International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 04 | Apr 2023 www.irjet.net p-ISSN: 2395-0072

Application of neural network and PSO-SVM in intrusion detection of network

Gopika S[1], Samitha T[2]

[1]Dept. of Electronics and Communication Engineering, Mahaguru Institute of Technology, Kerala
[2]Asst. Professor, Dept. of Electronics and Communication Engineering, Mahaguru Institute of Technology, Kerala

---

Abstract – *Imbalanced network traffic can often be a gateway for malicious cyber-attacks to penetrate networks and go undetected. In these situations, it is challenging for Network Intrusion Detection System (NIDS) to find the attacker since they can blend in with a lot of normal data. An intrusion detection system (IDS) monitors network traffic for suspicious activities and immediately provides notifications if it detects anything suspicious. The IDS looks for any activity that might be a sign of an attack or intrusion by comparing the network activity to a set of predetermined rules and patterns. Even the most sophisticated NIDS may have trouble identifying this type of assault because of its high degree of stealth and obfuscation in cyberspace. A new approach based on deep learning and machine learning using NSL-KDD dataset for intrusion detection is proposed in this paper. The proposed approach uses an SVM classifier for the attack classification task and a 1-Dimensional Convolutional Neural Network for feature extraction.*

Key Words: ***Machine learning, Deep learning, Convolutional Neural Network (CNN), Support Vector Machine (SVM), Particle Swarm Optimization (PSO)***

1. INTRODUCTION

Cybersecurity faces tremendous risks as a result of the rapid advancement of technologies like 5G, IoT, cloud computing, and others that have increased network scale, real-time traffic, and cyberattack complexity and diversity [1][2]. Security breaches might sneak in with a lot of regular traffic. As a result, it is simple to misclassify because the machine learning algorithm cannot fully learn the distribution of some categories. Most of the newly generated cyber-attacks are created by subtly altering already known ones, which is typically handled as regular traffic on the IoT network [3].

To find unusual or hostile activity in the network, a system called Network Intrusion Detection System (NIDS) is utilized. IDS keeps an eye out for harmful activity in network traffic. There are numerous ways to identify suspicious activity in network communications. IDS monitors network traffic persistently to look for network intrusions. A recent trend in many security applications is to combine deep learning methodologies with cybersecurity because of their excellent performance. For analysis, the system needs a dataset with past traffic data. The most widely utilized dataset is the publicly accessible NSL-KDD network dataset. It includes data on network traffic with 41 traffic features. A new deep-learning approach for intrusion detection based on the NSL-KDD dataset is presented in this paper. Deep learning and machine learning are the basis of the proposed effort. It applies the Support Vector Machine (SVM) classification algorithm, Convolutional Neural Network (CNN) feature extraction technique, and Particle Swarm Optimization (PSO) SVM algorithm optimization. In Chapter 3, the system description is explained. The experimental result of the system is presented in Chapter 4. The conclusion of the work is given in Chapter 5.

2. LITERATURE REVIEW

A network intrusion system based on Naive Bayes has been suggested in [4]. Across data sets that have been tagged by the services, the framework develops the network service patterns. The naive Bayes Classifier method, together with the built-in patterns, allows the framework to identify attacks in the datasets. This approach has a greater detection rate, requires less time to complete, and is less expensive than the neural network-based approach. However, it produces more false positives than true ones.

When it comes to meeting the demands of contemporary networks, there are questions about the viability and sustainability of current systems. These worries are more directly related to the declining levels of detection accuracy and the rising levels of required human intervention. To address these concerns, a deep learning-based NIDS approach was proposed in [5]. This unique deep-learning classification model was developed using stacked NDAEs.

In order to address the issue of network traffic domain model architecture design, a network architecture search algorithm (NAS) in the field of network traffic together with a surrogate model have been suggested in [6]. Under the premise of a specified optimization target, a neural architecture search (NAS) can automatically search the model's architecture. A surrogate model was used in the network architecture search task to determine how candidate architectures would perform. This approach increases the effectiveness of the architecture search and, to a certain extent, solves the issues of the network search algorithm's need for large computing resources and significant time consumption.

An effective IDS system is introduced in [7] using architectures like Convolutional Neural Networks (CNN) and Long-Short Term Memory (LSTM), Recurrent Neural Networks (RNN), and Gated Recurrent Units (GRU). The system uses a malicious traffic record made up of sequential data over a predetermined time period to construct the IDS. The network activity records that are benign and malicious are divided into categories. To demonstrate the effectiveness of DL techniques, three separate benchmark data sets—UNSW NB15, KDDCup '99, and NSL-KDD—have been used. It has been found that DL methods are compatible with network traffic time-sequence data contained in TCP/IP packet headers.

Unlike supervised and unsupervised learning, a new approach based on reinforcement learning has been proposed in [8]. This approach incorporates the observational power of deep learning with the decision-making power of reinforcement learning to enable the effective detection of various cyberattacks on the Industrial IoT. The approach is designed around GBM's feature selection algorithm, which pulls the most important feature set out of Industrial Internet of Things data. Following that, the PPO2 algorithm uses the hidden layer of the multilayer perception network as the shared network structure for the value network and strategic network in addition to the deep learning algorithm. Using the PPO2 algorithm and ReLU, the intrusion detection model is created (R). 99 percent of various network attacks on the Industrial Internet of Things are detected by the proposed IDS.

3. METHODOLOGY

The proposed Intrusion Detection methodology uses CNN for feature extraction and SVM for classification. A network intrusion detection model based on neural network feature extraction and particle swarm optimization technique to optimize SVM was created to address the issue that it is challenging to extract delicate intrusion attributes during the process of intrusion detection.

3.1 Data Collection

The practice of acquiring and measuring data from various sources is known as data collection. The suggested model makes use of the NSL-KDD dataset. The dataset, which resembles a CPL file, was collected from Kaggle. Figure 1 displays a sample NSL-KDD dataset. The dataset has a total of 42 columns, forty-one of which correspond to the input characteristics and one column for the output label. The 41 features consist of various network parameters, including protocol type, service, flag, source byte, etc. There are 23 network attacks in the NSL-KDD training set. The classifiers won't be skewed toward more frequent reco

duration	protocol_t	service	flag	src_bytes	dst_bytes	land	wrong_fra	urgent	hot	num_faile	logged_in	num_com	root_shell	su_attemp	num_root	num_file_	num_shell	num_acce	num_outb	is_host_lo	is_guest_l	count
0	tcp	ftp_data	SF	491	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
0	udp	other	SF	146	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	13
0	tcp	private	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	123
0	tcp	http	SF	232	8153	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	5
0	tcp	http	SF	199	420	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	30
0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	121
0	tcp	private	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	166
0	tcp	private	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	117
0	tcp	remote_jo	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	270
0	tcp	private	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	133
0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	205
0	tcp	private	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	199
0	tcp	http	SF	287	2251	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3
0	tcp	ftp_data	SF	334	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2
0	tcp	name	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	233
0	tcp	netbios_n	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	96
0	tcp	http	SF	300	13788	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	8
0	icmp	eco_i	SF	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
0	tcp	http	SF	233	616	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3
0	tcp	http	SF	343	1178	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	9
0	tcp	mtp	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	223
0	tcp	private	S0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	280
0	tcp	http	SF	253	11905	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	8
5607	udp	other	SF	147	105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Figure 1; Sample NSL-KDD dataset

rds because repetitive records are excluded from the train se t for NSL -KDD.

3.2 DATA PREPROCESSING

Pre-processing is done to make the data better for processing tasks. Non-numeric attributes are converted to numeric attributes using label encoding. To translate the protocol type, service, and flag columns' symbolic values into numerical values, label encoding is used. The target column must be divided into 5 classes because it has 23 items. The 23 values of the target class is spliced into 5 categories DOS, PROBE, U2R, R2L, and NORMAL.

3.3 Feature selection

By selecting only pertinent data and eliminating data noise, feature selection is a technique for minimizing the number of input variables to the model. It is necessary to identify essential characteristics among all features before performing feature extraction. The correlation coefficient is employed for this. The statistical concept of correlation is frequently used to describe how nearly linear, a connection exists between two variables. The correlation coefficient, which ranges from -1 to 1, represents the degree to which two parameters are linearly connected. With the use of just pertinent data and the elimination of irrelevant data, feature selection is a technique for limiting the input variable for the model. Positive correlation, negative correlation, and zero correlation are the three main types of correlation techniques. The Pearson coefficient spans from -1.0 to +1.0 and is the most often applied correlation coefficient.

3.4 Data Balancing

Following pre-processing and feature selection, the dataset should be subdivided into two groups: training and testing. 80:20 is the ratio that must be followed. In order to balance the training set, SMOTE (Synthetic Minority Oversampling Technique) is applied. In the SMOTE technique, each class

receives an equal amount of data. In the end, a classification model is trained based on the processed training set. SMOTE is a method of oversampling in which artificial samples are produced for the minority class. This method aids in resolving the issue of overfitting brought on by random oversampling. In order to generate artificial data, SMOTE uses the k-nearest neighbor technique.

3.5 Feature extraction

The important features need to be derived from the balanced dataset. The technique of turning raw data into quantifiable features that can be handled while keeping the information in the original data set is known as feature extraction. Convolutional Neural Networks (CNN) are employed in this implementation to extract features. The foundation of a CNN is a convolutional layer. It has a number of filters (or kernels), whose parameters must be learned over the course of training. By summarizing the existence of features in individual feature maps, pooling layers offer a method for down-sampling feature maps. A bias vector is introduced after the input has been multiplied by a weight matrix in a fully connected layer.

3.6 Model development

An unauthorized infiltration into a computer in your company or an address in your designated domain is referred to as a network intrusion. An intrusion may be passive (when access is achieved covertly and unnoticed) or active. There are five categories of network attacks: DoS, PROBE, U2R, R2L, and NORMAL. In a Normal Attack, the player just swings their weapon towards an enemy. A Denial-of-Service (DoS) attack attempts to shut down a computer system or network so that its targeted recipient is unable to access it. DoS attacks achieve this by providing the victim with an excessive amount of traffic or information that causes a failure. Probing attacks are intrusive methods of evading security measures by examining the real silicon architecture of a chip. When an intruding party previously had user-level access to a computer or network, a User-to-Root (U2R) attack allows a non-privileged user to get root access. Attacks called Remote-to-Local (R2L) involve transmitting packets to the target device.

The Support Vector Machine technique is utilized for classification. Here, the Particle Swarm Optimization (PSO) approach is applied to optimize the Support vector machine algorithm. As a result, the PSO-SVM is given the CNN's retrieved features for classification. SVM models can classify incoming text after being given labeled training data sets for each category. They offer greater speed and improved performance with fewer samples (in the thousands). As a result, the approach is excellent for text classification issues. SVM is used to identify a hyperplane in N-dimensional space (where N is the number of attributes) that categorizes the data points with precision. Hyperplanes, which serve as decision boundaries, aid in classifying the data points. Data points on either side of the hyperplane can be classified differently depending on where they reside.

One of the bio-inspired techniques, particle swarm optimization (PSO), is straightforward in its search for the optimum solution in the problem area. PSO is employed to optimize the challenging SVM data. It is a general methodology with three components: Swam (groups of particles), and Particle (smallest element), Optimization (easiest method). It aids in data optimization and produces better outcomes. By evaluating the fresh input with the trained model, classification is accomplished. After passing new input through CNN to extract features, the trained model receives it. Following prediction, it is divided into 5 classes.

4. EXPERIMENTAL RESULTS

The experiment uses 16GB of memory and an AMD R5-4600H processor running at 3GHz to verify the detecting effect of CNN and PSOSVM. VS Code was used to train the model. The NSL-KDD data set is used for this paper's experimental data. A total of 125974 samples, including 100779 training sets and 25194 test sets, were chosen from the NSL-KDD data set.

The proposed network intrusion detection system is a 5-class classification problem. DoS, PROBE, U2R, R2L, and NORMAL are the five classes. The network attack is categorized into one of the five categories using SVM. The system performance is compared with the Xgboost algorithm and the proposed system achieves an accuracy of 97%. Xgboost algorithm obtained 95% accuracy. The classification report, confusion matrix, and ROC curve of the proposed system and Xgboost algorithm for Intrusion detection are shown in Figure 3,4,5,6,7,8. A confusion matrix, sometimes referred to as an error matrix, is a condensed table used to evaluate how well a classification model performs. Count values are used to describe the number of accurate and inaccurate predictions for each class.

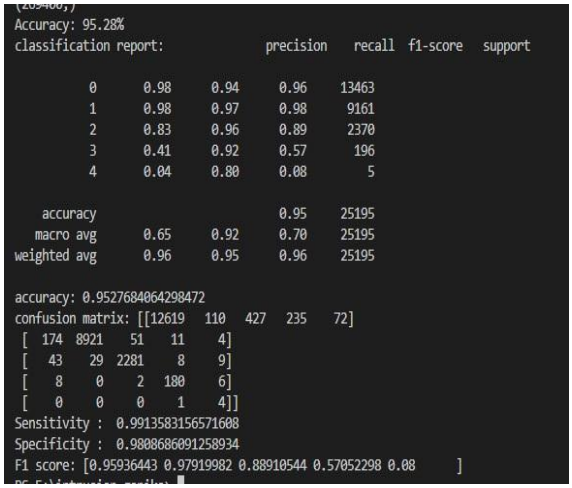

Figure 3: Xgboost algorithm Classification report

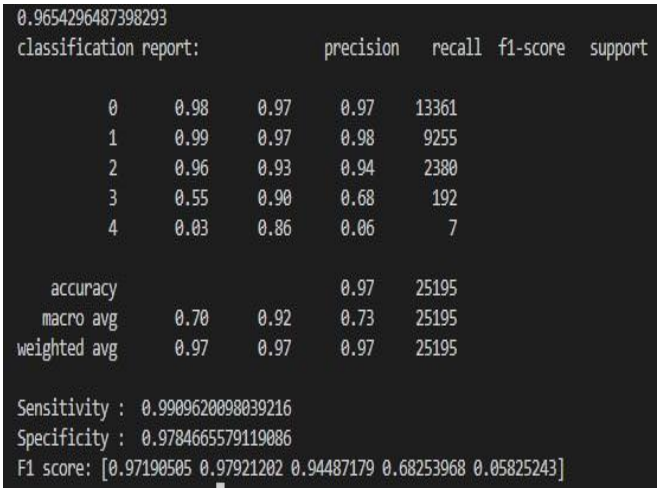

Figure 4: Classification report of the proposed system

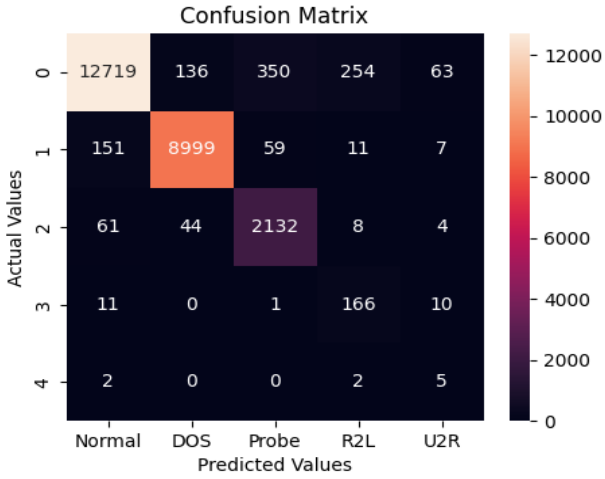

Figure 5: Confusion matrix (Xgboost Algorithm)

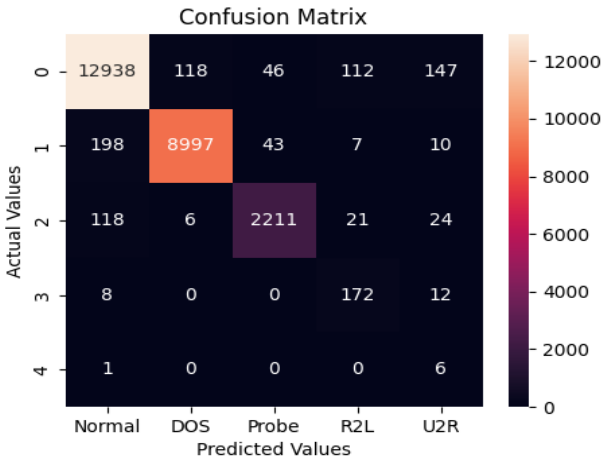

Figure 6: Confusion matrix (Proposed Algorithm)

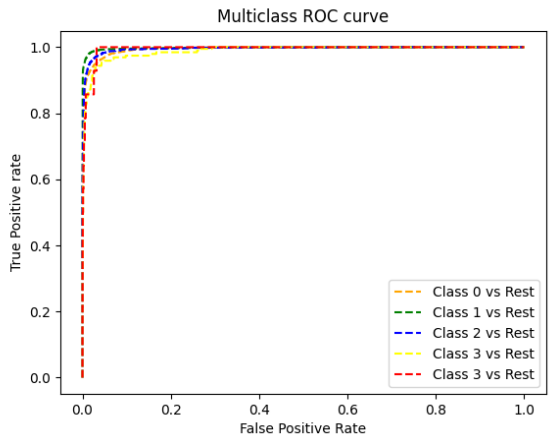

Figure 7: Multiclass ROC curve(Xgboost Algorithm)

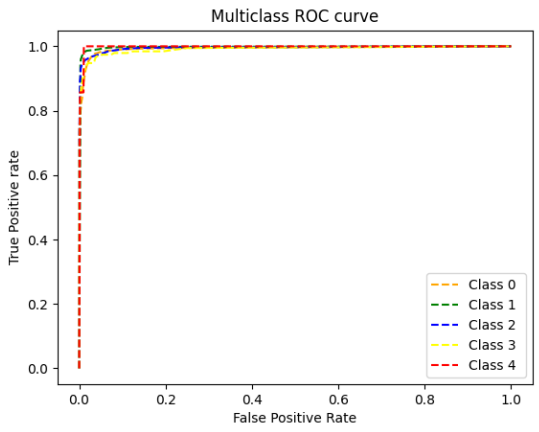

Figure 8: Multiclass ROC curve(Proposed Algorithm)

5. CONCLUSION

Challenges in safe digital data protection and communication arise from the internet's phenomenal growth and usage. Hackers utilize a variety of attacks in today's environment to obtain crucial data. Traditional methods can't handle advanced cyber threats very well. This paper addressed a novel intrusion detection system based on CNN and SVM classifier. Here, CNN has been used for feature extraction and the SVM classifier has been used for categorizing threats into one among the four classes of cyber-attacks named DoS, PROBE, U2R, R2L, and NORMAL. The performance of the proposed system has been compared with the Xgboost algorithm. It has been found that the proposed deep learning and SVM-based system obtains high accuracy of 97% than the Xgboost algorithm-based system.

REFERENCES

[1] Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*. 2020; 10(12):4102. https://doi.org/10.3390/app10124102

[2] Chen B, Qiao S, Zhao J, Liu D, Shi X, Lyu M, Chen H, Lu H, Zhai Y. A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture. IEEE Internet Things J. 2020 Nov 30;8(13):10248-10263. doi: 10.1109/JIOT.2020.3041042. PMID: 35783535; PMCID: PMC8768994.

[3] Abu Al-Haija Q, Zein-Sabatto S. An Efficient Deep-Learning-Based Detection and Classification System for Cyber-Attacks in IoT Communication Networks. *Electronics*. 2020; 9(12):2152. https://doi.org/10.3390/electronics9122152.

[4] Panda, M., & Patra, M. R. (2007). Network intrusion detection using naive bayes. *International journal of computer science and network security*, *7*(12), 258-263.

[5] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, *2*(1), 41-50..

[6] Lyu R, He M, Zhang Y, Jin L, Wang X. Network Intrusion Detection Based on an Efficient Neural Architecture Search. *Symmetry*. 2021; 13(8):1453. https://doi.org/10.3390/sym13081453

[7] Meliboev A, Alikhanov J, Kim W. Performance Evaluation of Deep Learning Based Network Intrusion Detection System across Multiple Balanced and Imbalanced Datasets. *Electronics*. 2022; 11(4):515. https://doi.org/10.3390/electronics11040515.

[8] Tharewal, S., Ashfaque, M. W., Banu, S. S., Uma, P., Hassen, S. M., & Shabaz, M. (2022). Intrusion detection system for industrial Internet of Things based on deep reinforcement learning. *Wireless Communications and Mobile Computing*, *2022*, 1-8..

[9] Latif, Shahid, Zeba Idrees, Zhuo Zou, and Jawad Ahmad. (2020) "DRaNN: A Deep Random Neural Network Model for Intrusion Detectionin Industrial IoT." 2020 International Conference on UK-China Emerging Technologies (UCET), 1-4. IEEE.

[10] Kasongo, Sydney Mambwe, and Yanxia Sun. (2020) "A deep learning method with wrapper based feature extraction for wireless intrusion detection system." Computers & Security 92: 101752.

[11] Choudhary, Sarika, and Nishtha Kesswani. (2020 "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT." Procedia Computer Science, 167: 1561-1573

[12] Vinayakumar, R., Mamoun Alazab, K. P. Soman, Prabaharan Poornachandran, Ameer Al-Nemrat, and Sitalakshmi Venkatraman. (2019) "Deep Learning Approach for Intelligent Intrusion Detection System." IEEE Access 7: 41525-41550.

[13] Khraisat, A., Gondal, I., Vamplew, P. et al. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecur 2, 20 (2019). https://doi.org/10.1186/s42400-019-0038-7

[14] S. Kumar, S. Gupta and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," in *IEEE Access*, vol. 9, pp. 157761-157779, 2021, doi: 10.1109/ACCESS.2021.3129775.

[15] R. Heady, G. Luger, A. Maccabe and M. Servilla, "The architecture of a network level intrusion detection system", 1990.