

AI-BASED NETWORK INTRUSION DETECTION SYSTEM

Vidyadheesha M Pandurangi


AICTE INTERNSHIP ID: STU667711a678b251719079334



INTERNSHIP ID: INTERNSHIP_1762343729690b3b31bb89f




APPLY ID: APPLY_176287263369134d39759c4

PROBLEM STATEMENT

- Modern computer networks generate large volumes of traffic, making manual monitoring impractical. 
- Traditional security mechanisms such as firewalls and signature-based IDS are ineffective against new and evolving cyber attacks.
- Many existing intrusion detection systems suffer from high false positives, poor scalability, and lack of real-time response.
- Security analysts require a system that can intelligently analyze network traffic, identify intrusions accurately, and provide quick, actionable alerts.
- There is a need for an AI-based, automated, and user-friendly intrusion detection system that can detect malicious activities efficiently and assist in proactive network security management.



PROJECT DESCRIPTION

- This project presents an AI-Based Network Intrusion Detection System (NIDS) that uses machine learning to identify malicious network activities. 
- A Random Forest classifier is trained on network traffic data to distinguish between benign and intrusive behavior.
- The system performs robust data preprocessing and selects the most important network features to improve detection accuracy and interpretability.
- A Streamlit-based web interface allows users to simulate live network traffic and receive real-time intrusion predictions.
- Detected intrusions are automatically logged to support monitoring and security analysis.
- The solution demonstrates the effective use of AI in cybersecurity for automated, scalable, and real-time intrusion detection. 


WHO ARE THE END USERS?

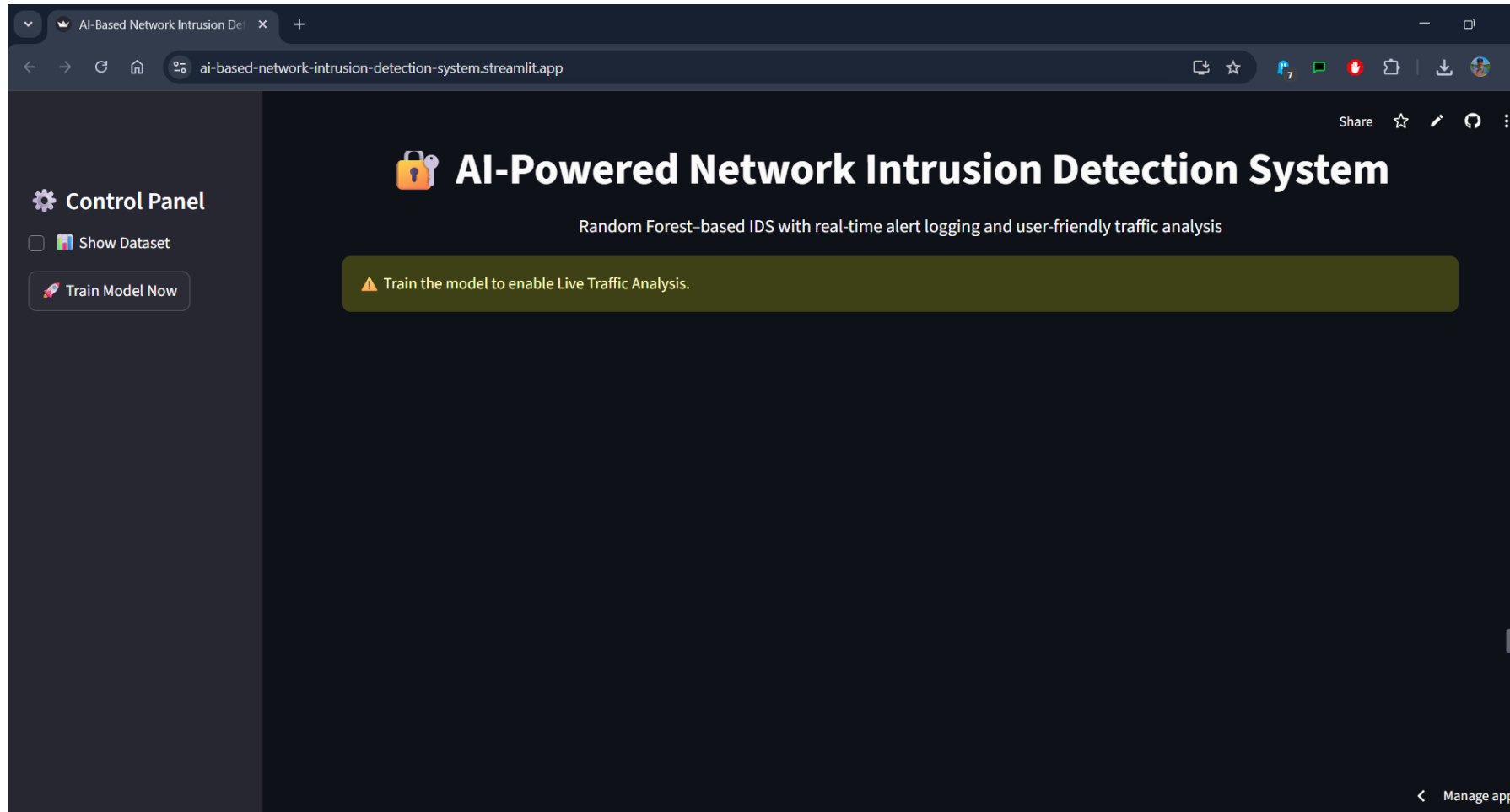
- **Network Security Administrators** – To monitor network traffic and identify potential intrusions in real time.
- **Cybersecurity Analysts** – To analyze suspicious activities and improve threat detection strategies.
- **IT Infrastructure Teams** – To enhance the security of enterprise and organizational networks.
- **Educational Institutions & Researchers** – For learning, experimentation, and research in network security and intrusion detection.
- **Students & Trainees** – To understand the practical application of AI and machine learning in cybersecurity.

TECHNOLOGY USED

- **Python** – Core programming language for data processing, model development, and application logic.
- **Scikit-learn** – Used to build and train the Random Forest machine learning model for intrusion detection.
- **Pandas & NumPy** – For data preprocessing, feature handling, and numerical computations.
- **Streamlit** – Web framework used to develop the interactive user interface for live traffic analysis.
- **Matplotlib & Seaborn** – For visualizing feature importance and model performance metrics.
- **Git & GitHub** – For version control, collaboration, and project deployment.



RESULTS



Website UI – Deployed using Streamlit

RESULTS

The screenshot displays a web application titled "AI-Powered Network Intrusion Detection System" running on Streamlit. The interface includes a sidebar with a "Control Panel" and buttons for "Show Dataset" and "Train Model Now". The main area features a "Dataset Preview" table with 10 rows of network flow data. Below the table, a green status bar indicates "Model Trained Successfully | Accuracy: 99.99%".

Dataset Preview

	Flow ID	Source IP	Source Port	Destination IP	Destination Port	Protocol	Timestamp	Flow Duration	Total Fwd Packets
0	192.168.10.5-104.16.207.165-54865-443-6	104.16.207.165	443	192.168.10.5	54865	6	7/7/2017 3:30	3	2
1	192.168.10.5-104.16.28.216-55054-80-6	104.16.28.216	80	192.168.10.5	55054	6	7/7/2017 3:30	109	1
2	192.168.10.5-104.16.28.216-55055-80-6	104.16.28.216	80	192.168.10.5	55055	6	7/7/2017 3:30	52	1
3	192.168.10.16-104.17.241.25-46236-443-6	104.17.241.25	443	192.168.10.16	46236	6	7/7/2017 3:30	34	1
4	192.168.10.5-104.19.196.102-54863-443-6	104.19.196.102	443	192.168.10.5	54863	6	7/7/2017 3:30	3	2
5	192.168.10.5-104.20.10.120-54871-443-6	104.20.10.120	443	192.168.10.5	54871	6	7/7/2017 3:30	1022	2
6	192.168.10.5-104.20.10.120-54925-443-6	104.20.10.120	443	192.168.10.5	54925	6	7/7/2017 3:30	4	2
7	192.168.10.5-104.20.10.120-54925-443-6	104.20.10.120	443	192.168.10.5	54925	6	7/7/2017 3:30	42	1
8	192.168.10.8-104.28.13.116-9282-443-6	104.28.13.116	443	192.168.10.8	9282	6	7/7/2017 3:30	4	2
9	192.168.10.5-104.97.123.193-55153-443-6	104.97.123.193	443	192.168.10.5	55153	6	7/7/2017 3:30	4	2

Model Trained Successfully | Accuracy: 99.99%

**Dataset Preview & Training of Model –
For Live Traffic Simulator**

RESULTS

The screenshot displays a web application titled "AI-Based Network Intrusion Detection System" running on a Streamlit app. The interface includes a sidebar with a "Control Panel" containing "Show Dataset" and "Train Model Now" buttons. The main area features a "Live Traffic Simulator" section with a note: "Only the most influential network traffic parameters are shown below. These features contribute the most to intrusion detection decisions." Below this, there are ten input fields for network parameters, each with a minus and plus button for adjustment. A "Detect Traffic" button is located at the bottom of the input fields. The result of the simulation is displayed as a green bar with the text "Traffic is Benign".

Parameter	Value
Average Forward Segment Size (bytes per segment)	30.00
Forward Packet Length - Maximum (bytes)	80.00
Forward Packet Length - Mean (bytes)	45.00
Act Data Pkt Fwd	2.00
Forward Inter-Arrival Time - Std Deviation	15.00
Subflow Forward Bytes (total)	300.00
Forward Header Length (duplicate feature)	1024.00
Total Forward Packets Count	6.00
Init Win Bytes Forward	1024.00
Forward Inter-Arrival Time - Maximum	150.00

Detect Traffic

☒ Traffic is Benign

Testing of the Model – Using Live-Traffic Simulation Data

CERTIFICATE - PROTECTION FROM BROWSER ATTACKS



VOIS



Certificate of Completion

Presented to

Vidyadheesha M Pandurangi

For the successful completion of

Protection from Browser Attacks

Issued on December 20, 2025

ID:VFLMS25_143657



CERTIFICATE - INTRODUCTION TO SYSTEM SECURITY



Vodafone Idea Foundation

VOIS



Certificate of Completion

Presented to

Vidyadheesha M Pandurangi

For the successful completion of

Introduction to System Security

Issued on December 20, 2025

ID:VFLMS25_143657



CERTIFICATE - SECURING ANDROID DEVICES



Vodafone Idea Foundation

VOIS



Certificate of Completion

Presented to

Vidyadheesha M Pandurangi

For the successful completion of

Securing Android Devices

Issued on December 20, 2025

ID:VFLMS25_143657



GITHUB REPOSITORY LINK

Github Repo Link: <https://github.com/Vidyadheesha-M-Pandurangi/Cyber-Security/tree/faf0025610bdc9f785ae82120a2e943419966d80/AI-Based%20Network%20Intrusion%20Detection%20System>

WEBSITE URL

Website Link: <https://ai-based-network-intrusion-detection-system.streamlit.app/>



THANK YOU