하는 IoT 디바이스에 대한 보안 위협은 그 대상의 운용 환경과 역할에 따라 여러 형태로 발생할 수 있다. 예를 들어, IoT 디바이스 자체가 인가되지 않은 접근에 노출될 경우, 물리적인 파괴나 분실, 도난의 위험이 있다. 또한, IoT 디바이스에 내장된 인터페이스를 통해 무단으로 침입한 공격자가 펌웨어를 위·변조하거나 악성코드를 삽입하여 디바이스의 정상적인 동작을 방해할 수도 있다[4][5]. IoT 디바이스에서 생성 및 수집되는 정보들은 실시간 네트워크를 통해 데이터를 교환하는 과정에서 외부로 유출되기 쉽고[6], 더불어 IoT 서비스가 클라우드와 같은 ICT 기술과 융합되며 IoT 디바이스에 대한 보안 위협이 광범위해지고 있다[7].

IoT 디바이스 보안 위협에 대응하기 위해 본 논문에서는 특정 IoT 디바이스로부터 실시간으로 수집한 네트워크 트래픽을 활용하여 이상징후를 탐지하기 위한 오토인코더 모델을 설계하였다. 실제 IoT 서비스 환경에서 각종 공격에 대한 네트워크 트래픽을 수집하는 것이 제한적이며, 보안 위협에 대응하기 위해서는 사전에 정의되지 않은 새로운 공격이나 변형 기술에 대해서도 탐지할 수 있어야 한다. 따라서 본 논문에서는 비지도 학습 기반의 오토인코더 신경망을 사용하였으며, 실험을 통해 비정상적인 네트워크 트래픽을 탐지하는 이상징후 탐지 모델의 성능 평가를 수행하였다.

본 논문의 구성은 다음과 같다. 2장에서는 배경지식과 관련 연구를 서술하고, 3장에서는 데이터셋 구성과 데이터 전처리 과정, 그리고 제안된 방법론에 대하여 자세하게 서술한다. 4장에서는 실험 결과를 논의하고 이상징후 탐지 성능을 평가하며, 마지막으로 5장에서 결론 및 추후 연구 방향으로 마무리한다.

II. 배경지식 및 관련 연구

2.1 오토인코더

오토인코더(AE, AutoEncoder)는 비지도 학습 기반의 인공 신경망으로, 데이터를 압축하고 다시 확장하는 과정을 통해 입력과 유사한 출력을 생성하도록 학습하는 모델이다[8]. 오토인코더는 데이터를 압축하는 인코더(encoder) 신경망과 압축된 데이터를 확장하는 디코더(decoder) 신경망이 잠재 공간(latent space)을 중심으로 대칭을 이루는 형태를 띠며, Fig.1.과 같은 구조로 나타낼 수 있다. 먼저, 인코더는 데이터 x를 입력받아 압축하는데, 입력 데이터의 특징을 추출하고 차원을 축소하여 저차원의 특징 벡터인 잠재 공간 h를 생성한다. 그리고 디코더는 잠재 공간 h를 확장하여 입력 x를 재구성하며, 그 결과로 입력 x와 같은 차원의 데이터 y를 출력한다. 즉, 디코더는 인코더의 출력으로부터 인코더의 입력을 재구성한다. 디코더가 데이터를 재구성하기 위해 인코더는 입력 데이터의 중요한 특징만을 추출해 저차원으로 압축해야 하며, 이러한 특성으로 인하여 인코더를 데이터 특징 추출 및 차원 축소 알고리즘으로 따로 사용하기도 한다[9].

오토인코더는 입력 데이터와 유사한 출력 데이터를 생성하도록 학습한다. 이 과정에서 오토인코더 모델은 입력 데이터 x와 출력 데이터 y의 재구성 손실(reconstruction loss)을 계산하고 해당 손실값을 줄이도록 학습하는데, 이를 위해 평균 제곱 오차(MSE, Mean Squared Error) 혹은 교차 엔트로피(cross entropy) 손실 함수를 주로 사용한다.

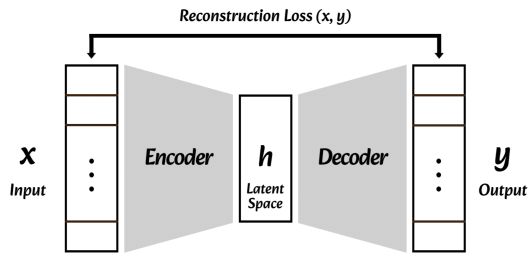

Fig. 1. Structure of Autoencoder Model

2.2 머신러닝 기반 네트워크 트래픽 이상 탐지 연구

Q. Ma 등[10]은 비정상적인 네트워크 트래픽을 탐지하기 위해 SVM(Support Vector Machine) 알고리즘과 클러스터링 기반의 분류 모델을 생성하였다. 해당 논문에서 통계 및 선형 투영 기반의 전처리 기법을 사용하였으며 제안된 모델을 통하여 높은 정확도와 F1-score를 달성하였다. M. Monshizade 등[11]은 네트워크 트래픽 데이터를 일반화하고 과적합 문제를 해결하기 위하여 특성 간의 유사성을 자동으로 학습하고 추출하는 CVAE(Conditional Variational AutoEncoder)와 특성을 분류하도록 학습하는 RF(Random Forest) 시스템을 제안하였다. Y. A. Farrukh 등[12]은 네트워크 트래픽을 3채널 이미지로 변환하여 CNN(Convolutional Neural Networks) 모델에 입력으로 사용하는 네트워크 침입 탐지 시스템을 제안하였다. 해당 논문에서 플로우 기반과 패킷 기반의 네트워크 트래픽 각각에 대하여 테스트를 진행하였고 각 데이터를 활용해 96%와 83%의 F1-score를 보여주었다. G. Shi 등[13]은 고차원 네트워크 트래픽의 대표적인 잠재적 특징을 추출하는 DCAE(Deep Convolutional AutoEncoder)를 사용하였고 GANs(Generative Adversarial Networks)를 통해 훈련 데이터셋을 확장하여 데이터 불균형 문제를 완화했으며, 실험을 통해 89%의 분류 정확도를 보여주었다.

III. 방법론

3.1 데이터셋 설명

본 논문에서는 오토인코더를 기반으로 IoT 환경에서 네트워크 트래픽의 이상징후를 탐지하기 위해 CIC(Canadian Institute for Cybersecurity)에서 제공하는 CICIoT2023 데이터셋이 사용되었다[14]. 해당 데이터셋은 105개의 IoT 디바이스로 구성된 IoT 토폴로지에서 다양한 시나리오에 따라 발생하는 트래픽을 실시간으로 모니터링 및 캡처하는 방식으로 수집되었다. 데이터셋 생성을 위해 수행된 시나리오는 크게 정상(benign)과 공격(attack) 시나리오로 구분되며, 정상 데이터는 별도의 공격이 없는 정상 시나리오에서 IoT 디바이스 간에 발생하는 네트워크 트래픽을 나타낸다. 그리고 공격 데이터는 7가지 공격 카테고리(DoS, DDoS, Recon, Web-based, brute force, spoofing, Mirai)를 수행하는 방식에 따라 33가지의 기법으로 세분화하고, 이 중 하나의 공격 기법을 적용한 스크립트를 수행하는 공격 시나리오를 통해 피해자와 공격자 간에 발생한 트래픽을 캡처한 것이다.

정상 및 공격 시나리오를 통해 수집된 트래픽 데이터는 라벨링되어 pcap과 csv 파일 형식으로 제공된다. 본 논문에서는 csv 형식의 데이터셋을 사용하였으며 각 데이터는 수집한 packet과 packet flow의 분석을 통해 flow duration과 IAT(Inter Arrival Time), 각종 packet의 값과 길이, 개수 등 46차원의 정보를 포함한다. 또한, 각 데이터는 사용된 시나리오와 공격 기법에 따라 라벨이 포함되는데, 정상 데이터는 모두 “BenignTraffic”이라는 문자열로 저장되며, 공격 데이터의 라벨은 “[공격카테고리]-[공격기법]”의 형태로 저장된다.

3.2 데이터셋 구성 및 데이터 전처리

해당 데이터셋을 이상징후 탐지 모델에 적용하기 위한 학습 데이터셋 및 테스트 데이터셋의 구성과 전처리 과정은 다음과 같다.

3.2.1 학습 및 테스트 데이터셋 구성

먼저, 모델 생성을 위한 학습 데이터셋과 테스트 데이터셋을 구성한다. 이상징후 탐지 모델 학습 과정에는 정상 데이터만 사용되므로 CICIoT2023 데이터셋에 포함된 정상 데이터 1,098,195개를 모두 추출하고 학습과 테스트 데이터셋에 8:2 비율로 적용하였다. 그리고 실험을 위하여 공격 데이터를 추가로 추출하며 테스트 데이터셋에 포함된 정상 데이터의 개수와 동일한 개수로 설정하였다. 공격 데이터는 공격 카테고리나 기법과 상관없이 랜덤하게 추출하였으며 이렇게 구성된 학습 및 테스트 데이터셋은 표 1과 같다. 표 1은 데이터셋에 포함된 Benign(정상) 데이터와 Attack(공격) 데이터의 개수를 나타낸다.

Table 1. Configuration of Train Dataset and Test Dataset

	Train	Test
Benign	878,195	220,000
Attack	0	220,000
Total	**878,195**	**440,000**

3.2.2 데이터 전처리

다음으로, 오토인코더 모델에 입력하기 전, 각 데이터셋의 전처리 과정을 수행한다. 학습 데이터셋은 정상 데이터로만 이루어지며 라벨을 제외한 46차원의 특징을 포함하고 있다. 공격이 없는 정상적인 상태의 공통된 특성에 대해 탐색 및 학습할 수 있도록 학습 데이터셋의 전처리 과정은 표준편차 및 상관도 분석을 통한 특징 선택과 정규화의 순서로 수행된다. 먼저, 특징 선택 과정은 학습 데이터셋에 포함된 데이터의 특징을 분석하여 선택 및 추출하는 과정이다. 우선 표준편차를 사용하여 특징을 분석하며, 학습 데이터셋에서 표준편차가 0인 특징은 모든 데이터가 동일한 값을 가지는 것을 의미하므로 이러한 특징 8개를 모두 제거하였다. 그리고 스피어만 상관도 분석을 통해 특징 간 비선형적인 상관관계를 파악하였다. 스피어만 상관계수는 -1부터 1 사이의 값을 가지며 절댓값이 0에 가까울수록 상관관계가 없음을 의미한다[15]. 그렇기 때문에 절댓값이 0에 가까운 특징 6개를 추가로 제거하여 특징 차원을 축소하였다. 특징 선택 과정이 끝나고 데이터의 분포를 조절하기 위하여 정규화를 수행하였으며 특징별 데이터의 평균값과 표준편차를 사용하는 Z-score 방식을 사용하였다.

테스트 데이터셋은 정상 데이터와 공격 데이터를 1:1 비율로 구성하였으며 총 44만 개의 데이터를 포함하고 있다. 그리고 각 데이터는 라벨을 포함하여 47차원의 특징을 가지며, 테스트 데이터셋의 전처리는 학습 데이터셋과 같은 순서로 진행된다. 이때, 테스트 데이터셋은 학습 데이터셋 전처리 과정과 일관된 기준으로 전처리 되는데, 특징 선택 과정에서는 학습 데이터셋의 표준편차와 스피어만 상관계수 분석을 통해 제거한 14개의 특징을 동일하게 제거하였다. 그리고 학습 데이터셋을 Z-score 방식으로 정규화할 때 사용한 평균값과 표준편차를 그대로 테스트 데이터셋에 적용하여 전처리를 마무리하였다.

3.3 오토인코더 기반 이상징후 탐지 모델 구현

본 연구에서 제안하는 오토인코더 기반의 이상징후 탐지 모델은 여러 개의 Linear 레이어와 ReLU 및 Sigmoid 활성화 함수로 이루어진다. 그리고 모델을 다음과 같이 구현하여 이상징후 탐지를 위한 최적의 구조와 파라미터를 탐색한다.

3.3.1 학습 데이터의 노이즈 적용에 따른 모델 구현

먼저 오토인코더 모델은 학습 데이터의 노이즈 적용 여부에 따라 두 가지 방식으로 구현된다. 첫 번째 방식은 모델 학습 과정에서 3.2.2장의 과정을 통해 전처리를 수행한 학습 데이터를 그대로 사용하는 방식이다. 그리고 두 번째 방식은 입력된 학습 데이터에 인위적으로 노이즈를 추가한 후 모델 학습에 사용하는 방식이며, 일반적으로 이러한 구조의 오토인코더 모델을 디노이징 오토인코더(DAE, Denoising AutoEncoder)라고 한다[16]. 디노이징 오토인코더는 노이즈가 추가된 데이터를 학습함으로써, 학습 데이터에만 지나치게 학습하여 새로운 데이터를 제대로 예측하지 못하는 과적합(overfitting) 문제를 방지할 수 있다[17]. 노이즈를 추가하기 위해 가우시안 노이즈를 사용하였으며, 이렇게 학습 데이터에 노이즈가 적용되지 않은 일반 오토인코더 모델과 노이즈가 적용된 디노이징 오토인코더 모델을 구현하여 비교하였다.

3.3.2 잠재 공간의 차원에 따른 모델 구현

다음으로 오토인코더 잠재 공간의 차원에 따라 모델을 구현한다. 오토인코더에서 잠재 공간은 입력 데이터를 압축하는 인코더를 통해 생성된 저차원의 특징 벡터이다. 잠재 공간의 차원은 입력 데이터의 특성을 얼마나 잘 압축하여 반영할 것인가와 연결되며, 지나치게 높은 차원의 잠재 공간은 입력 데이터의 불필요한 특성까지 포함하여 모델의 복잡성을 증가시킬 수 있다. 반면 차원이 너무 낮은 경우에는 입력 데이터의 특성을 제대로 포함하지 못하고 데이터 재구성 성능이 저하될 수 있다. 그러므로 적절한 잠재 공간의 차원을 탐색해야 하며, 이를 위해 2차원과 4차원, 그리고 8차원으로 설정하여 모델을 구현하였다.

3.3.3 모델 설계

3.2장에서 구성한 데이터셋을 활용하여 모델 학습 및 테스트를 진행한다. 일반 오토인코더 모델과 디노이징 오토인코더의 잠재 공간을 각각 2차원과 4차원, 8차원으로 설정하여 모델을 구현하였다. 모델 테스트 과정에서는 모델 학습의 최종 에포크에서 측정한 재구성 손실값을 임계값으로 설정하였다. 해당 값보다 재구성 손실이 작은 데이터는 정상 데이터로 판

단하며, 임계값보다 재구성 손실이 큰 데이터는 비정상 데이터로 판단하여 이상징후 탐지를 수행하도록 설계하였다. 그리고 모델 학습과 테스트를 수행하기 위한 손실 함수로는 평균 제곱 오차 함수를 사용하여 재구성 손실을 계산하였으며 평균 제곱 오차 함수는 수식 1과 같다.

$$MSE = \frac{1}{n}\sum_{t=1}^{n}\left(y_t - \hat{y}_t\right)^2 \quad (1)$$

IV. 실험 결과 분석

4.1 모델 성능 평가 지표

오토인코더 기반의 이상징후 탐지 모델의 성능을 평가하기 위해 4가지 평가 지표를 사용하였다. 사용된 평가 지표는 정확도(accuracy)와 정밀도(precision), 그리고 재현율(recall)과 F1-score이다. 그 중에서도 정밀도는 결과를 정상이라고 분류한 데이터 중 실제로도 라벨이 정상인 데이터의 비율을 나타내며, 정밀도가 높다는 것은 오탐률(FPR, False Positive Rate)을 줄일 수 있음을 의미한다. 비정상적인 공격 데이터를 정상 데이터로 잘못 분류할 경우, 악의적인 사용자가 내부로 침투하거나 시스템 통제력을 잃을 위험이 있다. 이를 방지하기 위해 이상징후 탐지 시스템에서는 비정상적인 데이터를 탐지하여 사전에 차단하는 것에 더 민감하게 반응해야 한다. 그렇기 때문에 사용된 4가지 성능 지표 중 정밀도를 중심으로 모델의 성능을 비교하였다. 정밀도가 높고 오탐률이 낮은 모델을 구현하는 것을 목표로 실험 결과를 도출하였으며, 사용된 지표는 수식 2부터 5와 같이 나타낼 수 있다.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (2)$$

$$\mathrm{Precision} = \frac{TP}{TP + FP} \quad (3)$$

$$Recall = \frac{TP}{TP + FN} \quad (4)$$

$$F1-score = 2 \times \frac{\mathrm{Precision} \times Recall}{\mathrm{Precision} + Recall} \quad (5)$$

4.2 모델 실험 결과 및 성능 평가

이상징후 탐지 모델의 성능 비교 및 평가를 위하여 모델 테스트를 수행하였다. 학습 데이터의 노이즈 적용 여부와 잠재 공간의 차원에 따라 구현한 총 6개의 모델에 대해 4가지 지표로 평가하였으며, 그 결과는 표 2와 표 3의 내용과 같다. 표 2는 학습 데이터에 노이즈를 추가하지 않은 일반 오토인코더 모델의 잠재 공간 차원을 변형하며 실험한 결과를 나타낸다. 그리고 표 3은 학습 데이터에 인위적으로 노이즈를 추가하여 학습한 디노이징 오토인코더 모델의 잠재 공간 차원을 변형하며 실험한 결과를 나타낸다.

Table 2. Performances of Anomaly Detection Models based on Autoencoder

	Autoencoder		
Latent size	2	4	8
Accuracy (%)	85.514	87.839	87.510
Precision (%)	95.179	**95.986**	95.215
Recall (%)	74.818	78.981	78.991
F1-score	83.779	86.657	86.347

Table 3. Performances of Anomaly Detection Models based on Denoising Autoencoder

	Denoising Autoencoder		
Latent size	2	4	8
Accuracy (%)	87.343	86.267	86.703
Precision (%)	95.472	**97.628**	97.383
Recall (%)	78.404	74.341	75.434
F1-score	86.101	84.407	85.015

표 2와 표 3을 바탕으로 일반 오토인코더와 디노이징 오토인코더의 성능을 비교해 보면, 전반적으로 디노이징 오토인코더 모델의 정밀도가 조금 더 높게 측정된 것을 확인할 수 있다. 디노이징 오토인코더는 인위적인 노이즈를 추가한 입력 데이터를 학습함으로써 학습 데이터에 대한 과적합을 방지하며 비정상적인 테스트 데이터를 탐지할 수 있었다. 그리고 잠재 공간의 차원에 따라 달라지는 결과를 통하여 4차원일 때 가장 높은 성능을 보이는 것을 확인하였다. 일반 오토인코더와 디노이징 오토인코더 모두 잠재 공간이 4차원일 때 가장 높은 정밀도를 보였으며, 잠재 공간이 2차원인 경우에 가장 낮은 성능을 보였다.

결과적으로 해당 데이터셋에서 4차원의 잠재 공간을 가진 디노이징 오토인코더 모델이 가장 높은 성능으로 이상징후를 탐지할 수 있음을 보여주었다.

V. 결 론

본 연구에서는 계속해서 발생하는 IoT 보안 위협에 대응하기 위해 IoT 디바이스로부터 수집된 네트워크 트래픽을 사용하여 이상징후 탐지 방법 연구를 수행하였다. 오토인코더를 기반으로 IoT 디바이스 트래픽 이상징후 탐지 모델을 구현하였으며 정상 트래픽 데이터로만 학습하고 새로운 데이터가 입력되면 해당 데이터가 정상 트래픽인지 아닌지를 분류하고자 하였다. 학습 및 테스트 데이터의 특성을 분석하고 이를 바탕으로 전처리를 수행하고 학습 데이터의 노이즈 실험을 통해 일반적인 오토인코더와 노이즈가 추가된 입력 데이터로 학습한 디노이징 오토인코더의 성능을 비교하였다. 또한 잠재 공간의 차원을 변형하며 그에 따른 결과를 분석하였다. 실험 과정에서 비정상적인 공격 트래픽을 정상 트래픽으로 잘못 분류하는 확률인 오탐률을 낮추고자 정밀도를 기준으로 모델의 성능을 비교하였으며, 구현한 6가지 모델 중 4차원 잠재 공간을 가지는 디노이징 오토인코더가 97.628%의 정밀도로 가장 뛰어난 성능을 보였다. 하지만 정확도와 F1-score가 90%를 넘지 못하였으며, 실제로 정상 데이터를 비정상 데이터로 분류할 확률과 연관된 재현율을 높이는 것이 필요할 것이다. 향후, 본 연구를 토대로 이상징후 탐지 모델의 정확도와 재현율, F1-score를 향상시키기 위한 파라미터 조정 등의 모델 최적화를 진행할 예정이며, 나아가 다른 전처리 기법 혹은 알고리즘을 적용하여 네트워크 트래픽을 공격 카테고리 및 공격 기법에 따라 효과적으로 분류할 수 있는 방식에 대해 연구를 진행하고자 한다.

References

[1] Y. Liu, H.-N. Dai, Q. Wang, M. K. Shukla, and M. Imran, "Unmanned aerial vehicle for internet of everything: Opportunities and challenges," Computer Communications, vol. 155, pp. 66-83, Mar. 2020.

[2] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions," Mobile Networks and Applications, vol. 28, pp. 296 - 312, Feb. 2023.

[3] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," The Journal of Supercomputing, vol. 79, no. 20, pp. 3392-3411, Feb. 2023.

[4] A. Bhardwaj, K. Kaushik, S. Bharany, and S. Kim, "Forensic analysis and security assessment of IoT camera firmware for smart homes," Egyptian Informatics Journal, vol. 24, no. 4, pp. 100409, Dec. 2023.

[5] M. Venkatasubramanian, A. H. Lashkari, and S. Hakak, "IoT Malware Analysis Using Federated Learning: A Comprehensive Survey," IEEE Access, vol. 11, pp. 5004-5018, Jan. 2023.

[6] A. A. Olazabal, J. Kaur, and A. Yeboah-Ofori, "Deploying Man-In-the-Middle Attack on IoT Devices Connected to Long Range Wide Area Networks (LoRaWAN)," 2022 IEEE International Smart Cities Conference (ISC2), pp. 1-7, Sep. 2022.

[7] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, and Z. Jalil, "Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey," Electronics, vol. 11, no. 1, pp. 16, 2022.

[8] S. P. S. Appalabatla and M. K. T., "Performance Analogy of Autoencoders for Image Denoising," 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), vol. 9, pp. 1-4, Aug. 2023.

[9] B. Lewandowski, R. Paffenroth, and

K. Campbell, “Improving Network Intrusion Detection Using Autoencoder Feature Residuals,” 2022 4th International Conference on Data Intelligence and Security (ICDIS), pp. 31-39, Aug. 2022.

[10] Q. Ma, C. Sun, and B. Cui, “A Novel Model for Anomaly Detection in Network Traffic Based on Support Vector Machine and Clustering,” Security and Communication Networks, vol. 104 pp. 102215, Nov. 2021.

[11] M. Monshizadeh, V. Khatri, M. Gamdou, R. Kantola, and Z. Yan, “Improving Data Generalization With Variational Autoencoders for Network Traffic Anomaly Detection,” IEEE Access, vol. 9, pp. 56893-56907, Apr. 2021.

[12] Y. A. Farrukh, S. Wali, I. Khan, and N. D. Bastian, “SeNet-I: An approach for detecting network intrusions through serialized network traffic images,” Engineering Applications of Artificial Intelligence, vol. 126, pp. 107169, Nov. 2023.

[13] G. Shi, X. Shen, F. Xiao, and Y. He, “DANTD: A Deep Abnormal Network Traffic Detection Model for Security of Industrial Internet of Things Using High-Order Features,” IEEE Internet of Things Journal, vol. 10, no. 24, pp. 21143-21153, Dec. 2023.

[14] E.C.P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, “CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment,” Sensors, vol. 23, no. 13, pp. 5941, Jun. 2023.

[15] D. Kim, and T.-Y. Heo, “Anomaly Detection with Feature Extraction Based on Machine Learning Using Hydraulic System IoT Sensor Data,” Sensors, vol. 22, no. 7, pp. 2479, Mar. 2022.

[16] L. Yasenko, Y. Klyatchenko, and O. Tarasenko-Klyatchenko, “Image noise reduction by denoising autoencoder,” 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 351-355, May. 2020.

[17] S. Hore, Q. H. Nguyen, Y. Xu, A. Shah, N. D. Bastian, and T. Le, “Empirical Evaluation of Autoencoder Models for Anomaly Detection in Packet-based NIDS,” 2023 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1-8, Nov. 2023.

〈저자소개〉

박 승 아 (Seung-A Park) 학생회원
2023년 2월: 고려대학교 인공지능사이버보안학과 졸업
2023년 3월~현재: 고려대학교 사이버보안학과 석사과정
〈관심분야〉 정보보호, 사이버보안, AI 보안, 임베디드 보안, 사용자 인증 시스템

장 예 진 (Yejin Jang) 학생회원
2024년 2월: 고려대학교 인공지능사이버보안학과 졸업
2024년 3월~현재: 고려대학교 사이버보안학과 석사과정
〈관심분야〉 정보보호, 사이버보안, AI 보안

김 다 슬 (Da Seul Kim) 학생회원
2021년 3월~현재: 고려대학교 인공지능사이버보안학과 재학
〈관심분야〉 정보보호, AI 보안

한 미 란 (Mee Lan Han) 종신회원
2002년 2월: 동덕여자대학교 컴퓨터과학과 졸업
2004년 8월~2012년 3월: ㈜넥슨 메이플스토리 해외사업본부 책임연구원
2015년 8월: 고려대학교 정보보호대학원 석사
2020년 8월: 고려대학교 정보보호대학원 박사
2020년 9월~2021년 8월: 고려대학교 정보보호연구원 연구교수
2021년 9월~2022년 8월: 고려대학교 인공지능사이버보안학과 산학협력중점교수
2022년 9월~현재: 고려대학교 인공지능사이버보안학과 조교수
〈관심분야〉 이상징후 탐지 및 식별, 범죄자 행위분석, 임베디드 보안