DATA FLOW Diagram

DATE	25-10-2023
TEAM ID	4.1
PROJECT NAME	NETWORK ANOMALY DETECTION

MENTOR : P MANOJ

Team Members :

C DEVAKI NANDAN REDDY

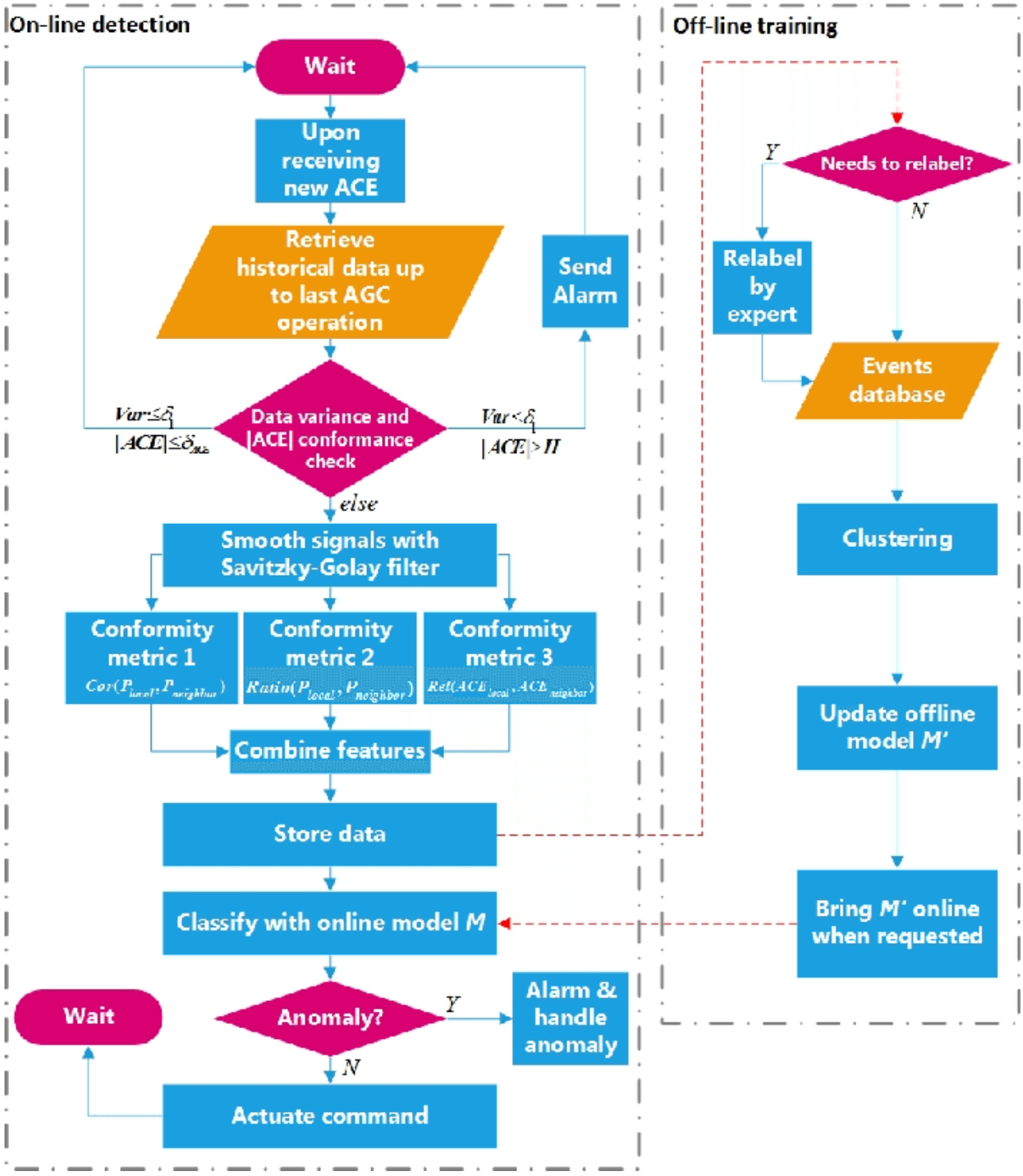
S NIHAL AHMED

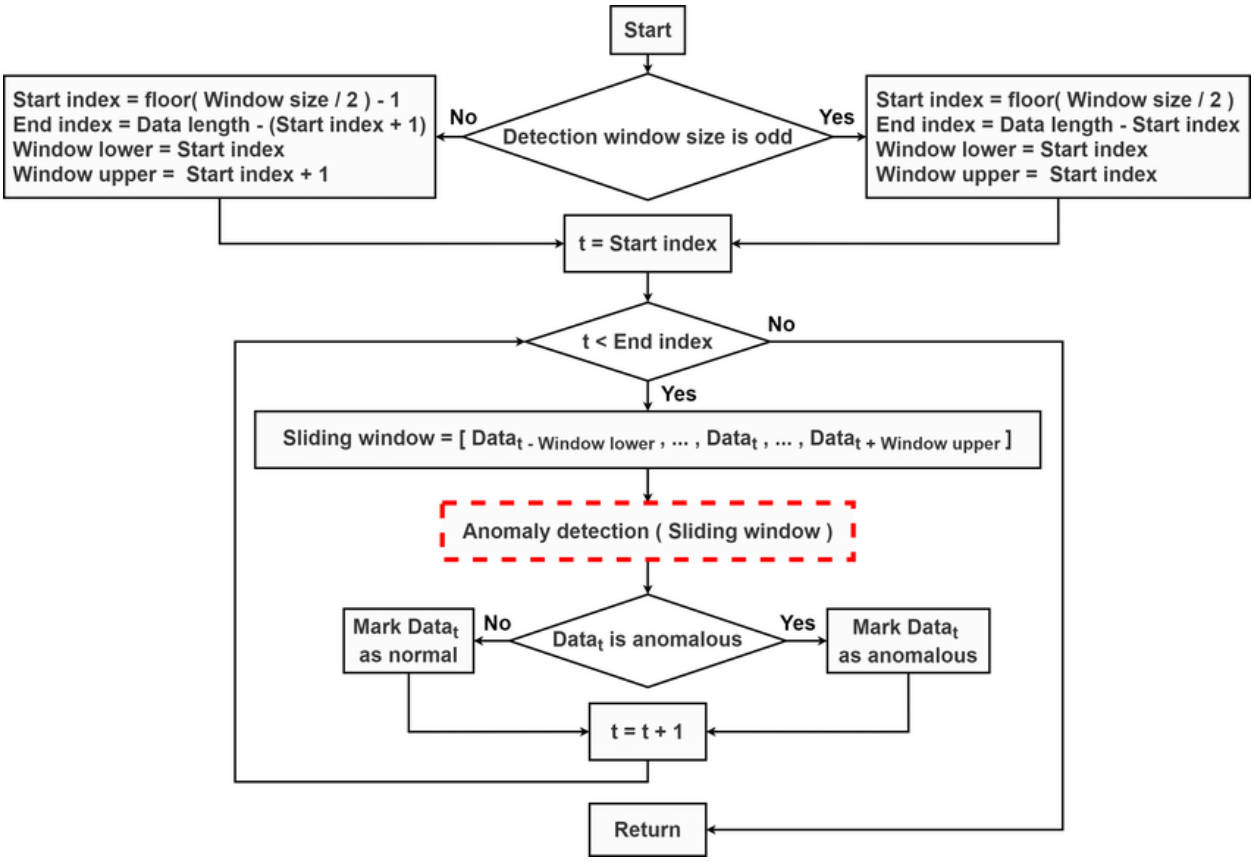
A data flow diagram for network anomaly detection typically illustrates the flow of data and processes involved in identifying and responding to anomalies in a network. Here are some key bullet points to include in such a diagram:

1. **Data Sources:**
   - Network traffic data from routers, switches, and firewalls.
   - System logs and event data from network devices.
   - External data sources like threat intelligence feeds.
2. **Data Ingestion:**
   - Collection and ingestion of raw data from various sources.
   - Data may be in the form of packets, logs, or event streams.
3. **Preprocessing:**
   - Data cleaning, normalization, and transformation.
   - Handling missing data and outliers.
4. **Feature Extraction:**
   - Extract relevant features from raw data.
   - Examples include IP addresses, port numbers, packet sizes, and protocols.
5. **Model Training:**
   - Machine learning algorithms, such as anomaly detection models or deep learning networks.
   - Use historical data to train models to recognize normal network behavior.
6. **Real-time Monitoring:**

- Continuous monitoring of network traffic and events.
- Data from live network feeds is compared to the trained model.

7. **Anomaly Detection:**
   - Identification of deviations from expected network behavior.
   - Triggering alerts for potential anomalies.
8. **Alerting System:**
   - Generate alerts when anomalies are detected.
   - Alerts can be sent to network administrators or security teams.
9. **Incident Response:**
   - Define procedures for responding to anomalies.
   - May involve isolating affected systems, capturing data, and analyzing the nature of the anomaly.
10. **Logging and Reporting:**
    - Record all activities, alerts, and responses.
    - Generate reports for post-incident analysis.
11. **Feedback Loop:**
    - Use feedback from detected anomalies to improve the model.
    - Continuously update the anomaly detection system.
12. **Integration with Security Tools:0+**
    - Integration with other security tools like SIEM (Security Information and Event Management) systems.
13. **Decision Points:**
    - Decision points for taking action, such as blocking traffic or escalating an incident.
14. **Data Storage:**
    - Store historical data for trend analysis and forensic investigations.
15. **Compliance and Audit:**
    - Ensure that the system complies with regulatory requirements and security standards.
16. **User Interface:**
    - Provide a user interface for administrators to configure and monitor the anomaly detection system.
17. **External Communication:**
    - Communicate with external entities, such as threat intelligence services or reporting to regulatory authorities.


On-line detection
Wait
Upon receiving new ACE
Retrieve historical data up to last AGC operation
Send Alarm
Data variance and |ACE| conformance check
Var≤δ1
|ACE|≤δ2
Var<δ1
|ACE|>H
else
Smooth signals with Savitzky-Golay filter
Conformity metric 1
Cor(P_local, P_neighbor)
Conformity metric 2
Ratio(P_local, P_neighbor)
Conformity metric 3
Rel(ACE_local, ACE_neighbor)
Combine features
Store data
Classify with online model M
Wait
Anomaly?
Y
N
Alarm & handle anomaly
Actuate command
Off-line training
Needs to relabel?
Y
N
Relabel by expert
Events database
Clustering
Update offline model M'
Bring M' online when requested


Start
Detection window size is odd
No
Yes
Start index = floor(Window size / 2) - 1
End index = Data length - (Start index + 1)
Window lower = Start index
Window upper = Start index + 1
Start index = floor(Window size / 2)
End index = Data length - Start index
Window lower = Start index
Window upper = Start index
t = Start index
t < End index
No
Yes
Sliding window = [Data t - Window lower , ... , Data t , ... , Data t + Window upper]
Anomaly detection (Sliding window)
Data t is anomalous
No
Yes
Mark Data t as normal
Mark Data t as anomalous
t = t + 1
Return