INTEL UNNATI INDUSTRIAL TRAINING 2025

TEAM DETAILS

TEAM NAME: AAA

S NO.	NAME	BRANCH	YEAR	ENROLLMENT NO
1	MELVIN JOSEPH	ECE	1ST	03414802824
2	AYUSHYA RANJAN	CSE	1ST	23814802724
3	KAMRAN AHMAD	ECE- ACT	1ST	04214815924

PROBLEM STATEMENT

Modern networks struggle with escalating data volumes, encrypted traffic, and advanced cyber threats. Traditional methods like rule-based systems and deep packet inspection (DPI) fail to detect threats in encrypted traffic, while manual processes delay responses and increase vulnerabilities. AI-driven solutions address these gaps by analyzing traffic patterns, detecting anomalies, classifying applications, and enabling real-time adaptive security for proactive, intelligent network defense.

PROPOSED SOLUTIONS

Our goal is to create an AI-based traffic analysis system with an emphasis on detection enhancement within encrypted environments. The system will utilize machine learning to analyze flow-based metadata, not packets, to identify indicators of malicious behavior or anomalies. Our system provides the following features:

- Traffic Anomaly Detection:
- Malicious Software and Attack Recognition:
- Anomaly Detection Component:
- Improved detection accuracy and precision,
- Watching network traffic over a certain period will be combined with simulated traffic or test datasets

OBJECTIVES

- Develop an automated system for **real-time traffic classification** using AI/ML techniques.
- Detect **malicious behaviors and anomalies** using advanced threat detection models.
- Ensure **high accuracy** in detecting known and unknown threats.

- Support **scalable deployment** in both enterprise and small-scale network environments.
- Maintain **user privacy** by focusing on metadata analysis in encrypted traffic.
- Visualize and alert on real-time network behavior to assist security teams.

METHODOLOGY

1. Research AI & ML basics relevant to network traffic.
2. Use public datasets (e.g., CIC-IDS, ISCX VPN) for training.
3. Extract features like packet count, size, duration, etc.
4. Train models like Random Forest or Autoencoders for classification/anomaly detection.
5. Evaluate model accuracy using test data.
6. Integrate results into a basic visualization tool or dashboard.

TOOLS AND TECHNOLOGY

Component	Tools/Technologies
Operating System	Linux (Ubuntu, Kali)
Programming Languages	Python, C/C++
Data Capture	Wireshark, CICFlow meter
Machine Learning	scikit-learn, PyTorch, XGBoost
Anomaly Detection	Isolation Forest, Autoencoder, One-Class SVM
Deployment	Docker, Flask, Raspberry Pi 5(for autonomous applications)
Communication Protocols	TCP, UDP, TLS, QUIC, ICMP

EXPECTED OUTCOME / SCOPE OF USE

- DRONE/AUTONOMOUS VEHICLES : specialisation in Edge computing for autonomous systems, detecting anomalies and potential attacks in long range missions

- LAB/OFFICE MONITORING SETUP: Detecting anomalies in sensitive data transmission

- FINANCIAL SETUP: Detect fraud, insider threats, API abuse, and malware in real-time; monitor transactions and access; enable rapid post-incident forensics.

REFERENCE

1. **"Practical Machine Learning for Network Security" - Book**
   Author: Sumeet Dua, Xian Du
   ISBN: 9780128038437

2. **Kaggle – Network Intrusion Detection Projects**
   Network Intrusion Detection

3. **JA3 SSL/TLS Fingerprinting**
   salesforce/ja3: JA3 is a standard for creating SSL client fingerprints in an easy to produce and shareable way.

4. **OpenWRT (Router firmware platform)**
   [OpenWrt Wiki] Welcome to the OpenWrt Project