Int. J. Sci. R. Tech., 2025 2(1)
A Multidisciplinary peer-reviewed Journal
www.ijsrtjournal.com [ISSN: 2394-7063]

Original Article

A Review on Network Intrusion Detection

Hiba Fathima K. P.*, Anugraha P. P.

Government Engineering College Wayanad

ABSTRACT

Network intrusion detection is a critical component of cybersecurity, aimed at safeguarding networks from unauthorized access and malicious activities. This review paper provides an extensive examination of the current landscape of network intrusion detection techniques, encompassing both signature- based and anomaly-based approaches.The review delves into the intricacies of signature-based methods, which rely on predefined patterns and signatures to identify known threats. It analyzes the strengths and limitations of this approach, exploring recent ad- vancements in signature-based detection. Furthermore, the paper scrutinizes anomaly-based techniques, which focus on detecting deviations from normal network behavior. Various machine learning and statistical methods employed in anomaly detection are thoroughly evaluated, considering their effectiveness and adaptability in dynamic network environments. Moreover, the pa- per discusses the integration of artificial intelligence and machine learning algorithms to enhance the accuracy and efficiency of intrusion detection systems.Drawing from a comprehensive anal- ysis of the literature, this review offers insights into the strengths and weaknesses of existing approaches, providing a foundation for future research directions. The concluding remarks highlight the evolving nature of network threats and the imperative for continuous innovation in intrusion detection strategies. The synthesis of current trends and prospective advancements aims to guide researchers, practitioners, and policymakers in fortifying network security against an ever-evolving cyber threat landscape.

Keywords: Network intrusion detection,LSTM,CNN

INTRODUCTION

With the significant expansion of services reliant on net- works and the proliferation of sensitive information within these networks, the importance of network security has never been more pronounced. Network security now surpasses its previous significance. Intrusion detection techniques serve as the ultimate defense against computer attacks, positioned after secure network architecture design, firewalls, and individual screening. Despite the array of available intrusion prevention techniques, successful attacks on computer systems persist. Consequently, intrusion detection systems (IDSs) assume a critical role in fortifying network security. According to a re- cent report by Symantec[1], phishing attacks aimed at pilfering confidential data such as credit card numbers, passwords, and financial information have escalated from 9 million attacks in June 2004 to over 33 million in less than a year.

One proposed remedy involves the adoption of network intrusion detection systems (NIDS), which discern attacks by monitoring diverse network activities. Therefore, it is imperative for such systems to possess accuracy in identifying attacks, swift training capabilities, and minimize false positives. This paper outlines the scope and current status of our research in anomaly detection. It conducts a comparative study of various anomaly detection schemes to pinpoint novel network intrusion detections. This paper contributes to the assurance of network and data security by examining the attributes of network traffic data, identifying malicious network behavior, and devising effective defense strategies. In line with the demands of cybersecurity protection, there is a need not only to swiftly detect network intrusions within network traffic data but also to precisely cate- gorize the specific types of network intrusions. This facilitates the implementation of targeted defense strategies and response measures.

II. RELATED WORK

A. A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE

[1] This article explores the use of deep neural network (DNN) and convolutional neural network

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

(CNN) as deep learning models for developing an Intrusion Detection System (IDS) capable of effectively detecting cyber attacks. The constant evolution of network behavior and the increasing frequency of attacks necessitate the continuous development and evaluation of IDS using various datasets and methods. The study introduces a novel two-stage deep learning technique that combines Long-Short Term Memory (LSTM) and Auto-Encoders (AE) for attack detection. The research utilizes the CICIDS2017 and CSE-CICDIS2018 datasets to determine op- timal network parameters for the proposed LSTM-AE model. Experimental results indicate that the hybrid model performs well and is suitable for detecting attacks in contemporary scenarios. The process involved in this study begins with data cleaning. Subsequently, a sequence-to-sequence Auto-Encoder (AE) and Long-Short Term Memory (LSTM) network are employed in both the encoder and decoder layers. The primary goal is to predict both short-term and long-term network attacks. The AE consists of an encoder and a decoder, where the input sequence is initially encoded and then decoded in the forecasting process.Fig 1 depicts the LSTM-AE model architecture. The AE encodes the original data and forms a bottleneck, and the decoding network restores all the data. The main challenges of the proposed model are the combination of two types of architectures and the training with smoothing constraints.

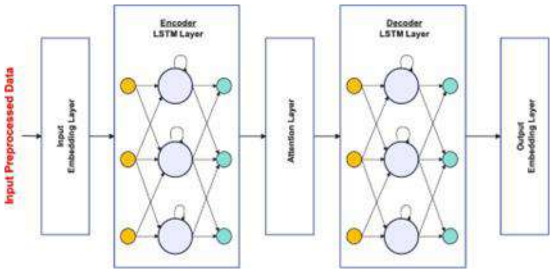

Fig. 1. LSTM-AE model architecture

B. Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques

[2] The research paper introduces a novel hybrid network In- trusion Detection System (IDS) named NID-Shield, designed to classify datasets based on different attack types. NID-Shield employs a feature subset selection technique called CAPPER and utilizes various machine learning methods. The system classifies attack names individually, aiding in predicting the vulnerability of specific attacks across diverse networks. Eval- uation using UNSW-NB15 and NSL-KDD datasets demon- strates that NID-Shield, when combined with the CAPPER approach, achieves high accuracy and low False Positive Rate (FPR). The proposed Hybrid NID-Shield Network Intrusion Detec- tion System (NIDS) is designed with a focus on classifying datasets based on different attack types. This classification offers the advantage of identifying arbitrary features within the dataset. Additionally, the system leverages the information about attack names within attack types to predict the vulnera- bility of individual attacks across diverse networks. The design involves analyzing distinct machine learning algorithms for each attack type, selecting those with high accuracy and low False Positive Rate (FPR) for different attacks in the hybrid NID-Shield NIDS. The hybrid approach, known as CAPPER, is applied for op- timal feature subset selection. CAPPER combines the strengths of the Correlation-based Feature Subset Selection (CFS) and Wrapper methods. The CFS approach yields a superior feature subset by eliminating irrelevant and redundant features, while the Wrapper method uses induction learning algorithms to achieve a highly accurate feature subset. By integrating filter and wrapper approaches, the hybrid NID-Shield NIDS obtains high-merit and accurate feature subsets, which are then utilized for training and testing purposes.

C. A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM

[3] The paper introduces a Double-Layered Hybrid Ap- proach (DLHA) as a solution to address a specific problem in intrusion detection. The approach involves creating Principal Component Analysis (PCA) variables to capture common characteristics of different attack categories. Notably, R2L and U2R attacks exhibit behavior similar to normal users. DLHA incorporates a Naive Bayes classifier in Layer 1 to detect Denial of Service (DoS) and Probe attacks, and a Support Vector Machine (SVM) in Layer 2 to distinguish R2L and U2R attacks from normal instances. The study compares DLHA with other existing IDS tech- niques using the NSL-KDD dataset. Experimental results indicate that DLHA outperforms several state-of-the-art IDS techniques and demonstrates significant superiority over individual machine learning classifiers. Moreover, DLHA exhibits outstanding performance in detecting rare

attacks. The proposed Double-Layered Hybrid Approach (DLHA) aims to enhance overall detection rates, particularly for rare and more hostile attacks like R2L and U2R. Emphasizing real- time efficiency, DLHA incorporates Information Gain and Chi-Square-based Feature Selection (ICFS) and Principal Compo- nent Analysis (PCA) to reduce data dimensions. The DLHA algorithm involves capturing network connection packages, subjecting them to Data Transformation 1, and passing the transformed data to Layer 1 (Naive Bayes Classifier - NBC) for determining if the connection is DoS, Probe, or Normal. If negative, indicating it's unlikely to be DoS or Probe, Layer 2 (Support Vector Machine - SVM) is activated through Data Transformation 2 to identify R2L, U2R, or normal connec- tions. If either classifier predicts positive, the connection is terminated and marked as an anomaly. The computational efficiency of DLHA is highlighted by its prioritized detection of DoS and Probe attacks before addressing R2L and U2R.

D. An Adaptive Ensemble Machine Learning Model for Intru- sion Detection

[4] This paper introduces an adaptive ensemble learning model that incorporates various common machine learning algorithms, including decision trees, SVM (support vector machines), logistic regression, kNN (k-nearest neighbors) [27], Adaboost, random forest, and deep neural networks, as al- ternative classifiers. Through comparative tests, five voting classifiers are chosen. The model enhances detection perfor- mance by adjusting sample proportions, setting data weights, employing multi-layer detection, and combining other meth- ods to boost the effectiveness of each algorithm. Ultimately, an adaptive voting algorithm, incorporating different class weights, is employed to achieve optimal detection results.

The adaptive ensemble learning model comprises the fol- lowing steps:

1. Input the NSL-KDD training dataset.
2. The preprocessing module transforms character-type fea- tures like labels and services into numerical values, standard- izes the data, and removes unnecessary features.
3. Train candidate algorithms using the preprocessed data.
4. Conduct cross-validation training for all algorithms using the training data. Select the algorithm with superior detection accuracy and operational performance for voting. Boost each algorithm further to enhance detection accuracy, employ- ing methods such as feature selection, unbalanced sampling, class weights, multi-layer detection, etc. The paper proposes optimizing the decision tree algorithm and introducing the MultiTree algorithm.
5. Set classification weights for each algorithm based on training accuracy, generating an adaptive voting algorithm model.
6. Input the entire NSL-KDD test set data and preprocess it as in step 2.
7. Utilize each selected algorithm to detect the test set, output preliminary predicted classifications, and calculate final voting results using the adaptive voting algorithm.

E. Early Detection of Network Intrusions Using a GAN-Based One-Class Classifier

[5] The paper addresses the challenge of early detection of network intrusions, emphasizing the common limitation in existing studies that focus on full session features, hindering timely intrusion detection. To overcome this, the proposed method utilizes packet data to identify potentially malicious traffic, but acknowledges the risk of false positives. The solution involves creating a new training dataset for a Gen- erative Adversarial Network (GAN) by using misclassified data from an original training dataset. The GAN, trained with this dataset, assesses whether currently received packets can be accurately classified by an LSTM-DNN model. If uncertainty is detected, the detection process is postponed until the next packet arrives. The method combines a carefully designed classification algorithm based on LSTM-DNN with a GAN validation model, allowing for real-time intrusion detection without session termination or delay. Experimental results confirm the algorithm's ability to detect intrusions early, before session completion, while maintaining performance comparable to existing methods. The proposed method utilizes LSTM for per-session in- trusion detection, directly analyzing packet data as features. Intrusion detection is performed using a classifier, and if no intrusion is detected, the classification result is temporarily stored. This result, along with packet data, is used when the next packet of the same session is received. Detecting network intrusions solely based on packet data may fail due to fragmented information

for the entire session. While classifying performance from a single packet improves, the challenge remains in selecting the final result from packet classifications within the session. To address this issue, the proposed method employs a Gen- erative Adversarial Network (GAN). The GAN discriminator is trained exclusively with packets misclassified by the LSTM classifier, accurately learning characteristics of packets prone to misclassification. Upon receiving a packet, the LSTM clas- sifier determines the session's malicious nature, and the GAN verifies the result. If the GAN indicates low reliability, the classification result is ignored; if high reliability is confirmed, the session is processed accordingly.

F. HC-DTTSVM: A Network Intrusion Detection Method Based on Decision Tree Twin Support Vector Machine and Hierarchical Clustering

[6] This paper introduces a network intrusion detection method called HC-DTTWSVM, which combines decision tree, twin support vector machine (TWSVM), and hierarchical clus- tering. The proposed method aims to effectively detect various categories of network intrusion.Fig 2 depicts The general process of HC-DTTWSVM for network intrusion detection.

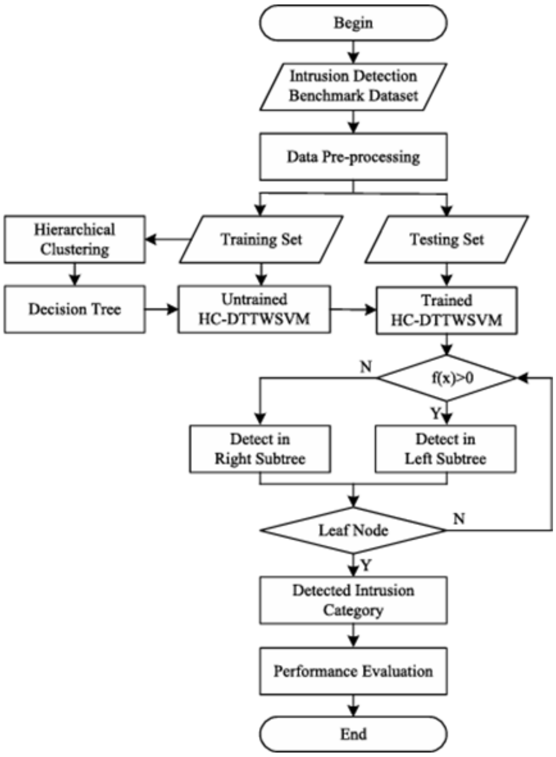

Fig. 2. The general process of HC-DTTWSVM for network intrusion detection

The process begins with applying a hierarchical clustering algorithm to construct a decision tree for network traffic data. The bottom-up merging approach is employed to enhance the separation of upper nodes in the decision tree, reducing error accumulation during construction. Twin support vector machines are then integrated into the decision tree to create the network intrusion detection model. This model operates in a top-down manner, effectively identifying the category of network intrusion. The performance of the HC-DTTWSVM method is evaluated using the NSL-KDD and UNSW-NB15 intrusion detection benchmark datasets.

G. Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network

[7] This paper introduces a wireless network intrusion de- tection method known as Improved Convolutional Neural Network (ICNN). The approach involves characterizing and preprocessing network traffic data, followed by modelling intrusion traffic data using ICNN. The method utilizes a Convolutional Neural Network (CNN) to abstractly represent low-level intrusion traffic data as advanced features, extract- ing sample features autonomously. Network parameters are optimized using the stochastic gradient descent algorithm to converge the model. The proposed method is evaluated through a sample test to detect network intrusion behavior. Addressing the inefficiency and susceptibility to overfitting and generalization issues in the current wireless network intru- sion detection technology based on deep learning, this paper suggests an enhancement through an improved convolutional neural network (IBWNIDM). The proposed method is eval- uated through classification training and test experiments in IBWNIDM, utilizing pre-processed training and test set data. Results indicate higher accuracy and true positive rates with a lower false positive rate for intrusion detection in IBWNIDM. The paper emphasizes leveraging the deep learning model's feature extraction capabilities for sample data. In IBWNIDM, two key aspects are targeted in future im- provements. First, in the stochastic gradient descent algorithm (SGD), where gradient dispersion and local optima challenges exist, the suggestion is to explore alternatives like simulated annealing or group intelligent optimization algorithms (e.g., particle swarm optimization, ant colony algorithm) for param- eter tuning. Second, diversifying training and testing datasets is recommended to refine algorithms and methods, enhancing the intrusion detection model's

generalization ability and overall effectiveness based on experimental results.

H. Method of Network Intrusion Discovery Based on Convolu- tional Long-Short Term Memory Network and Implementation in VSS

[8] The paper introduces an enhanced network intrusion detection method based on a Convolutional Long Short-Term Memory (CLSTM) network. This approach incorporates the convolution operation from deep learning into the structure of long short-term memory networks, ultimately improving the accuracy of network intrusion detection. Through experimental comparisons with similar methods, the proposed approach demonstrates advantages in overall network intrusion discovery, detection across different types, and AUC evalua- tion. Furthermore, when applied to video surveillance system (VSS) scenarios, the method exhibits superior accuracy, recall, precision, and overall performance compared to other similar methods. The LSTM and CNN models excel in processing temporal and spatial information, respectively. However, the intricate structure of LSTM poses computational challenges, particu- larly with massive input data, and the convolution operation proves effective in reducing the considerable number of pa- rameters. This paper proposes an enhanced network intrusion detection method, emphasizing the need to consider spatial and temporal information in the dataset. The ConvLSTM model is chosen for its suitability in addressing these considerations, with the introduced convolution operation aiding in faster model convergence, particularly for large-scale intrusion data. The method involves the following steps: 1. Traffic Data Acquisition: - Real-time network traffic data is obtained using the network traffic collection module. - Characteristics of the traffic data, such as service types, protocols, network connection time, and connection status, are analyzed.

2. Traffic Data Preprocessing: - For discrete features like connection status and service type, one-hot encoding is applied to map feature values into Euclidean space. - Neural Net- works' sensitivity to numeric range differences is addressed by normalizing continuous feature values, ensuring values fall between 0 and 1.

3. Sequence Feature Extraction: - The preprocessed data packet's feature vector is fed into the ConvLSTM model to extract spatio-temporal features.

4. Network Data Classification: - Features are input into the fully connected layer, integrating complete feature informa- tion. - The classification result of network intrusion discovery data is obtained using the Softmax function. The proposed model architecture includes an input layer, two ConvLSTM layers with batch normalization and dropout layers, a Convolutional3D layer, and two fully connected layers. The model is end-to-end, transforming from input to state nodes. Convolution operations extract spatial characteristics, and the input and output of current data are determined by the input and forget gates, with the output of the current node determined by the output gate. The convolution oper- ation, featuring local linkage and weight sharing, reduces the time complexity of the LSTM network, accelerating model convergence. The ConvLSTM model introduces convolution into the LSTM, directly inputting eigenvalues obtained from convolution into the prediction network structure, thereby speeding up convergence.

I. An End-to-End Framework for Machine Learning-Based Network Intrusion Detection System

[9] This research paper introduces the AB-TRAP frame- work, a five-step approach designed for the deployment of an updated network traffic solution, considering operational concerns. The framework includes the generation of attack and bonafide datasets, machine learning model training, model implementation, and performance evaluation after deployment. The AB-TRAP framework was applied to detect TCP port scanning attacks in both local (LAN) and global (internet) environments. In the LAN study case, the framework achieved a high f1-score of 0.96 and an area under the ROC curve of 0.99. The implementation utilized a decision tree with minimal CPU and RAM usage on kernel-space.

The AB-TRAP framework is introduced, consisting of steps for creating Attack and Bonafide datasets, training machine learning models, implementing the solution in a target ma- chine, and evaluating the performance of the protection mod- ule. The framework allows for design decisions during its ap- plication, such as modifying datasets during machine learning model training or making changes post non-compliance with performance evaluation. These new requirements in perfor- mance evaluation may necessitate adjustments in the training phase, such as using different algorithms, or modifying the approach used in the realization step, such as choosing between kernel-space and userspace deployment.

J. Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data

[10] The paper introduces a novel approach to network intrusion detection by avoiding manual feature design and directly analyzing raw flow data information. A new model, the deep hierarchical network, is proposed, combining im- proved LeNet-5 and LSTM neural network structures to learn both spatial and temporal features of flows. The hierarchical network is trained simultaneously using a designed cascading method, eliminating the need to train two networks separately. The evaluation is conducted on the CICIDS2017 and CTU datasets, known for their large number and diverse types of flows with relatively new attack patterns. Experimental results demonstrate that the proposed hierarchical network outperforms other intrusion detection models, achieving the highest detection accuracy. Additionally, the paper presents an analysis method for traffic features, contributing to abnormal traffic detection and providing meaningful interpretations for these important features. We believe that artificially designing and extracting flow features for network intrusion detection may result in the loss of crucial traffic information, impacting detection accuracy. Our approach, outlined in this paper, involves extracting the original flow information and utilizing our specially designed hierarchical network for abnormal flow detection. This network, a combination of CNN and LSTM models, is tailored to learn spatial and temporal features directly from the original flow data. To our knowledge, this marks the first instance of leveraging the original flow infor- mation for feature learning. Our proposed hierarchical network model surpasses other network intrusion detection models significantly. Using the CICIDS2017 and CTU datasets, our experiments demonstrate that our model achieves remarkably high accuracy, precision, recall, and F1-measure. Additionally, our analysis of features contributing significantly to abnormal traffic detection revealed previously underutilized features by other researchers.

III. CONCLUSION

In conclusion, this comprehensive review underscores the multifaceted nature of network intrusion detection tech- niques and their critical role in contemporary cybersecurity. Signature-based methods have proven effective in identifying known threats, yet their limitations in addressing novel and evolving attacks necessitate ongoing innovation. Anomaly- based approaches, leveraging machine learning and statistical models, showcase promising advancements in adapting to dynamic network behaviors, but challenges such as false positives persist. The synthesis of current literature reveals a growing need for holistic intrusion detection systems that integrate the strengths of both signature-based and anomaly-based methods. The future of network intrusion detection lies in the seamless fusion of advanced machine learning algorithms, real-time processing capabilities, and adaptive strategies that can discern sophisticated, evolving threats. As the cyber threat landscape continues to evolve, with attackers employing increasingly sophisticated techniques, the importance of continuous research and development in intru- sion detection cannot be overstated. The integration of artifi- cial intelligence, behavior analysis, and collaborative defense mechanisms emerges as a promising direction for enhancing the resilience of network security. Ultimately, this review provides a valuable resource for researchers, practitioners, and policymakers in understanding the current state of network intrusion detection and envisioning future directions. The ongoing pursuit of innovative approaches, coupled with a proactive stance against emerging threats, will be essential to maintaining the integrity and security of networked systems in the face of an ever-changing digital landscape.

REFERENCE

1. Vanlalruata Hnamte , Hong Nhung-Nguyen , Jamal
2. Hussain , Yong Hwa-Kim,"A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE"
3. Thomas Rincy N 1 , Roopam Gupta,"Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques"
4. Treepop Wisanwanichthan ,Mason Thammawichai,"A

5. Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM”
6. Xianwei Gao , Chun Shan , Changzhen Hu, Zequn Niu ,
7. And Zhen Liu,”An Adaptive Ensemble Machine Learning Model For Intrusion Detection”
8. Taehoon Kim , Wooguil Pak,”Early Detection Of Network Intru- Sions Using A Gan-Based One-Class Classifier”
9. Li Zou , Xuemei Luo , Yan Zhang , Xiao Yang , And
10. Xiangwen Wang 1gansu Provincial Meteorological Informat,”Hc- Dttsvm: A Network Intrusion Detection Method Based On Decision Tree Twin Support Vector Machine And Hierarchical Clustering ”
11. Hongyu Yang , Fengyan Wang,”Wireless Network Intrusion Detection Based On Improved Convolutional Neural Network”
12. Zhijie Fan , Zhiwei Cao,”Method Of Network Intrusion Discov- Ery Based On Convolutional Long-Short Term Memory Network And Implementation In Vss”
13. Gustavo De Carvalho Bertoli , Lourenc¸O Alves Pereira Ju´ Nior , Osamu Saotome , Aldri L. Dos Santos
14. , Filipe Alves Neto Verri , Cesar Augusto Cavalheiro Marcondes , Sidnei Barbieri , Moises S. Rodrigues ,
15. And Jose´ M. Parente De Oliveira,”An End-To-End Framework For Machine Learning-Based Network Intrusion Detection System ”
16. Yong Zhang, Xu Chen, Lei Jin, Xiaojuan Wang, Da
17. GUO,”Network Intrusion Detection: Based on Deep Hierarchical Net- work and Original Flow Data”.

HOW TO CITE: Hiba Fathima K. P.*, Anugraha P. P., A Review on Network Intrusion Detection, Int. J. Sci. R. Tech., 2025, 2 (1), 60-66. https://doi.org/10.5281/zenodo.14598998