**Instruction detection system using kdd cup datasets**

*PROJECT REPORT*

*Submitted in the partial fulfilment of the requirements for award of the*

Six Months Online Certificate Course

In

**Cyber Security/**

**Data Science with Python Programming/ Artificial Intelligence and Machine Learning**

**Course Duration: [22-01-2024 to 21-07-2024]**

**By**

BAYAMMA GARI REVATHI

(Ht. No.2406CYS108)

Under the Esteemed Guidance

Prof. /Dr. /Mr. NILADRI DEY,

Coordinator of Cyber Security Course Professor & HOD,

Department of CSE,

JNTUH University College of Engineering



DIRECTORATE OF INNOVATIVE LEARNING & TEACHING (DILT)

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**

(Formerly SCDE\_SCHOOL OF CONTINUING AND DISTANCE EDUCATION)

Kukatpally, Hyderabad, Telangana State, INDIA- 500 085

**JULY 2024**

***Abstract — Intrusion Detection provides a technique of identifying unwanted packets so the attacks or harm made from these intrusions can be minimize. Since various techniques are implemented for the discovery and categorization of intrusions. Some of the IDS is implemented on the network based and some are implemented for Host based. Here in this paper a survey of all the techniques implemented for the discovery and categorization of intrusions on KDDCup 99 dataset is discussed, so that by identifying their various issues a new and efficient technique is implemented which can classify and detection intrusions in KDDCup 99 dataset.***

Introduction :

Intrusion Detection Systems (IDS) are crucial for securing network infrastructure against cyber threats. They monitor network traffic for suspicious activities and potential intrusions. The KDD Cup 1999 dataset, derived from DARPA’s 1998 intrusion detection system evaluations, provides a benchmark for evaluating IDS performance. This project leverages the KDD Cup dataset to design, implement, and evaluate an effective IDS using various machine learning techniques.

Security is an important issue in the web log data where the flow of packets contains a number of intruders. Intrusion detection can be detected using misuse detection or anomaly detection. It can be implemented at Host level or network level.

Protecting networks from computer security attacks is a vital apprehension of computer security. As network traffic may lead to variety of information exchange and sensitive data transfer. Although it is also well known that the dependency of network are also emerging rapidly. Due to this the network condition are very crucial now a days and it will become more complicated in forthcoming time. This traffic may lead to massive damage of network system and its related resources.

Anomaly detection is a way of analyzing the traffic network on the basis of traffic pattern so that the unwanted and malicious attacks can be detected.

Network behaviors that cannot be characterized by any model for such condition non-model based approaches are used. Non-model based approaches can be auxiliary classified based on the unambiguous implementation and accuracy constraints that have been imposed on the detector.

Misuse Detection is the way of analyzing the identity of intrusions so that the malicious activity is detected. Misuse detection approaches analyze host or network activity, looking for events that match patterns of known attacks (signatures). First a reference database of attack signatures is constructed, and then monitored events from sensors data are compared against this database for evidence of intrusions Signature matching is the most commonly

employed misuse detection technique. For instance, Snort is a well-known open source signature-based network intrusion detection system.

Other misuse detection approaches include rule-based systems, state transition analysis, machine learning and data mining techniques.

All Traffic

Benign Traffic

Malicious Traffic

ALert

No Alert

Alert

No Alert

FN

TP

TN

FP

Anomaly Identification Process

# KDD Cup99 Dataset

KDD Cup99 dataset contains about 4GB of compressed data in hwihc nearly 7 weeks of network traffic data is collected. It contains 41 feature attributes of the network traffic and contains classes as normal and attacks. The Dataset contains various attacks such as Denial of Service Attack (DOS), User to Root Attack (U2R), Remote to Local Attack (R2L) and Probing Attack.

The table shown below is the summary statistics of the KDD Train Set.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Original Records** | **Distinct Records** | **Reduction Rate** |
| **Attacks** | 3,925,650 | 262,178 | 93.2% |
| **Normal** | 972,781 | 812,814 | 16.44% |
| **Total** | 4,898,431 | 1,074,992 | 78.05% |

Training Dataset

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Original Records** | **Distinct Records** | **Reduction Rate** |
| **Attacks** | 250,436 | 29,378 | 88.26% |
| **Normal** | 60,591 | 47,911 | 20.92% |
| **Total** | 311,027 | 77,289 | 75.15% |

Testing Dataset

Literature Survey:

Summarize existing research and developments related to intrusion detection using the KDD Cup 99 dataset. Discuss various approaches, techniques, and models that have been applied. Highlight the strengths and limitations of these methods and identify gaps that your work aims to address.

Overview of KDDCup99 Dataset:

**Description:**

The KDDCup99 dataset is a widely used benchmark dataset for evaluating intrusion detection systems. It contains network traffic data labeled with various types of attacks, including Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and Probing attacks.

**Structure:**

The dataset includes a variety of features such as connection duration, protocol type, and error rates, which are used to classify network connections as either normal or attack-related.

Common Research Themes:

**Feature Selection and Engineering:**

Many studies focus on selecting the most relevant features from the KDDCup99 dataset to improve IDS performance. Techniques like Principal Component Analysis (PCA) and feature scaling are commonly explored.

**Classification Techniques:**

Research often evaluates different machine learning algorithms for classifying network traffic, including:

**Decision Trees:**

Used for their interpretability and performance.

Support Vector Machines (SVM):

Known for their ability to handle high-dimensional data.

\*Neural Networks\*:

Explored for their capability to model complex patterns.

\*Ensemble Methods\*:

Combining multiple classifiers to improve accuracy.

\*Anomaly Detection\*:

Some studies focus on detecting deviations from normal behavior using statistical methods or machine learning models.

\*Performance Evaluation\*:

Papers frequently evaluate IDS performance using metrics such as accuracy, precision, recall, and F1-score. They may also address issues like false positives and false negatives.

**Methodological Approaches:**

Data Preprocessing:

Research often discusses techniques for handling missing values, normalizing data, and encoding categorical variables.

Model Training and Testing:

Studies vary in their approach to splitting the dataset for training and testing, with some using cross-validation methods to ensure robustness.

- \*Hybrid Models\*: Some research explores combining multiple models or techniques to enhance detection capabilities.

Challenges and Limitations

\*Imbalanced Data\*:

The KDDCup99 dataset is known for its imbalanced distribution of attack types, which can skew performance metrics.

Evolving Threats:

The dataset's relevance may decrease over time as new attack techniques emerge, requiring ongoing adaptation of IDS models.

Overfitting:

Researchers need to ensure that their models do not overfit the dataset, which can impact generalization to real-world scenarios.

Notable Studies and Contributions

Classical Approaches:

Many early studies utilized traditional machine learning algorithms and provided baseline comparisons.

Recent Advances:

More recent research often explores deep learning and other advanced techniques, addressing some limitations of earlier methods.

**Future Directions**

-\*Enhanced Features\*: Research is ongoing to incorporate additional features or use more advanced feature engineering techniques.

\*Real-Time Detection\*: There's a growing focus on developing IDS systems capable of real-time detection and response.

Dataset Improvements\*: Proposals for updating or expanding the KDDCup99 dataset to include more diverse and current attack scenarios.

Problem Statement

Clearly define the problem your IDS aims to solve. This could involve improving detection accuracy, reducing false positives, or enhancing the system's ability to identify new types of attacks. Explain why this problem is significant and what impact solving it would have.

\*Objective:\*

Develop an Intrusion Detection System (IDS) that can effectively identify and classify different types of network attacks using the KDDCup99 dataset.

\*Background:\*

The KDDCup99 dataset is a widely used benchmark dataset for intrusion detection research. It contains network traffic data with various features and is labeled with attack types and normal traffic. The dataset is divided into training and testing sets, with the training set containing a broad range of attack types.

\*Key Challenges:\*

1. \*Data Imbalance:\* The dataset is highly imbalanced with a disproportionate number of normal instances compared to attack instances.

2. \*Feature Selection:\* The dataset has many features, some of which may be irrelevant or redundant. Effective feature selection is crucial for improving the performance of the IDS.

3. \*Class Labeling:\* The dataset includes multiple types of attacks, which need to be accurately classified into categories such as Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R).

\*Tasks:\*

1. \*Data Preprocessing:\*

- Clean the dataset by handling missing values and normalizing features.

- Address the class imbalance through techniques like oversampling, undersampling, or using synthetic data generation methods.

2. \*Feature Selection:\*

- Identify and select the most relevant features that contribute to intrusion detection.

- Implement feature reduction techniques such as Principal Component Analysis (PCA) or feature importance ranking.

3. \*Model Development:\*

- Train various machine learning models (e.g., Decision Trees, Random Forest, Support Vector Machines, Neural Networks) using the processed data.

- Evaluate models based on performance metrics such as accuracy, precision, recall, F1-score, and AUC-ROC.

4. \*Evaluation and Tuning:\*

- Use cross-validation to assess model performance and avoid overfitting.

- Fine-tune model parameters and select the best-performing model.

5. \*Deployment and Testing:\*

- Test the IDS on the unseen test set to evaluate its effectiveness in real-world scenarios.

- Ensure that the system can handle real-time data and adapt to evolving attack patterns.

\*Expected Outcomes:\*

A well-trained IDS capable of accurately detecting and classifying network intrusions.

Improved detection rates for various types of attacks with minimized false positives and false negatives.

Insights into the most important features and the overall effectiveness of different machine learning approaches in intrusion detection.

This problem statement sets the stage for developing a robust IDS using the KDDCup99 dataset, addressing the complexities and challenges associated with network security and intrusion detection.

Objectives

List the specific goals of your IDS project, such as:

- To develop an IDS model using the KDD Cup 99 dataset.

- To compare the performance of different algorithms.

- To achieve a certain level of accuracy or other performance metrics.

\*Data Preparation and Cleaning\*

- \*Objective:\* Clean and preprocess the KDDCup99 dataset to ensure high-quality input for model training.

- \*Tasks:\*

- \*Handle Missing Values:\* Impute or remove records with missing feature values.

- \*Normalize Data:\* Scale features to a consistent range to improve model performance.

- \*Encode Categorical Variables:\* Convert categorical features into numerical format using techniques like one-hot encoding.

\*Feature Engineering and Selection\*

- \*Objective:\* Enhance the dataset by selecting and engineering relevant features to improve model accuracy.

- \*Tasks:\*

- \*Feature Selection:\* Identify and retain the most informative features while discarding irrelevant or redundant ones.

- \*Feature Transformation:\* Apply transformations or create new features that may capture underlying patterns better.

Handling Class Imbalance:

Objective: Address the imbalance between normal and attack records to ensure the model performs well across all classes.

Tasks:

Resampling Techniques:

Implement oversampling (e.g., SMOTE) or undersampling methods to balance the class distribution.

Cost-sensitive Learning:

Modify the learning algorithm to account for class imbalance by adjusting misclassification costs.

Model Development and Training:

Objective:

Develop and train various machine learning models to detect and classify network intrusions.

Tasks:

Model Selection:

Evaluate different algorithms such as Decision Trees, Random Forests, Support Vector Machines, and Neural Networks.

Model Training:

Train the selected models using the training subset of the dataset.

Model Evaluation and Validation:

Objective: Assess the performance of the trained models to ensure they effectively detect and classify attacks.

Tasks:

Cross-Validation:

Use techniques like k-fold cross-validation to validate the models and prevent overfitting.

Performance Metrics:

Measure model performance using metrics like accuracy, precision, recall, F1-score, and AUC-ROC.

Model Tuning and Optimization:

Objective:

Fine-tune model parameters to enhance performance and generalizability.

Tasks:

Hyperparameter Tuning:

Optimize model parameters using grid search or random search techniques.

Ensemble Methods:

Combine multiple models to improve overall detection performance through techniques like bagging or boosting.

Deployment and Real-time Testing:

Objective:

Implement the IDS in a real-time environment and test its effectiveness with live data.

Tasks:

Real-time Integration:

Ensure the IDS can process and analyze network traffic in real-time.

Continuous Monitoring:

Monitor the system's performance and make adjustments as needed to address new types of attacks or changes in network traffic.

Reporting and Documentation:

Objective:

Document the development process, model performance, and system deployment details.

Tasks:

Results Analysis:

Provide a detailed analysis of model performance, including strengths and limitations.

Technical Documentation:

Create comprehensive documentation outlining the methodologies, models used, and system integration details.

Methodology

Describe the overall approach and steps you will take to develop your IDS. This should include:

- Data preprocessing (cleaning, normalization, encoding).

- Feature selection and extraction.

- Model training and testing.

- Evaluation methods.

Algorithms

Detail the algorithms and models you will use for intrusion detection, such as:

- \*Decision Trees\*: Describe how decision trees work and their advantages.

- \*Random Forests\*: Explain the ensemble approach and how it improves performance.

- \*Support Vector Machines (SVM)\*: Discuss SVM's role in classification tasks.

- \*Neural Networks\*: Include details on using deep learning techniques if applicable.

- \*Clustering Methods\*: Mention any unsupervised methods like K-means if used.

Implementation

Provide details on how you will implement your IDS, including:

- \*Data Preparation\*: Steps taken to prepare the dataset.

- \*Model Training\*: Configuration of the chosen algorithms and training process.

- \*Evaluation\*: Methods used to assess model performance.

- \*Tools and Libraries\*: Python, Scikit-learn, TensorFlow, etc.

Conclusion

Summarize the key findings of your work. Discuss the effectiveness of your IDS, how well it met the objectives, and the significance of your results.

Future Scope

Outline potential areas for future research and improvements. This might include exploring new algorithms, enhancing feature selection, or adapting the system to handle more recent attack vectors.

References

List all the sources you referenced while preparing the document. This includes research papers, books, articles, and any online resources used.