

MACHINE LEARNING BASED NETWORK MONITORING SYSTEM

Date: 18 November 2025

SUPERVISOR:

DR. MUHAMMAD ZAIN SIDDIQI

CO-SUPERVISOR:

DR. KHURRAM JADOON

MADAM BEENISH, LECTURER

GROUP MEMBERS:

MUHAMMAD YOUNAS – 2022456

MUHAMMAD UMAR MAQSOOD – 2022447

SHAMINA DURRANI – 2022453

ML – Based Network Monitoring System

Revision History:

<i>Revision History</i>	<i>Date</i>	<i>Comments</i>
1.00	November 18, 2025	Draft SRS Document and submit it for review to supervisor and Co-Supervisors
2.00	November 19, 2025	Finalize the documents, make changes suggested by our Supervisors.

Document Approval:

The following document has been accepted and approved by the following:

<i>Signature</i>	<i>Date</i>	<i>Name</i>
	November 19, 2025	Dr. Muhammad Zain Siddiqi
	November 19, 2025	Madam Beenish

Disclaimer:

This document outlines the functional and non-functional requirements for the "Machine Learning-based Network Monitoring System" a Final Year Project (FYP) developed by the project team members: Muhammad Umar Maqsood, Shamina Durrani and Muhammad Younas, at the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology.

List of Figures

Figure 1: Use Case Diagram 25

Figure 2: Data Flow Diagram 26

Figure 3: Development View Diagram 27

Figure 4: Process View Diagram..... 28

Figure 5: Dashboard Login Interface 29

Figure 6: ML-NMS Dashboard Interface 30

Figure 7: ML -NMS Recent Incident Interface 30

List of Contents

1	INTRODUCTION.....	6
1.1.	PURPOSE.....	6
1.2.	PRODUCT SCOPE.....	6
1.1.1	<i>Document Conventions.....</i>	<i>9</i>
2	OVERVIEW.....	10
2.1	THE OVERALL DESCRIPTION.....	10
2.2	PRODUCT PERSPECTIVE.....	10
2.2.	PRODUCT FUNCTIONS.....	10
2.3.	USER CHARACTERISTICS.....	11
2.3.	CONSTRAINTS	11
2.4.	ASSUMPTIONS AND DEPENDENCIES.....	11
3	STATE OF THE ART	12
4	USER/SYSTEM REQUIREMENTS	13
4.1	EXTERNAL INTERFACE REQUIREMENTS	13
4.1.1	<i>User Interfaces.....</i>	<i>13</i>
4.1.2	<i>Hardware Interfaces.....</i>	<i>13</i>
4.1.3	<i>Software Interfaces.....</i>	<i>13</i>
4.1.4	<i>Communication Interfaces</i>	<i>13</i>
5	FUNCTIONAL REQUIREMENTS	13
5.1	FUNCTIONAL REQUIREMENTS WITH TRACEABILITY INFORMATION	14
5.1.1	<i>Feature 1: Network Traffic Capture & Processing.....</i>	<i>14</i>
5.1.2	<i>Feature 2: ML Anomaly Detection Engine</i>	<i>16</i>
5.1.3	<i>Feature 3: Data Storage & Management.....</i>	<i>19</i>
5.1.4	<i>Feature 4: Alert Mechanism.....</i>	<i>20</i>
5.1.5	<i>Feature 5: Web Dashboard & Visualization</i>	<i>21</i>
5.1.6	<i>Feature 6: User Management & RBAC</i>	<i>22</i>
6	NONFUNCTIONAL REQUIREMENTS & SOFTWARE SYSTEM ATTRIBUTES	24
6.1	PERFORMANCE REQUIREMENTS	24
6.2	SECURITY REQUIREMENTS	24
6.3	RELIABILITY.....	24
7	PROJECT DESIGN/ARCHITECTURE.....	25

List of Tables

Table 1: Terms used in this document and their description	6
Table 2: Conventional terms used in this document and their description	9
Table 3: Conventional terms used in this document	9
Table 4: Existing Systems	12
Table 5: First FR OF Feature 1	14
Table 6: FR-02 OF Feature 1	14
Table 7: FR-03 OF Feature 1	15
Table 8: FR-04 OF Feature 1	15
Table 9: FR-05 OF Feature 2	16
Table 10: FR-06 OF Feature 2	17
Table 11: FR-07 OF Feature 2	17
Table 12: FR-08 OF Feature 3	18
Table 13: FR-09 OF Feature 3	19
Table 14: FR-10 OF Feature 3	19
Table 15: FR-11 OF Feature 4	20
Table 16: FR-12 OF Feature 4	20
Table 17: FR-13 OF Feature 5	21
Table 18: FR-14 OF Feature 5	22
Table 19: FR-15 OF Feature 6	22
Table 20: FR-16 OF Feature 6	23
Table 21: FR-17 OF Feature 6	23

ML – Based Network Monitoring System

1 INTRODUCTION

The Machine Learning-based Network Monitoring System is a FYP being developed at the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology (GIKI). Aims to provide real-time anomaly detection within a LAN to enhance network security and assist network administrators in identifying and responding to cyber threats.

The platform will serve as a prototype for advanced network intrusion detection, demonstrating the application of machine learning techniques to network traffic analysis for security purposes.

1.1. PURPOSE

The purpose of this Software Requirements Specification (SRS) is to define the functional and non-functional requirements for the **Machine Learning-Based Network Monitoring System**. This system is a Final Year Project (FYP) designed to enhance network security by detecting anomalies in network traffic behavior. Unlike traditional signature-based systems, this project leverages machine learning to identify novel and polymorphic threats in real-time within a Local Area Network (LAN). This document serves as the roadmap for development, testing, and validation.

1.2. PRODUCT SCOPE

The Machine Learning-based Network Monitoring System is a FYP being developed at the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology (GIKI). The system aims to provide real-time anomaly detection within a LAN to enhance network security and assist network administrators in identifying and responding to cyber threats.

The platform will serve as a prototype for advanced network intrusion detection, demonstrating the application of machine learning techniques to network traffic analysis for security purposes.

Table 1: Terms used in this document and their description

Name	Description
SRS	(Software Requirements Specification). A document that describes the nature of a project, software or application.
ML-NMS	Machine Learning-Based Network Monitoring System.
ML	Machine Learning: algorithms that enable systems to learn from data.
SPAN	Switched Port Analyzer: a method to copy network

ML – Based Network Monitoring System

	traffic to a monitoring device.
CLI	Command-Line Interface
RBAC	Role-Based Access Control
SRS	Software Requirement Specification
METADATA	High level data (e.g., packet size, flow duration e.tc) used for analysis, protecting privacy by ignoring payloads.
IDS	Intrusion Detection System
FYP	(Final Year Project). A substantial project undertaken by university students in their final year of study.
AI	(Artificial Intelligence). The simulation of human intelligence processes by machines, especially computer systems.
IPS	(Intrusion Prevention System). A network security device that monitors network and/or system activities for malicious or unwanted behavior and can react to block or prevent those activities.
PCAP	(Packet Capture Format). A file format for recording network traffic.
TLS	(Transport Layer Security). A cryptographic protocol designed to provide communications security over a computer network
FPR	(False Positive Rate). The proportion of actual negatives that are incorrectly identified as positives.
FNR	(False Negative Rate). The proportion of actual positives that are incorrectly identified as negatives.
TPR	(True Positive Rate). The proportion of actual positives that are correctly identified as positives.
TNR	(True Negative Rate). The proportion of actual negatives that are correctly identified as negatives.
IT	(Information Technology). The use of computers, storage, networking, and other physical devices, infrastructure, and processes to create, process, store, secure, and exchange all forms of electronic data.
SIEM	(Security Information and Event Management). A software solution that aggregates and analyzes security alerts and log data from various sources across an IT infrastructure.
LAN	(Local Area Network). A computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building.
Client	In a network context, typically refers to a device (e.g., workstation, server, IoT device) that requests resources or services from another device (the server).
Server	A computer program or device that provides functionality or services for other programs or devices (clients) over a network.
SPAN	(Switched Port Analyzer). A feature on network switches

ML – Based Network Monitoring System

	that allows traffic from one or more source ports to be copied and sent to a designated destination port for monitoring.
Mirror Port	A common alternative term for a SPAN port, used to describe the capability of duplicating network traffic to another port for analysis.
Data Collectors	Components (software agents or dedicated hardware) deployed within a network responsible for gathering various types of telemetry data (e.g., metrics, logs, network flows) for monitoring and analysis.
Telemetry Data	Data collected from various sources (e.g., network devices, servers, applications) that provides information about the performance, health, and activity of a system.
MFA	(Multi-Factor Authentication). An authentication method that requires users to provide two or more verification factors to gain access to a resource.
OAuth	(Open Authorization). An open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites without giving them their passwords.
METADATA	High-level descriptive information about network traffic (e.g., packet size, timestamps, source/destination IPs, ports)
FLOW	A unidirectional sequence of packets sharing common attributes such as IP addresses, ports, and protocol
FEATURE VECTOR	A structured representation of extracted attributes used as input for ML models
SUPERVISED LEARNING	ML approach using labeled data to train classification algorithms
UNSUPERVISED LEARNING	ML approach used to identify patterns or anomalies in unlabeled data
ANOMALY DETECTION	ML-based identification of unusual patterns or deviations from normal traffic behavior
ALERT	A system generated notification indicating detected anomalous or suspicious activity
JSON	(JavaScript Object Notation). A lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate.
REAL-TIME PROCESSING	Data analysis and detection performed with minimal latency
IT Teams	Information Technology teams (which could be internal to an SMB or a managed service provider supporting SMBs)
DATASET	A structured collection of network samples used for training and testing ML models
MODEL DRIFT	Degradation of ML performance when input data characteristics change over time
CLASS IMBALANCE	Unequal representation of classes within the dataset
PREPROCESSING	Transformation steps applied to raw data before model

ML – Based Network Monitoring System

	training
--	----------

1.1.1 Document Conventions

Table 2: Conventional terms used in this document and their description

Term	Description
SHALL	Referring to a mandatory requirement that must be fulfilled as part of the core project scope for this Final Year Project. This feature is essential for the system's successful completion.
SHOULD	Indicates a desirable requirement that, if feasible, ought to be implemented to enhance the system. It is a high-priority consideration for inclusion.
MAY	Refers to an optional requirement that could be considered for future enhancements or if time and resources permit beyond the core scope. The developer is encouraged to consider this requirement generally.
TBD	To Be Determined, indicates information that is not yet available but will be provided in future iterations or updates of this document.
Note	Provides additional information or clarification relevant to the preceding text.

Requirements are categorized as follows:

Table 3: Conventional terms used in this document

Requirement Number	Description
FR-XX	Functional Requirements
NFR-XX	Non-Functional Requirements
UC-XX	Use Case

2 OVERVIEW

2.1 THE OVERALL DESCRIPTION

The Machine Learning-Based Network Monitoring System is a standalone security solution designed to address the limitations of traditional signature-based IDSs. As we outlined in our project scope (FYP-Presentation -1), traditional systems often struggle with **unknown attack patterns** and high-volume traffic. This system employs behavioral analysis and machine learning algorithms to identify irregular patterns in real-time.

The system captures network packets, extracts flow-based features, and compares them against a dynamic baseline. If the "anomaly score" exceeds a threshold, the system alerts the network administrator. The primary goal is to provide a scalable, adaptive system that enhances security in high-traffic environments while minimizing false positives.

2.2 PRODUCT PERSPECTIVE

The system operates as an independent monitoring node within a LAN. It interfaces with:

- **Network Infrastructure:** Captures traffic via a Switched Port Analyzer (SPAN/Mirror) port or a direct network interface.
- **System Administrator:** Interacts with the system via a Web Dashboard and Command Line Interface (CLI) to view alerts and configure settings.
- **Local Storage:** Stores trained ML models, traffic feature datasets, and anomaly logs.

2.2. PRODUCT FUNCTIONS

To ensure the project is achievable within the FYP timeline, the system focuses on these 7 core functions:

1. **Network Traffic Capture:** Real-time ingestion of packets from a designated LAN interface.
2. **Feature Extraction:** Processing raw packet data into ML-ready metadata (e.g., packet size, timestamp, protocol) to reduce dimensionality.
3. **ML Anomaly Detection:** Using unsupervised learning algorithms to detect novel threats and assign anomaly scores.
4. **Basic Data Storage:** Persisting extracted features and anomaly logs in a structured database.
5. **Alerting Mechanism:** Generating email and dashboard notifications for high-severity anomalies.
6. **Web Dashboard:** A visualization interface for monitoring "Network Health" and viewing active incidents.
7. **User Management & RBAC:** Secure authentication with "Administrator" and "Observer" roles.

2.3. USER CHARACTERISTICS

- **Network Administrator:** Technical user responsible for setting up the capture interface, managing ML models, and investigating alerts.
- **Observer:** Non-technical or junior staff who view the dashboard for status updates but cannot modify configurations.

2.3. CONSTRAINTS

- **Timeframe:** Core development must be completed within 2-3 months (Simplified Scope).
- **Computational Resources:** Must run on standard commodity hardware (e.g., a high-spec laptop or standard server).
- **Privacy:** Analysis is performed strictly on metadata; packet payloads are not inspected or stored.
- **Connectivity:** The system requires a specific network configuration (e.g., Port Mirroring) to see LAN traffic.

2.4. ASSUMPTIONS AND DEPENDENCIES

- **Assumption:** The network switch/router supports SPAN or Port Mirroring.
- **Assumption:** A dataset of "normal" network traffic is available or can be captured to train the initial baseline.
- **Dependency:** Availability of Python libraries (Scikit-learn, Pandas) and stable network drivers for packet capture.

3 STATE OF THE ART

- LITERATURE REVIEW

The project builds upon research into ML-based intrusion detection.

- *Sommer & Paxson (2010)* highlighted the challenges of applying ML to network intrusion detection, emphasizing the need for generalization.
- *Ahmad et al. (2021)* reviewed ML/DL techniques, confirming their potential for encrypted traffic analysis.
- *J. Dromard et al. (2018)* demonstrated the efficacy of unsupervised learning (Autoencoders) for online attack detection.

- EXISTING SYSTEMS

The following table outlines well-known commercial platforms that utilize machine learning for network anomaly detection, security event monitoring, and intelligent alerting. These systems represent the current methodology in the industry that validates the approach taken by this project.

Table 4: Existing Systems

System Name	Key Features & Methodology
1. Darktrace	Uses AI and machine learning for real-time network threat detection and autonomous response. It learns the "pattern of life" of devices and users, identifying anomalous behavior and security breaches without relying only on signatures. It provides continuous learning and adapts to network changes automatically.
2. Dynatrace	Employs the "Davis" AI engine for root cause analysis, anomaly detection, and predictive insights. It discovers application, service, and infrastructure dependencies automatically, mapping network topology in real-time. It forecasts performance issues and can auto-remediate common problems using ML.
3. LogicMonitor	Uses machine learning to reduce false positives and alert noise. It forecasts resource utilization, adjusts monitoring thresholds based on historical data, and detects anomalies before they escalate into critical failures.
4. Juniper Mist AI & Marvis	Automates network troubleshooting, detecting anomalies and root causes using ML. It provides natural language chatbot support to answer network questions and simulate user connections to preemptively identify problems.

4 USER/SYSTEM REQUIREMENTS

4.1 External Interface Requirements

4.1.1 User Interfaces

- **Web Dashboard:** A clean, responsive interface displaying a list of recent anomalies, a traffic volume graph, and system status.
- **CLI:** A terminal-based interface for initial configuration (e.g., selecting the network interface).

4.1.2 Hardware Interfaces

- **Network Interface Card (NIC):** Must support promiscuous mode for packet capture.
- **Storage:** Minimum 256GB SSD recommended for efficient database read/write operations.

4.1.3 Software Interfaces

- **Backend Framework:** Python (Flask or Django).
- **Frontend Framework:** HTML, CSS, JavaScript/ React, Vue.js, and Angular
- **ML Engine:** Scikit-learn / ML Algorithms.
- **Database:** SQLite (for prototype) or PostgreSQL.

4.1.4 Communication Interfaces

- **HTTP/HTTPS:** For accessing the Web Dashboard.
- **SMTP:** For sending email alerts to administrators.

5 Functional Requirements

This section details the functional requirements of the ML-Based Network Monitoring System, organized by major system features. Each requirement is identified with a unique ID (FR-XX) for traceability and reference.

5.1 Functional Requirements with Traceability information

5.1.1 Feature 1: Network Traffic Capture & Processing

Core Capability to ingest and parse raw network data.

Table 5: First FR OF Feature 1.

Requirement ID	FR-01		Requirement Type		Functional		Use Case #		UC-01
Status	New		Agreed-to	-	Baselined	-	Rejected	-	
Parent Requirement #	N/A								
Description	The system SHALL captures real-time network packets from a designated Local Area Network (LAN) interface.								
Rationale	Without packet capture, the system has no data to analyze for security monitoring.								
Source	Project Scope				Source Document		SRS		
Acceptance/Fit Criteria	The system successfully binds to the network interface and begins ingesting packets without errors								
Dependencies	N/A								
Priority	Essential		Conditional	-	Optional	-			
Change History	v1.0								

Table 6: FR-02 OF Feature 1

Requirement ID	FR-02		Requirement Type	Functional		Use Case #	UC-01	
Status	<i>New</i>		<i>Agreed-to</i>	-	<i>Baselined</i>	-	<i>Rejected</i>	-
Parent Requirement #	FR-01							
Description	The system SHALL support "Promiscuous Mode" on the network interface card to capture all traffic on the segment, not just traffic addressed to the host.							
Rationale	Essential for an IDS to monitor the entire network segment, not just the monitoring device itself.							
Source	Technical Requirement				Source Document	SRS		

ML – Based Network Monitoring System

Acceptance/Fit Criteria	The system captures packets destined for other IP addresses on the LAN.						
Dependencies	FR-01						
Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-	
Change History	v1.0						

Table 7: FR-03 OF Feature 1

Requirement ID	FR-03			Requirement Type		Functional		Use Case #		UC-01
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	FR-01									
Description	The system SHALL parse captured packets to identify protocols (TCP, UDP, ICMP) and headers.									
Rationale	Raw binary data must be decoded into understandable protocols for feature extraction.									
Source	Project Scope				Source Document		SRS			
Acceptance/Fit Criteria	Network Logs show correctly identified protocols for incoming traffic.									
Dependencies	FR-01									
Priority	Essential		Conditional	-	Optional	-				
Change History	v1.0									

Table 8: FR-04 OF Feature 1

Requirement ID	FR-04		Requirement Type		Functional		Use Case #		UC-01	
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	FR-03									

ML – Based Network Monitoring System

Descriptor	The system SHALL extract specific features (Packet Size, Timestamp, Source/Dest IP, Source/Dest Port) from the parsed data to create a feature vector.						
Rationale	Machine Learning models require structured numerical input (vectors), not raw packet dumps.						
Source	ML Requirement			Source Document		SRS	
Acceptance/Fit Criteria	A valid feature vector (e.g., CSV format) is generated for every flow/packet.						
Dependencies	FR-03						
Priority	Essential		Conditional	-	Optional	-	
Change History	v1.0						

5.1.2 Feature 2: ML Anomaly Detection Engine

The brain of the system using ML Algorithms

Table 9: FR-05 OF Feature 2

Requirement ID	FR-05		Requirement Type		Functional		Use Case #		UC-02	
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	N/A									
Description	The system SHALL load a pre-trained or self-learning ML model upon startup.									
Rationale	The detection engine requires an active model instance to process incoming data.									
Source	Project Scope				Source Document		SRS			
Acceptance/Fit Criteria	System startup logs confirm "ML Model Loaded Successfully."									
Dependencies	N/A									
Priority	Essential		Conditional	-	Optional	-				
Change History	v1.0									

ML – Based Network Monitoring System

Table 10: FR-06 OF Feature 2

Requirement ID	FR-06	Requirement Type	Functional			Use Case #	UC-02	
Status	<i>New</i>		<i>Agreed-to</i>	-	<i>Baselined</i>	-	<i>Rejected</i>	-
Parent Requirement #	FR-04							
Description	The system SHALL input the extracted feature vectors into the ML model to generate a real-time prediction.							
Rationale	This is the actual "detection" step where traffic is analyzed.							
Source	Project Scope				Source Document	SRS		
Acceptance/Fit Criteria	A valid feature vector (e.g., CSV format) is generated for every flow/packet.							
Dependencies	FR-04, FR-05							
Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-		
Change History	v1.0							

Table 11: FR-07 OF Feature 2

Requirement ID	FR-07		Requirement Type		Functional		Use Case #		UC-02	
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	FR-06									
Description	The system SHALL calculate an "Anomaly Score" (e.g., -1.0 to 1.0) based on the ML model's output.									
Rationale	A binary "Good/Bad" is not enough; a score helps determine the severity of the deviation.									
Source	ML Requirement				Source Document		SRS			
Acceptance/Fit Criteria	Each analyzed record has an associated numerical score.									
Dependencies	FR-06									

ML – Based Network Monitoring System

Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-	
Change History	v1.0						

Table 12: FR-08 OF Feature 3

Requirement ID	FR-08	Requirement Type	Functional			Use Case #	UC-02	
Status	<i>New</i>		<i>Agreed-to</i>	-	<i>Baselined</i>	-	<i>Rejected</i>	-
Parent Requirement #	FR-07							
Description	The system SHALL classify traffic as "Anomalous" if the calculated score exceeds a configurable threshold.							
Rationale	Defines the cut-off point for what constitutes a threat versus normal noise.							
Source	Project Scope				Source Document	SRS		
Acceptance/Fit Criteria	Traffic with high scores is flagged as "Anomaly"; traffic with low scores is "Normal."							
Dependencies	FR-07							
Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-		
Change History	v1.0							

ML – Based Network Monitoring System

5.1.3 Feature 3: Data Storage & Management

Persistence layer for logs and training data.

Table 13: FR-09 OF Feature 3

Requirement ID	FR-09		Requirement Type		Functional		Use Case #		UC-03
Status	New		Agreed-to	-	Baselined	-	Rejected	-	
Parent Requirement #	N/A								
Description	The system SHALL maintain a structured local database (e.g., SQLite/PostgreSQL) to store system data.								
Rationale	Data persistence is required for reporting and historical analysis.								
Source	System Design				Source Document		SRS		
Acceptance/Fit Criteria	Database file is created and accessible by the application. Database file is created and accessible by the application.								
Dependencies	N/A								
Priority	Essential		Conditional	-	Optional	-			
Change History	v1.0								

Table 14: FR-10 OF Feature 3

Requirement ID	FR-10		Requirement Type	Functional		Use Case #	UC-03	
Status	<i>New</i>		<i>Agreed-to</i>	-	<i>Baselined</i>	-	<i>Rejected</i>	-
Parent Requirement #	FR-04							
Description	The system SHALL store detailed records of all detected anomalies (Time, IP, Score) in a dedicated "Incidents" table.							
Rationale	Ensures a permanent record of security threats for the administrator to review later.							
Source	Project Scope				Source Document	SRS		

ML – Based Network Monitoring System

Acceptance/Fit Criteria	"Anomalous" records are successfully written to the Incidents table.						
Dependencies	FR-08, FR-09						
Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-	
Change History	v1.0						

5.1.4 Feature 4: Alert Mechanism

Notification System.

Table 15: FR-11 OF Feature 4

Requirement ID	FR-11		Requirement Type		Functional		Use Case #		UC-04	
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	FR-08									
Description	The system SHALL generate an Alert Event whenever an anomaly is classified.									
Rationale	The internal trigger required to initiate notifications.									
Source	Project Scope				Source Document		SRS			
Acceptance/Fit Criteria	System logs show "Alert Generated" immediately following anomaly detection.									
Dependencies	FR-08									
Priority	Essential		Conditional	-	Optional	-				
Change History	v1.0									

Table 16: FR-12 OF Feature 4

Requirement ID	FR-12		Requirement Type	Functional		Use Case #	UC-04	
-----------------------	-------	--	-------------------------	------------	--	-------------------	-------	--

ML – Based Network Monitoring System

[illegible]

5.1.5 Feature 5: Web Dashboard & Visualization

User (Administrator) interface for monitoring.

Table 17: FR-13 OF Feature 5

Requirement ID	FR-13	Requirement Type	Functional		Use Case #	UC-05
Status	<i>New</i>	<i>Agreed-to</i>	-	<i>Baselined</i>	-	<i>Rejected</i> -
Parent Requirement #	N/A					
Description	The system SHALL provide a web-based dashboard accessible via a standard browser.					
Rationale	Provides a graphical interface for the administrator to interact with the system.					
Source	Project Scope			Source Document	SRS	
Acceptance/Fit Criteria	The dashboard loads successfully on Chrome/Edge.					
Dependencies	N/A					

ML – Based Network Monitoring System

Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-	
Change History	v1.0						

Table 18: FR-14 OF Feature 5

Requirement ID	FR-14		Requirement Type		Functional		Use Case #		UC-05	
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	FR-13									
Description	The dashboard SHALL display a real-time line graph showing traffic volume and anomaly spikes.									
Rationale	Visual aids help administrators quickly understand network status.									
Source	User Experience				Source Document		SRS			
Acceptance/Fit Criteria	Graph updates dynamically as new data is processed.									
Dependencies	FR-13, FR-04									
Priority	Essential		Conditional	-	Optional	-				
Change History	v1.0									

5.1.6 Feature 6: User Management & RBAC

Security and Access Control.

Table 19: FR-15 OF Feature 6

Requirement ID	FR-15		Requirement Type		Functional		Use Case #		UC-06	
Status	New		Agreed-to	-	Baselined	-	Rejected	-		
Parent Requirement #	N/A									
Description	The system SHALL require users to authenticate using a username and password to access the dashboard.									

ML – Based Network Monitoring System

Rationale	Prevents unauthorized personnel from viewing sensitive network security data.						
Source	Security Requirement			Source Document		SRS	
Acceptance/Fit Criteria	Unauthenticated access redirects to a login page.						
Dependencies	N/A						
Priority	<i>Essential</i>		<i>Conditional</i>	-	<i>Optional</i>	-	
Change History	v1.0						

Table 20: FR-16 OF Feature 6

Requirement ID	FR-16		Requirement Type		Functional		Use Case #		UC-07
Status	New		Agreed-to	-	Baselined	-	Rejected	-	
Parent Requirement #	FR-15								
Description	The system SHALL implement Role-Based Access Control (RBAC) supporting 'Administrator' and 'Observer' roles.								
Rationale	Different users require different levels of access (Full Control vs Read-Only).								
Source	Project Scope				Source Document		SRS		
Acceptance/Fit Criteria	Users are assigned a specific role upon account creation.								
Dependencies	FR-15								
Priority	Essential		Conditional	-	Optional	-			
Change History	v1.0								

Table 21: FR-17 OF Feature 6

Requirement ID	FR-17		Requirement Type		Functional		Use Case #		UC-07
Status	<i>New</i>		<i>Agreed-to</i>	-	<i>Baselined</i>	-	<i>Rejected</i>	-	

ML – Based Network Monitoring System

Parent Requirement #	FR-16						
Description	The system SHALL hide configuration settings and user management options from users with the 'Observer' role.						
Rationale	Enforces the principle of least privilege; observers should not change system settings.						
Source	Security Requirement			Source Document	SRS		
Acceptance/Fit Criteria	"Settings" menu is invisible or disabled for Observer accounts.						
Dependencies	FR-16						
Priority	Essential		Conditional	-	Optional	-	
Change History	v1.0						

6 Nonfunctional Requirements & Software System Attributes

6.1 Performance Requirements

- **NFR-01:** Real-time anomaly scoring must complete within minimum time of data ingestion to ensure timely detection.
- **NFR-02:** Dashboard page load times should be minimum under normal load conditions.

6.2 Security Requirements

- **NFR-04:** All user passwords must be hashed before storage in the database.
- **NFR-05:** Access to the web dashboard must require valid authentication.
- **NFR-06:** Input validation must be implemented to prevent injection attacks.

6.3 Reliability

- **NFR-07:** The system should handle unexpected input data (e.g., malformed packets) gracefully without crashing.
- **NFR-08:** The system must automatically attempt to reconnect to the database if the connection is lost.

7 Project Design/Architecture

- 4+1 ARCHITECTURE VIEW MODEL (mandatory for Software Projects)
 - Use Case View

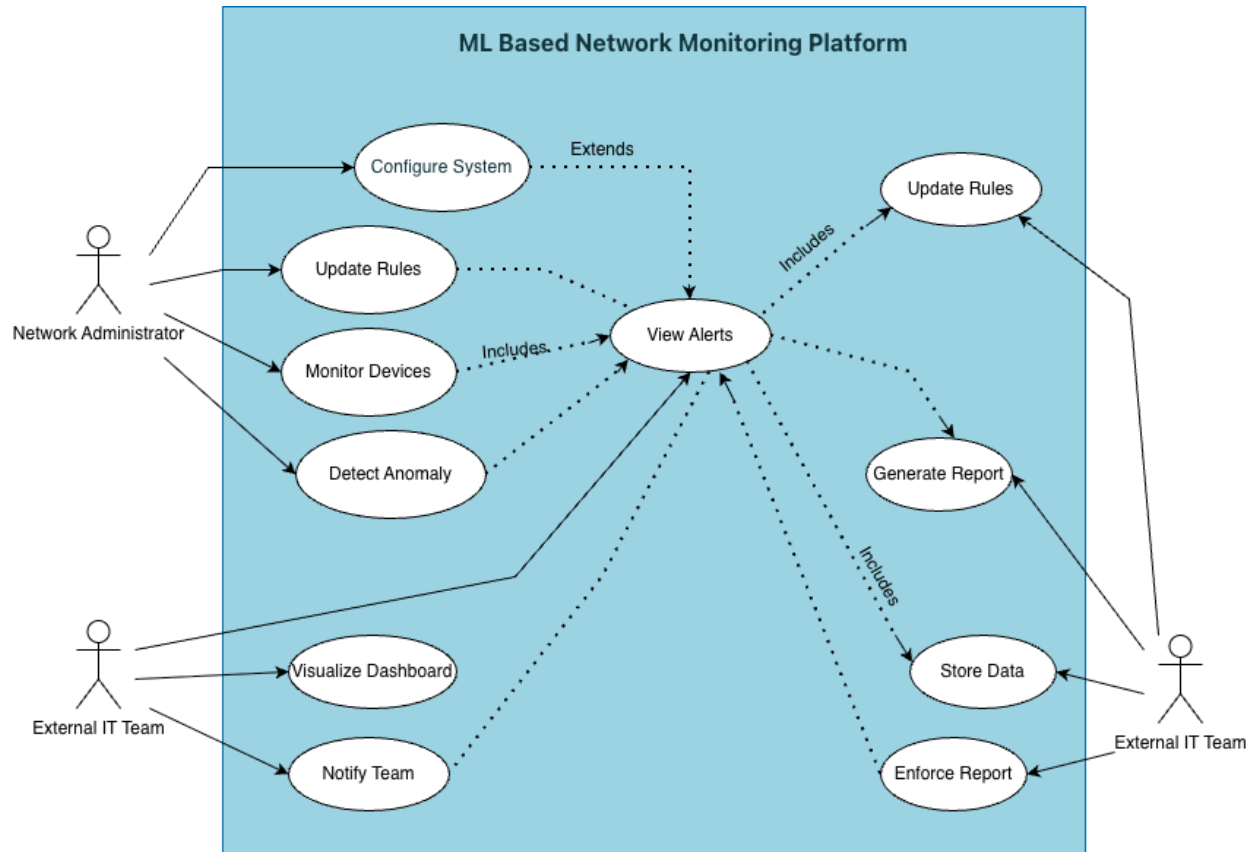


Figure 1: Use Case Diagram

ML – Based Network Monitoring System

○ Data Flow Diagram:

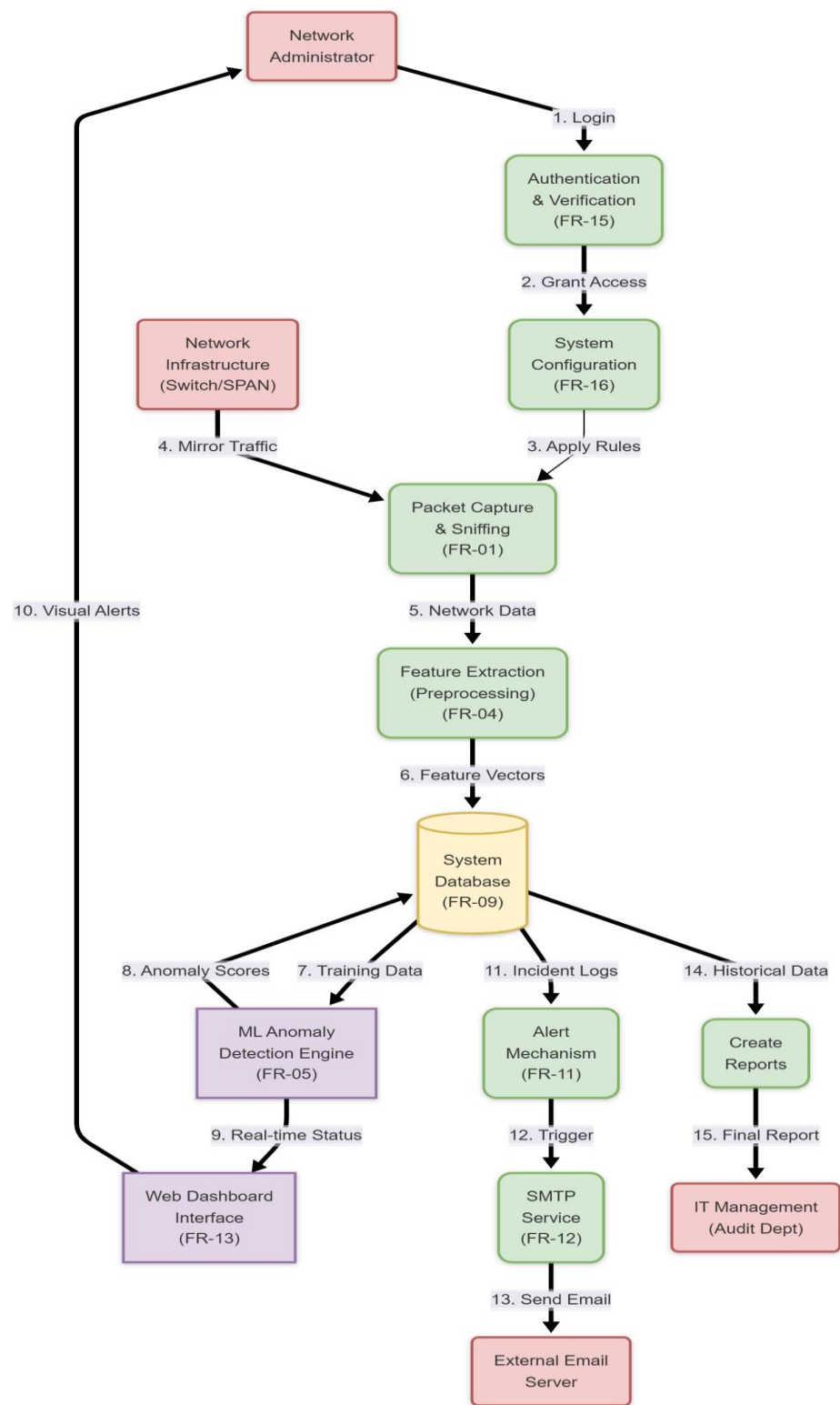


Figure 2: Data Flow Diagram

ML – Based Network Monitoring System

○ Development View

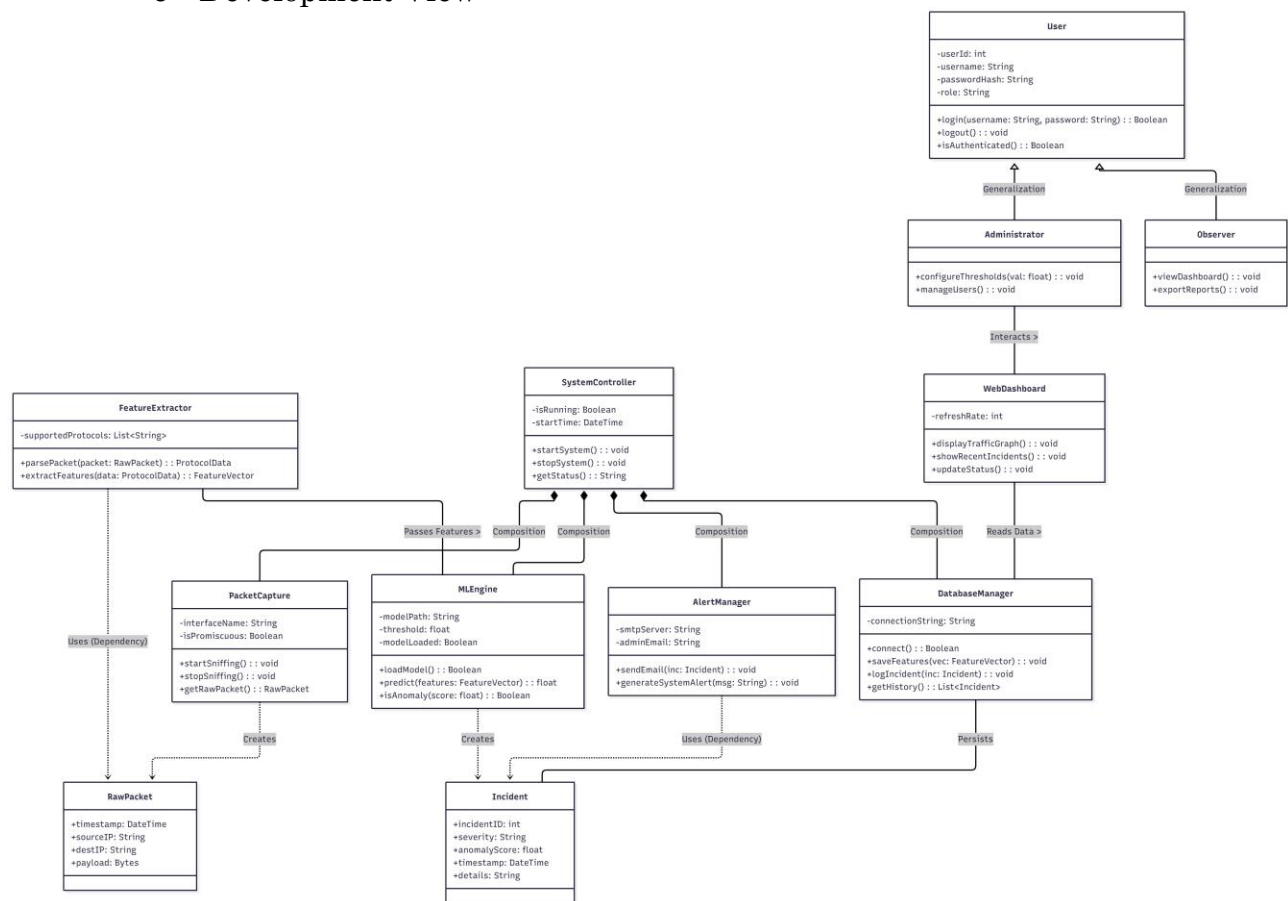


Figure 3: Development View Diagram

ML – Based Network Monitoring System

○ Process View

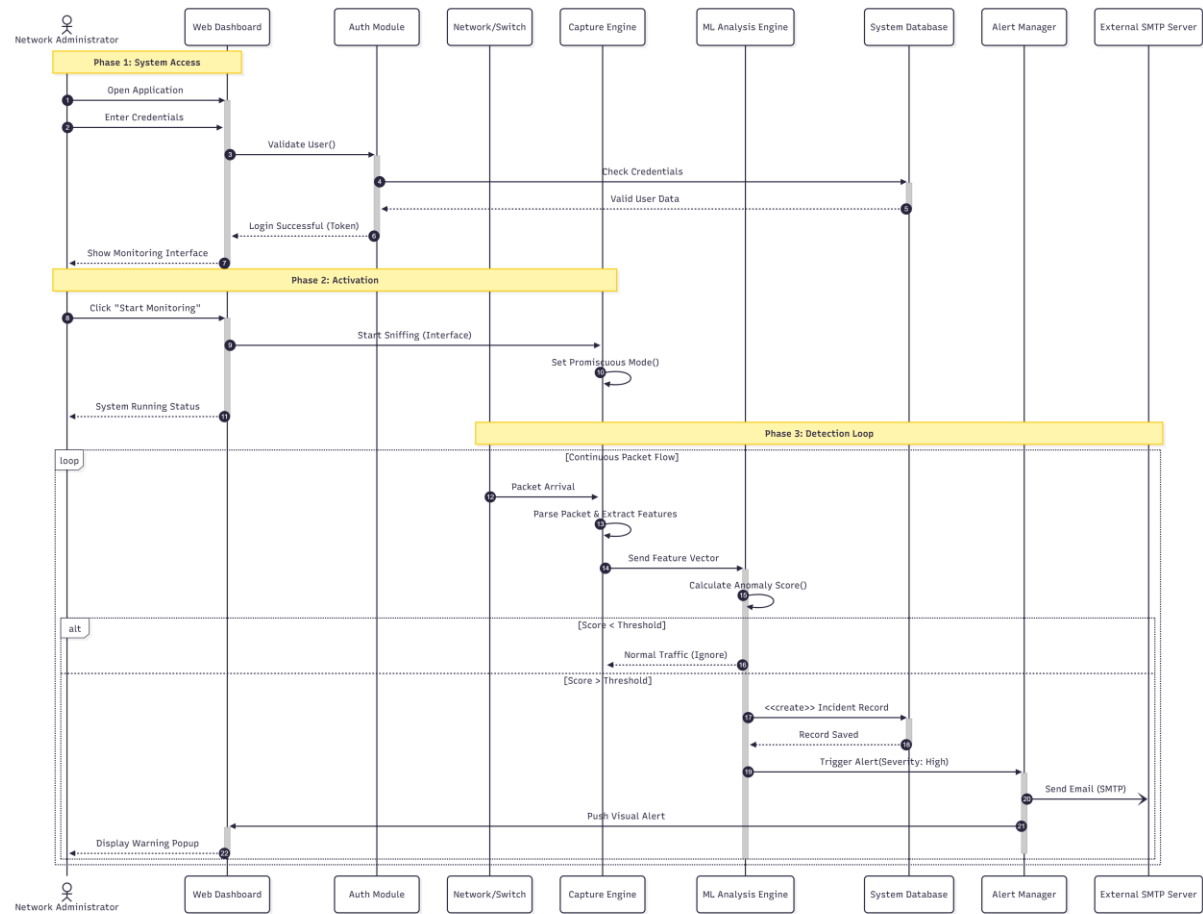
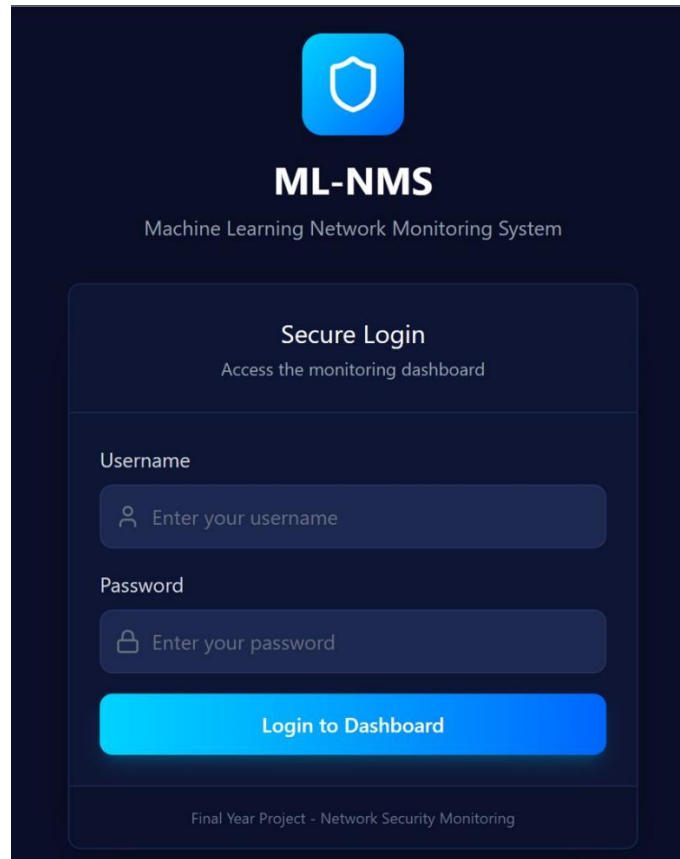


Figure 4: Process View Diagram

ML – Based Network Monitoring System

- User Interface Design



The image shows a login interface for a system called ML-NMS. At the top, there is a blue shield icon with a white outline. Below it, the text "ML-NMS" is displayed in a large, bold, white font, followed by "Machine Learning Network Monitoring System" in a smaller, lighter blue font. The main section is titled "Secure Login" in white, with the subtitle "Access the monitoring dashboard" in a lighter blue font. Below this, there are two input fields: "Username" and "Password". The "Username" field has a placeholder text "Enter your username" and a small user icon. The "Password" field has a placeholder text "Enter your password" and a small lock icon. Below these fields is a large, bright blue button with the text "Login to Dashboard" in white. At the bottom of the interface, there is a small line of text: "Final Year Project - Network Security Monitoring".

Figure 5: Dashboard Login Interface

ML – Based Network Monitoring System

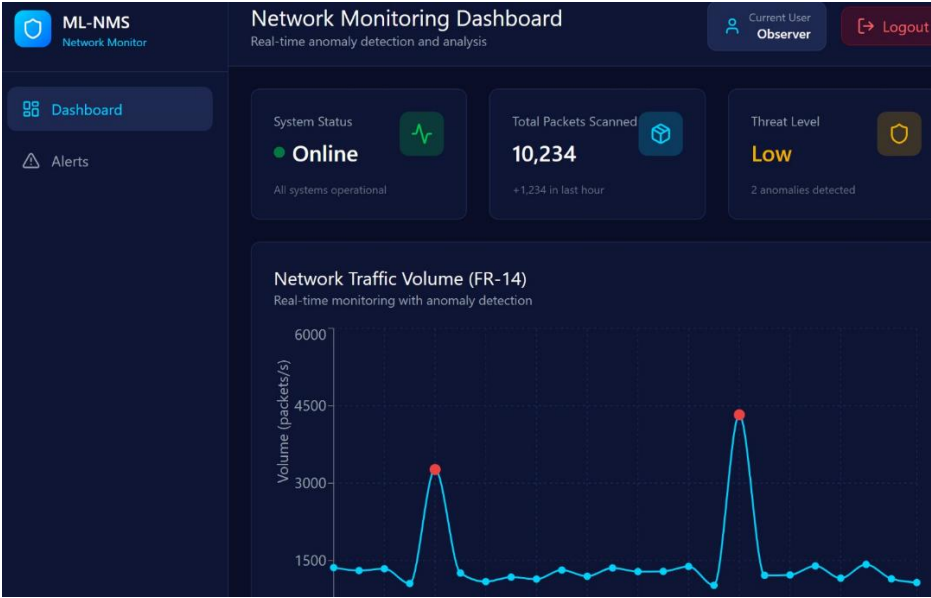


Figure 6: ML-NMS Dashboard Interface

Recent Network Incidents (FR-10)					
Anomaly detection alerts and events					
Timestamp	Source IP	Destination IP	Protocol	Anomaly Score	Severity
2025-11-19 10:00:23	192.168.1.50	8.8.8.8	TCP	0.95	Critical
2025-11-19 09:45:12	10.0.0.15	1.1.1.1	UDP	0.87	Critical
2025-11-19 09:30:45	192.168.1.100	192.168.1.1	TCP	0.45	Medium
2025-11-19 09:15:33	172.16.0.50	185.125.190.36	ICMP	0.23	Medium
2025-11-19 09:00:18	192.168.1.75	208.67.222.222	UDP	0.12	Low
2025-11-19 08:45:05	10.0.0.25	216.58.214.206	TCP	-0.15	Low
Showing 6 recent incidents					Critical Alerts: 2

Figure 7: ML -NMS Recent Incident Interface