**Proposal: Network Intrusion Detection using Supervised Machine Learning Techniques with Feature Selection**

**Abstract**

Network intrusion detection is critical for maintaining the security and integrity of computer networks. In this proposal, we outline a research project focused on developing effective intrusion detection models using supervised machine learning techniques. Our approach includes feature selection to enhance model performance and reduce complexity. The proposed study aims to contribute to the field of cybersecurity by improving the accuracy and efficiency of network intrusion detection systems.

**1. Introduction**

Network intrusion detection involves identifying unauthorized or malicious activities within a network. Traditional rule-based methods have limitations, and machine learning offers an alternative approach. This proposal outlines our research plan to build robust intrusion detection models.

**2. Problem Statement**

The primary objective is to detect network intrusions accurately while minimizing false positives. We aim to address the following questions:

* How can we leverage supervised machine learning algorithms for intrusion detection?
* Which features are most relevant for effective detection?
* How can we optimize model performance while maintaining interpretability?

**3. Data Sources**

We will use publicly available network traffic datasets, including both benign and malicious traffic. Additionally, we may collect real-time data from organizational networks (ensuring privacy and ethical considerations).

**4. Modeling Approach**

We propose the following modeling techniques:

1. **Decision Trees**: A simple yet interpretable algorithm for binary classification.
2. **Support Vector Machines (SVM)**: Effective for high-dimensional data.
3. **Neural Networks**: Deep learning models for complex patterns.

**5. Feature Selection**

Feature selection is crucial to enhance model performance. We will explore techniques such as:

* Recursive Feature Elimination (RFE)
* Feature Importance from tree-based models

**6. Project Approach**

We will follow the CRISP-DM methodology:

1. **Business Understanding**: Define objectives and success criteria.
2. **Data Preparation**: Clean, preprocess, and engineer features.
3. **Modeling**: Train and evaluate models iteratively.
4. **Evaluation**: Validate model performance using appropriate metrics.
5. **Deployment**: Implement the best-performing model in a real-world environment.

**7. Assumptions and Constraints**

* Assumes labeled datasets are available for training.
* Computational resources may limit model complexity.
* Privacy and security considerations must be maintained.

**8. Adaptation from Existing Work**

We build upon existing machine learning models for intrusion detection. Our focus is on integrating advanced feature selection techniques.

**9. Deviations from Requirements**

None anticipated; adherence to outlined requirements is planned.

This proposal outlines our research plan for network intrusion detection using supervised machine learning techniques. We aim to contribute valuable insights to the field of cybersecurity.