AI-BASED NETWORK INTRUSION DETECTION SYSTEM

Project Documentation

INTRODUCTION

With the rapid growth of internet technologies, computer networks have become an essential part of modern communication, business operations, and data sharing. However, this growth has also led to a significant increase in cyber threats such as Distributed Denial of Service (DDoS) attacks, port scanning, infiltration attacks, and unauthorized access. These attacks can compromise sensitive information, disrupt network services, and cause financial losses to organizations.

Traditional security mechanisms like firewalls and signature-based intrusion detection systems are no longer sufficient to protect modern networks. These systems rely on predefined rules and known attack patterns, which makes them ineffective against new or evolving cyber threats. As a result, there is a growing need for intelligent and adaptive security systems.

This project focuses on developing an AI-Based Network Intrusion Detection System (NIDS) that uses machine learning techniques to analyze network traffic and identify malicious activities. By learning patterns from real-world network data, the system can automatically detect abnormal behavior and improve network security.

PROBLEM STATEMENT

Modern computer networks generate massive volumes of traffic every second. Manually monitoring this traffic for suspicious behavior is impractical and error-prone. Traditional intrusion detection systems are limited in their ability to detect new or unknown attacks due to their dependency on static rules and signatures.

The key challenges addressed in this project are:

- Detecting malicious network traffic in large datasets
- Differentiating between normal and attack traffic accurately
- Providing understandable explanations for detection results
- Creating an interactive and user-friendly monitoring system

Therefore, the problem is to design and implement an intelligent network intrusion detection system that can efficiently analyze network traffic, detect cyberattacks, and assist users in understanding the results.

PROJECT OVERVIEW

The AI-Based Network Intrusion Detection System is developed using machine learning techniques and real-world network traffic data. The project uses the **CIC-IDS2017 dataset**, which contains labeled network flows representing both benign and various attack scenarios such as DDoS, port scanning, and brute-force attacks.

A **Random Forest classifier** is used to train the intrusion detection model. Random Forest is chosen due to its robustness, high accuracy, and ability to handle large datasets. The model is trained on selected flow-level statistical features extracted from network traffic.

The system also includes a **web-based dashboard built using Streamlit**, allowing users to interact with the model, simulate network traffic, and view intrusion detection results in real time. To improve transparency, the system integrates an **AI explanation module using Groq LLM**, which explains why a particular traffic flow is classified as an attack or normal traffic.

The complete application is deployed on **Hugging Face Spaces**, making it accessible through a web browser without requiring local installation.

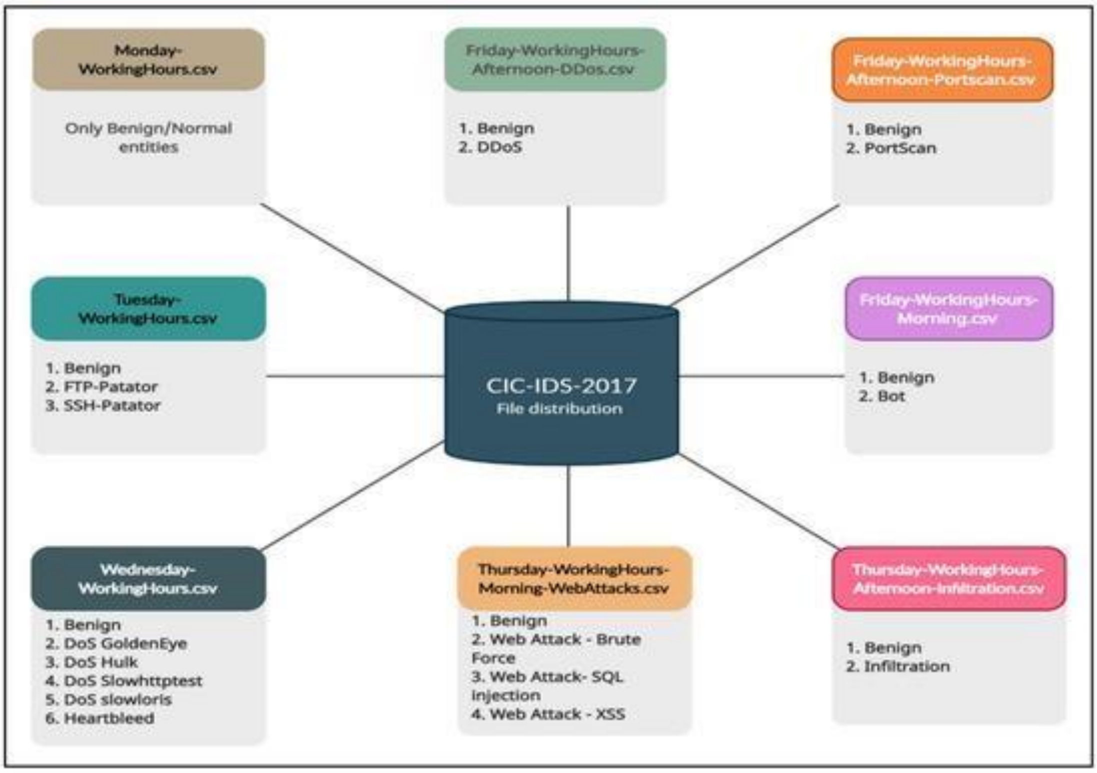
OBJECTIVES OF THE PROJECT

The main objectives of this project are:

- To analyze real-world network traffic using machine learning
- To detect malicious activities in network traffic
- To classify traffic as benign or attack traffic
- To provide AI-based explanations for detection results
- To build an interactive web-based intrusion detection dashboard
- To deploy the system on a cloud platform for easy access

DATASET DESCRIPTION

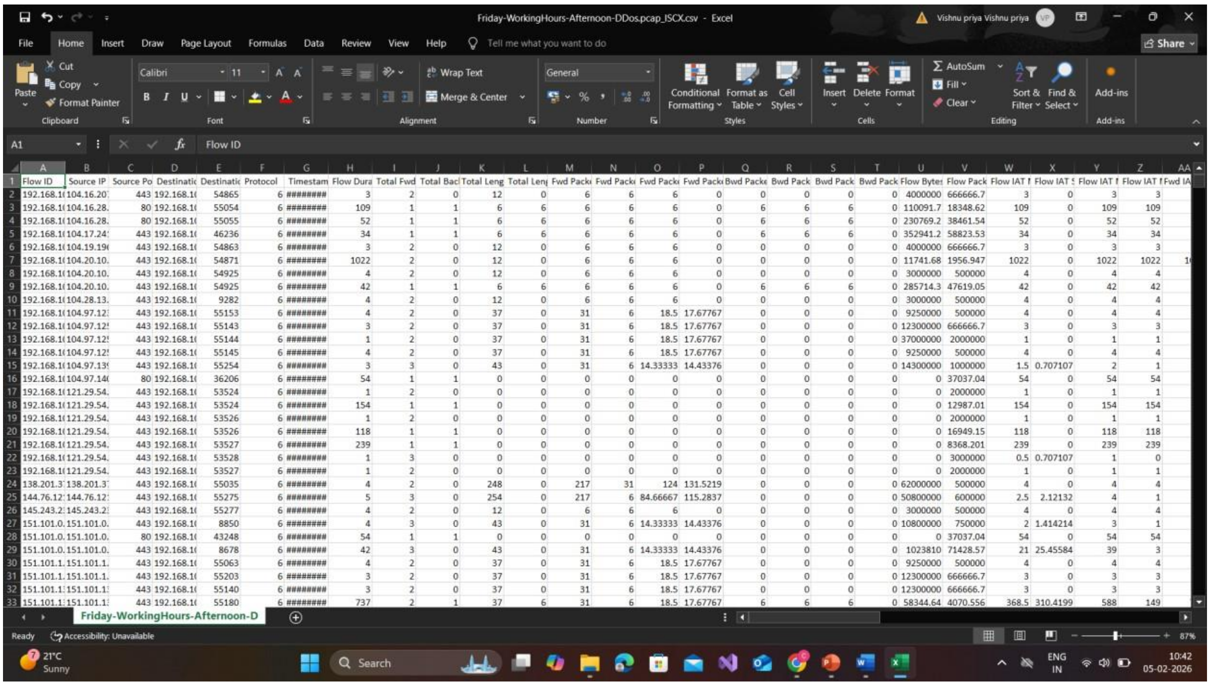
The **CIC-IDS2017 dataset**, developed by the Canadian Institute for Cybersecurity, is used in this project. This dataset contains realistic network traffic collected from a simulated enterprise environment.



Key Features of the Dataset:

- Real-world traffic patterns
- Multiple attack types (DDoS, Port Scan, Infiltration, Web Attacks, etc.)
- Flow-level statistical features
- Labeled data for supervised learning

The dataset is preprocessed to remove missing values, infinite values, and irrelevant features. Only important features related to traffic behavior are selected for training the machine learning model.



METHODOLOGY

1 Data Preprocessing

- Removal of missing and infinite values
- Cleaning and formatting feature names
- Selection of important flow-level features

2 Feature Selection

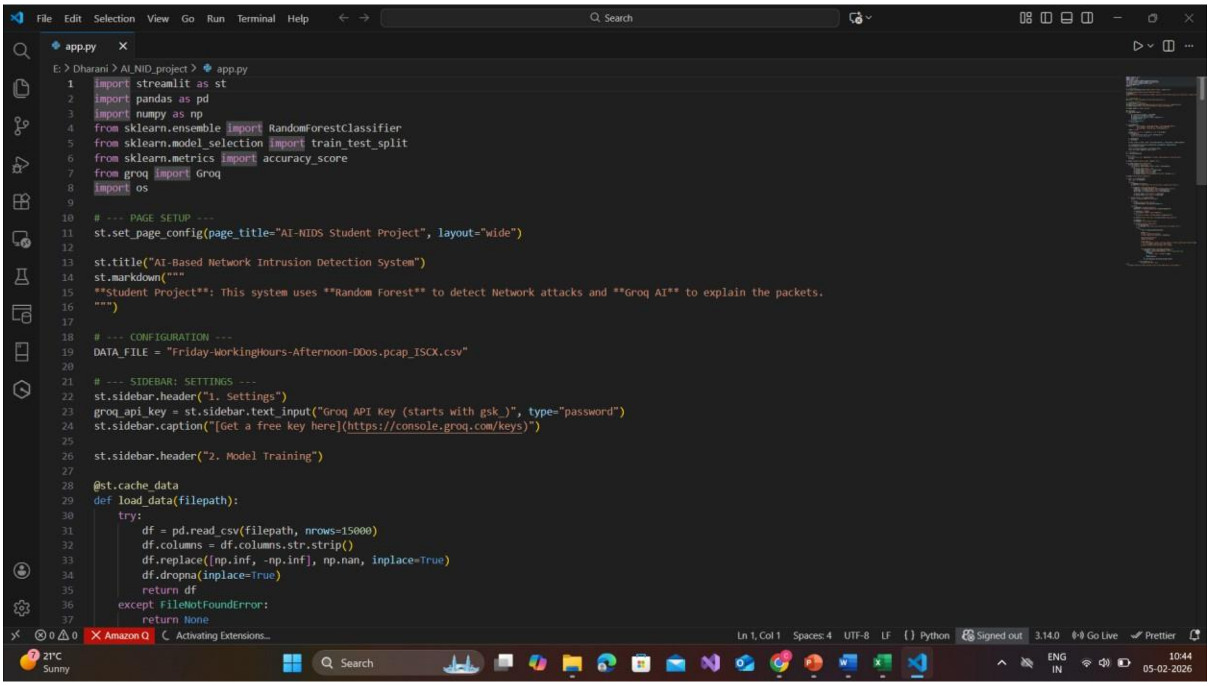
Key features such as:

- Flow Duration
- Total Forward Packets
- Packet Length Statistics
- Flow Inter-Arrival Time
- Packet Rate

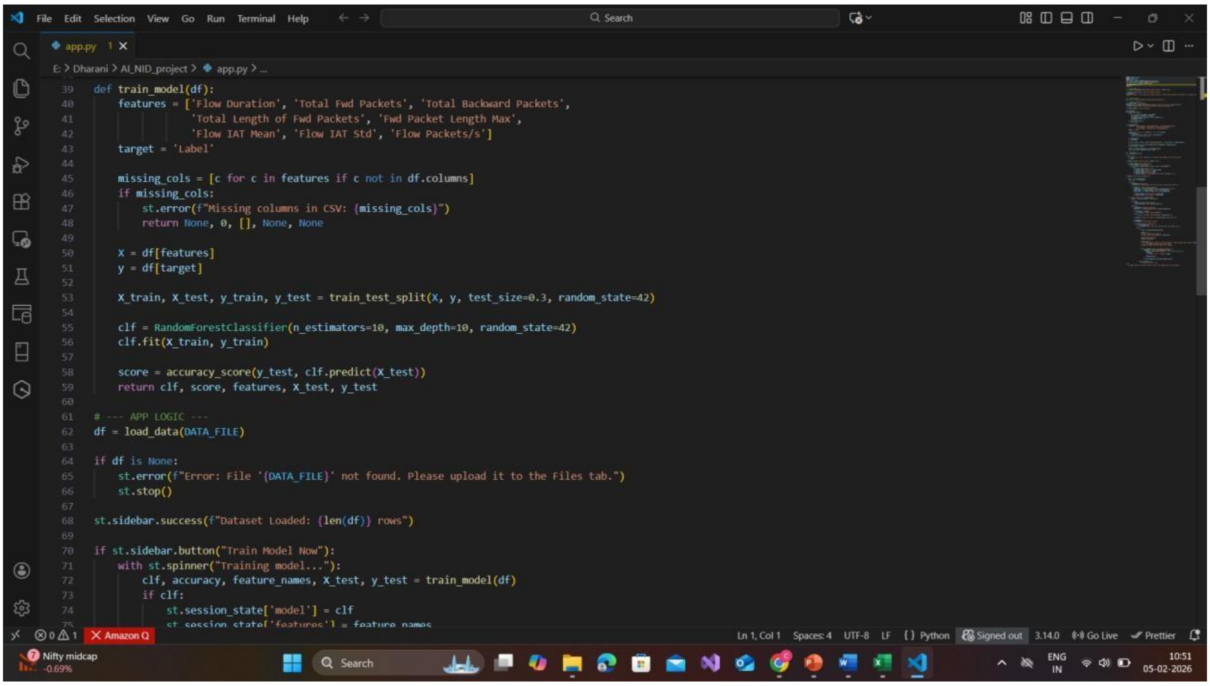
are used to train the model.

3 Model Training

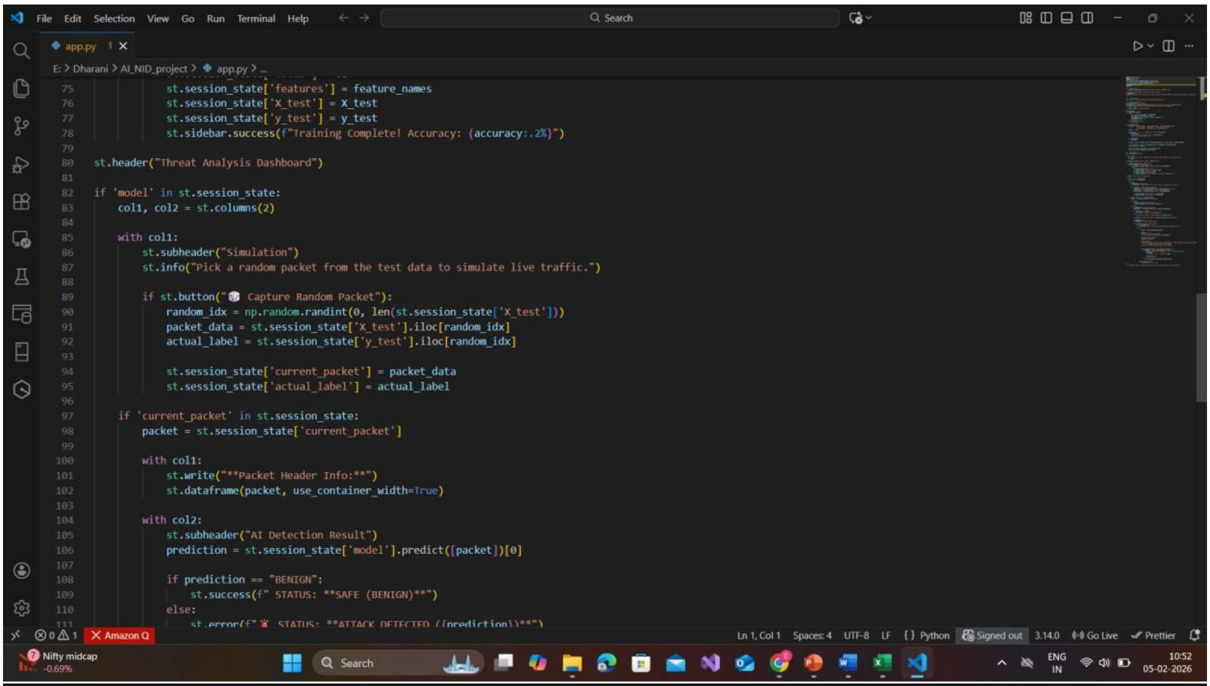
A **Random Forest classifier** is trained using the preprocessed dataset. The data is split into training and testing sets to evaluate model performance.

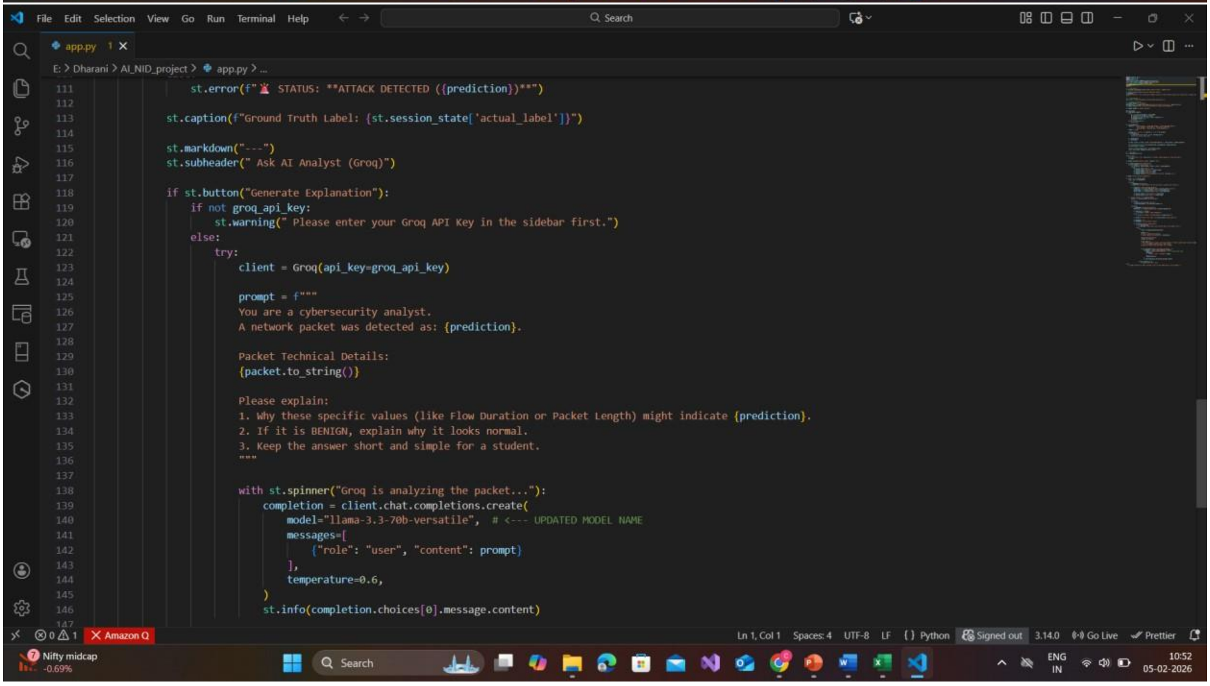


```python
import streamlit as st
import pandas as pd
import numpy as np
from sklearn.ensemble import RandomForestClassifier
from sklearn.model_selection import train_test_split
from sklearn.metrics import accuracy_score
from groq import Groq
import os

# --- PAGE SETUP ---
st.set_page_config(page_title="AI-NIDS Student Project", layout="wide")

st.title("AI-Based Network Intrusion Detection System")
st.markdown("""
**Student Project**: This system uses **Random Forest** to detect Network attacks and **Groq AI** to explain the packets.
""")

# --- CONFIGURATION ---
DATA_FILE = "Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv"

# --- SIDEBAR: SETTINGS ---
st.sidebar.header("1. Settings")
groq_api_key = st.sidebar.text_input("Groq API Key (starts with gsk_)", type="password")
st.sidebar.caption("[Get a free key here](https://console.groq.com/keys)")

st.sidebar.header("2. Model Training")

@st.cache_data
def load_data(filepath):
    try:
        df = pd.read_csv(filepath, nrows=15000)
        df.columns = df.columns.str.strip()
        df.replace([np.inf, -np.inf], np.nan, inplace=True)
        df.dropna(inplace=True)
        return df
    except FileNotFoundError:
        return None
```



```python
def train_model(df):
    features = ['Flow Duration', 'Total Fwd Packets', 'Total Backward Packets',
                'Total Length of Fwd Packets', 'Fwd Packet Length Max',
                'Flow IAT Mean', 'Flow IAT Std', 'Flow Packets/s']
    target = 'Label'

    missing_cols = [c for c in features if c not in df.columns]
    if missing_cols:
        st.error(f"Missing columns in CSV: {missing_cols}")
        return None, 0, [], None, None

    X = df[features]
    y = df[target]

    X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3, random_state=42)

    clf = RandomForestClassifier(n_estimators=10, max_depth=10, random_state=42)
    clf.fit(X_train, y_train)

    score = accuracy_score(y_test, clf.predict(X_test))
    return clf, score, features, X_test, y_test

# --- APP LOGIC ---
df = load_data(DATA_FILE)

if df is None:
    st.error(f"Error: File '{DATA_FILE}' not found. Please upload it to the Files tab.")
    st.stop()

st.sidebar.success(f"Dataset Loaded: {len(df)} rows")

if st.sidebar.button("Train Model Now"):
    with st.spinner("Training model..."):
        clf, accuracy, feature_names, X_test, y_test = train_model(df)
        if clf:
            st.session_state['model'] = clf
            st.session_state['features'] = feature_names
```





4 Model Evaluation

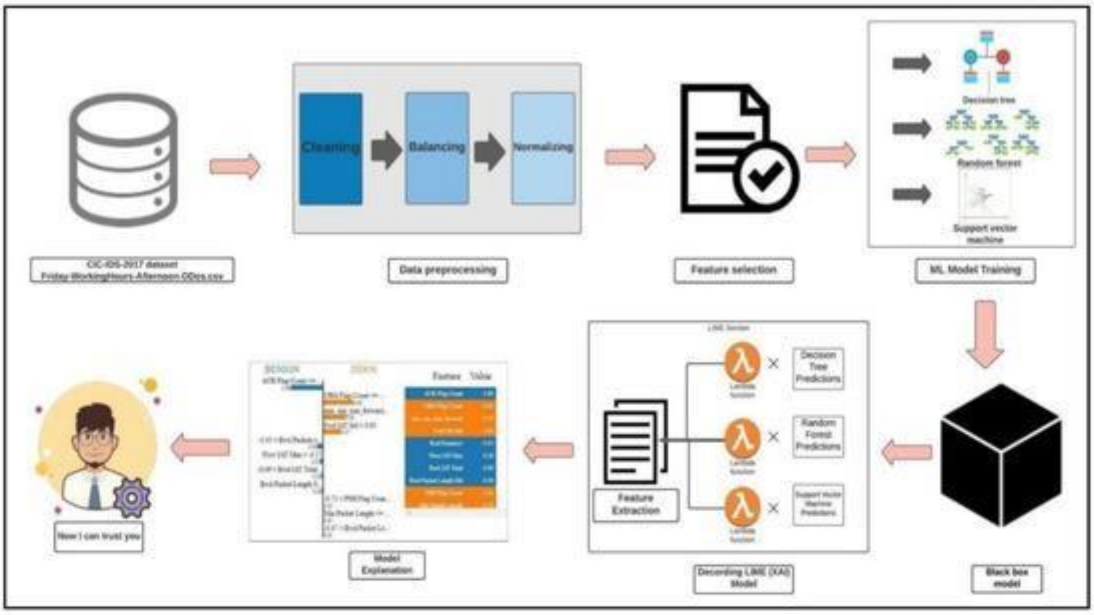
The trained model is evaluated using accuracy as the primary metric. The model demonstrates effective performance in distinguishing between benign and malicious traffic.

SYSTEM ARCHITECTURE

The system follows a modular architecture consisting of:

1. Data Input Module
2. Data Preprocessing Module

3. Machine Learning Model
4. Intrusion Detection Module
5. AI Explanation Module
6. Web Dashboard Interface
7. Deployment Platform



Each module works independently and communicates with other components to provide a complete intrusion detection solution.

Flowchart

Internet / Network Traffic

↓

CIC-IDS2017 Dataset (Real-World Network Flows)

↓

Data Preprocessing (Cleaning & Feature Selection)

↓

Machine Learning Model

(Random Forest Classifier)

↓

Traffic Classification

(BENIGN / ATTACK)

↓

AI Explanation Module

(Groq LLM)

↓

Web-Based Dashboard

(Streamlit Application)

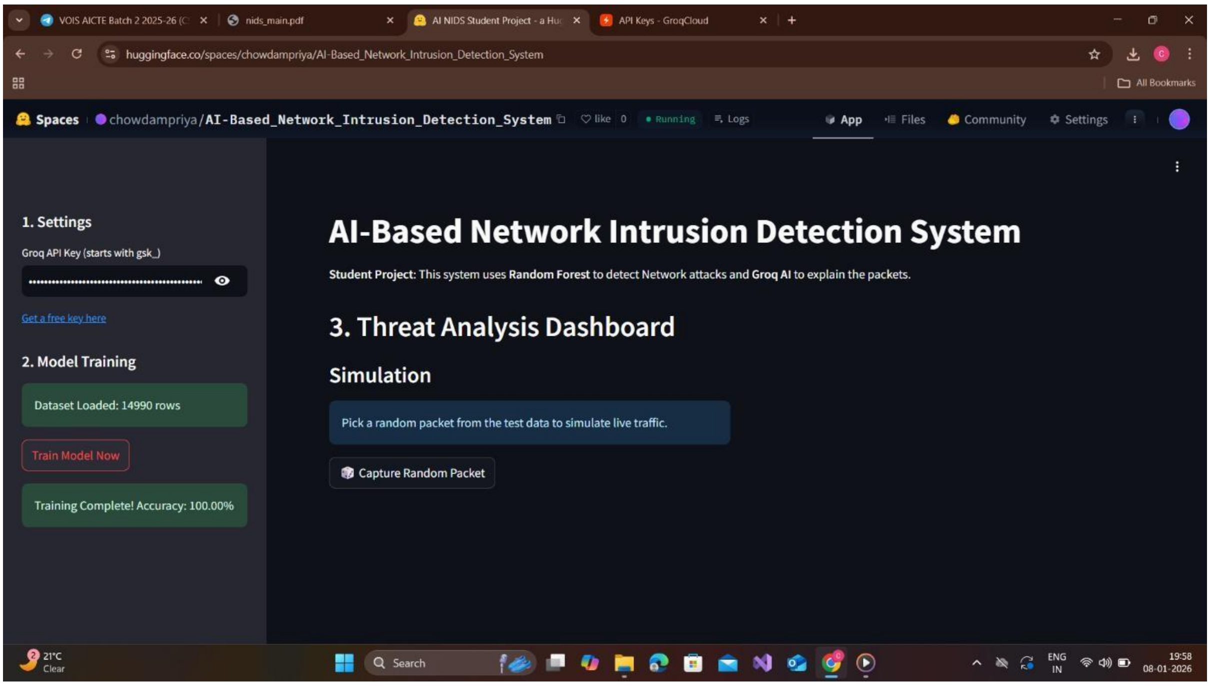
↓

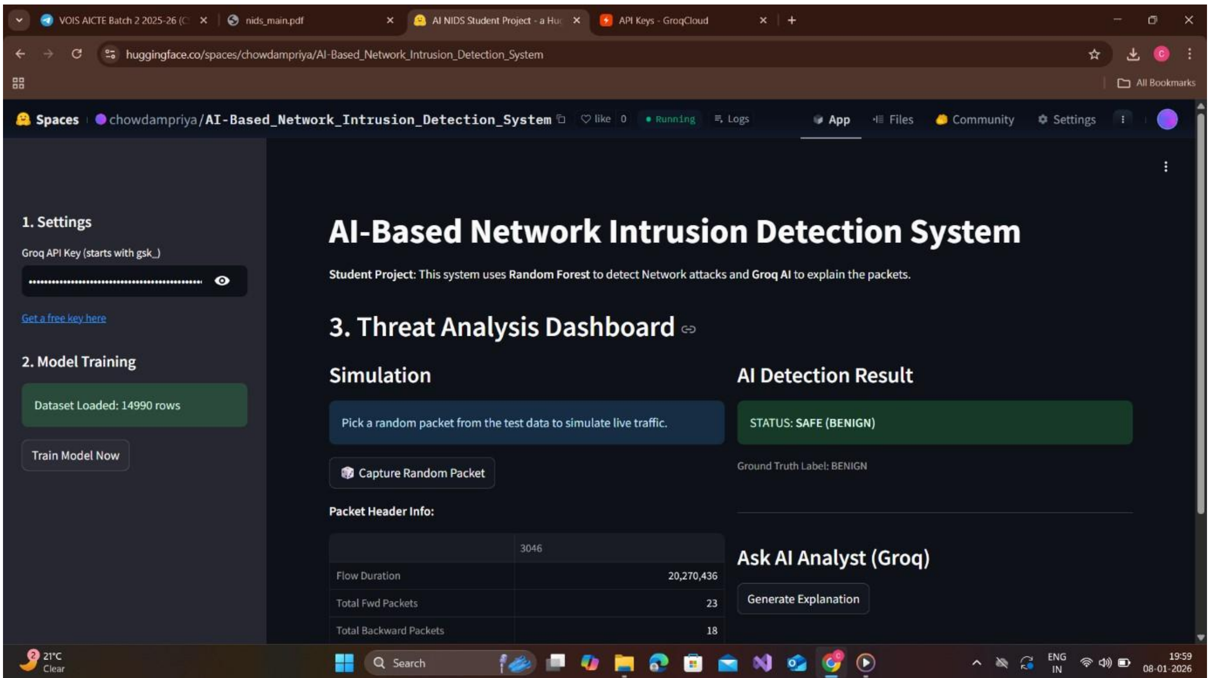
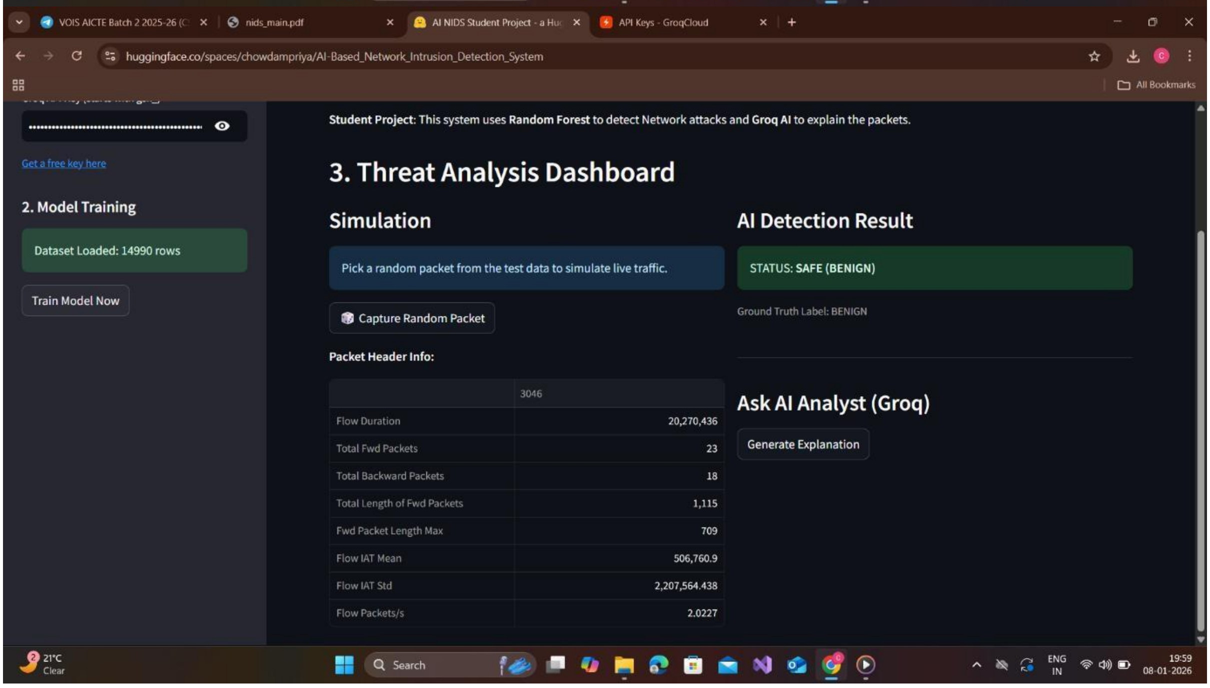
Deployment Platform

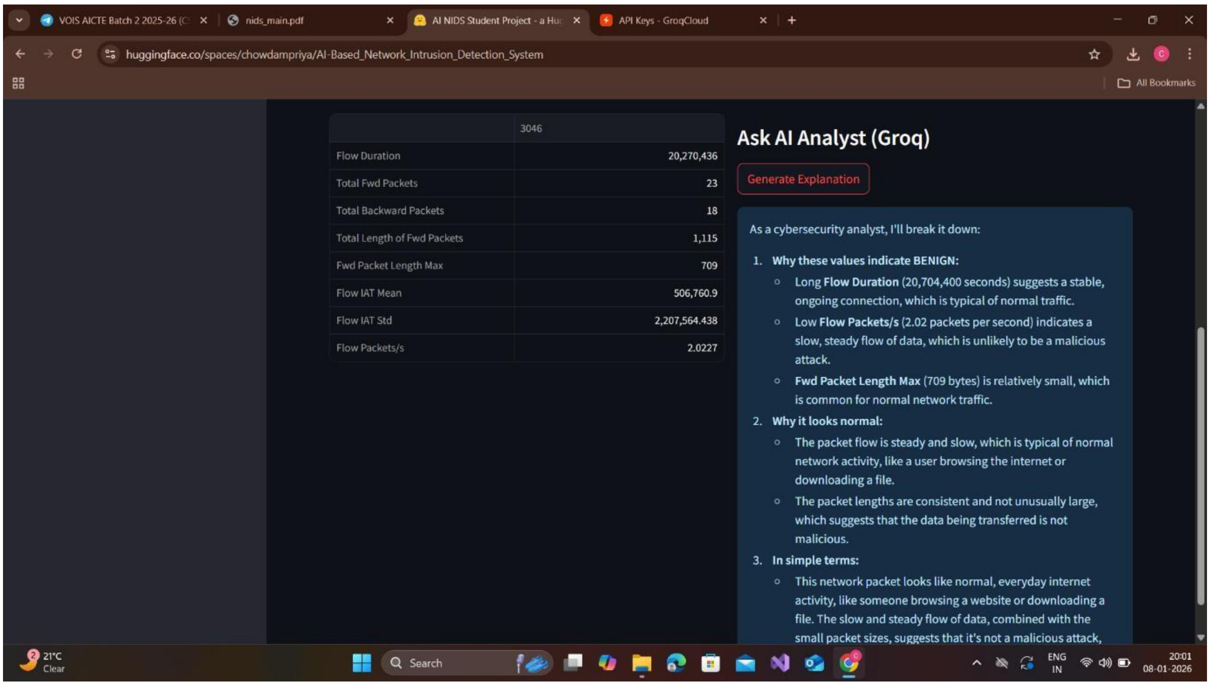
(Hugging Face Spaces)

RESULTS AND OUTCOMES

- Successful detection of network intrusions
- High classification accuracy using Random Forest
- Clear AI-based explanations for detection results
- Interactive and user-friendly web dashboard
- Successful cloud deployment on Hugging Face Spaces

- 
huggingface.co/spaces/chowdampriya/AI-Based_Network_Intrusion_Detection_System
Spaces chowdampriya/AI-Based_Network_Intrusion_Detection_System
Running
App
Files
Community
Settings
1. Settings
Groq API Key (starts with gsk_)
Get a free key here
2. Model Training
Dataset Loaded: 14990 rows
Train Model Now
Training Complete! Accuracy: 100.00%
AI-Based Network Intrusion Detection System
Student Project: This system uses Random Forest to detect Network attacks and Groq AI to explain the packets.
3. Threat Analysis Dashboard
Simulation
Pick a random packet from the test data to simulate live traffic.
Capture Random Packet

- 
VOIS AICTE Batch 2 2025-26
nids_main.pdf
AI NIDS Student Project - a Hu
API Keys - GroqCloud
huggingface.co/spaces/chowdampriya/AI-Based_Network_Intrusion_Detection_System
All Bookmarks
Spaces
chowdampriya/AI-Based_Network_Intrusion_Detection_System
like 0
Running
Logs
App
Files
Community
Settings
1. Settings
Groq API Key (starts with gsk_)
Get a free key here
2. Model Training
Dataset Loaded: 14990 rows
Train Model Now
AI-Based Network Intrusion Detection System
Student Project: This system uses Random Forest to detect Network attacks and Groq AI to explain the packets.
3. Threat Analysis Dashboard
Simulation
Pick a random packet from the test data to simulate live traffic.
Capture Random Packet
Packet Header Info:
3046
Flow Duration 20,270,436
Total Fwd Packets 23
Total Backward Packets 18
AI Detection Result
STATUS: SAFE (BENIGN)
Ground Truth Label: BENIGN
Ask AI Analyst (Groq)
Generate Explanation
21°C
Clear
Search
ENG
IN
19:59
08-01-2026
- 
VOIS AICTE Batch 2 2025-26
nids_main.pdf
AI NIDS Student Project - a Hu
API Keys - GroqCloud
huggingface.co/spaces/chowdampriya/AI-Based_Network_Intrusion_Detection_System
All Bookmarks
Get a free key here
2. Model Training
Dataset Loaded: 14990 rows
Train Model Now
Student Project: This system uses Random Forest to detect Network attacks and Groq AI to explain the packets.
3. Threat Analysis Dashboard
Simulation
Pick a random packet from the test data to simulate live traffic.
Capture Random Packet
Packet Header Info:
3046
Flow Duration 20,270,436
Total Fwd Packets 23
Total Backward Packets 18
Total Length of Fwd Packets 1,115
Fwd Packet Length Max 709
Flow IAT Mean 506,760.9
Flow IAT Std 2,207,564.438
Flow Packets/s 2.0227
AI Detection Result
STATUS: SAFE (BENIGN)
Ground Truth Label: BENIGN
Ask AI Analyst (Groq)
Generate Explanation
21°C
Clear
Search
ENG
IN
19:59
08-01-2026

- 

APPLICATIONS

- Network security monitoring
- Cyberattack detection and prevention
- Academic research and learning
- Enterprise network protection
- Security operations centers (SOC)

FUTURE ENHANCEMENTS

- Real-time packet capture using Scapy
- Deep learning-based intrusion detection
- Multi-class attack classification
- Automated alert and reporting system
- Integration with enterprise security tools

CONCLUSION

This project demonstrates the effective use of machine learning and explainable AI in network security. The AI-Based Network Intrusion Detection System provides accurate detection of cyberattacks while offering transparency through AI explanations. The system is scalable, interactive, and suitable for real-world security applications as well as academic research.