COMSATS University Islamabad,
Abbottabad Campus

Business Process Engineering

Assignment # 2

Submitted By:	**Nayab Zahra**	**SP22-BSE-083**
	Syeda Sumayya	**SP22-BSE-100**
	Zarmeena Khan	**SP22-BSE-111**
	Safihullah	**SP22-BSE-090**

Section: **BSE-8C**
Date: **October 24, 2025**
Submitted to **Sir Mukhtiar Zamin**

DESIGNATION PHASE:

In our final year project following are the core business processes:

Our final year project is:

AI- Powered Emergency Response System for Threat

List of Business Processes

- User Management & Authentication
- Data Collection & Preparation
- Model Training & Validation
- Model Deployment & Integration
- Real-Time Threat Detection
- Manual Emergency Trigger
- Alert & Notification Management
- Location Tracking & High-Risk Zone
- Incident Logging & Analytics
- Admin Dashboard & Operations Monitoring
- API Gateway & Microservices Orchestration
- Offline-First / GSM SMS Fallback
- Testing, QA & Performance Monitoring
- Security & Privacy
- Maintenance & Continuous Model Improvement

Process	Overview (As per your project)
1. User Management & Authentication	Handles registration, login, and authentication of users (citizens, emergency responders, admin). Uses secure login with encryption to protect personal information.
2. Data Collection & Preparation	Collects user voice data, distress audio samples, and movement patterns. Cleans, labels, and formats this data for model training.
3. Model Training & Validation	Involves training AI models for distress detection using machine learning techniques, validating accuracy, and testing model reliability.

4. Model Deployment & Integration	Deploys the trained AI model into the mobile app and backend system, ensuring smooth integration with other modules like alerting and tracking.
5. Real-Time Threat Detection	Detects distress through voice tone, sound patterns, or sudden movements using real-time audio and sensor inputs. Triggers automated alerts when danger is detected.
6. Manual Emergency Trigger	Allows users to manually press an SOS button or use a keyword to trigger an emergency alert when AI detection is not activated.
7. Alert & Notification Management	Manages the process of sending alerts to emergency contacts, police, or rescue teams via push notifications, SMS, or app alerts.
8. Location Tracking & High-Risk Zone Identification	Tracks the user's GPS location, maps high-risk areas based on previous incidents, and provides early warnings when users enter unsafe zones.
9. Incident Logging & Analytics	Records each incident (time, location, type of distress) and generates analytics for pattern recognition, system improvement, and law enforcement reports.
10. Admin Dashboard & Operations Monitoring	Allows administrators to monitor user activities, view incidents, manage AI model performance, and ensure system uptime.
11. API Gateway & Microservices Orchestration	Coordinates communication between app modules, AI services, and external APIs to ensure scalability and performance.
12. Offline-First / GSM SMS Fallback	Ensures emergency alerts and minimal operations still function without the internet, using GSM or SMS channels for backup.
13. Testing, QA & Performance Monitoring	Includes continuous testing of app features, AI performance, latency, and reliability under various conditions.
14. Security & Privacy	Protects sensitive data (voice, location, user identity) through encryption, secure transmission, and compliance with data privacy policies.
15. Maintenance & Continuous Model Improvement	Focuses on updating AI models with new datasets, fixing bugs, and maintaining system performance and uptime.

16. User Feedback & System Update Cycle	Gathers user feedback after incidents or app usage and uses it to improve UI, AI accuracy, and reliability in updates.
17. Disaster Recovery & Backup Management	Ensures backup of data, system logs, and AI model configurations to recover quickly in case of server failure or cyberattacks.

Process	Clarity	Correctness	Consistency
User Management & Authentication	Clear and easy for end users to understand and use.	Logins and roles correctly defined and secure.	Same authentication logic used across all modules.
Data Collection & Preparation	Well-documented data flow and preprocessing steps.	Correct methods used for labeling and filtering.	Consistent data structure for training and testing.
Model Training & Validation	Clear input/output datasets and evaluation metrics.	Follows correct ML training practices.	Uses same datasets and parameters across sessions.
Model Deployment & Integration	Deployment process clearly defined.	Model integrated with mobile and backend correctly.	Consistent model version control used.
Real-Time Threat Detection	Clear workflow for AI decision-making.	Model correctly classifies distress in real-time.	Same detection logic across all app versions.
Manual Emergency Trigger	Simple and clear SOS trigger mechanism.	Works accurately when activated.	Consistent with alert module.
Alert & Notification Management	Clear hierarchy for sending alerts.	Correct contact and message routing.	Consistent message formats.
Location Tracking & High-Risk Zone	Clear mapping of zones.	Correct GPS integration.	Same tracking module used across all alerts.
Incident Logging & Analytics	Logs are clearly categorized.	Correct data entries and timestamps.	Consistent logging format.

Admin Dashboard & Operations Monitoring	Dashboard layout is intuitive.	Correct metrics displayed.	Consistent UI and real-time updates.
API Gateway & Microservices Orchestration	Clear API documentation.	Correct routing between services.	Consistent API response formats.
Offline-First / GSM SMS Fallback	Process well defined.	Correctly sends alerts via SMS when offline.	Consistent across device types.
Testing, QA & Performance Monitoring	Testing plan clear and continuous.	Test cases executed correctly.	Consistent testing across versions.
Security & Privacy	Security policies clearly documented.	Encryption correctly implemented.	Consistent security across modules.
Maintenance & Continuous Model Improvement	Clear update schedule.	Correct re-training and testing cycles.	Consistent improvements based on feedback.
User Feedback & System Update Cycle	Clear collection channels.	Feedback integrated correctly into updates.	Consistent follow-up improvements.
Disaster Recovery & Backup Management	Clear backup procedures.	Correct data restoration steps.	Consistent daily backup policy.

Process	CMMI Level	Reason
User Management & Authentication	Level 3 (Defined)	Standardized login system with security protocols.
Data Collection & Preparation	Level 2 (Managed)	Managed data gathering and cleaning but semi-automated.
Model Training & Validation	Level 4 (Quantitatively Managed)	Uses measurable AI performance metrics and validation.
Model Deployment & Integration	Level 3 (Defined)	Defined and repeatable deployment steps.

Real-Time Threat Detection	Level 5 (Optimizing)	Continuously improving AI accuracy and adaptability.
Manual Emergency Trigger	Level 2 (Managed)	Function is reliable but basic and user-triggered.
Alert & Notification Management	Level 3 (Defined)	Defined alert protocols with integration.
Location Tracking & High-Risk Zone	Level 4 (Quantitatively Managed)	Uses location data analytics for predictions.
Incident Logging & Analytics	Level 3 (Defined)	Well-documented and standardized data logs.
Admin Dashboard & Operations Monitoring	Level 3 (Defined)	Clearly structured monitoring interface.
API Gateway & Microservices Orchestration	Level 4 (Quantitatively Managed)	Uses scalable and measurable service orchestration.
Offline-First / GSM SMS Fallback	Level 3 (Defined)	Defined fallback plan for network failures.
Testing, QA & Performance Monitoring	Level 4 (Quantitatively Managed)	Data-based testing and performance measurement.
Security & Privacy	Level 4 (Quantitatively Managed)	Security protocols continuously assessed.
Maintenance & Continuous Model Improvement	Level 5 (Optimizing)	Continuous learning and model refinement.
User Feedback & System Update Cycle	Level 3 (Defined)	Standardized collection and improvement cycle.
Disaster Recovery & Backup Management	Level 3 (Defined)	Defined backup and restore processes.

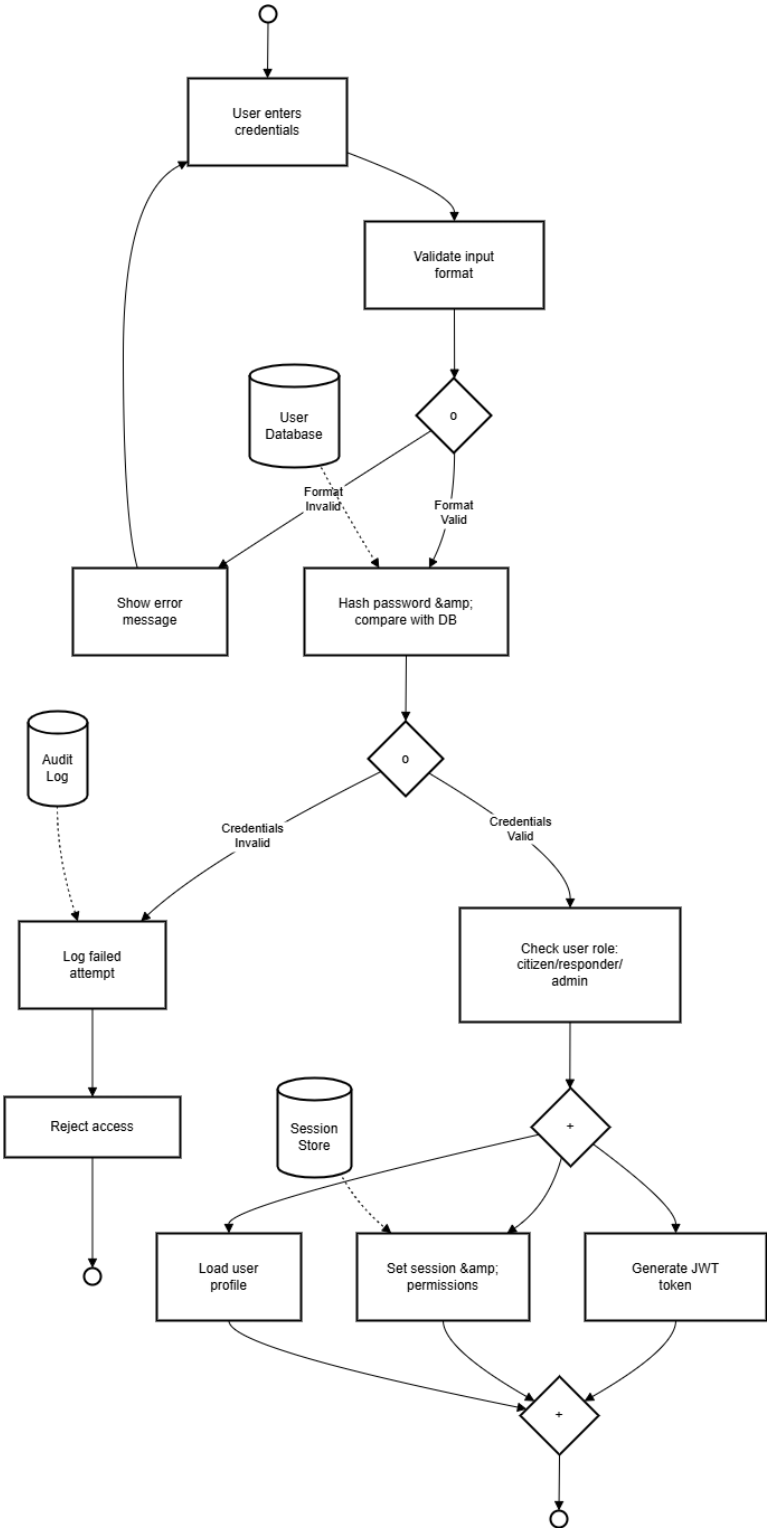
Evaluation Phase:

PROCESS MODELING DONE BY:

Nayab Zahra

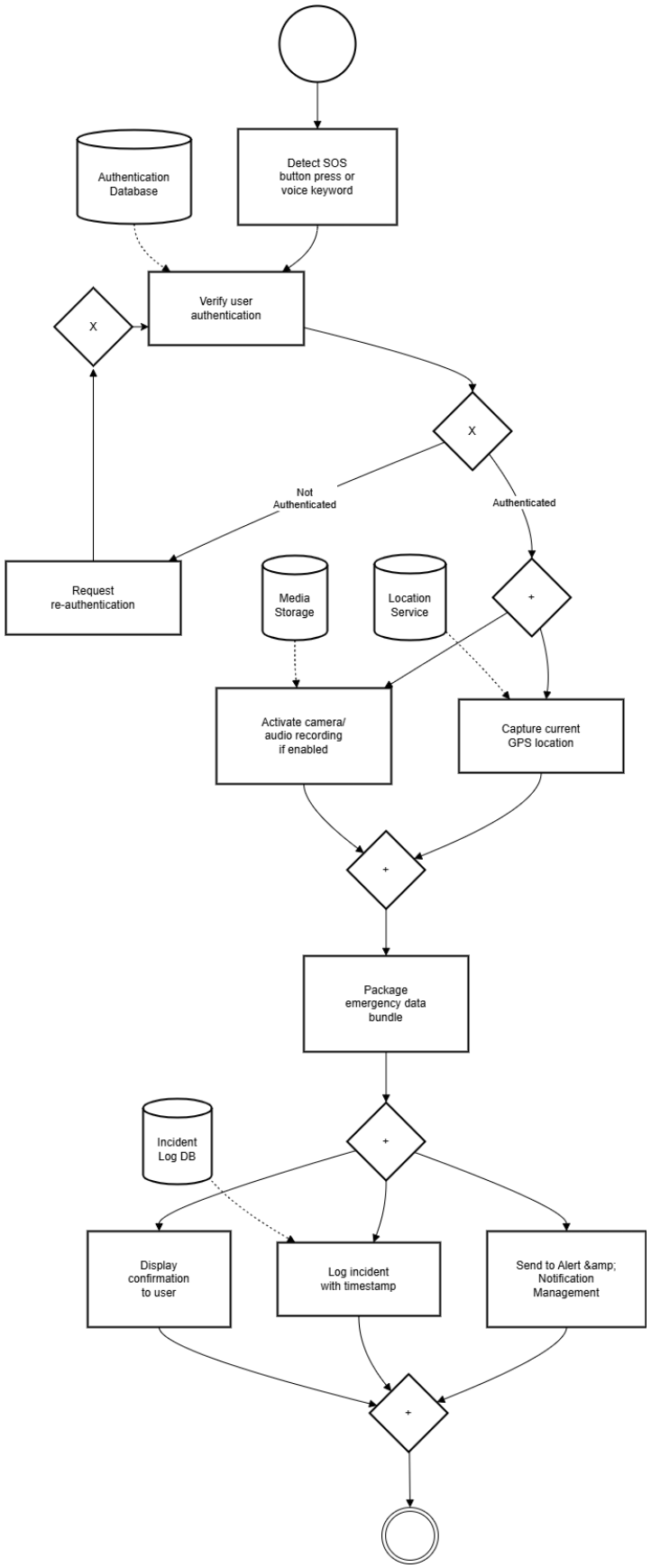
PROCESS 1:

USER MANAGEMENT AND AUTHENTICATION



PROCESS 2:

MANUAL EMERGENCY TRIGGER SYSTEM

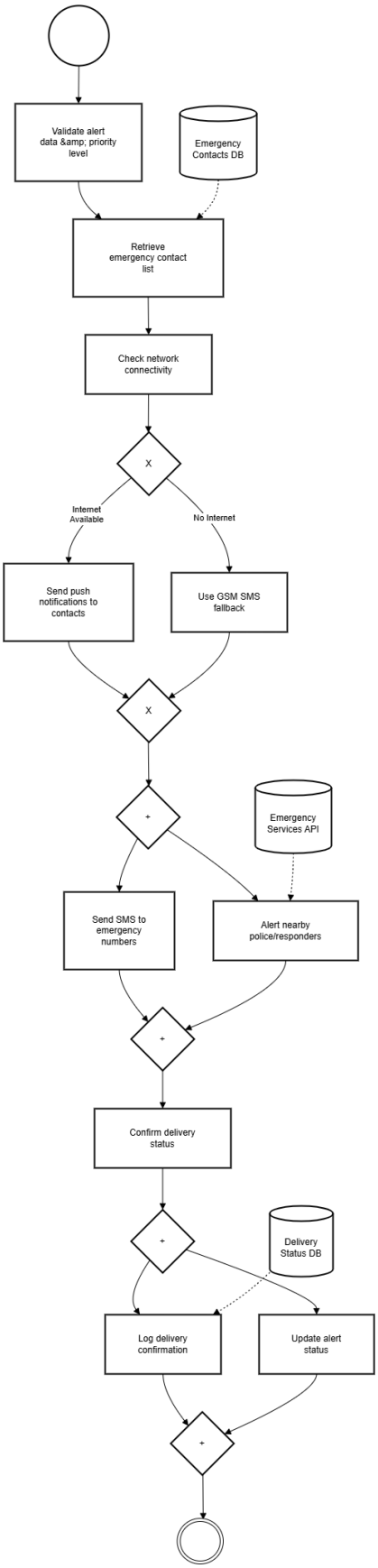


PROCESS MODELING DONE BY:

Safih Ullah

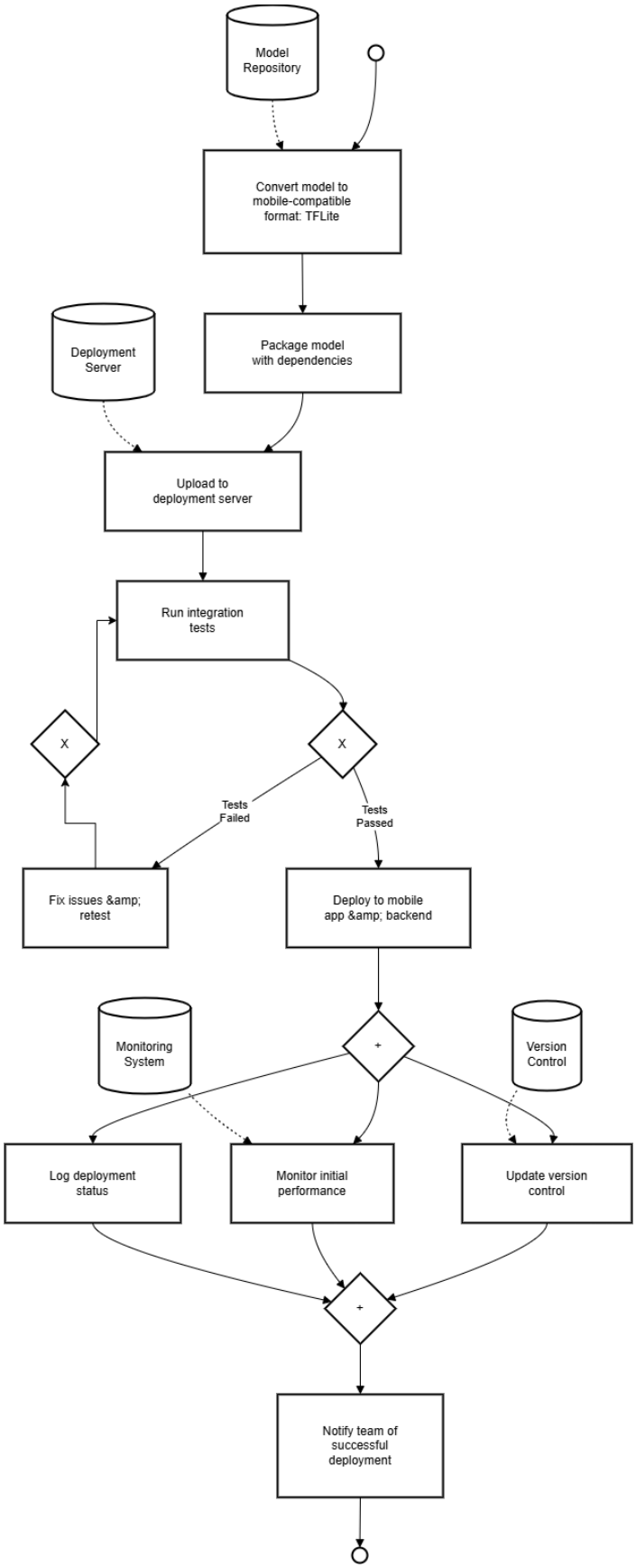
PROCESS 3:

ALERT AND NOTIFICATION SYSTEM



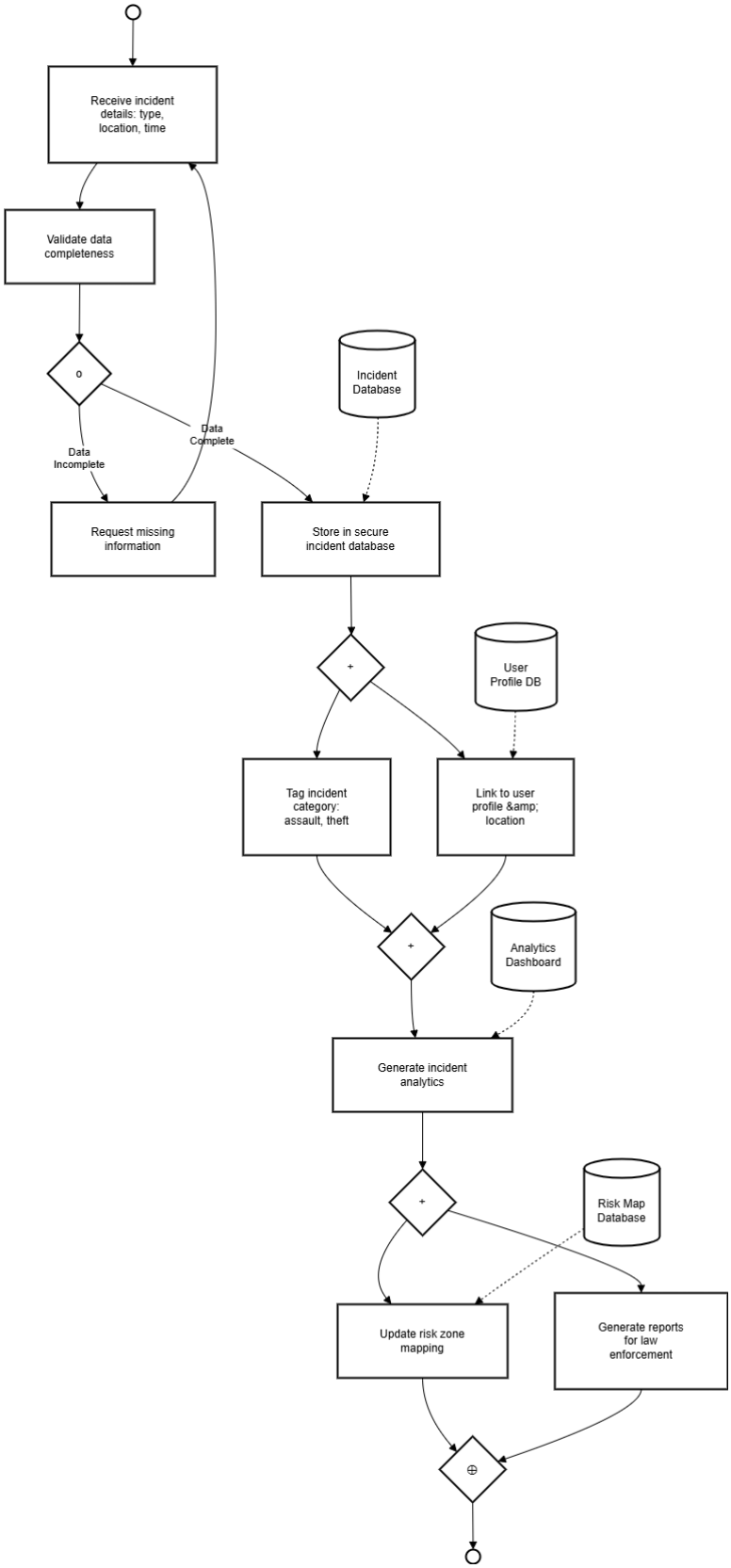
PROCESS 4:

MODEL DEPLOYMENT AND INTEGRATION



PROCESS 5:

INCIDENT LOGGING AND ANALYTICS

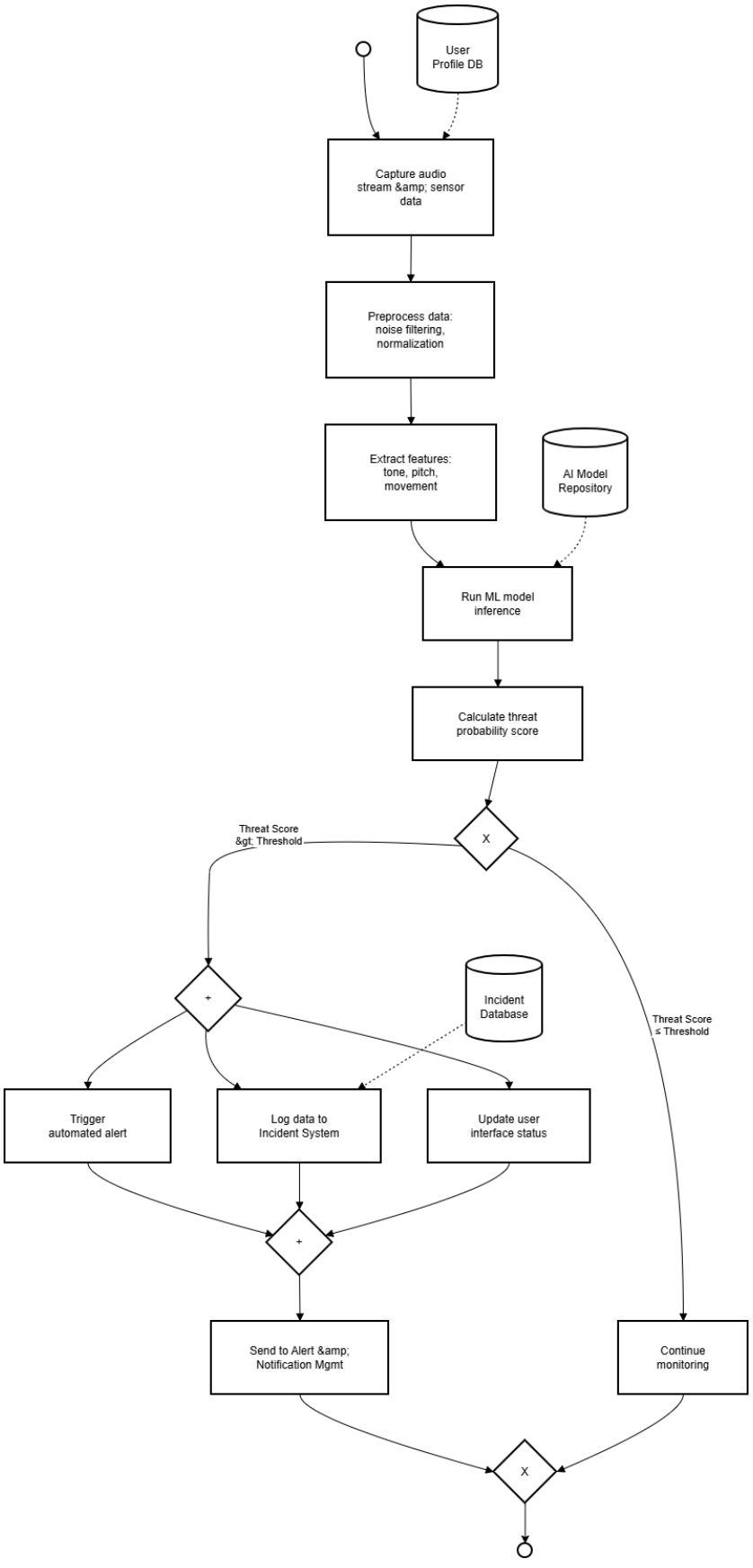


PROCESS MODELING DONE BY:

Zarmeena Khan

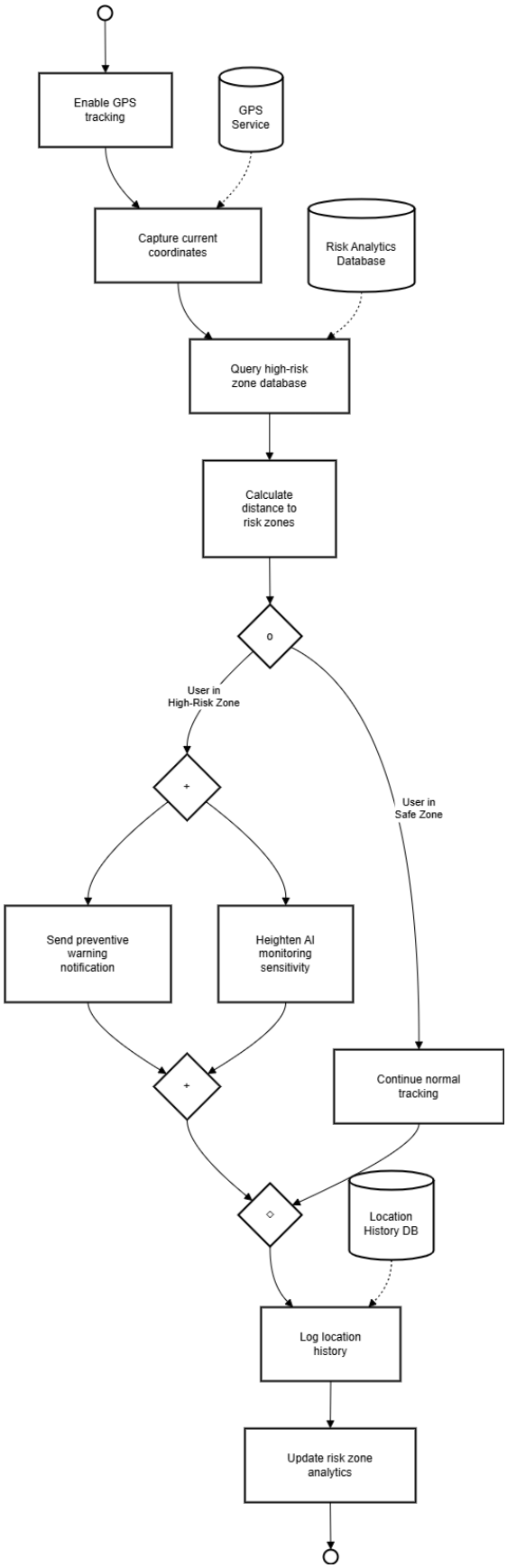
PROCESS 6:

REAL TIME THREAT DETECTION



PROCESS 7:

LOCATION TRACKING AND HIGH-RISK ZONE

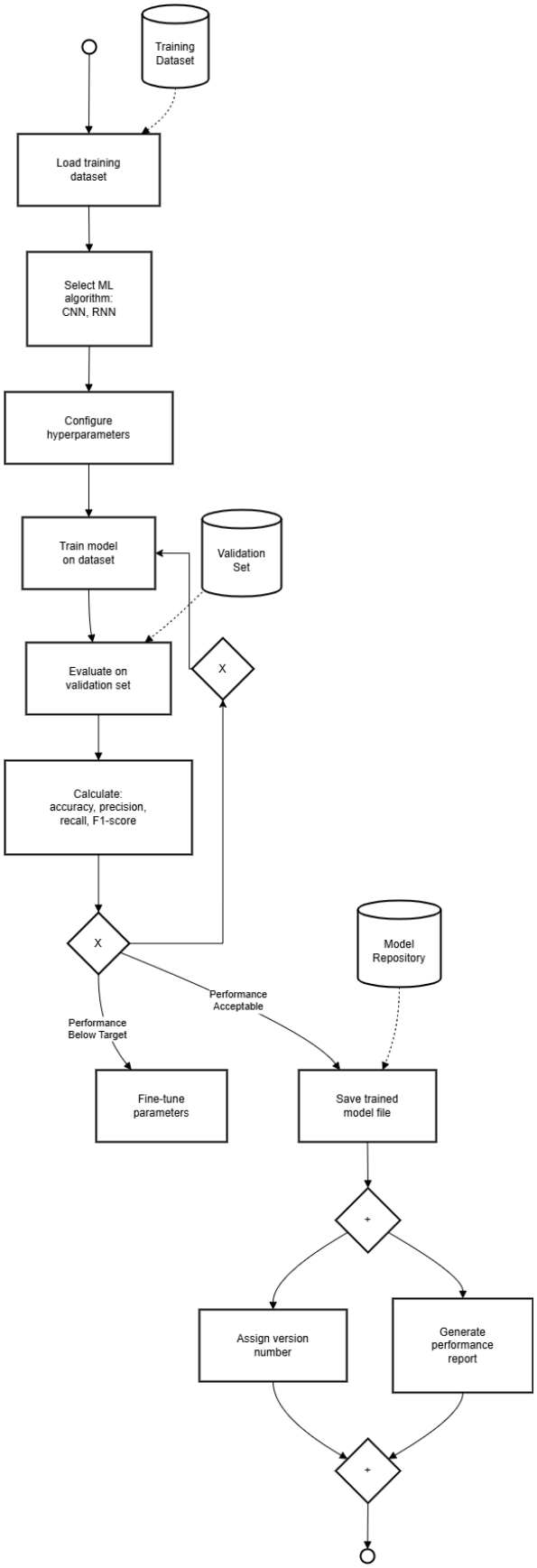


PROCESS MODELING DONE BY:

Syeda Sumayya

PROCESS 8:

MODEL TRAINING AND VALIDATION



PROCESS 9:

DATA COLLECTION AND PREPARATION