COURSE PROJECT: CS-725: FUNDAMENTALS OF MACHINE LEARNING

INTRUSION DETECTION USING STACKED ENSEMBLE CLASSIFIER

Introduction:

The project focuses on developing an automated intrusion detection system leveraging machine learning techniques to enhance cybersecurity measures. Given the increasing sophistication and volume of cyber threats, traditional manual intrusion response methods have become inadequate for timely and effective mitigation. This work utilizes the UNSW-NB15 dataset, which is extensively employed for cybersecurity research, containing network traffic data with a variety of cyber attacks, including denial-of-service (DoS), worms, and exploits. The dataset is rich, comprising 100 GB of raw traffic captured via Tcpdump and processed into feature sets extracted by tools such as Argus and Bro-IDS. It contains 45 features with a total of approximately 257,673 records split into a training set of 175,341 records and a testing set of 82,332 records.

Data Pre-processing:

The initial data preprocessing phase involved the removal of irrelevant columns, followed by splitting the data into a training set (95%) and a validation set (5%). Categorical features were transformed into numeric format using label encoding. To ensure uniformity and to facilitate the convergence of learning algorithms, Min-Max scaling was applied to normalize all feature values to a range between 0 and 1. This preprocessing pipeline aimed to enhance the learning process by reducing noise and ensuring that feature scales did not disproportionately influence the models.

Models/Algorithms used for intrusion detection:

The project explored two primary modeling approaches for intrusion detection. The first model centered around an autoencoder, a type of unsupervised neural network used here for feature compression and extraction. The autoencoder was structured with 42 input neurons corresponding to input features, followed by hidden layers with 64 and 20 neurons respectively, and then expanded back through additional layers, all activated by the ReLU function. The training configuration used mean squared error (MSE) as the loss function and Adam optimizer with 10 epochs and a batch size of 32. After training, the compressed 20-dimensional encoded features from the bottleneck layer were extracted and augmented with the original dataset to serve as inputs for classification models. Two classifiers were tested: a Random Forest and a Stacking classifier. The stacking approach combined support vector machines (SVM), Random Forest, and logistic regression as the meta-classifier, capturing complex decision boundaries for better detection performance.

The second modeling approach replaced the autoencoder with Principal Component Analysis (PCA) for dimensionality reduction. Here, PCA-transformed features derived from the normalized data were used as input to a Random Forest classifier. This method aimed to capture the most significant variance components in the data, providing a simpler yet effective feature representation for classification.

Results:

The performance results from the experiments demonstrated that both approaches successfully distinguished between normal and attack traffic, with varying degrees of effectiveness. The PCA combined with the Random Forest classifier overall accuracy and balanced performance metrics, including weighted precision, recall, and F1-score, all reaching approximately 0.89. The PCA combined with the stacking classifier performed well among the all, with an accuracy close to 0.92

and balanced F1-score, outperforming the autoencoder with only Random Forest. Loss curves from the autoencoder training reflected a steady decrease in training and validation loss, indicating effective learning and generalization.

Conclusion:

In summary, the study highlights the value of advanced feature extraction and dimensionality reduction techniques such as autoencoders and PCA in the cybersecurity domain for intrusion detection. Combining these techniques with robust classification models like Random Forest and Stacking classifiers can significantly improve detection accuracy and responsiveness to complex cyber threats. The project also underscores the importance of rigorous data preprocessing steps and the use of large and diverse datasets to build reliable machine learning-based security systems.