ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN 2454-9940

www.ijasem.org

Vol 19, Issue 2, 2025

Design and Performance Analysis of an Anti-Malware System Based on Generative Adversarial Network Framework

Jajjara Bhargav [1], Yeluri Trivikram [2], Siribabu Inavolu[3], Potu Yogesh[4], Venkata Akhila[5]

[1] HOD& Assistant Professor, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

[2,3,4,5] Students, Department of Computer Science Engineering, Chalapathi Institute of Engineering and Technology, Chalapathi Rd, Nagar, Lam, Guntur, Andhra Pradesh- 522034

Email id: bhargavchalapathi@gmail.com[1], trivikramyeluri07@gmail.com[2], siribabuinavolu@gmail.com[3], naniyogesh50@gmail.com[4], ratnakaramvenkataakhila@gmail.com[5]

Abstract:

Malware remains a major threat to computer systems, with a vast number of new samples being identified and documented regularly. Windows systems are particularly vulnerable to malicious programs like viruses, worms, and trojans. Dynamic analysis, which involves observing malware behavior during execution in a controlled environment, has emerged as a powerful technique for detection. In the current digital era, cyber threats have become increasingly sophisticated, posing severe challenges to the integrity, confidentiality, and availability of information systems. This paper proposes a secure framework that integrates feature selection and advanced attack detection techniques to enhance the defense mechanisms of critical network infrastructures. The framework aims to reduce the dimensionality of large-scale intrusion datasets, improve the accuracy of anomaly detection, and ensure real-time threat identification with minimal false alarms.

Keywords: Performance Analysis, framework, Anti-Malware System

Introduction

Government, banking, business, and health care all require robust, dependable cyber security solutions It's certain, the difficulty has grown significantly in the big data age in comparison to already applied solutions, such as classic intrusion detection systems (IDS) The rapid development of technical capabilities has made way for cyber threats that use a variety of hostile tactics to target persons or businesses. Traditional security measures such as firewalls, anti-virus software, and virtual private networks (VPNs) are not necessarily sufficient in this threat environment, and effective systems for detecting intrusions must be established Thus, installing IDS with other traditional security solutions is a critical approach IDS are software applications that monitor network traffic to detect malicious content or activity The IDS is structured in a way that it gives alarms and tells when harmful information is obtained. Even though most IDS systems are created to identify and outline dubious network activity, it's important to note that sophisticated systems can block suspicious network traffic In general, the IDS are divided into misuse detection systems where the detection is based upon the signature and anomaly detection systems where the detection is based on profile In Anomaly detection systems there is a variation in ordinary system profile which is the main goal of this method, but in misuse detection systems, the main goal is to match with the attack case The fake alarm rate is normally high in anomaly detection systems because it is used to identify

unfamiliar attacks having high-performance rates. These drawbacks are normally reduced by using the misuse detecting system that depends upon the difference between the normal and malicious behavior of the signature Even though, both systems are having a direct impact on detection rules freshness, enhancement in the accuracy of detection and studying the speed of the detection system is more difficult. Recently, a high accuracy rate and identification of various attack methods are achieved by using the data mining method in network intrusion detection systems The statistics and artificial intelligence methods are used by data mining methods to make knowledge from the large datasets to produce the solutions for complex problems. The machine learning method is used as a technical tool in data mining techniques to produce information from the raw data. The data present in the data mining technique is saved in electronic form and both the automatic and semiautomatic methods are used to find the pattern. Currently, data mining-based IDS turns to be very challenging due to, false positives, false negatives, low detection accuracy, high running time, adversarial attacks, and uncertain attacks. To address this issue, the work has developed a DataMIDS framework using the Bengio Nesterov Momentum-based Tuned Generative Adversarial Network (BNM-tGAN) detection technique.

2.Related work

Sarnovsky et al. [1] developed a new IDS topology which is the symmetrical combination of machine learning technique and knowledge-based technique designed to evaluate the network attacks Predictive models capable of detecting normal connections from assaults and then forecasting attack classes and specific attack types comprised the multi-stage hierarchical prediction. We were able to travel through the attack taxonomy and select the right model to do a prediction on the given level using the knowledge model Knowledge Discovery in Databases (KDD) 99 dataset consists of a set of data that's reviewed and incorporates different intrusions reproduced in a military network environment [2]. On the widely used KDD, Designed IDS was examined and compared to similar techniques. However, the characteristics' useless data resulted in erroneous attack detection. Vinayakumar et al. [3] developed the effective IDS and flexible by considering a Deep Neural Network (DNN) to predict and unforeseen the cyber-attacks detection and classification. Based on the Hyperparameter selection methods the optimal network parameters and network topologies for DNNs were chosen with the KDDCup 99 dataset. Then conducting more experiments by the DNNs till the learning rate reaches 1,000 epochs that ranged between [0.01–0.5]. The DNN model which performed well on KDDCup 99 was applied on other datasets such as University of New South Wales (UNSW)-NB15, Network Security Laboratory (NSL)-KDD, Kyoto, CICIDS 2017, and WSN-DS to conduct the benchmark. Finally, develop a Scale-Hybrid-IDS-AlertNet (SHIA) which is a highly scalable, and hybrid DNNs framework called Scale-Hybrid-IDS-AlertNet (SHIA) was developed, that is used to monitor host-level events and the network traffic which alert the cyber-attacks possibility. As the training of DNN was not sufficient, this led to the underfitting of the model and increased the error rate. Zavrak et al. [4] developed a semi-supervised learning approach with unsupervised deep learning methods for monitoring the irregular traffic from low-based data. And to identify unknown attacks the Autoencoder and Variational Autoencoder methods were introduced with flow features. This approach used the features which are extracted out of network traffic data with flow features, which included typical and different types of attacks. The One-Class Support Vector Machine is compared with the Receiver Operating Characteristics (ROC) and the area under the ROC curve is calculated.

The performance is analyzed using the ROC curves at various threshold levels. The final result shows that the Variational Autoencoder performance to a great degree was better than the Autoencoder and One-Class Support Vector Machine. But the approach was vulnerable to adversarial and uncertain attacks. Mayuranathan et al. [5] illustrated an effective feature subset selection-based classification model for Distributed Denial of Service (DDoS) attack detection. DDoS is a subclass of DOS attack. They target an online website by overwhelming it with the traffic using the online connected devices like router and server. The Random Harmony Search (RHS) optimization model is used to detect the DDoS attack in IDS, with maximum detection the best feature sets were selected. After the features selection, the DDoS detection is done by introducing a Deep learning-based classifier model with Restricted Boltzmann Machines (RBM). The DDoS attack detection rate was improved, and seven additional levels were added in between the RBM's visible and hidden layers. The experimentation is done for the RHS-RBM model against the KDD′99 dataset. The experimental results showed that the RHS-RBM model achieved a specificity of 99.96, maximum sensitivity of 99.88, F-score of 99.93, the accuracy of 99.92, and kappa value of 99.84, but it was not able to handle dynamic and random behavior of malicious attack. Su et al. [6] combined attention mechanism and BLSTM (Bidirectional Long Short-term memory) for IDS. The network flow vector consisted of packet vectors created by the BLSTM model, which may obtain the main features for network traffic classification, which was screened using the attention mechanism. In addition, it used many convolutional layers to collect traffic data's local properties. The network classification is done through the SoftMax classifier. The testing is performed for this approach using the public benchmark dataset, and the experimental results show that the performance is better than the other comparison methods. The performance-based on metrics was better but it took more computational time, which may be helpful for attackers to trap data. Devan et al. [7] utilized XGBoost–DNN for feature selection and categorization of network intrusion, followed by a deep neural network (DNN). The XGBoost–DNN model had three steps: feature selection, normalization, and classification. DNN used learning rate optimization in the Adam optimizer, and classification of network intrusions is completed through the SoftMax classifier. The tests were carried out on the benchmark NSL-KDD dataset.

3. Methodology

Intrusion detection is a tough technique in cyberspace security that protects a system from hostile assaults. As shown in figure, a unique accurate and effective misuse IDS that depends on distinct attack signatures to discriminate between normal and malicious activities is offered to identify various assaults based on the Data MIDS architecture utilising the BNM-tGAN detection approach.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

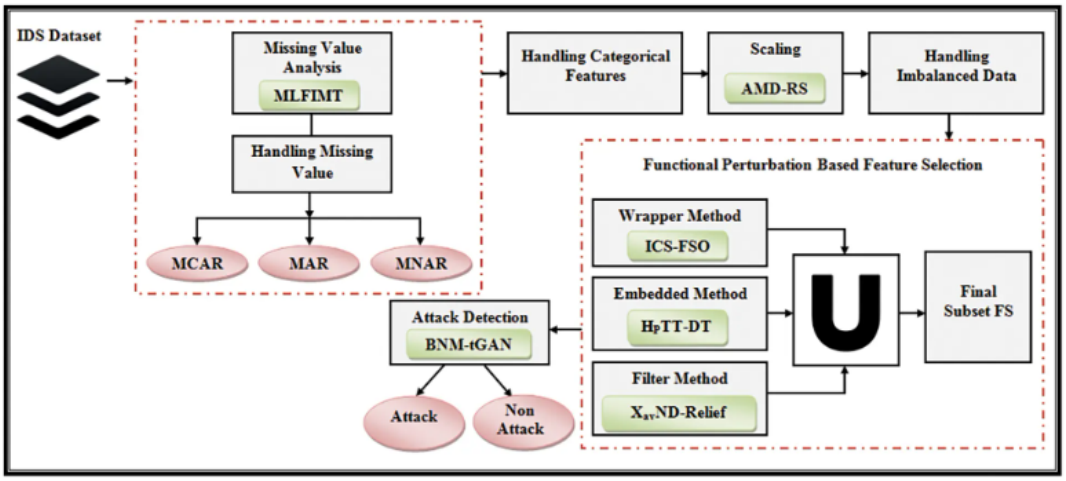

Figure: Proposed data mining intrusion detection system (Data MIDS) framework

Missing Value Analysis

Missing value analysis can assist to improve the IDS by identifying and resolving issues caused by missing data. If cases with missing data are consistently different from those without missing values, the conclusions of attack behaviour may be deceiving. Another difficulty is that many statistical procedures' assumptions are based on datasets, and missing numbers may make understanding the attack more difficult.

Detection

Feature selection data calculate the attack detection which is used to train the given model. The introduced work uses a Bengio Nesterov Momentum-based Tuned Generative Adversarial Network (BNM-tGAN). The existing GAN leads to a high error rate for performing IDS due to complex loss function and high computed optimizer to handle the loss. The poor performance of the GAN leads to misclassification of attack which in turn gives an unsecured IDS system. To conquer this issue, the work has used the Wasserstein loss function that is used as a tuned factor in GAN, which make the training model more stable and produce a lossy function that correlates with the quality of generated attack or noise and the loss function is compiled using Bengio Nesterov momentum optimizer that selects moderate weight value and computes within low time with high accuracy. Basically, BNM-tGAN uses the machine learning algorithm which is an unsupervised method that spontaneously finds and learns the pattern used in input data. Similarly, this method is utilized to produce or generate the new outputs from the given original dataset as shown in Fig.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN 2454-9940
www.ijasem.org
Vol 19, Issue 2, 2025

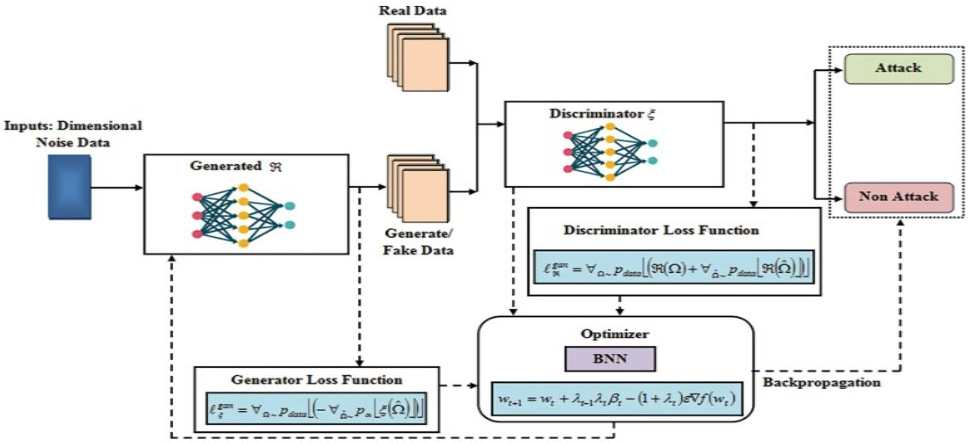

Figure: Proposed Bengio Nesterov momentum-based tuned generative adversarial network (BNM-tGAN) architecture

4. Results and Discussion

The proposed framework for a highly secured intrusion detection system for IoT has been analysed and compared with the existing techniques to determine its strength. The following experiments were set up 5PK8T Intel Core 11th Generation i7-1165G7 Processor (Quad Core, Up to 4.70 GHz, 12MB Cache), 64-bit Windows 11 OS. The work has been implemented in Python v3.7 platforms based on the NSL-KDDCUP99 available on the kaggle website (https://www.kaggle.com/). The UNSWNB15 data set is a mix of real, modern, normal, and contemporary artificial network traffic attack activities. Existing and novel methods are utilized to totally generate 49 features with the class label of the UNSWNB15 data set. Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms are among the nine types of attacks in this dataset. From the dataset, 80% of data is used for training and 20% of data is used for testing.

The KDD Cup'99 dataset is used to build an IDS. It contains 41 features per network connection which are listed into certain groups. Here, 80% of data is used for training and 20% is used for testing. A drawback of this dataset is that a huge amount of redundant data is duplicated for the testing and training set making the learning algorithm biased. This prevents from detecting infrequent records that are more harmful to U2R attacks. Due to this, a new dataset termed NSL-KDD was made to solve the poor evaluation of anomaly detection methods and performance of the evaluated system The experimental analysis is done using this. Here, 70% of data is taken for training and 30% for testing.

Performance Evaluation of Classification Technique

Here, the performance evaluation of the proposed BNM-tGAN method is analysed using the existing Elman Neural Network (ENN), Convolution Neural Network (CNN), Generative Adversarial Network (GAN), and Adaptive neuro-fuzzy interface system (ANFIS) methods based on accuracy, sensitivity, specificity, precision, F-measure, False Positive Rate (FPR), False Negative Rate (FNR), and Mathews Correlation Coefficient (MCC). Then, the performance analysis is given for the computation time and attack detection time of the proposed and existing methods. The various performance metrics for the Attack Detection is calculated as follows

The proposed BNM-tGAN based on performance measures like Accuracy, Specificity, Sensitivity, Precision, F-Measure, FPR, FNR, and MCC. The metrics value is decided by four key parameters: true positive (TP), true negative (TN), false positive (FP), and false negative (FN). These factors are the base for the performance measures. TP asserts that the actual value and the predicted value is not an attack while TN asserts that they are an attack. Whereas FP asserts that the actual value is an attack but the predicted value is not an attack, and FN asserts that the actual value is not an attack but the predicted value is interpreting an attack. So, identifying an assault depends on the four factors and the metric values are produced and represented visually based on these.

Table: shown below depicts the assessment of the proposed BNM-tGAN

Performance metrics/Techniques	ENN	CNN	ANFIS	GAN	Proposed BNM-tGAN
Accuracy	79.68	82.14	84.78	86.98	92.14
Specificity	78.48	83.14	85.69	86.55	91.14
Sensitivity	79.65	84.14	86.78	87.77	90.14
Precision	81.45	85.45	87.14	88.97	91.58
F-Measures	82.58	85.88	87.14	88.98	90.14
FPR	25.64	24.17	23.14	22.98	11.47
FNR	27.89	26.98	25.47	23.54	10.24
MCC	83.12	84.78	85.77	86.89	93.12

The suggested technique achieves 92.14% classification accuracy, where the existing ENN, CNN, ANFIS, and GAN methods obtain 79.68%, 82.14%, 84.78%, and 86.98%, respectively, which are lower than the proposed BNM-tGAN method. And, the given technique has sensitivity, specificity, and accuracy of 91.14%, 90.14%, and 91.58%, respectively, which is more than the existing methods, which vary from 78.48% to 88.97%. The proposed BNM-tGAN method has FPR and FNR of 11.47% and 10.24%, respectively, which is lower than the existing CNN, ENN, ANFIS, and GAN. Similarly, the F-measure and MCC are 90.14% and 93.12%, respectively, which are more than the existing approaches. According to the results of the analysis, the suggested strategy surpasses the current methods in all aspect.

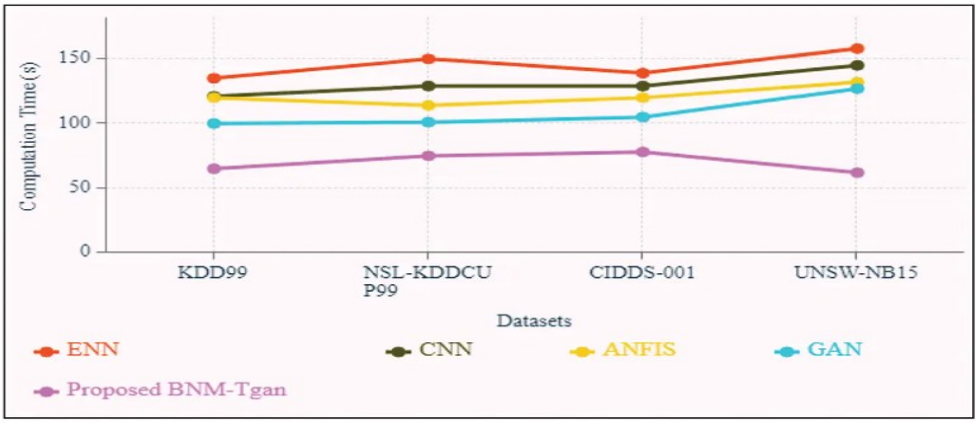

Figure: Computation time of the proposed and existing methods

The figure given below compares the computation times of the proposed BNM-tGAN approach to those of the existing CNN, ANFIS, ENN, and GAN techniques. It's performed on a variety of datasets, including NSL-KDDCUP99, KDD99, UNSW-NB15 and CIDDS-001. The computation time should be minimized for an efficient classifier. The BNM-tGAN method takes 65, 75, 78 and 62 s to compute KDD99 dataset, NSL-KDDCU99 dataset, CIDDS-001

dataset, and UNSW-NB15 dataset. Existing approaches take more time to compute for all datasets. The final result shows that the proposed method more efficient in the detection of assaults than the existing methods.

Conclusion

This paper presents a secure, intelligent framework for intrusion detection by integrating efficient feature selection methods with advanced attack detection techniques. The results validate the potential of this approach in enhancing the accuracy, responsiveness, and robustness of cybersecurity systems. Future work will focus on real-time deployment, multi-class attack classification, and integration with blockchain-based audit trails for improved traceability. The work performs shallow learning of the feature and analyzes the missing values to get in-depth knowledge of missing values' impact over the attack classes. The false alarm rate of detecting attack is decreased and higher accuracy with low computation time is achieved by the proposed framework. The chances of uncertain attacks and adversarial attacks are conquered by the proposed framework and can evaluate illegal system usage, misuse, and abuse. Experimental analysis declared that the model tends to obtain an accuracy of 92.14%, sensitivity of 90.14%, and specificity of 91.14%. In addition to that, the proposed model reduces the false alarm rate by obtaining an FPR, FNR of 11.47% and 10.24% respectively. In comparison to the currently available state-of-the-art method the proposed model tends to perform well

References

1. Han, R., Kim, K., Choi, B., and Jeong, Y. (2023). A study on detection of malicious behavior based on host process data using machine learning. Appl. Sci., 13.
2. Almaleh, A., Almushabb, R., and Ogran, R. (2023). Malware API Calls Detection Using Hybrid Logistic Regression and RNN Model. Appl. Sci., 13.
3. AV-TEST (2024, June 07). Malware Statistics & Trends Report. Available online: https://www.av-test.org/en/statistics/malware/.
4. Cannarile, A., Carrera, F., Galantucci, S., Iannacone, A., and Pirlo, G. (2022, January 20–23). A Study on Malware Detection and Classification Using the Analysis of API Calls Sequences Through Shallow Learning and Recurrent Neural Networks. Proceedings of the Italian Conference on Cybersecurity ITASEC22, Rome, Italy.
5. Gibert, The rise of machine learning for detection and classification of malware: Research developments, trends and challenges, J. Netw. Comput. Appl., № 153, c. 102526
6. Gençaydin, B., Kahya, C.N., Demirkiran, F., Düzgün, B., Çayir, A., and Dağ, H. (2022, January 14–16). Benchmark Static API Call Datasets for Malware Family Classification. Proceedings of the 2022 7th International Conference on Computer Science and Engineering (UBMK), Diyarbakir, Turkey.
7. Aslan, A comprehensive review on malware detection approaches, IEEE Access, № 8, c. 6249
8. Sikorski, M., and Honig, A. (2012). Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software, No Starch Press.