BOOSTING NETWORK SECURITY: A COMPARATIVE ANALYSIS OF DEEP LEARNING TECHNIQUES FOR INTRUSION DETECTION USING CNN & RNN

Project Reference No.: *47S_BE_4602*

College *: East Point College of Engineering and Technology, Bengaluru*
Branch *: Department of Computer Science and Engineering*
Guide(s) *: Dr. Heena Kousar*
Student(S) *: Mr. Adarsh Pawar*
Mr. Mohnish Reddy G
Mr. Mukeshreddy Nagireddygari
Mr. Shaik Athiq Rehaman

Keywords:

Adaptive Learning, Deep learning, Intrusion Detection System, Adaptive Synthetic Sampling

Background:

As 5G technology continues to expand, wireless networks are becoming increasingly vulnerable to attacks, leading to heightened concerns about network security. Traditional security measures like firewalls and encryption are often insufficient in addressing modern threats such as Denial of Service (DoS) and probing attacks.
Intrusion Detection Systems (IDS) play a crucial role in detecting these threats by classifying network traffic based on acquired attributes, enabling early anomaly detection and preventive measures. Conventional machine learning methods are commonly used for attack detection, involving stages like data gathering, feature selection, and classification. Feature encoding strategies enhance classifier performance, with increased discretization generally improving model effectiveness.
Efforts to improve IDS efficiency have led to innovations like using Principal Component Analysis (PCA) for feature selection and optimizing feature sets with edge density algorithms. Classification techniques like decision trees, support vector machines, and artificial neural networks are widely employed for categorizing network traffic. Hybrid approaches, combining classifiers like SVM with k-means clustering, have shown promise in enhancing detection capabilities. Despite the effectiveness of traditional machine learning techniques, adapting to dynamic network environments remains a challenge.
Deep learning (DL) has emerged as a powerful tool in intrusion detection due to its ability to autonomously generate key features without complex feature engineering. Techniques like Particle Swarm Optimization (PSO) applied to Deep Belief Networks (DBN) have shown high accuracy in detecting attack. Recurrent neural networks and convolutional neural networks (CNNs) are also utilized for intrusion detection tasks, with CNNs often exhibiting higher accuracy compared to traditional DL methods. Ongoing research aims to develop

novel attack recognition methods using techniques like residual networks and data augmentation algorithms like ADASYN.

Objectives of the Project

• Develop and deploy a deep learning-based intrusion detection system tailored for cloud environments.
• Evaluate the system's performance in detecting various types of intrusions, including known and zero-day attacks, and assess its ability to adapt to new threats.
• Investigate the scalability of the intrusion detection system to accommodate the dynamic and resource-intensive nature of cloud computing.
• Implementation of these technology in latest datasets.

Methodology:

The proposed system consists of the following listed modules

1. Data Acquisition and Preprocessing: Leverage the paper's recommendation of using cloud APIs and network capture tools to gather diverse data sources (logs, network traffic) from your cloud environment. Implement data preprocessing steps like cleaning, filtering, and normalization as described in the paper, potentially utilizing tools like Flink or Kafka Streams for real-time processing and Spark/Hadoop for offline tasks.

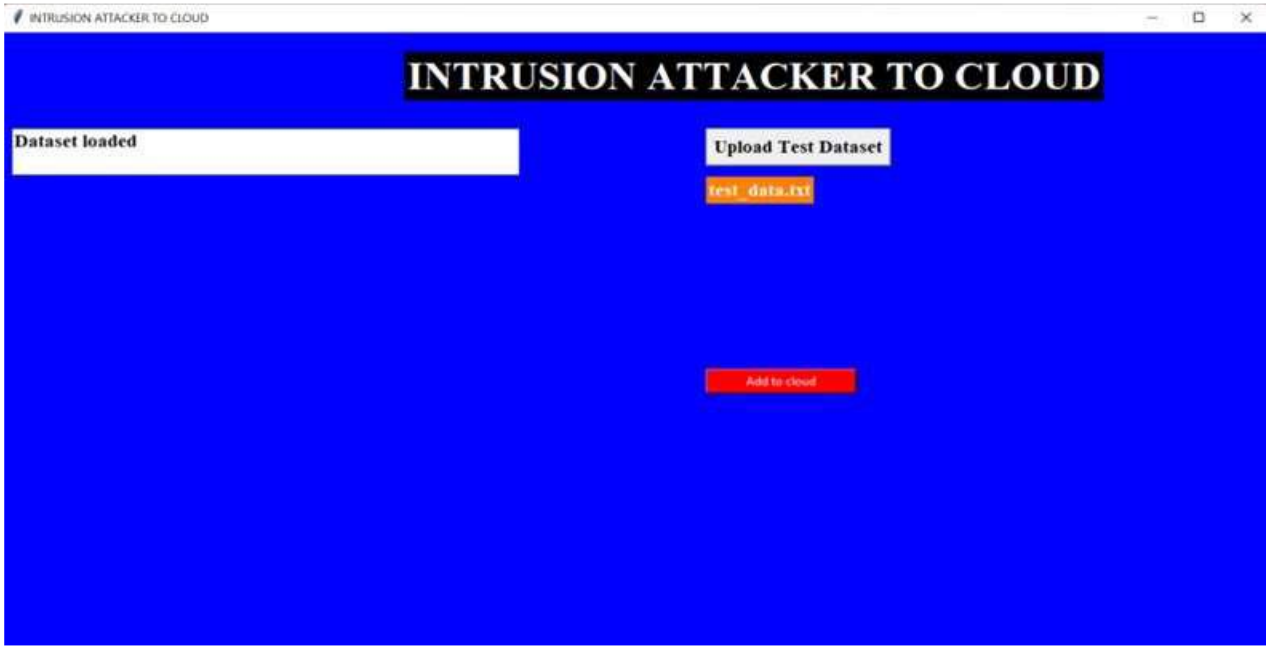
2. Feature Engineering: Key features are extracted and scaled from the image, encoded for compatibility, and then processed by a deep neural network to classify it accurately.

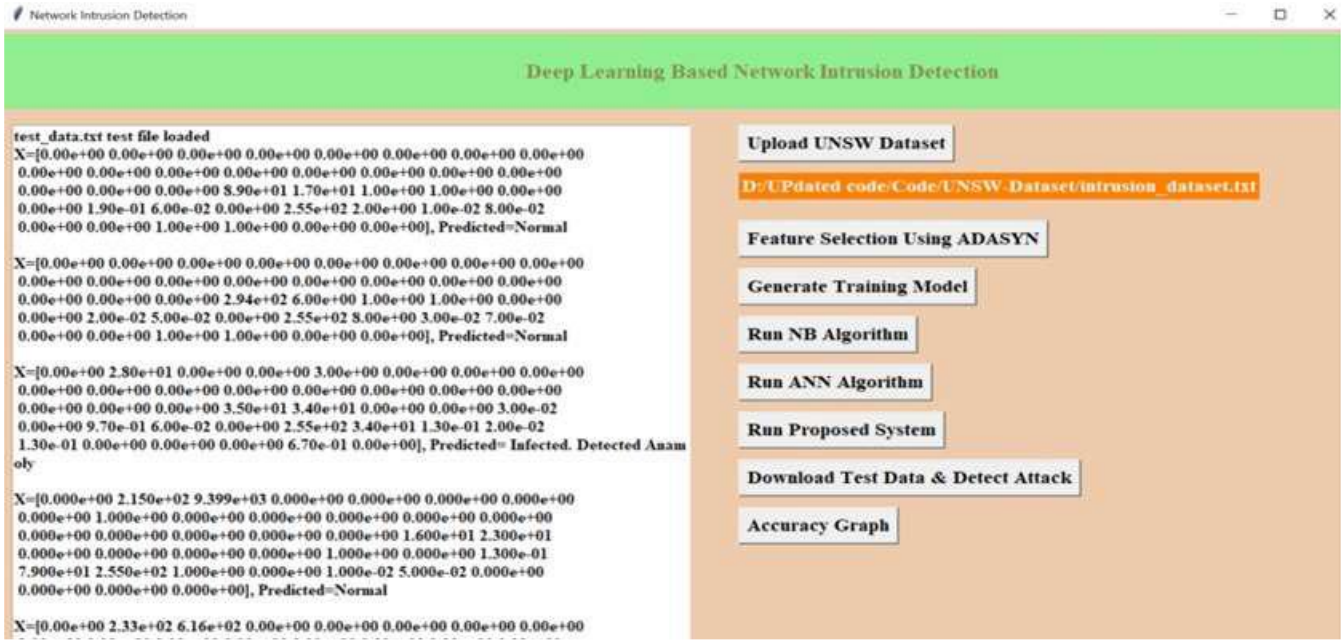
3. Model Training and Classification: Using deep learning algorithms like Recurrent Neural Network (RNN), and Convolutional Neural Network (CNN) to train the model. Using a platform like AWS Sage Maker or Azure Machine Learning for training and deploying the model as a microservice or serverless function for near-real-time predictions.

4. Intrusion Detection and Response: Integrate the system with a Security Information and Event Management (SIEM) platform like Splunk or Elastic Stack to generate alerts and investigate potential intrusions based on predicted anomalies. Implement automated response playbooks within the SIEM or cloud platform to block suspicious traffic, isolate infected resources, and notify security personnel.

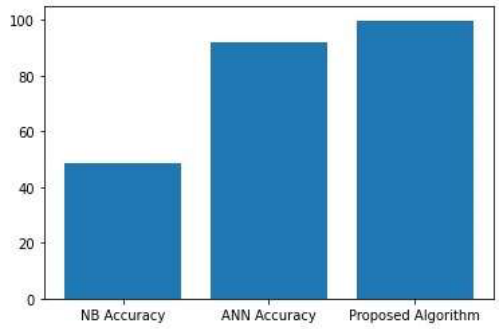
5. Model Management and Evaluation: Monitoring key metrics like accuracy, precision, and recall using dashboards within your chosen platform or custom visualization tools.

Result:





The performance evaluation results are presented in the bar graph, comparing the accuracy of three different algorithms: NB (Naive Bayes) Algorithm, ANN (Artificial Neural Network) Algorithm, and Proposed Algorithm. As we can see from the graph, the Proposed Algorithm showed the highest accuracy among the three models that have been assessed.



The Proposed Algorithm outperforms the other two algorithms in terms of accuracy as indicated by its larger bar representation. Although the ANN Algorithm outperformed the NB Algorithm, it lacked the efficiency of the Proposed Algorithm.

The algorithm with the NB performance produced the lowest accuracy rate, arrived as the shortest bar in the graph.

Conclusion:

In conclusion, our examine tackles critical challenges faced by means of intrusion detection systems (IDS), that specialize in records distribution imbalances and interchannel redundancy in current neural network (NN)-based fashions. Our approach aims to reinforce IDS by means of leveraging superior strategies in information balancing, feature extraction, and model architecture. We stress the significance of records balance to save you model bias closer to massive samples even as neglecting smaller ones. The Adaptive Synthetic Sampling Method (ADASYN) correctly addresses this imbalance, making sure a truthful and consultant dataset for schooling.

Our split-based ResNet framework introduces key advancements. It enables multiscale characteristic extraction through more than one convolution phases, enriching network visitors statistics representation. It additionally mitigates interchannel redundancy, enhancing the model's capability to capture nuanced patterns. Furthermore, the incorporation of a soft hobby operation in ResNet enables sensible characteristic utilization, significantly boosting version expressiveness and performance in intrusion detection tasks. Our experimental effects, specifically with the hybrid ResNet model and ADASYN, display brilliant enhancements across diverse assessment criteria.

Despite these improvements, optimization for execution efficiency and accuracy for smaller samples stays a focus. Moving forward, we goal to refine our method, that specialize in improving IDS identification skills thru a streamlined residual network structure with more desirable residual blocks. By innovating and integrating superior methodologies, we contribute notably to intrusion detection and cybersecurity.

Description of the innovation in the project:

This project addresses demanding situations in Intrusion Detection Systems (IDS) by way of combining the Adaptive Synthetic Sampling (ADASYN) method with a break up-primarily based Resnet framework. ADASYN balances sample distribution, overcoming biases in the direction of large samples. Our method extracts multiscale functions, reduces interchannel redundancy, and enhances the version's capability using a smooth hobby operation. We recommend a Residual Neural Network (ResNN) version for intrusion detection, displaying massive enhancements in recognition accuracy and execution performance. Ongoing work targets to optimize performance further, highlighting the capacity for extra strong IDS solutions.

Future work scope:

Analysing the statistics and research provided, several avenues for destiny enhancement in intrusion detection structures (IDS) and community security emerge.
Firstly, exploring advanced sampling techniques past ADASYN and RENN may want to show fruitful. Techniques like SMOTE-NC or Borderline-SMOTE offer ability enhancements in dealing with imbalanced datasets and producing artificial samples more effectively. Secondly, endured advancements in deep getting to know architectures which include variations of ResNet, DenseNet, or EfficientNet can beautify function extraction and getting to know capabilities for complicated community visitors information. Thirdly, ensemble methods like Random Forests or Gradient Boosting Machines may be incorporated to improve version robustness and decrease fake positives. Additionally, growing adaptive characteristic choice algorithms, incorporating real-time stream processing frameworks, integrating explainable AI strategies, and discovering modern techniques for zero-day assault detection are promising areas for boosting IDS talents and addressing rising cybersecurity challenges efficiently. These avenues together goal to make IDS more adaptive, accurate, and responsive in mitigating evolving community threats.