Basic Details of the Team and Problem Statement

Problem Statement Title: Network Traffic Analysis

Team Name: AltF4

Team Leader Name: Raman Biju

Institute Name: Sandip University, Nashik

Sub Domain Name: Cyber Security

Idea/Approach Details

Our project aims to revolutionize network security through advanced AI-driven traffic analysis. By integrating real-time packet capture, machine learning models, and intuitive visualization, we empower organizations to detect and respond to cyber threats proactively.

Components involved in this project are:

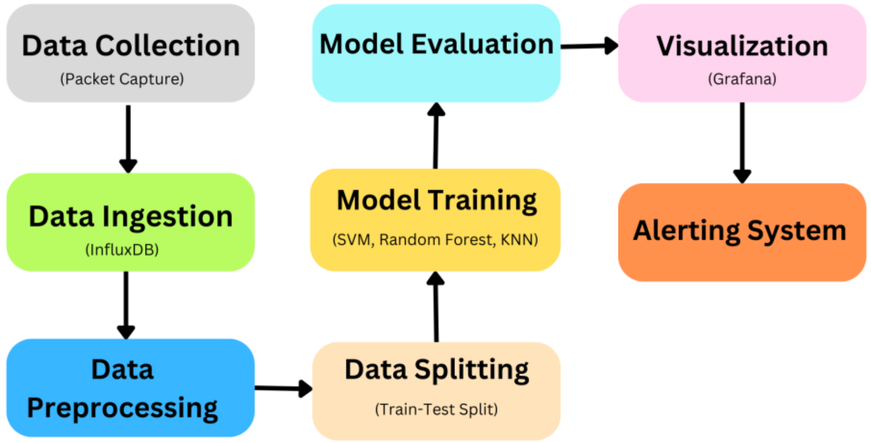
- Packet Capture and Storage
- Data Visualization and Monitoring
- Machine Learning for Anomaly Detection
- Alerting and Response Mechanism

Benefits associated with this project are:

- Enhanced Security Posture
- Operational Efficiency

Technology Stack

Flow Chart



Data Collection (Packet Capture)

Data Ingestion (InfluxDB)

Data Preprocessing

Data Splitting (Train-Test Split)

Model Training (SVM, Random Forest, KNN)

Model Evaluation

Visualization (Grafana)

Alerting System

pandas
jupyter
AI
NLP
influxdb

Idea/Approach Details

➢ USE CASES

1. **Anomaly Detection**:
   The AI model can detect unusual patterns in network traffic, indicating potential cyber threats such as DDoS attacks, MITM attacks, Network Eavesdropping and Malware attacks.

2. **Threat Prioritization**:
   Detected threats are prioritized based on their severity, allowing network administrators to focus on the most critical issues first.

3. **Real-Time Monitoring**:
   The Grafana dashboards provide real-time insights into network traffic, enabling proactive monitoring and quick response to anomalies.

4. **Alerting and Notifications**:
   The system generates real-time alerts for detected threats, ensuring timely notification and response to potential cyber-attacks.

➢ SHOW STOPPERS

Network Outage: Halts data collection

Insufficient Bandwidth: Impedes real-time analysis

Software Bugs: Causes data inaccuracies

Hardware Failures: Disrupts analysis

Packet Tampering: Affects ML algorithm integrity

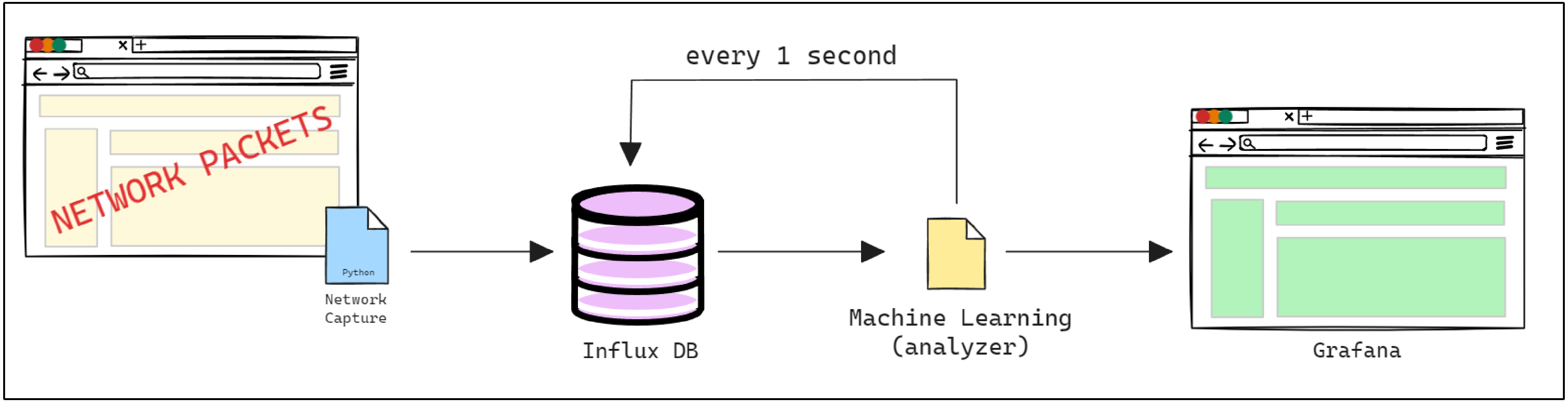
➢ DEPENDENCIES

Software: Properly configured tools

Data Availability: Continuous traffic logs

External Services: Third-party integrations

Flow Diagram of Network Traffic Analysis


every 1 second
NETWORK PACKETS
Python
Network Capture
Influx DB
Machine Learning (analyzer)
Grafana