Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine Learning Based Intrusion Detection System

Mr. Mahendra S Dalvi[1], Dr. N. R. Wankhade[2]

1PG Student, LGNSCOE, Nashik
Savitribai Phule Pune University (SPPU), Maharashtra, India
dalvimahendra21@gmail.com
2 Dr. (Professor), Computer Engineerin departmentg, LGNSCOE, Nashik
Savitribai Phule Pune University (SPPU), Maharashtra, India
Nileshrw2000@yahoo.com

ARTICLE INFO

Received: 20 Dec 2024

Revised: 15 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

System administrators use a network intrusion detection system (NIDS) to identify network security breaches inside their own firm. Building a clever and robust NIDS for irregular and capricious attacks, however, raises various challenges. One of the key subjects in NIDS research in recent years has been the application of machine learning understanding of strategies. This approach provides a network intrusion detection tool that effectively identifies several kinds of network intrusions, including Dos, U2R, R2L, Probe, and Normal.It employs twin support vector machines and decision trees. The trees serve to construct the decision tree for network traffic data. Then, to maximize the separation of the top nodes of the decision tree, the bottom-up merging approach is applied, hence minimizing error buildup during generation. Embedding twin support vector machines inside the decision tree allows one to subsequently use the network intrusion detection model. This performance assessment is based on network intrusion detection analysis datasets—namely KDD-CUP99 and NSLKDD.

Keywords: NIDS, Twin SVM(TSVM), Decision Tree (DT), KDD-NSL, Auto Encoder.

INTRODUCTION

Unfortunately, most existing NIDSs still rely on signature-based approaches, which aren't great at spotting evolving threats, and they can't cope with the sheer volume and diversity of modern network data. The accuracy and timeliness of threat identification are compromised by existing methodologies due to high traffic volume and insufficient monitoring granularity. More sophisticated cyberattacks, such as Denial of Service (DoS) attacks or sophisticated malware, can find ways to bypass these defenses, leaving critical vulnerabilities unpatched. While NIDS has shown potential with machine learning, shallow learning techniques don't always transfer effectively across different data situations. More accurate and real-time detection of both known and unknown threats across several protocols and data formats is made possible by a deep learning-based NIDS, which automatically learns complex features from raw traffic. This approach also helps to reduce false positives and enhances network security resilience, thereby overcoming these constraints.

OBJECTIVES

- Present techniques performance and accuracy can be improved to provide a method that can provide consistent supervised feature learning.
- To research the various kinds of Network Intrusion Detection Systems (NIDSs) currently in use. To research different machine learning techniques for classifying traffic.
- Examining stacking non-symmetric deep auto-encoders to extract unsupervised features. To investigate the results of trials on recommended Twin Support Vector Machine and Decision Tree classification methods for intrusion detection systems.
- Reduce the time spent training.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

LITERATURE REVIEW

Deep learning methods that educate from basic characteristics to more abstract concepts are highly valued by B. Dong and X. Wang, who find inspiration in the brain's layered architecture. Our multi-level abstraction allows the Deep Belief Network (DBN) to transport functions from input to output without relying on characteristics that have been artificially created by humans. In a DBN, the Restricted Boltzmann Machine (RBM) is the unsupervised learning method used in every layer. A strength of DBN is its ability to do deep coding, which allows it to analyze data thoroughly and adapt to new situations. An other area where DBN shines is anomaly detection, which involves monitoring system activity for out-of-the-ordinary patterns of traffic. Processing data more efficiently and quickly is essential to the method [2].

R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao review and compile the literature on the use of deep learning for machine health monitoring. Focusing on Autoencoders (AEs) and their variants, Restricted Boltzmann Machines (RBMs) and their variants (including Deep Belief Networks (DBNs) and Deep Boltzmann Machines (DBMs)), Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs), the paper investigates deep learning applications in machine health monitoring systems. DL-based Machine Health Monitoring Systems (MHMS) offer one advantage in their greater adaptability to different machine kinds and their lower demand for specific knowledge and human work. On the other hand, a major drawback is that the quantity and quality of the data used greatly affect the performance of DL-based MHMS [3].

It's possible to extract features and classify them all at once. The SdA model can find errors even with measurement noise since it can recognize global and invariant patterns in sensor inputs. By constructing a SdA with a layer-by-layer denoising technique, the model can learn global features from complicated input data, including multivariate time-series datasets and high-resolution pictures. The capacity of the SdA model to learn normal and fault-related features from sensor data without preprocessing is highly beneficial for real-world applications. The trained SdA needs more investigation to determine which process components are most important for categorization, which is a drawback [4].

Using a new model based on deep learning recurrent neural networks (RNNs), L. You, Y. Li, Y., and Y. Yang want to automatically audit the security of prisoners' brief messages. This model can differentiate between secure and unsafe communications. We collect data on word order and use Word2vec to extract features from short messages. Then, we map each sentence to a feature vector. In the vector space, RNNs order these vectors similarly for words with comparable meanings. Compared to the SVM, the RNN model achieves a superior mean accuracy of 92.7%. When several feature extraction and classification methods are combined in an ensemble framework, performance gains may be even more substantial. One potential drawback is that the strategy might not work so great for very long messages [5].

K. Alrawashdeh and C. Purdy's deep learning method for anomaly detection uses a Restricted Boltzmann Machine (RBM) and a Deep Belief Network (DBN). Unsupervised feature reduction is done using a single-hidden-layer RBM in this approach. One RBM's weights are sent to another RBM to build a DBN. A layer using a Logistic Regression (LR) classifier with multi-class softmax is used to further hone the pre-trained weights. With a low false-negative rate of 2.47%, this method provides a 97.9% accuracy rate. The approach might be strengthened, nevertheless, by enhancing the dataset and the feature reduction technique of the deep learning network [6].

A deep learning-based method for building a strong and flexible Network Intrusion Detection System (NIDS) is provided by A. Javaid, Q. Niyaz, W. Sun, and M. Alam The proposed network intrusion detection system uses deep learning technique Self-taught Learning (STL). On the NSL-KDD benchmark dataset, it uses softmax regression and a sparse autoencoder. One benefit of STL is its classification accuracy rate of over 98% for all classification categories. On the other hand, one drawback of this deep learning technique is that for actual networks it calls for the use of a real-time network intrusion detection system [7].

In this study, S. Potluri and C. Diedrich test how well an intrusion detection system (IDS) based on deep neural networks (DNNs) performs when presented with large volumes of network data processed by multi-core CPUs and GPUs. Because it is a neural network, the DNN has the ability to process network traffic in parallel, which allows it to do so fast and effectively. The use of DNNs in intrusion detection systems has several benefits, including increased efficiency and reliability. Particularly when dealing with the necessary number of training samples to detect specific types of attacks, this is true. The results demonstrated that serial training approaches were inferior

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

to multi-core CPUs. One drawback is the need to improve the accuracy of intrusion detection systems that rely on DNNs [8].

C. Garcia Cordero, S. Hauke, M. Muhlhauser, and M. Fischer use replicator neural networks (RNNs) to create anomaly detection models as part of their approach for spotting large network-wide assaults. The approach is unsupervised and does not need tagged data, hence accurately spotting network-wide anomalies without assuming the training data is completely free of attacks. One of the benefits of the proposed approach is its capacity to effectively identify all well-known Distributed Denial of Service (DDoS) attacks and SYN port scans. Moreover, it is resistant to learning under assault, which is a disadvantage in related initiatives. One disadvantage is that the method has to be improved using stacked autoencoder deep learning approaches [9].

T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho propose a deep learning-based anomaly detection system leveraging Software-Defined Networking's (SDN) flow-based architecture. Their approach detects anomalies in an SDN environment depending on flow using a deep learning model. Among the advantages are locating the perfect hyperparameters of the Deep Neural Network (DNN) and confirming detection and false alarm rates. The model's performance accuracy of 75.75% is really reasonable given only six basic network characteristics. One disadvantage is that the model might not operate effectively in a real SDN environment [10].

In a technique put forth by NileshWankhade, patterns connected to malicious activity are found in network logs or transaction datasets for intrusion detection systems (IDS) by applying data mining techniques like frequent itemset mining (specifically using the Apriori algorithm) and association rule mining. Aiming on high-frequency patterns that are statistically more likely to indicate invasions, the Apriori algorithm filters out lower-frequency patterns as benign. Moreover, transaction data is encrypted using the DES (Data Encryption Standard) technique before to client-to-server transfer, hence enhancing security by ensuring that only authorised individuals may decrypt and inspect the data. This encryption reduces the likelihood of unwanted access in the framework of intrusion detection systems [11] by means of protecting communication between network nodes and the central monitoring system[11].

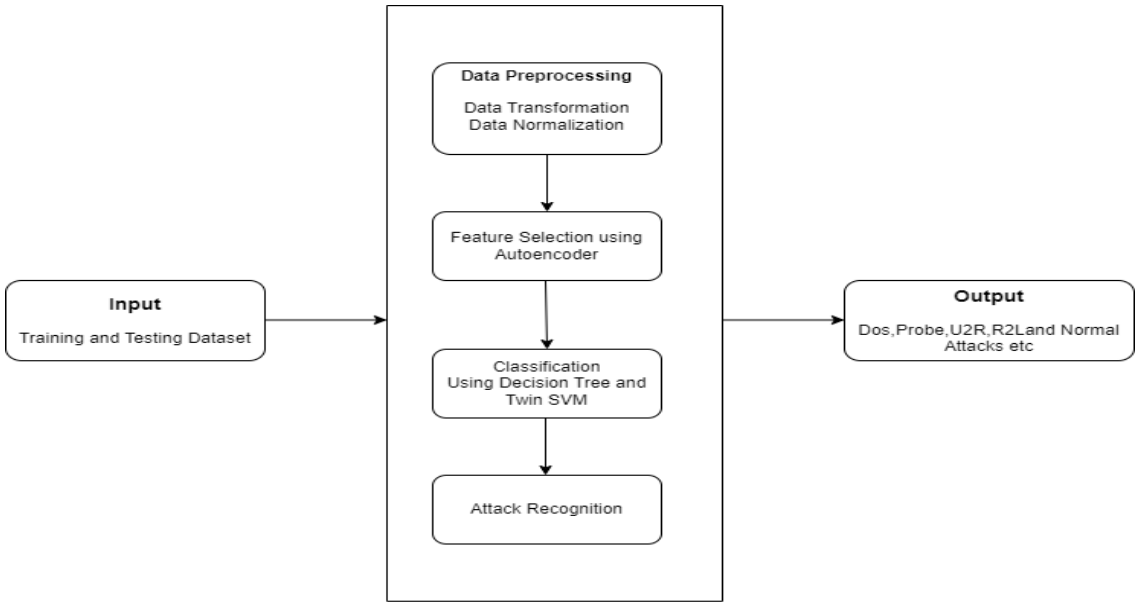

Figure 1: System Architecture

METHODOLOGY

The framework of the proposed intrusion detection system is shown in Figure 1. The detection system has four main stages:

1. Data Collection: Gathering relevant data is the initial and most important step in intrusion detection. Two critical aspects of an intrusion detection system's design and performance are the data source type and the

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

location of data collection. This study suggests an intrusion detection system (IDS) that operates on a network to verify our suggested methods and offer optimal protection for the specific host or networks in question. By analyzing incoming network traffic, the suggested intrusion detection system (IDS) operates on the router closest to the victim or victims. The training process involves sorting the acquired data samples according to the protocols used by the transport and Internet layers and then labeling them using the domain knowledge. In order to categorize the data gathered during the test phase, the protocol types are used exclusively.

2. Data Pre-processing: Step two is data pre-processing, which entails transforming the raw data acquired during data collection into the foundational features used in datasets like KDD Cup 99. This phase mostly consists of the following three elements: Data Normalization, Data Transfer, and Feature Selection.
3. Classifier Training: When training a classifier with DT and Twin SVM, the optimal subset of features is used following feature selection. Because DT and Twin SVM are only good for binary classification, we'll have to use classifiers. Five optimal feature subsets are selected for each category in the KDD Dataset. Differentiating across record types is the fundamental goal of any classifier. As an example, the Normal classifier is able to distinguish between Normal data and non-Normal data, which includes all types of attacks. The DoS class differentiates between DoS traffic and non-DoS data, such as Normal, Probe, R2L, and U2R instances. Classifiers that are able to distinguish between all classes are combined to form the intrusion detection model.
4. Attack Recognition: Utilizing the stored learned classifier, one may distinguish between normal and intrusion data; to train the classifier, it is optimal to employ the most associated and relevant attributes. Then, we check the test data for any infiltration using the previously trained model that was saved. Records are classified as attacks if they do not conform to the typical class; otherwise, they are regarded as regular data. The subclass of the anomalous record that corresponds to the type of assaults can help us determine the type of record if the classifier model confirms that it is out of the ordinary. usual or unusual outcomes (timing of detector development, false positive rate, and accuracy of detection). After the classification step, the system successfully identified the type of assault in the network traffic. According on the results of the classification, we were able to divide the input data into different kinds of attacks, such as: The terms "DoS" and "R2L" (remote to local) are two acronyms. User-to-root (U2R) Plain old (No Harm) After classifying the system, we evaluated its performance using industry-standard measures. A number of measures are employed, including recall, precision, exactness, and FPR. When thinking about all these factors, accuracy is king.

RESULTS AND DISCUSSION

As part of our work, we used the KDD Cup 99 / NSL-KDD dataset to detect and categorize network intrusions. The method began with data pretreatment, which involved removing irrelevant or unwanted features from the dataset.

We used two preprocessing techniques:

1. Normalization - To ensure uniformity, we used the Min-Max normalization technique and scaled all feature values to a range of 0 to 1.
2. Transformation - All categorical (non-numeric) data is converted to numeric format because further processing requires only numerical inputs.

Following preprocessing, we used an Autoencoder for feature extraction and selection. The Autoencoder reduced dimensionality by preserving only the most significant features, improving classification model performance.
We applied two classification systems:
We used two classification systems: Twin Support Vector Machine (SVM) Decision Tree Classifier.
These models were used to accurately detect and categorize various forms of network attacks. Depicted in Figure 1.1

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

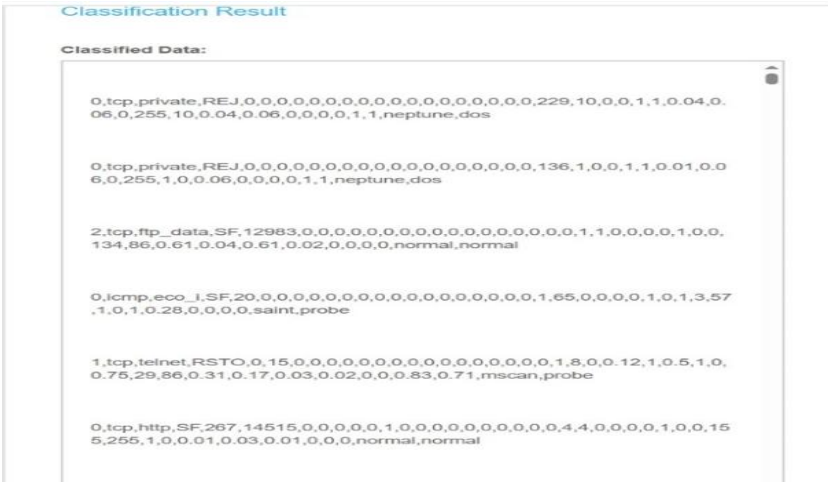

Figure 1.1: Classification Result

Figure 2. Performance Evaluation

The key assessment criteria for our suggested intrusion detection system are shown in Figure 2.
Accuracy, False Positive Rate (FPR), Recall, F Measure, Precision.
All of these outcomes appear in Figure 2.
Our study's main objective was to maximize accuracy; we could achieve an accuracy of 97.01%[Depict in Figure 2], which is better than many current models, hence demonstrating the efficacy of our suggested approach.

. ADVANATGES AND APPLICATIONS

ADVANTAGES:

High Accuracy, Efficient Preprocessing, Feature Reduction with Autoencoder, Hybrid Classification Approach, Enhanced Security, OpenSource Compatible.

APPLICATIONS:

Monitoring network traffic in real time to detect suspicious activities. Corporate IT Infrastructure-Protect internal networks against insider risks and illegal access. Healthcare Sector, Educational Institutions.

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Journal of Information Systems Engineering and Management
2025, 10(36s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CONCLUSION

We have addressed the issues with current NIDS techniques and, in response, developed our own NDAE method for unsupervised feature learning. Subsequently, we have expanded on this by introducing a novel classification model that utilizes stacked NDAEs, the TSVM, and the DT classification technique. Furthermore, we have implemented an intrusion protection system. Results demonstrate that our approach delivers high levels of recall, accuracy, and precision, accompanied by reduced training time.

REFRENCES

[1] LI ZOU, XUEMEI LUO, YAN ZHANG, XIAO YANG AND XIANGWEN WANG "HC-DTTSVM: A Network Intrusion Detection Method Based on Decision Tree Twin Support Vector Machine and Hierarchical Clustering".
[2] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in Proc. 8th IEEE Int.Conf. Commun. Softw. Netw, Beijing, China, Jun. 2016, pp. 581–585.
[3] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016. [Online]
[4] H. Lee, Y. Kim, and C. O. Kim, "A deep learning model for robust wafer fault monitoring with sensor measurement noise," IEEE Trans. Semicond. Manuf., vol. 30, no. 1, pp. 23–31, Feb. 2017.
[5] L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016, pp. 225–229
[6] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 195–200
[7] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. 9th EAI Int.Conf. Bio-Inspired Inf. Commun. Technol., 2016, pp. 21–26
[8] Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom., Berlin, Germany, Sep. 2016, pp. 1–8
[9] C. Garcia Cordero, S. Hauke, M. Muhlhauser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using replicator neural networks," in Proc. 14th Annu. Conf. Privacy, Security. Trust, Auckland, New Zeland, Dec. 2016, pp. 317–324
[10] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun., Oct. 2016, pp. 258–263
[11] Chopda, K., Rote, A., Gaikwad, K., Gachale, P., & Wankhade, N. R. (2017). Association Rule Mining Method for Applying Encryption Techniques in Transaction Data. International Journal of Engineering Science and Computing

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.