K.R. MANGALAM UNIVERSITY

THE COMPLETE WORLD OF EDUCATION

Recognised under the section 2 (f) of the UGC Act 1956

Empowering the Youth; Empowering the Nation

K.R. MANGALAM UNIVERSITY

THE COMPLETE WORLD OF EDUCATION

NETWORK INTRUSION DETECTOR USING ML

Second Year Project Synopsis
Submitted by

ROLL	NAME
2301730287	Kashish Negi

Industry Mentor: Mr. Surendra Singh

Faculty Mentor: Ms. Megha

Project Overview

Network Intrusion Detection Systems (NIDS) are designed to monitor network traffic for suspicious activity and alert the system or network administrator. Using machine learning, we can build models that automatically detect and potentially even prevent intrusions by analyzing patterns and anomalies in network data.

- **Key Approaches:**
- **Supervised Learning:** Trains on labeled data (e.g., decision trees, SVM).
- **Unsupervised Learning:** Identifies anomalies in unlabeled data (e.g., clustering, autoencoders).
- **Reinforcement Learning:** Learns from feedback to improve detection over time.

- **Benefits:**
- Adaptable to new threats
- Scalable for large datasets
- Reduced false positives and real-time detection

Specific Objectives

- To develop an adaptive, scalable, and efficient network intrusion detection system using machine learning to enhance security and reduce response times.
- Implement machine learning algorithms to detect both known and unknown network threats.
- Minimize false positives to improve detection accuracy and reduce alert fatigue.
- Enable real-time intrusion detection for large-scale network environments.
- Continuously adapt the system to evolving attack patterns and new vulnerabilities.

Key Features

Key Features of Network Intrusion Detection System:-

1.Machine Learning Integration:

•Utilizes advanced machine learning algorithms (e.g., Decision Trees, Random Forest, SVM) for accurate intrusion detection.

2.Real-time Monitoring:

•Continuously monitors network traffic for any signs of malicious activity, providing instant alerts.

3.Comprehensive Data Analysis:

•Analyzes large datasets with high accuracy and minimal false positives.

4.Scalability:

•Capable of scaling to accommodate increasing network traffic and data volume.

Project Use cases & Scope

Project Use Cases:-

•**Enterprise Network Security:**

•Detects and mitigates intrusions in large-scale corporate networks.

•Protects sensitive data and intellectual property from cyber threats.

•**Cloud Infrastructure Protection:**

•Monitors and secures cloud-based environments.

•Ensures compliance with security standards and regulations.

Scope of the Project:-

•**Data Collection:**

•Collect network traffic data from various sources, including routers, switches, and firewalls.

•**Algorithm Development:**

•Develop and implement machine learning algorithms for intrusion detection.

•**System Integration:**

Integrate the intrusion detection system with existing network infrastructure.

•**Real-time Monitoring:**

Implement real-time monitoring and alerting mechanisms.

•**Performance Evaluation:**

Evaluate the system's performance using various metrics like accuracy, precision, and recall.

•**User Interface:**

Design a user-friendly interface for managing and monitoring the system.

Data & Resources

- **Tools, Software, and Techniques Used:**
- **Programming**: Python
- **Libraries**: Scikit-learn, TensorFlow, Pandas, NumPy,Seaborn, Joblib, Flask
- **Datasets**: KDD 2011
- **Algorithms**: Random Forest
- Training and Testing data for the model was gathered from a website called NSL_KDD_TEST.

Methodology, Tools, and Techniques

1. Data Collection:

- Gathered network traffic data from various sources, including routers, switches, and firewalls.

2. Data Preprocessing:

- Clean and normalize the data to remove any inconsistencies and noise.

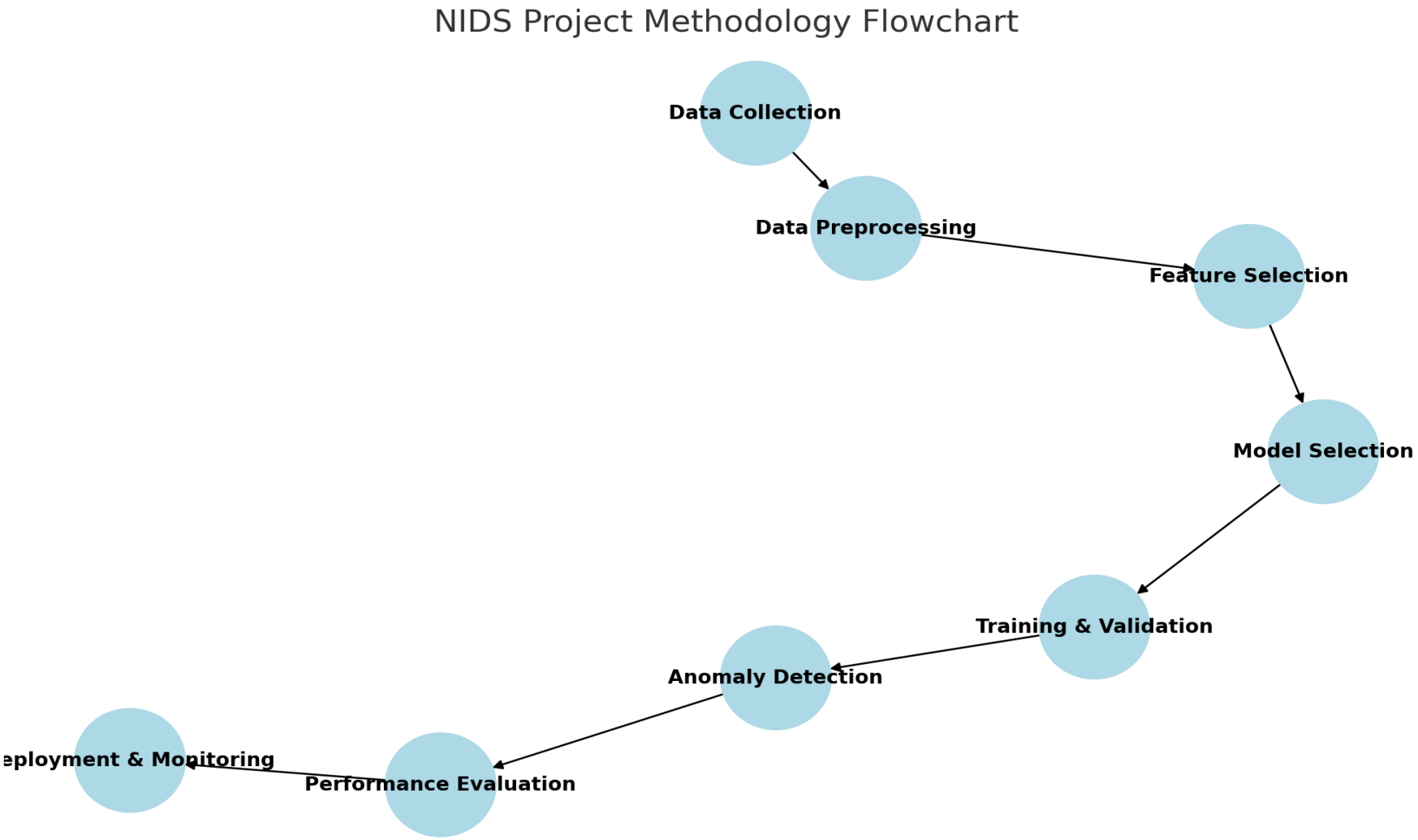
3. Algorithm Selection:

- Selected machine learning algorithms such as Decision Trees, Random Forest, and Support Vector Machines (SVM) for detection.
- Considered both supervised and unsupervised learning techniques.

4. Model Training:

- Divided the dataset into training and testing sets.
- Trained the selected machine learning models using the training set.

Methodology Flowchart



- Evaluated the performance of the model using metrics like accuracy, precision, recall, and F1 score.
- Conducted cross-validation to ensure robustness and reliability.

6. System Implementation:

- Integrated the trained models into the network intrusion detection system.
- Developed a real-time monitoring and alerting mechanism.

7. Testing and Validation:

- Conducted extensive testing on different network environments to validate the system's effectiveness.
- Fine-tuned the models based on feedback and performance results.

8. Deployment:

- Deployed the intrusion detection system in a live network environment.
- Continuously monitored and updated the system to adapt to new threats.

Expected Results & Impact

•**High Detection Accuracy:** The system will accurately detect known and unknown intrusions with minimal false positives/negatives, improving network security.

•**Real-Time Detection:** It will provide instant alerts for quick threat response, reducing potential damage from attacks.

•**Reduced Human Intervention:** Automated detection reduces reliance on manual monitoring, increasing operational efficiency.

•**Adaptability to New Threats:** The system will evolve with new attack patterns, ensuring long-term effectiveness.

•**Cost Reduction:** By automating detection, the system lowers operational costs and minimizes the risk of costly breaches.

•**Scalability:** The solution can handle growing network traffic, ensuring sustained performance as the organization expands.

THANK YOU