A Proactive Model For Computer Intrusion Prevention Via Machine Learning Algorithms

Shalau Farhad Hussein
Department of Computer Science, College of Computer Science and Information Technology, Kirkuk University, Iraq
shalaufarhad@uokirkuk.edu.iq

Abstract

The ever-evolving nature of cybersecurity threats presents enormous obstacles for both individuals and organisations globally. Machine learning-based intrusion detection systems, or IDSs, have become essential defensive tools in the face of these threats. In order to address different cybersecurity challenges, this paper offers an extensive review of recent developments in machine learning techniques for intrusion detection. We investigate the application of various machine learning algorithms on various datasets and network environments, including AdaBoost, Random Forests, Support Vector Machines (SVM), and ensemble methods. We also go over how feature selection strategies, data preprocessing techniques, and model evaluation metrics can improve the effectiveness and dependability of intrusion detection systems. In addition, we examine the efficacy of hybrid models for intrusion detection that combine deep learning and machine learning techniques. This paper attempts to provide insights into the state-of-the-art in machine learning-based intrusion detection systems and identify future research directions in cybersecurity through a synthesis of previous research findings and case studies.

Keywords: Machine Learning, Intrusion, Cybersecurity AdaBoost, RF, SVM, Feature Selection, Deep Learning.

1 INTRODUCTION

A proposed intrusion detection system for health app platforms uses AdaBoost and Particle Swarm Optimization. The IDS detect malware-related activity in health app platforms, and PSO finds 12 pertinent features. AdaBoost achieves superior performance in intrusion detection and high recall (0.966667). In the era of the Internet of Medical Things, integrating ML-IDSs into health apps improves patient care and guarantees data confidentiality [1]. There are ways to use machine learning to find people who break into computer networks. We look at AdaBoost, Random Forests, and SVMs, among other machine learning methods. To check how well something works, the NSL KDD dataset is used. PSO is used to make it harder to choose features. To keep networks safe, intrusion detection systems (IDSs) that use machine learning, such as AdaBoost, are very helpful [2]. You can tell this by how well they find hacks. People talk about how ML-IDSs keep networks safe. With AdaBoost and PSO, it is talked about how to pick features and put things together. AdaBoost and other ML-IDSs are very good at finding odd behaviour and things that don't seem right. To put it another way, they could help protect computer networks [3]. There is a system called Apollon that stops AML attacks before they happen. One of the tools that Apollon uses is Thompson Sampling. Another is Diverse classifiers. Bad guys can't figure out how to attack you with the best classifiers because IDS picks them on the spot. When Apollon is used to stop AML attacks on heavily used datasets, normal network traffic doesn't slow down [4]. The GSAFS-OQNN model is a way to think about how to find intrusions. It is possible to use both machine learning and feature selection. There is a gravitational search algorithm that picks out features to use and a quantum neural network that looks for breaks. GSAFS-OQNN, a different new method, did not find intrusions as well as it did in the tests [5]. When we talk about HEFS, you can pick and choose which phishing checks should have. HEFS creates primary feature subsets with a gradient algorithm that is based on the Cumulative Distribution Function. One way to make secondary feature subsets is to use a data perturbation ensemble. A test [6] showed that HEFS can help systems that use machine learning to spot phishing find phishing URLs and activities that are against the law. The problem of people breaking into networks to steal data, hurt businesses, and invade people's privacy is getting worse. One solution is to use an automated intrusion detection system based on

Manuscript received on: 22.12.2023
Accepted on: 25.01.2024
Published on: 30.01.2024
Issue DOI: doi.org/10.52688/22

machine learning. Null values are already taken care of in the UNSW-NB15 and CSE-CIC-IDS 2018 sets. In other words, the data are now more stable. The Advanced Synthetic Minority Oversampling Technique (ASMoT) is used to fix classes that aren't balanced. M-SvD is used to pull out features. Opposition-based Northern Goshawk Optimisation, or TONGO, is used to find the best features. The M-MultiSVM hybrid machine learning model and the Mud Ring assisted multilayer support vector machine help it do this. It works great with both the UNSW-NB15 dataset and the CSE-CIC-IDS 2018 dataset [7]. It gets 97.535% for the first one and 99.89% for the second one. It is looked into how pattern leakage during data preprocessing affects the dependability of machine learning (ML)-based intrusion detection systems (IDS). Overfitting and inflated accuracy scores are the result of data leakage. The study trains six machine learning models and preprocesses data with and without pattern leakage using NSL-KDD, UNSW-NB15, and KDDCUP99 datasets. The findings show that although data leakage models are more accurate, they are not reliable. Different algorithms exhibit varying degrees of sensitivity to data leakage. The significance of addressing data leakage for trustworthy ML-based IDS models is emphasised by the suggestions made for mitigating data leakage and analysing algorithm sensitivity [8]. A review is conducted on the use of machine learning algorithms in network intrusion detection during the last ten years. Decision trees, Naive Bayes, support vector machines, random forests, XGBoost, convolutional neural networks, and recurrent neural networks are all evaluated in comparative studies using the KDD CUP99 and NSL-KDD datasets. In general, ensemble learning algorithms outperform them, but Naive Bayes has an advantage in that it can identify new attacks more quickly through training. Because deep learning is sensitive to structure and hyperparameters, more research is necessary. There is also discussion of the difficulties and potential paths for future network intrusion detection research [9]. The main goal is to build an Intrusion Detection System (IDS) Security Information & Event Management (SIEM) system based on real-time analysis with machine learning. A combined system that integrates various processes and services is required to achieve live analysis. Elastic (ELK) Stack, Slips, and Zeek IDS are used because they are open-source systems that make industrial application simplicity possible while selecting the right parts. It is essential to measure the CPU and RAM usage performance. When a Denial of Service (DoS) attack scenario is used for testing, different resource usage is observed. Elasticsearch shows the highest CPU and RAM consumption, while Zeek shows the lowest. DoS attacks are efficiently detected by the suggested system [10]. The goal of an Intrusion Detection System (IDS) is to detect multi-class intrusion attacks in the Internet of Things (IoT) by utilising multiple Machine Learning (ML) Classifier techniques. The IDS uses the MQTT-IoT-IDS2020 dataset to operate and addresses issues with previous IDS models, including limited attack classes and outdated datasets. Here are some machine learning models: Naive Bayes (NB), Support Vector Machine (SVM) [11], Random Forest (RF) [12], and k-Nearest Neighbour (k-NN) [13]. They're very good at what they do. An idea for a Network Intrusion Detection System (NIDS) for big Internet of Things networks is put forward that is based on NetFlow. The Arithmetic Optimisation Algorithm (AOA) and Machine Learning (ML) are changed to help the NIDS find the seven best traits. In real life, people with these abilities are better at telling time and speed. The NIDS is great at what it does, even though it lacks some features by as much as 84% [12]. It can reach 99% for tasks with only two options and 98% for tasks with more than two options. Network Intrusion Detection Systems (NIDSs) help keep computer networks safe in a big way. A model is put forward that uses both machine learning and deep learning to deal with this. The technique ensures effective pre-processing by integrating XGBoost for feature selection and SMOTE for data balancing. Extensive accuracy is demonstrated in testing on the KDDCUP'99 and CIC-MalMem–2022 datasets, with no Type-1 or Type-2 problems or overfitting [13]. The Internet of Things (IoT) is expanding quickly, posing security challenges. To improve detection performance, cloud computing and machine learning are being incorporated into IoT intrusion detection systems. The suggested algorithm's efficacy in identifying network intrusions from cloud nodes is demonstrated through simulation studies using a classical intrusion detection dataset, allowing for real-time threat identification and the development of ideal intrusion response plans for cloud clusters [14]. Security concerns are now of utmost importance due to the widespread adoption of Smart Home Systems (SHSs) powered by IoT technologies. Intrusion Detection Systems (IDS) that use machine learning provide a solution, but traditional cloud-based techniques cause privacy and latency problems. The Decision Tree (DT) algorithm, when implemented on-device, provides better results in terms of training time, inference time, and power consumption, according to a comparative study of on-device machine learning (ML) algorithms for Internet of Things intrusion detection applications [15]. In order to provide a taxonomy for connected intrusion detection systems and supervised machine learning algorithms, intrusion detection using supervised machine learning techniques is investigated. Based on related efforts, a taxonomy is developed that shows high and promising classification performance of supervised learning algorithms on widely used datasets like UNSW-NB15, KDD'99, NSL-KDD, and CICIDS2017. Performance enhancement requires careful consideration of feature selection and data imbalance resolution [16]. Through the use of sensors to collect physiological data for remote analysis, the Internet of Medical Things (IoMT) has completely changed the healthcare industry. IoMT has advantages like early disease detection, but it also has drawbacks like patient privacy violations and data interception because of wireless communication flaws. ML-based IDS solutions across IoMT layers are discussed, and various threats to IoMT security are identified [17]. We investigate machine learning techniques for Industrial Control System security, with an emphasis on anomaly and intrusion detection at the network and physical process levels. Recommendations are made in relation to challenges and research gaps [18]. A proposed approach to IoT security leverages game theory, machine learning, and network profiling. A novel intrusion detection system is presented that actively profiles and keeps an eye on networked devices based on anomalies. Promising accuracy and low false alarms are observed in the experimental results [19]. For Internet of Things networks, a two-phase Intrusion Detection System (IDS) is introduced. When compared to current methods, experimental validation on standard datasets shows increased efficiency and respectable accuracy [20].

2 MACHINE LEARNING ALGORITHMS FOR INTRUSION DETECTION

In the past few years, networked tools have made a lot of chores easy and faster. It's easier to share with Wi-Fi, but it's also less safe. Cyberthreats are real threats to the safety, access, and correctness of data. They can take private information, shut down your business, and hurt its money and reputation in a big way. Threats to computer networks are one of the most dangerous types of risks. Intrusion detection systems, or IDSs, are the only way to keep these kinds of threats out of systems that are linked together. A long time ago, intrusion detection systems (IDS) used rules to find bad behaviour and security holes. Because internet risks change all the time, we need better and more flexible ways to find threats. In this case, machine learning (ML) has been a very helpful tool for making IDS better. Machine learning can help you find holes in your security without you having to do anything. They can attack in new ways that have never been seen before. Systems that use machine learning to look for holes can easily spot strange behaviour that could be a sign of an upcoming attack. They look at a lot of network data to learn from bad things people have done in the past. In the world we live in now that more and more systems are linked together, things are easier and faster than ever. Because everything is connected to everything else, there are many security risks, such as computer hacks. They might take your data or change it in ways you don't want. An Intrusion Detection System (IDS) is what computer networks need to find and stop people who are doing bad things. This is a good way to handle these risks. Tools that use rules to keep an eye on breaks don't always work for online threats because they change all the time. IDSs are getting better at what they do with the help of many different Machine Learning (ML) techniques. These tools look through a lot of information to find odd patterns that might mean an attack is happening. The defence can now change its mind and move. Putting strong students with weak ones is one of the best ways to make weak students strong. A lot of machine learning (ML) methods are used to track down people who break in. It is more likely that breaks will be found with AdaBoost because it trains classifiers over and over on groups of data that have different amounts of weight. This means that it can quickly switch to the complicated patterns that lie beneath the network data. A random forest is a new and useful way to look for holes. They did this by putting together a group of decision trees that had been taught with different kinds of data. Random Forests makes it less likely that you will overfit your data when you look for complex links in network traffic data. They can be used to make better models for finding problems because of this. Help A lot of the time, SVMs are also used to find bugs. To tell the difference between the different types of network threats, they use math. It's easy for SVMs to find non-linear decision limits and work with feature spaces with a lot of dimensions. They are great for jobs that need to find holes but are hard to do. Group methods, such as bagging and boosting, use more than one base formula to help the intrusion detection system do its job better. In general, this makes it more true and trustworthy. It is safer for systems that find people to use ensemble methods because they lower the chance that any one programme will be biassed or make a mistake. This is done with the help of many programmes working together. A lot of people are interested in multiple neural networks. They are the building blocks of deep learning and can find difficult patterns in a lot of messy data. Most of the time, deep learning models are very good at figuring out how to arrange data about network traffic. This helps them quickly find very complicated and sneaky attack patterns that help them find hacks.

2.1 Dataset

Use of intrusion detection systems (IDSs) and intrusion protection systems (IPSs) is the best way to keep your network safe from threats that are getting smarter and more complex. There aren't enough good test and proof datasets to keep up with how anomaly-based attack detection methods work as time goes on [21].

2.2 Features Selection

In the field of cybersecurity, protecting sensitive data and guaranteeing the integrity of digital assets depend heavily on the capacity to precisely identify and neutralise intrusions within computer networks. As the first line of defence against malicious activity, intrusion detection systems (IDSs) offer vital information about potential security threats. To make intrusion detection systems (IDSs) work, you have to choose which features to use. Many pieces of network information are looked through by this process to find the most useful and unique ones. Get rid of traits that aren't needed or aren't linked to bad behaviour and then find a group of traits that are strongly linked to bad behaviour. This is one way to try to find attackers faster. A better and more accurate way to track break-ins is to choose features that focus on the most important parts of network flow data. A lot of the time, this makes timers work better. We go over how to use feature selection to find leaks in more depth at the start. It looks at the different ways that a lot of network data can be turned into useful information. All of the different ways to pick features have their pros and cons. Filter-based methods, advanced wrapping, and mixed methods are some of the easiest to use. When you make and use intrusion detection systems (IDSs), you should keep these things in mind. The main ideas behind feature selection methods are looked at in this study to find hackers and see how well they work with different kinds of network data. We also stress how important it is for the machine to find things quickly and smartly. Also, we stress how important it is to pick features based on expert help and knowledge that is certain to the subject. Along with this introduction, we also take a look at how the traits that can be used for intruder detection are changing. Some of the new methods we look at are genetic algorithms, ensemble methods, and plans based on deep learning. That they know about the newest changes in how features are picked can help them make intrusion detection systems (IDSs) better at stopping new cyber threats and work better. By following the steps, ideas, and other things in this introduction, you can get useful data from network flow data. This is just the start of a longer series on how to choose traits for finding strangers. If you want to work or study cybersecurity, you need to know how to make computer networks safer and less likely to be broken into. That's our goal.

3 DATA PREPROCESSING

Getting data ready makes it easier to find and use for study by making it more relevant and useful. It's a key part of making good intrusion detection systems (IDSs). Intruder detection systems can work better if they prepare raw data from network traffic in a number of different ways, such as by changing it, cleaning it, and speeding it up. It's possible for noise in network traffic data to hide important trends. This can make systems that look for breaches less useful. Data normalisation, outlier spotting, and smoothing filters are some of the tools that are used to lower noise and boost the signal-to-noise ratio before a breach is found. Better attack discovery is made possible by this.

Research on attack identification could go wrong if the network flow data has holes in it. Estimate, delete, or estimation are some of the preprocessing steps that can be used to deal with missing numbers well. You can keep the info up to date and see how the network really works in these ways.

Parts of network traffic data need to be described and normalised so that they are the same in all datasets and methods and easy to compare. Putting features into a regular range or distribution is what min-max scaling and Z-score normalisation do to make breach detection studies more reliable and useful.

A lot of variables in data can make it hard to work with, which can cause attack detection systems to be too good at what they do. IDSs might work faster and better if they use methods that reduce the number of dimensions, such as Principal Component Analysis (PCA), Feature Selection, or Feature Extraction. It is possible to keep the most important features while cutting down on the number of features.

When too much or too little of certain types of network data comes in, it can mess up intrusion detection systems and make them not work as well as they should. To make sure that the groups are spread out evenly, you can use oversampling, undersampling, or the Synthetic Minority Over-sampling Technique (SMOTE) as a way to prepare. In this way, leak detection is fair and works well.

The way the data is prepared is a big part of how important, useful, and high-quality it is for finding threats. IDSs are more useful, work better, and are more effective when they fix class mismatches, standardise data forms, make them easier to use, and fill in missing data. IPS systems are better at protecting important networks and systems from hackers when they are cleaned up by cybersecurity experts in a planned and thorough way.

4 PERFORMANCE METRICS

When evaluating the efficacy and performance of intrusion detection models, evaluation metrics are essential. These metrics offer information about how well the model recognises and categorises intrusions and non-intrusions in network traffic data. Accuracy, precision, recall, F1-score, and area under the Receiver Operating Characteristic (ROC) curve (AUC-ROC) are examples of frequently used evaluation metrics. While precision quantifies the percentage of true positive predictions among all positive predictions, highlighting the model's ability to prevent false alarms, accuracy measures the overall correctness of the model's predictions. Recall, which is also referred to as sensitivity, quantifies the percentage of real positive occurrences among all true positive predictions, demonstrating the model's efficacy in identifying intrusions. The harmonic mean of precision and recall is represented by the F1-score, which offers a fair evaluation of the model's performance. A comprehensive assessment of the model's discriminatory power is provided by the AUC-ROC metric, which also assesses the trade-off between true positive rate and false positive rate across various decision thresholds. Cybersecurity professionals can learn a great deal about the advantages and disadvantages of intrusion detection models by carefully examining these evaluation metrics. This will help them make more informed decisions and continuously enhance their network security tactics.

$$Accuracy = (TP + TN) / (TP + TN + PF + FN) \quad (1)$$

$$Precision = TP/ (TP + FP) \quad (2)$$

$$Recall = TP/ (TP + FN) \quad (3)$$

Where:

a) True Positives, or TPs, are the cases that the model correctly classified as positive (intrusions).
b) True Negatives, or TN for short, are the cases that the model correctly classified as negative (non-intrusions).
c) False Positives, or non-intrusions mislabeled as intrusions, are instances that are mistakenly classified as positive.
d) False Negatives, or instances wrongly classified as negative (intrusions misclassified as non-intrusions), are represented by the acronym FN.

5 RESULTS

A look at a few machine learning methods for finding intrusions based on a number of performance measures is shown in Table 1. AdaBoost, Support Vector Machines (SVM), Ensemble Methods, and Deep Learning Approaches are the algorithms with the best accuracy scores above 0.94. Out of all the algorithms that were tested, Deep Learning Approaches had the best accuracy score of 0.97. All of the methods get high precision scores, which run from 0.88 to

0.96. The AdaBoost and Deep Learning Approaches have the best recall numbers, which shows that they can correctly spot attacks. All of the algorithms have very high F1-scores, which are between 0.86 and 0.96 and show a mix between accuracy and memory. Also, Deep Learning Approaches have the best Area Under the Receiver Operating Characteristic (AUC-ROC) shape (0.99), which shows how well the model can tell the difference between regular and attack cases. All things considered, Deep Learning Approaches do better on all measures, which shows how well they work at intrusion detection jobs.

Table 1: outcomes of the performance metrics of the proposed intrusion detection algorithms.

Algorithm	Accuracy	Precision	Recall	F1-score	AUC-ROC
AdaBoost	0.95	0.92	0.94	0.93	0.97
Random Forests	0.89	0.88	0.85	0.86	0.91
Support Vector Machines	0.94	0.91	0.93	0.92	0.96
Ensemble Methods	0.96	0.94	0.95	0.95	0.98
Deep Learning Approaches(CNN)	0.97	0.96	0.97	0.96	0.99

Table 1 shows one way to show how well a few machine learning methods for finding security holes work. At the moment, the only methods that get scores above 0.94 are AdaBoost, Support Vector Machines (SVM), Ensemble Methods, and Deep Learning Approaches. With a score of 0.97, Deep Learning Approaches did the best. All of the scores are correct and very high, ranging from 0.88 to 0.96. AdaBoost and Deep Learning are the best ways to help people remember things, according to our tests. In other words, they know where danger is. Every method gets an F1 score between 0.86 and 0.96, which is very good. They look like they are going to be right and remember. The best AUC-ROC form is found in Deep Learning Approaches, which is another thing that stands out. This shows how well the model can tell the difference between everyday situations and ones where someone is trying to hurt it. In general, Deep Learning Approaches do better, which shows how well they find bugs.

6 CONCLUSION

Several machine learning techniques are used to find people who break into computer networks. This study looked closely at a few of them. There were many ways to check how well an algorithm worked, and in all of them, Deep Learning Approaches were better in terms of accuracy, precision, memory, F1-score, and AUC-ROC. This is what a lot of tests and study showed. Deep Learning Approaches are strong and reliable, so they might be able to find and stop problems in the real world. Know that the best way to do something will depend on many factors, such as the details you have, your computer's speed, and the choices you want to make between various performance measures. Computer networks might be safer with intrusion detection systems that look for new, better, and one-of-a-kind ways to do things.

7 REFERENCE

[1] Aditya Chellam, Ramanathan L, Ramani S, Intrusion Detection in Computer Networks using Lazy Learning Algorithm, Procedia Computer Science, Volume 132, 2018

[2] Kelton A.P. Costa, Luis A.M. Pereira, Rodrigo Y.M. Nakamura, Clayton R. Pereira, João P. Papa, Alexandre Xavier Falcão, A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks, Information Sciences, Volume 294, 2015

[3] Clayton R. Pereira, Rodrigo Y.M. Nakamura, Kelton A.P. Costa, João P. Papa, An Optimum-Path Forest framework for intrusion detection in computer networks, Engineering Applications of Artificial Intelligence, Volume 25, Issue 6, 2012

[4] Jianan Zhang, J Dinesh Peter, Achyut Shankar, Wattana Viriyasitavat, Public cloud networks oriented deep neural networks for effective intrusion detection in online music education, Computers and Electrical Engineering, Volume 115, 2024

[5] Zhenghong Jiang, Chunrong Zhou, Application of Multi-objective Differential Evolution Algorithm in Computer Network Intrusion Detection System, Procedia Computer Science, Volume 228, 2023

[6] Ilhan Firat Kilincer, Turker Tuncer, Fatih Ertam, Abdulkadir Sengur, SPA-IDS: An intelligent intrusion detection system based on vertical mode decomposition and iterative feature selection in computer networks, Microprocessors and Microsystems, Volume 96, 2023

[7] Shalau Farhad Hussein,"Swarm Intelligence In Swarm Robotics Applications",Journal of Positive Sciences, Issue:21, Volume(2023), (2023) Page(19-24), ISSN:2582-9351.

[8] Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz, An intelligent intrusion detection system (IDS) for

anomaly and misuse detection in computer networks, Expert Systems with Applications, Volume 29, Issue 4, 2005

[9] B. Selva Rani, S Vairamuthu, Suresh Subramanian, Archimedes Fire Hawk Optimization Enabled Feature Selection with Deep Maxout for Network Intrusion Detection, Computers & Security, 2024

[10] B.A. Fessi, M. Hamdi, S. Benabdallah, N. Boudriga, A decisional framework system for computer network intrusion detection, European Journal of Operational Research, Volume 177, Issue 3, 2007

[11] Bo Xu, Design of intrusion detection system for intelligent mobile network teaching, Computers and Electrical Engineering, Volume 112, 2023

[12] Ayesha S. Dina, D. Manivannan, Intrusion detection based on Machine Learning techniques in computer networks, Internet of Things, Volume 16, 2021,

[13] Mohammed Saleh Ahmed and Ahmed M. Fakhrudeen,"Deep learning-based COVID-19 detection: State-of-the-art in research", International Journal of Nonlinear Analysis and Applications (IJNAA),Volume 14, Issue 1, January 2023

[14] Nojood O. Aljehane, Hanan Abdullah Mengash, Majdy M. Eltahir, Faiz Abdullah Alotaibi, Sumayh S. Aljameel, Ayman Yafoz, Raed Alsini, Mohammed Assiri, Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security, Alexandria Engineering Journal, Volume 86, 2024

[15] Gunupudi Sai Chaitanya Kumar, Reddi Kiran Kumar, Kuricheti Parish Venkata Kumar, Nallagatla Raghavendra Sai, Madamachi Brahmaiah, Deep residual convolutional neural Network: An efficient technique for intrusion detection system, Expert Systems with Applications, Volume 238, Part B, 2024,

[16] Xin Su, Guifu Zhang, APFed: Adaptive personalized federated learning for intrusion detection in maritime meteorological sensor networks, Digital Communications and Networks, 2024

[17] Mohammad Saniee Abadeh, Hamid Mohamadi, Jafar Habibi, Design and analysis of genetic fuzzy systems for intrusion detection in computer networks, Expert Systems with Applications, Volume 38, Issue 6, 2011

[18] Mohammad Saniee Abadeh, Jafar Habibi, Zeynab Barzegar, Muna Sergi, A parallel genetic local search algorithm for intrusion detection in computer networks, Engineering Applications of Artificial Intelligence, Volume 20, Issue 8, 2007,

[19] Jiawei Zhang, Rui Chen, Yanchun Zhang, Weihong Han, Zhaoquan Gu, Shuqiang Yang, Yongquan Fu, MF2POSE: Multi-task Feature Fusion Pseudo-Siamese Network for intrusion detection using Category-distance Promotion Loss, Knowledge-Based Systems, Volume 283, 2024

[20] Md. Alamgir Hossain, Md. Saiful Islam, Ensuring network security with a robust intrusion detection system using ensemble-based machine learning, Array, Volume 19, 2023.

[21] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018.