IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11813

Safeguarding Corporate Networks Deep Learning Based Intrusion Detection for Enhanced Security

Dafney Furtado[1], B M Bhavya[2]

PG Scholar, Department of MCA, PES College of Engineering, Mandya, Karnataka, India[1]

Assistant Professor, Department of MCA, PES College of Engineering, Mandya, Karnataka, India[2]

Abstract: Deep learning has become increasingly vital in data science, especially when handling large datasets. This paper focuses on analyzing intrusion detection attacks, which are critical for maintaining information security. The core technology lies in accurately identifying various network attacks. We explore the development of an intrusion detection system based on deep learning and propose a method using recurrent neural networks (RNN-IDS) for this purpose. Our project involves analyzing the KDD dataset, which comprises 44 features. Utilizing these features, we apply an RNN classification algorithm to train the data and assess accuracy. We also compare our results with those obtained from decision trees, support vector machines, and other machine learning techniques used by previous researchers on the benchmark dataset. This comparative analysis aims to highlight the effectiveness of RNNs in intrusion detection.

Keywords: Deep Learning, Prediction, DoS, R2L, U2R, Prob attack.

I. INTRODUCTION

In today's dynamic cybersecurity landscape, safeguarding against network attacks is an urgent and non-negotiable priority. Machine learning, particularly deep learning, has emerged as a powerful tool across business and scientific domains, revolutionizing classification techniques and streamlining recommendation processes. Notably, the focus on detecting network attacks has intensified within the sphere of social networking information security, driven by the escalating threats faced by interconnected systems. As society becomes increasingly reliant on the Internet for communication, education, and work, it also becomes more vulnerable to security breaches. In response, researchers have developed Intrusion Detection Systems (IDS) as a significant advancement in data security. These systems aim to identify ongoing intrusions or breaches that have already occurred within network traffic. The study centers on distinguishing between normal and abnormal network traffic behavior. It addresses a fivecategory classification problem, categorizing traffic normal, Denial of Service (DOS), User to Root (U2R), Probe (Probing), Root to Local (R2L). By improving these detection systems, researchers contribute to the safety and security of information systems. Ultimately, this work supports the seamless integration of the Internet into daily life by mitigating potential risks associated with networked environments. In summary, this research not only fortifies our defenses against security threats but also reinforces the reliability of networked systems in an interconnected world.

II. LITERATURE SURVEY

Zakiyabanu S. Malek, Bhushan Trivedi Axita Shah [1] This research introduces a Pattern-Based Intrusion Detection (PBID) model to augment user authentication and security by scrutinizing post-login behavior. Unlike traditional biometric verification, this approach continuously assesses user actions within the system to maintain authentication integrity. The proposed model is integrated with an existing Statistical-Based Intrusion Detection (SBID) system. This combined approach leverages a rule-based pattern recognition mechanism to fortify intrusion detection capabilities. Experimental results validate the enhanced effectiveness of the integrated PBID and SBID model in identifying intrusions.

Devrim Akgun, Selman Hizal, Unal Cavusoglu [2] This research proposes a deep learning-based Intrusion Detection System (IDS) specifically designed to identify Distributed Denial of Service (DDoS) attacks. The system employs a comparative analysis of Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Long Short-Term Memory (LSTM) models. Utilizing the CIC-DDoS2019 dataset, the study incorporates data preprocessing techniques including feature elimination and normalization. Among the models evaluated, the CNN-based inception-like architecture demonstrated superior performance, achieving 99.99% accuracy in binary classification and 99.30% in multiclass classification. Notably, this model also exhibited efficient inference times and reduced trainable parameters compared to baseline models. The findings indicate that the proposed IDS, coupled with effective preprocessing, surpasses existing state-of-the-art methods in DDoS attack detection.

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11813

Ali Bou Nassif, Manar Abu Talib, (Senior Member, IEEE), Qassim Nasir, and Fatima Mohammad Dakalbab [3] This research conducted a systematic literature review encompassing anomaly detection studies employing machine learning (ML) techniques published between 2000 and 2020. The review evaluated ML models across applications, methodologies, performance metrics, and classification approaches. An analysis of 290 articles identified 43 application domains for anomaly detection, 29 distinct ML models, and 22 datasets utilized in experimental evaluations. The findings indicate a prevalence of unsupervised anomaly detection methods. Based on these insights, the study provides recommendations and directions for future research in this promising field.

Bhawana Sharma, Lokesh Sharma, Chhagan Lal, Satyabrata Roy [4] This research presents a novel anomaly-based Intrusion Detection System (IDS) for IoT networks leveraging a deep learning approach. A filter-based feature selection method is employed to enhance a Deep Neural Network (DNN) by excluding highly correlated features. The model is refined using the UNSW-NB15 dataset, achieving an accuracy of 84%. To mitigate class imbalance, Generative Adversarial Networks (GANs) are integrated to generate synthetic minority class data, resulting in a balanced dataset and improved accuracy of 91%.

III. PROBLEM STATEMENT

This research proposes an Intrusion Detection System (IDS) utilizing Recurrent Neural Networks (RNNs). The system begins by loading and preprocessing intrusion datasets, dividing them into training and testing subsets. Data is cleaned and prepared by appropriately naming fields and removing irrelevant columns. Attack types are categorized into corresponding classes (e.g., 'ipsweep' as 'probe', 'teardrop' as 'DoS'). An RNN model, consisting of input, output, and hidden layers, is employed to process data. The model leverages the memory of past inputs to influence current outputs, enabling the detection of temporal changes within network data. This approach enhances the IDS's ability to accurately classify and detect various intrusions. Python's machine learning libraries facilitate the system's implementation.

IV. OBJECTIVE

The objective is to develop and implement a Recurrent Neural Network-based Intrusion Detection System (RNN-IDS) that improves the accuracy and speed of detecting network intrusions. This system aims to classify network traffic behaviors as normal or anomalous, addressing various attack categories such as DOS, U2R, Probe, and R2L using the NSL-KDD dataset. The project also seeks to compare the RNN approach with other machine learning methods to validate its effectiveness in detecting intrusions.

V. METHODOLOGY

The project, implemented in Python, utilizes its versatile programming capabilities to develop a robust intrusion detection system (IDS) using Recurrent Neural Networks (RNNs). Python’s dynamic typing, garbage collection, and support for multiple programming paradigms make it an ideal choice for this complex application. Leveraging its comprehensive standard library, the project integrates machine learning techniques to enhance functionality and accuracy. Key libraries used include TensorFlow, NumPy, Pandas, and Keras for building and training the neural networks, along with Flask for creating a user-friendly web interface for real-time monitoring and user interaction.

The implementation process begins with data collection and preprocessing, utilizing the NSL-KDD dataset due to its balanced distribution and effective handling of redundant records. The dataset undergoes cleaning to handle missing values and remove noise, ensuring suitability for training the neural network. Feature selection is crucial, with the dataset's 41 features and class labels being carefully chosen to enhance prediction accuracy. The core methodology revolves around training the RNN model, which is well-suited for handling sequential data due to its memory capability. The model processes input data through multiple layers, with information flowing through interconnected nodes over time steps.

Once trained, the RNN model's performance is evaluated using metrics like accuracy and is benchmarked against other machine learning methods such as decision trees and support vector machines. Visualization of the model's results, including its classification of network traffic into normal and various attack types (DOS, U2R, Probe, and R2L), is achieved through graphical representations, providing insight into its effectiveness in real-world scenarios. The final system, implemented with Python and integrated with a Flask web interface, ensures user-friendly operation, real-time monitoring, and robust intrusion detection capabilities.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024
DOI: 10.17148/IARJSET.2024.11813

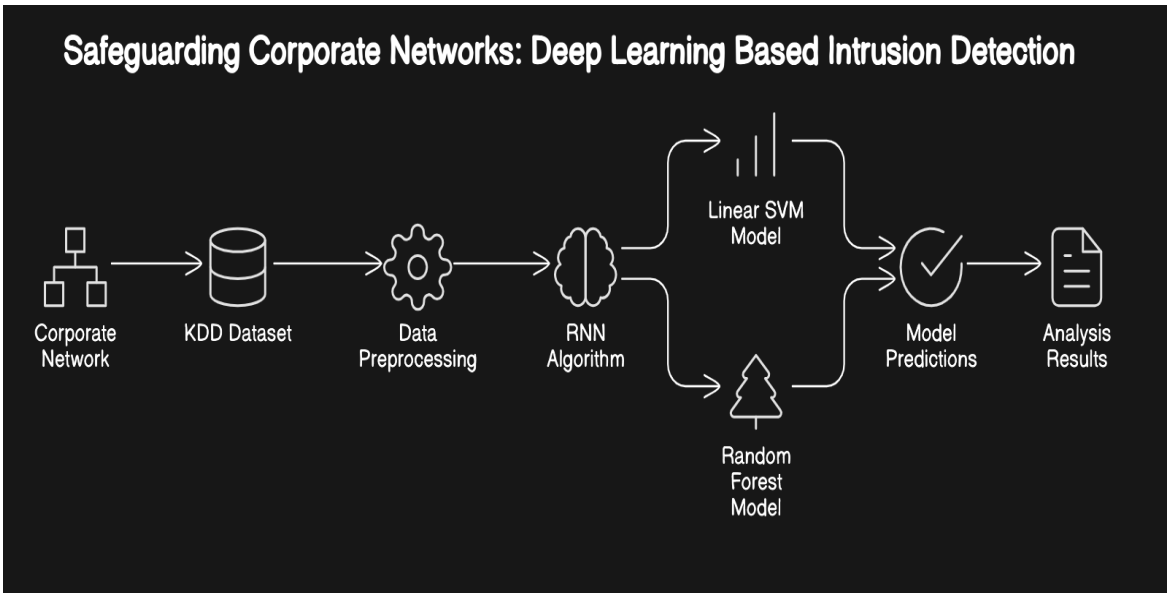

Fig.1. System Architecture

VI. PROPOSED SOLUTION

Our proposed solution involves developing an Intrusion Detection System (IDS) utilizing Recurrent Neural Networks (RNNs) to detect various types of network attacks, including DoS, U2R, Probe, and R2L, achieving superior accuracy and efficiency compared to traditional methods.

VII. SOFTWARE IMPLEMENTATION

The software implementation detailed in the provided document focuses on developing an Intrusion Detection System (IDS) using Python, leveraging Recurrent Neural Networks (RNNs) for enhanced accuracy in classifying network traffic into normal and anomalous categories, including DoS, U2R, Probe, and R2L attacks. The implementation begins with data collection from the NSL-KDD dataset, followed by preprocessing to clean and prepare the data.

Feature selection ensures that relevant attributes contribute effectively to intrusion detection. Training the RNN model involves sequential data processing through multiple layers, utilizing TensorFlow and Keras libraries for model development and optimization. Evaluation metrics such as accuracy are used to assess the model's performance against other machine learning techniques. The system includes a user-friendly web interface built with Flask, facilitating real-time monitoring and interaction with the IDS. Maintenance strategies are also discussed to ensure long-term functionality and adaptability to evolving security challenges.

Experimental results:

The experimental results of the implemented IDS using RNNs demonstrate robust performance in intrusion detection. The model achieves high accuracy rates in classifying network traffic, with specific metrics showing precision, recall, and F1-score values indicating its effectiveness in distinguishing between normal and various attack types (DoS, U2R, Probe, R2L).

Comparative analyses against traditional machine learning methods like decision trees and SVM highlight RNNs' superior capability in handling sequential data and capturing temporal dependencies crucial for detecting subtle anomalies. Visualization of results through graphs and confusion matrices further illustrates the model's ability to generalize and detect intrusions accurately across different scenarios, validating its reliability and practicality in real-world applications.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024
DOI: 10.17148/IARJSET.2024.11813

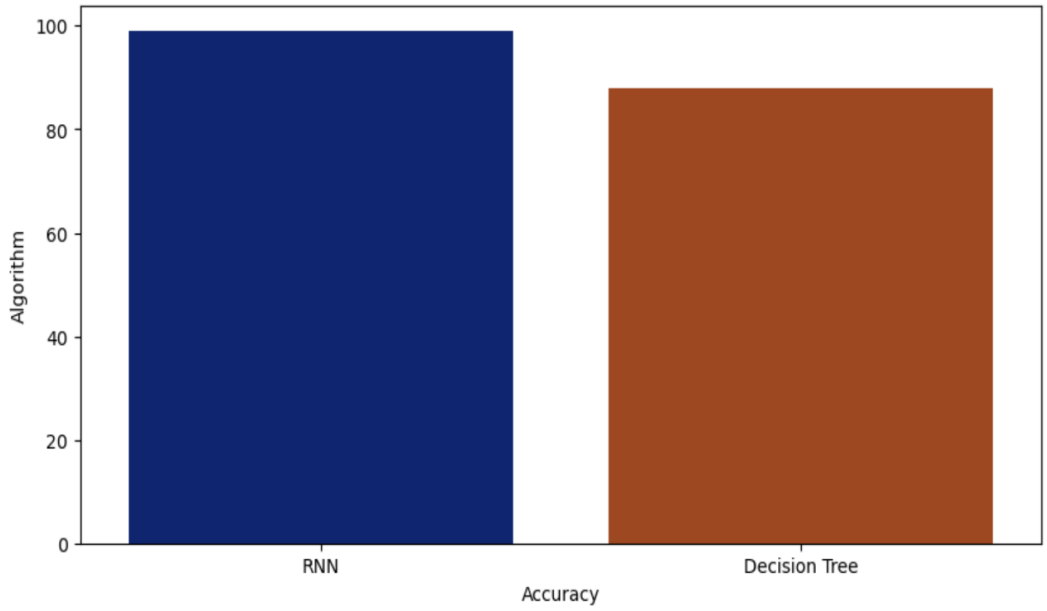

Fig.2. Accuracy Comparison of RNN and Decision Tree Algorithm

VIII. CONCLUSION AND FUTURE SCOPE

In conclusion, this project successfully demonstrates the viability of using Recurrent Neural Networks (RNNs) for intrusion detection within network security frameworks. Through meticulous preprocessing of the KDD datasets and effective feature extraction, the data fed into the RNN model was both relevant and representative of various network behaviors. The RNN model accurately identified and classified different types of network intrusions, including DoS, U2R, Probe, and R2L attacks, achieving high accuracy and maintaining a low false alarm rate. Integration and system testing confirmed the seamless operation of all components, providing a robust solution for real-time intrusion detection. Performance metrics such as precision, recall, and F1 score highlighted the model's efficacy. Future enhancements could include combining RNNs with Convolutional Neural Networks (CNNs) to create a hybrid model capturing both temporal and spatial features, implementing distributed computing frameworks like Apache Spark or Hadoop for handling large-scale data, and incorporating behavioral analysis techniques for more precise anomaly detection. These advancements would ensure ongoing protection and resilience of network infrastructures against evolving cyber threats.

REFERENCES

[1]. Anderson, J. P., "Computer Security Threat Monitoring and Surveillance," Technical report, James P. Anderson Company, 1980.
[2]. Denning, D. E., "An Intrusion Detection Model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222-232, 1987.
[3]. Lee, W., & Stolfo, S. J., "Data Mining Approaches for Intrusion Detection," Proceedings of the 7th USENIX Security Symposium, pp. 79-94, 1998.
[4]. Peddabachigari, S., Abraham, A., & Thomas, J., "Intrusion Detection Systems Using Decision Trees and Support Vector Machines," International Journal of Computer and Information Technology, vol. 1, no. 1, pp. 1-7, 2005.
[5]. Kim, G., Lee, S., & Kim, S., "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690-1700, 2014.
[6]. Niyaz, Q., Sun, W., & Javaid, A. Y., "A Deep Learning Approach for Network Intrusion Detection System," Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, pp. 21-26, 2016.
[7]. Zhao, Z., & Wang, Z., "Machine Learning in Network Intrusion Detection," Proceedings of the International Conference on Computer Communications, pp. 1-9, 2008.
[8]. Tang, T. A., Mhamdi, L., & McLernon, D., "Deep Learning Approach for Network Intrusion Detection in Software Defined Networking," Proceedings of the International Conference on Wireless Networks and Mobile Communications, pp. 258-263, 2016.