# REAL-TIME NETWORK INTRUSION DETECTION

# (USING WIRESHARK AND ADVANCED ENSEMBLE LEARNING TECHNIQUES)

# SOFTWARE REQUIREMENTS SPECIFICATION

## Version 1.0



**Group ID**: F24PROJECT5982F

**Supervisor:** Laraib Sana

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description** | **Author** |
| 30-11-2024 | 1.0 | Introduction of the project | BC220422797 |

**TABLE OF CONTENTS**

1. Scope of the Project
2. Functional Requirements
3. Non-Functional Requirements
4. Use Case Diagram
5. Usage Scenarios
6. Adopted Methodology
7. Work Plan

**SRS Document**

### SCOPE OF PROJECT

This project aims to develop a real-time ***Intrusion Detection System (IDS)*** for Network Security using ***Machine Learning Models***. The system will capture network data via **Wireshark**, preprocess it, and apply Advanced Ensemble Learning Techniques like TabNet, CatBoost, and LightGBM for intrusion detection. The project includes creating a web application to upload and analyze network data, displaying detection results and relevant network parameters.

### FUNCTIONAL REQUIREMENTS

### DATA CAPTURE AND PREPROCESSING

### Capture network traffic data in real-time using Wireshark.

### Export the captured data to a CSV file format for analysis.

### Preprocess the data: clean it, encode categorical features (e.g., protocol types), and normalize numerical features (e.g., packet size).

### MACHINE LEARNING MODEL TRAINING AND EVALUATION

### Use the processed network traffic data to train Advanced Ensemble Learning Models including TabNet, CatBoost, LightGBM, and stacking ensembles.

### Evaluate models using metrics such as accuracy, precision, recall, F1-score, and ROC-AUC.

### WEB APPLICATION INTERFACE

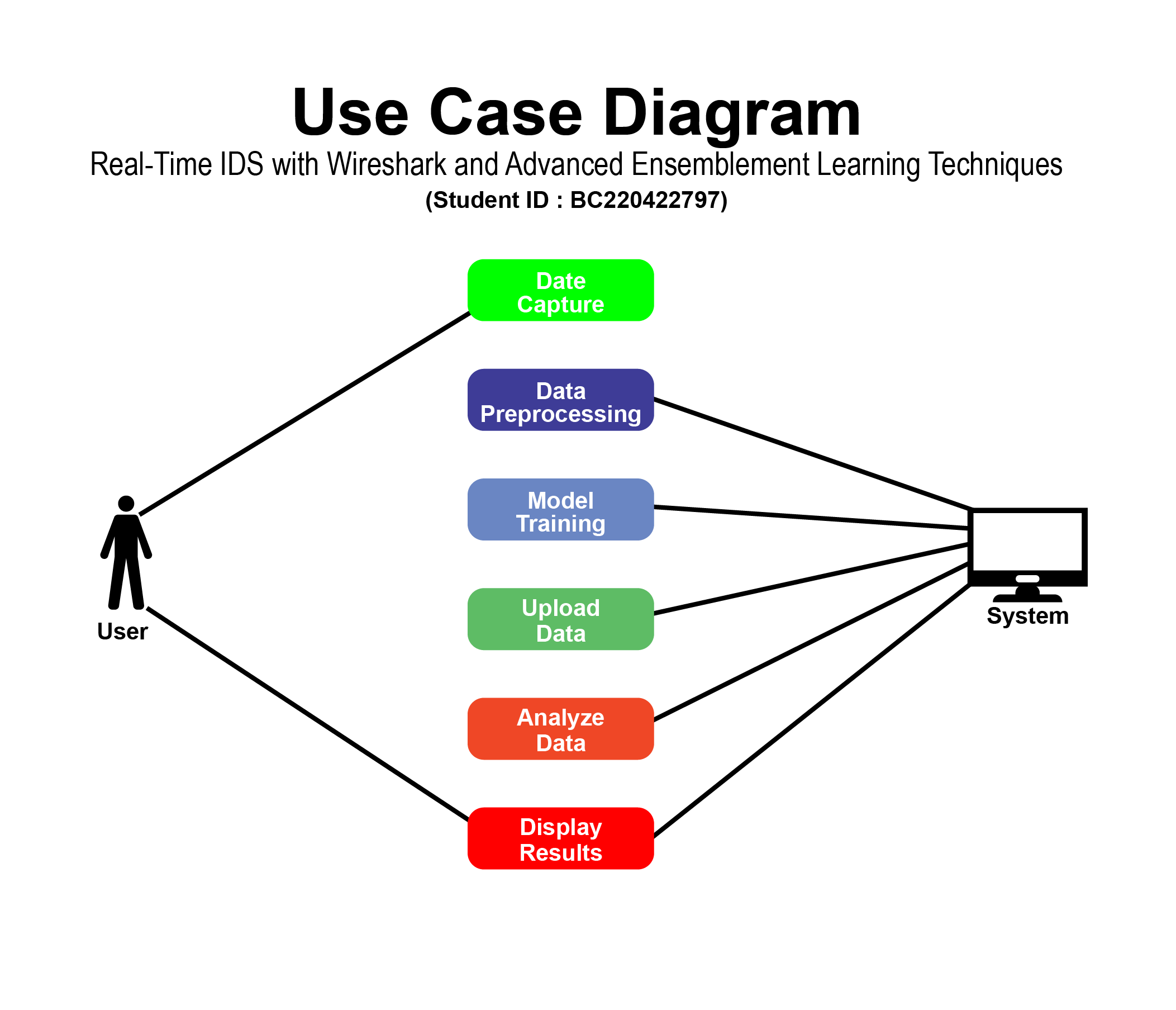
### Provide an interface where users can upload network traffic data files.

### Analyze the uploaded data for potential intrusions using the Trained Ensemble Models.

### Display the detection results and highlight key network parameters affecting the classification.

### NON-FUNCTIONAL REQUIREMENTS

1. **Performance:** The system should handle real-time data efficiently and complete analysis within a few seconds for uploaded files.
2. **Scalability:** Ability to process larger network datasets as required.
3. **Usability:** Provide an intuitive and easy-to-navigate web interface for users.
4. **Reliability:** Ensure high accuracy in detection to minimize false positives and negatives.
5. **Security:** Protect user-uploaded data and the overall system from unauthorized access.



### USE CASE SCNARIO

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Use Case Title** | **Use Case ID** | **Actions** | **Description** | **Alternative Paths** | **Pre**  **Conditions** | **Post**  **Conditions** | **Author** | **Exceptions** |
| Network Traffic Capture | UC1 | Start Wireshark, Capture Data, Save As CSV | Captures Live Network Traffic For Analysis | - | Wireshark Installed | CSV File Generated | BC220422797 | Wireshark Crash |
| Intrusion Detection | UC2 | Upload File, Run Analysis, View Results | Detects Intrusions Using ML Models | - | File Uploaded | Display Results | BC220422797 | Upload Failure |

### ADOPTED METHODOLOGY

The VU Process Model will be used, which combines **VU** **Waterfall and Spiral models.** This model allows for iterative development with sequential stages, ensuring continuous feedback and adjustments, ideal for balancing structured stages with flexibility.

### WORK PLAN

