Journal of Digital Convergence
Vol. 19. No. 9, pp. 463-468, 2021

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2021.19.9.463

IoT 네트워크에서 악성 트래픽을 탐지하기 위한 머신러닝 알고리즘의 성능 비교연구

현미진
경남대학교 교양융합대학 MSC교육부 교수

A comparative study of the performance of machine learning algorithms to detect malicious traffic in IoT networks

Mi-Jin Hyun
Professor, Division of Mathmatics, Science, and Computers, Kyungnam University

요 약 IoT는 기술의 발전과 IoT 기기의 보급 및 서비스의 활성화로 폭발적인 증가세를 보이고 있지만, 최근 다양한 봇넷의 활동에 의해 심각한 보안 위험과 재정적 피해가 발생하고 있다. 따라서 이러한 봇넷의 활동을 정확하고 빠르게 탐지하는 것이 중요하다고 할 수 있다. IoT 환경에서의 보안은 최소한의 프로세싱 성능과 메모리로 운영을 해야 하는 특성이 있는 만큼, 본 논문에서는 탐지를 위한 최소한의 특성을 선택하고, KNN(K-Nearest Neighbor), Naïve Bayes, Decision Tree, Random Forest와 같은 머신러닝 알고리즘이 봇넷의 활동을 탐지하는 성능을 비교연구 하였다. Bot-IoT 데이터셋을 사용한 실험 결과는 적용한 머신러닝 알고리즘 중 KNN이 DDoS, DoS, Reconnaissance 공격을 가장 효과적이고 효율적으로 탐지할 수 있음을 보여주었다.

주제어 : 사물인터넷, 봇넷, 머신러닝, 보안, 데이터셋

Abstract Although the IoT is showing explosive growth due to the development of technology and the spread of IoT devices and activation of services, serious security risks and financial damage are occurring due to the activities of various botnets. Therefore, it is important to accurately and quickly detect the activities of these botnets. As security in the IoT environment has characteristics that require operation with minimum processing performance and memory, in this paper, the minimum characteristics for detection are selected, and KNN (K-Nearest Neighbor), Naïve Bayes, Decision Tree, Random A comparative study was conducted on the performance of machine learning algorithms such as Forest to detect botnet activity. Experimental results using the Bot-IoT dataset showed that KNN can detect DDoS, DoS, and Reconnaissance attacks most effectively and efficiently among the applied machine learning algorithms.

Key Words : IoT, Botnet, Machine Learning, Security, Data Sets

*This work was supported by Kyungnam University Foundation Grant in 2020.
*Corresponding Author : Mi-Jin Hyun(idream@kyungnam.ac.kr)
Received August 11, 2021 Revised August 31, 2021
Accepted September 20, 2021 Published September 28, 2021

1. 서론

최근 IoT(Internet of Things) 기술의 발전과 더불어 IoT 기기의 보급 및 서비스의 활성화로 산업영역 및 일상생활에 큰 변화와 편리함을 가져다주었다. IoT 장치는 의료, 스마트 시티, 지능형 교통 시스템과 같은 여러 영역의 사례에서 볼 수 있듯이 사람, 사물, 프로세스, 데이터가 인터넷은 물론 상호 간에 연결되는 보편적인 시스템으로 자리 잡았다[1].

IoT는 인터넷에 연결된 인터랙티브 환경으로, 더 많은 기능을 통해 개인의 다양한 정보를 생성하고 수집한다[2]. 가정에서 사용하는 가전 기기에 부착된 센서를 통해 집안 내 상황에 대한 정보를 비롯하여 생활패턴과 같은 정보 등이 수집되거나, 웨어러블 디바이스를 통해 생체 분야에서 수집되는 대부분의 정보는 건강 상태, 질병 여부, 신체 정보 등 개인정보보호법상 민감정보에 해당할 여지가 큰 민감도가 높은 정보이다[2]. 또한 그 데이터의 양도 폭발적으로 증가하고 있어 이러한 정보들에 대한 보안이 필요한 시점이다. 그러나 IoT는 유선, 무선, 블루투스 등 다양한 유형에 따른 복잡성 및 보안 의식이 낮아 기존보다 심각하고 다양한 보안 위협을 내포하고 있고, 봇넷과 같은 복잡한 사이버 공격과 함께 취약성이 현저하게 증가한다[3].

봇넷 네트워크(Botnet Network)는 사이버 범죄자가 인터넷을 통해 악의적인 활동을 시작하는데 사용하는 여러 개의 IoT로 구성된 봇(Bot)들의 네트워크이다. 봇넷 기반 공격은 주로 DDoS(Distributed Denial of Service) 공격, Port scanning과 OS fingerprint와 같은 Probing 공격, Keylogging과 Data theft와 같은 Information theft 공격과 같은 활동을 한다. 2001년에 최초의 봇넷 공격을 시작으로 이후 다양하게 변형되고 정교해지면서 2016년 10월 DNS(Domain Name System) 서비스 업체인 Dyn이 대규모 DDoS 공격을 받았다. 미라이 봇넷(Mirai botnet) 공격이라 일컬어지는 이 사건으로 인해 Dyn이 맡고 이는 넷플릭스, 트위터, 뉴욕 타임즈, 아마존 등 총 1,200개 이상 도메인의 사용자들이 원하는 서비스에 접속하지 못했다[4]. 미라이 봇넷은 카메라나 DVR 같은 보안이 허술한 IoT 기기가 포함되었는데, 악성코드를 설치하고 인터넷 트래픽을 라우팅하는 Dyn의 데이터 센터 서버를 공격하는 방식으로 이루어졌다[4].

이러한 봇넷 기반 공격을 탐지하고 방어하는 것은 IoT의 주요 과제 중 하나이다. 따라서 주요 사이버 공격에 참여하는 봇넷의 활동을 탐지하는 연구가 필요하다. 그러나 IoT 네트워크의 악성 트래픽 탐지는 낮은 대기시간(low latency), 이동성(mobility) 및 IoT 장치의 수와 특성으로 엄청난 양의 데이터를 생성하므로 많은 어려움이 있다[5]. 그리고 현실적인 IoT 생성 트래픽이 포함된 데이터셋이 많지 않다는 문제점도 있다.

이러한 문제점들을 해결하기 위해 본 논문에서는 IoT 네트워크 환경에서 악성 트래픽을 탐지하기 위한 머신러닝 알고리즘들의 성능을 비교하는 연구를 실시하였다.

머신러닝 알고리즘들의 악성 트래픽 탐지 성능을 비교하기 위해 IoT trace가 포함된 Bot-IoT 데이터셋을 활용한다. 상관 계수와 엔트로피를 이용하여 10가지 특성을 추출하였다. [6]에서 조사된 바와 같이 침입탐지를 위해 대부분의 연구에서 주로 사용하는 알고리즘인 KNN(K-Nearest Neighbor), Naïve Bayes, Decision Tree, Random Forest로 탐지 성능을 평가하였다.

본 논문의 구성은 다음과 같다. 2장에서는 연구 동향과 IoT 악성 트래픽 탐지에 활용되고 있는 데이터셋에 대한 소개를 한다. 3장에서는 본 논문에서 사용한 데이터셋 및 전처리에 대해 기술한다. 4장에서는 머신러닝 알고리즘들의 성능을 비교하고. 5장에서는 결론 및 향후 연구계획을 기술한다.

2. 연구 동향

2.1 관련 연구

최근 IoT 환경에서의 침입탐지 연구로 머신러닝을 적용한 모델들이 많이 연구되고 있다[6].

Nickilaos Koroniotis[7]등은 머신러닝 알고리즘이 봇넷의 공격과 추적을 효과적으로 탐지하는 네트워크 포렌식 아키텍처를 제안하였다.

Saeid Soheily-Khah[8]등은 K-means와 Random Forest를 결합한 하이브리드 침임 탐지 모델(km-RF)을 제안하였고, ISCX 2012 데이터셋을 이용하여 5가지 머신러닝 알고리즘과의 성능을 비교하였다.

Hayretdin Bahsi[9]등은 IoT 환경에서 IoT봇을 감지할 때 탐지에 필요한 특성의 수를 최소화하는 것이 필요하므로 Fisher's score를 이용하여 특성추출을 실시한 후 KNN과 Decision Tree의 성능을 비교하였다.

Maede Zolanvari[10]등은 산업용 사물인터넷(IIoT) 환경에서 다양한 불균형 비율을 통해 침입을 감지하는 인공신경망(ANN) 알고리즘의 효율성을 평가하였다.

Muhammad Shafiq[11]등은 악성 트래픽의 탐지를 위하여 CorrAUC라는 새로운 특성 선택 메트릭을 제안한 후 4가지 머신러닝 알고리즘(Decision Tree(C4.5), Support Vector Machine, Naïve Bayes, Random Forest)을 사용하여 성능을 측정 비교하였다.

2.2 IoT 관련 데이터셋

기존 네트워크 환경에서의 침입탐지 시스템과 관련한 연구는 많이 이루어졌으나 적절한 공개 데이터셋의 부족은 가장 큰 문제 중 하나이다[12].

DARPA98, KDD99, ISC2012 및 ADFA13과 같은 데이터셋은 침입탐지 및 침입 방지 접근 방식의 성능을 평가하는 데 사용해왔다. 그러나 1998년 이후 11개의 사용 가능한 데이터셋에 대한 연구에 따르면 이러한 데이터셋은 오래되어 사용할 수 없다. 이러한 데이터셋 중 일부는 트래픽 다양성 및 볼륨 부족으로 어려움을 겪고 있으며, 일부는 다양한 공격을 다루지 않는 반면, 다른 일부는 현재 추세를 반영할 수 없는 익명화 된 패킷 정보 및 페이로드 또는 특성 세트 및 메타 데이터가 부족하기 때문이다[13].

그러나 최근 들어 네트워크 데이터셋을 생성하기 위한 다양한 연구가 수행되었고, 상당수의 데이터셋이 프라이버시 우려로 인해 비공개 상태로 남아있지만, 일부는 공개적으로 사용할 수 있게 되었다. 가장 일반적으로 사용되는 데이터셋은 Table 1에 정리한 것과 같다.

BoT-IoT 데이터셋은 UNSW Canberra의 Cyber Range Lab에서 현실적인 네트워크 환경을 설계하여 생성하였다. BoT-IoT 데이터셋을 생성하기 위해 7,200만 개 이상의 레코드를 캡처하였다. 이 데이터셋의 주요 특징은 봇넷 트래픽의 99% 이상을 포함하는 반면 일반 트래픽은 1% 미만이다[14].

UNIBS(University of Brescia) 데이터셋은 구성 과정에서 Ground Truth 데몬을 실행하는 20대의 워크 스테이션을 설치했으며 트래픽이 수집된 라우터에서 tcpdump를 통해 수집되었다. 이 데이터셋에는 몇 가지 단점이 있다. 첫째, 공격 시나리오는 DoS 공격으로 제한된다. 둘째, 데이터셋은 추가 속성이 생성되지 않은 패킷 형태로 존재한다. 또한 레이블에 대한 정보가 제공되지 않는다[15].

CAIDA(Center for Applied Internet Data Analysis) 데이터셋은 페이로드를 제외하고 익명 처리된 헤더 트래픽으로 구성되어 있다. 데이터셋은 DDoS와 같은 매우 특정한 공격으로 구성된다. CAID 컬렉션에서 인기 있는 데이터 집합 중 하나는 CAIDA DDoS 2007인데, 이 데이터 집합에는 2007년 8월 4일에 발생한 DDoS 공격의 익명화된 공격 흔적 1시간이 포함되어 있다. CAIDA 데이터셋의 한 가지 단점은 공격 사례에 대한 근거가 없다는 것이다[15].

UNSW-NB15는 Mustafa 등이 UNSW Canberra에서 개발한 데이터셋이다. 연구자들은 IXIA 퍼펙트 스톰을 사용하여 양성 트래픽과 공격 트래픽을 혼합하여 생성된 새로운 특성이 상당히 많은 PCAP 파일 형태의 데이터셋을 생성했다[16].

ISCX(Information Security Centre of Excellence) 데이터셋은 캐나다 사이버 보안 연구소에서 작성되었다. 같은 기관인 CICDS2017에서 새로운 데이터 집합이 생성되었다. CICIDS2017은 B-Profile 시스템을 사용하여 실제 사용자 관련 배경 트래픽을 생성되는 다양한 공격 시나리오로 구성되어 있다. 그러나 라벨링 프로세스의 신뢰성을 향상시킬 데이터셋의 실측은 공개되지 않았다[17].

Table 1. Comparison of datasets(T=true, F=false)

Dataset	Realistic traffic	Labeled data	Iot traces
Bot-IoT[13]	T	T	T
UNIBS[14]	T	T	F
CAIDA[14]	T	F	F
UNSW-NB15[16]	T	T	F
ISCX[17]	T	T	F

3. 데이터셋

3.1 BoT-IoT 데이터셋

본 논문에서 IoT 네트워크에서 악성 트래픽의 탐지 성능을 측정하기 위하여 BoT-IoT 데이터셋[18]을 사용하였다. IoT에서 봇넷 탐지를 위하여 필요한 IoT trace에 대한 충분한 정보가 포함된 데이터셋이다.

BoT-IoT 데이터셋은 생성된 데이터셋이 csv의 경우 15.6GB로 매우 커서, 데이터셋을 쉽게 처리하기 위해 MySQL 쿼리를 사용하여 원본 데이터셋의 5%를 추출했다. 추출된 5%는 총 크기가 약 0.97GB인 파일 4개로, 45개의 특성과 3,668,522개의 레코드로 구성되어 있다. 또한 이 데이터셋에는 DDoS, DoS, Reconnaissance, Data theft 공격이 포함되어 있다. 훈련 데이터셋과 테

스트 데이터셋은 Table 2에서 보는 바와 같이 각각 전체 데이터셋의 80%, 20%로 분할 하여 사용하였다.

Table 2. The number of train and test dataset consisting of normal and attack classes

Category	Training	Test
DDoS	1,541,315	385,309
DoS	1,320,148	330,112
Reconnaissance	72,919	18,163
Normal	370	107
Data theft	65	14
Total	2,934,817	733,705

3.2 데이터 전처리

실험에 사용할 데이터 특성들의 값을 일정한 수준으로 맞추어 머신러닝 알고리즘을 훈련 시키는데 있어서 사용되는 특성들이 모두 같은 정도의 스케일로 반영되도록 하기 위하여 정규화를 실시하였다. 본 논문에서는 수식 (1)에 따라 데이터에 대해 Min-Max변환을 수행하였다.

$$x' = \frac{x - \min}{\max - \min} \quad (1)$$

3.3 특성추출

실험에 사용할 특성을 추출하기 위해 데이터셋 특성 간의 상관 계수와 특성들 간의 joint 엔트로피를 이용하여 10개의 특성을 추출하였다. 특성을 추출하여 차원을 감소시킴으로써 악성 트래픽의 탐지 시간을 줄이고, 더불어 학습 모델의 성능을 개선하기 위한 목적이 있다. 선택된 특성은 seq, stddev, N_IN_Conn_P_SrcIP, min, state_number, mean, N_IN_Conn_P_DstIP, drate, srate, max이다.

4. 실험 및 분석

실험은 IoT 네트워크 환경에서 수집된 BoT-IoT 데이터셋을 활용하여, KNN, Naïve Bayes, Decision Tree, Random Forest로 성능을 측정하였다.

4.1 실험환경

실험은 클라우드 기반의 Jupyter 노트북 개발환경인 구글 코랩(Corlab)pro에서 실시하였다.

4.2 성능 평가

본 논문에서 결과를 측정하기 위하여 Confusion matrix에 기반한 메트릭을 사용한다. Confusion matrix의 정의는 Table 3에 나와 있다.

Table 3. Confusion matrix

		Actual	
		positive	Negative
Predicted	Positive	TP	FP
	Negative	FN	TN

실험 성능 평가는 Accuracy(정확도), Precision(정밀도), Recall(재현율), F1-score를 측정하였다. 성능 측정의 방법은 수식 (2),(3),(4),(5)와 같다.

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

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

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

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

4.3 실험 결과

IoT 네트워크 환경에서 BoT-IoT 공격을 탐지하기 위하여 KNN, Decision Tree, Naïve Bayes, Random Forest 알고리즘을 적용하였다.

전반적으로 KNN 알고리즘의 성능이 가장 높고, Naive Bayes 알고리즘이 가장 좋지 않은 것으로 나타났다.

Table 4는 각 알고리즘에서 트래픽을 검출하는 정확도를 나타낸 것이다. Table 4에서 보는 바와 같이 KNN이 DDoS, DoS 공격 및 Normal 트래픽을 분류하는 정확도가 가장 높았다. Naïve Bayes는 Normal 트래픽은 거의 탐지를 못하는 반면, Data theft 공격은 100% 탐지하였다.

Table 5은 각 알고리즘에서의 정밀도를 나타낸 것이다. Table 5에서 보면, KNN과 Random Forest의 성능이 대체로 높다. DDoS와 DoS 공격에 대한 성능은 KNN이 더 좋고, Normal과 Data theft 공격에 대해서는 Random Forest의 성능이 더 높다. Naïve Bayes는 Normal 트래픽을 포함한 대부분의 공격 유형에 대한 정밀도가 대체로 낮지만, Dos 공격에 대한 정밀도는 다른

알고리즘들보다 높았다.

Table 6은 각 알고리즘에서의 재현율을 나타낸 것이다. Table 6에서 보면, KNN이 DDoS, DoS 공격 및 Normal 트래픽에 대한 성능이 가장 높았고, Random Forest 또한 성능이 좋은 것으로 나타났다.

Table 7은 각 알고리즘에서의 f1-score을 나타낸 것이다. Table 7에서 보면, KNN이 DDoS, DoS, Reconnaissance 공격에 대한 성능이 가장 높았고, Random Forest도 Reconnaissance 공격의 탐지 성능이 좋은 것으로 나타났다.

Table 4. Accuracy Results

Category	KNN	Decision Tree	Naive Baye's	Random Forest
DDoS	99.14	89.88	98.75	97.56
DoS	99.11	78.44	40.53	97.58
Reconnaissance	99.43	99.68	88.84	99.44
Normal	96.26	92.52	3.74	92.52
Data theft	92.86	92.86	100.00	92.86

Table 5. Precision Results

Category	KNN	Decision Tree	Naive Baye's	Random Forest
DDoS	99.00	83.00	67.00	98.00
DoS	99.00	95.00	99.00	97.00
Reconnaissance	100.00	40.00	58.00	100.00
Normal	94.00	86.00	12.00	99.00
Data theft	93.00	100.00	25.00	100.00

Table 6. Recall Results

Category	KNN	Decision Tree	Naive Baye's	Random Forest
DDoS	99.00	90.00	99.00	98.00
DoS	99.00	78.00	41.00	98.00
Reconnaissance	99.00	100.00	89.00	99.00
Normal	96.00	90.00	4.00	93.00
Data theft	93.00	93.00	100.00	93.00

Table 7. f1-score Results

Category	KNN	Decision Tree	Naive Baye's	Random Forest
DDoS	99.00	87.00	80.00	98.00
DoS	99.00	86.00	58.00	97.00
Reconnaissance	100.00	57.00	70.00	100.00
Normal	95.00	88.00	6.00	96.00
Data theft	93.00	96.00	40.00	93.00

5. 결론 및 향후 연구

본 논문에서는 IoT 네트워크 환경에서 봇넷 공격을 탐지하기 위하여, IoT 네트워크 환경에서 수집된 BoT-IoT 데이터셋을 기반으로 KNN, Decision Tree, Naïve Bayes, Random Forest 알고리즘으로 성능을 측정하였다.

효과적인 탐지를 위하여 데이터 전처리로 상관 계수와 엔트로피를 이용하여 10개의 특성을 추출하였고, 최대-최소 정규화를 실시하였다. 그 후 정확도, 정밀도, 재현율, f1-score로 알고리즘의 성능을 평가한 결과 KNN 알고리즘이 가장 성능이 좋은 것으로 나타났다. 특히 DDoS, DoS, Data theft에 대한 탐지 성능이 99% 이상인 것으로 확인하였다. 그 외 Normal 트래픽과 Data theft 공격에 대한 탐지 성능이 다소 낮게 나타난 측면이 있는데 이는 희소 클래스의 문제라고 볼 수 있다.

따라서 향후 클래스 불균형 문제를 해결하기 위한 데이터 전처리 부분 및 더 적은 특성들로 더 좋은 탐지 효과를 얻을 수 있도록 다양한 특성 추출법을 시도하여 탐지 성능을 높여 나갈 예정이다.

REFERENCES

[1] Cisco. (2018). Cisco Cisco Visual NetworkingIndex: Forecast and Trends, 2017-2022

[2] Yang, Y. M., Park, S. T., & Kim, Y. M. (2020). A Study on Reinforcing Non-Identifying Personal Sensitive Information Management on IoT Environment. *The Journal of the Korea Contents Association, 20(8),* 34-41.

[3] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy & H. Ming. (2019). "AD-IoT: Anomaly Detection of IoT Cyberattacks in Smart City Using Machine Learning" *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 305-310. DOI: 10.1109/CCWC.2019.8666450

[4] T. Greene. (2016). *IT WORLD. https:// www.itworld.co.kr/news/101726*

[5] S. Pokhrel, R. Abbas & Bhulok Aryal.(2021). IoT Security: Botnet detection in IoT using Machine learning. arXiv:2104.02231

[6] L. Xiao, X. Wan, X. Lu, Y. Zhang & Di Wu. (2018). IoT Security Techniques Based on Machine Learning. *IEEE Signal Processing Magazine Sept.* 41 - 49, DOI: 10.1109/MSP.2018.2825478

[7] N. Koroniotis, N. Moustafa1, E. Sitnikova & J. Slay. (2017). Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on

Machine Learning Techniques. *International Conference on Mobile Networks and Management*, 30-44. DOI: 10.1007/978-3-319-90775-8_3

[8] S.S-Khah, P.F Marteau, N. Béchet. (2017). Intrusion detection in network systems through hybrid supervised and unsupervised mining process-a detailed case study on the ISCX benchmark dataset. Data Intelligence and Security (ICDIS). DOI: 10.1109/ICDIS.2018.00043

[9] Hayretdin Bahsi, Sven Nomm, Fabio Benedetto & La Torre.(2018). Dimensionality Reduction for Machine Learning Based IoT Botnet Detection. *15th International Conference ICARCV Singapore, November*. DOI: 10.1109/ICARCV.2018.8581205

[10] M. Zolanvari, M.A. Teixeira, L. Gupta ,K.M. Khan, & R.Jain. (2019) Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE Internet of Things Journal Volume: 6.* DOI: 10.1109/JIOT.2019. 2912022

[11] M. Shafiq, Z. Tian, A.K. Bashir & X. Du. (2020). CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques. *IEEE Internet of Things Journal Volume: 8*, DOI: 10.1109/JIOT.2020.3002 255

[12] R. Sommer & V. Paxson.(2010). Outside the Closed World: On Using Machine Learning For Network Intrusion Detection. *IEEE Symposium on Security and Privacy, IEEE*, 305-316. DOI:10.1109/SP. *Computer Systems 100* ,779-796. https://doi.org/10.1016/ j.future. 2019.05.041

[13] I. Sharafaldin, A. H Lashkari & A. Ghorbani.(2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. *In Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 108-116. DOI: 10.5220/0006639801080116

[14] K. Nickolaos, N. Moustafa, E. Sitnikova, & B. Turnbull. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics Bot-Iot dataset. *Future Generation*

[15] M. H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita. (2015). Towards generating reallife datasets for network intrusion detection, *IJ Network Security 17(6)*. 675-693.

[16] N. . Moustafa, J. Slay. (2015). Unsw-nb15: a comprehensive data set for network intrusion detection systems(unsw-nb15 network data set), *Military Communications and Information Systems Conference (MilCIS), IEEE*, pp. 1-6. DOI: 10.1109/MilCIS.2015. 7348942

[17] A. Ammar.(2015) A decision tree classifier for intrusion detection priority tagging, *Journal of Computer and Communications 3(4)* 52-58, DOI:10.4236/ jcc.2015. 34006

[18] The BoT-IoT Dataset https://cloudstor.aarnet.edu.au/ plus/s/umT99TnxvbpkkoE?path=%2FCSV

현 미 진(Mi-Jin Hyun) [정회원]

· 1997년 2월 : 경남대학교 전산통계학과(이학사)
· 1999년 2월 : 경남대학교 컴퓨터공학부(공학석사)
· 2020년 4월 ~ 현재 : 경남대학교 교양융합대학 조교수
· 관심분야 : 통계, 데이터사이언스
· E-Mail : idream@kyungnam.ac.kr