International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

AI-Powered Women's Safety Ecosystem with Proactive Risk Analytics

Guided by: **Prof. Vaibhav Ingole .**

Vedant Pise, Samruddhi Aher, Siddharth Salve, Sonal Rathod, Swayam Kawale.

Zeal Polytechnic Pune

Abstract

Women's safety remains a critical issue in India, with NCRB 2024 reporting 4,41,534 crimes against women. Existing safety applications are reactive, requiring the user to press an SOS button after danger has already begun. This paper proposes an AI-Powered Women's Safety Ecosystem that shifts from reactive to proactive safety. The system integrates six core features: Heatmaps (using K-Means Clustering), Risk Scores (using Random Forest), Alternative Routes (using A Algorithm), an AI Chatbot (using Rasa and DistilBERT), Autonomous Detection (using YAMNet and LSTM via TensorFlow Lite), and Evidence Capture (using SHA-256 hashing). By combining location intelligence, machine learning, and on-device AI, the system aims to predict risk before an incident occurs, reduce emergency response times, and provide reliable offline and evidence-capturing capabilities.

I. INTRODUCTION

In 2024, the National Crime Records Bureau (NCRB) recorded 4,41,534 crimes against women in India [1]. Despite the proliferation of mobile safety applications, a 2016 survey found that 72% of users who installed a safety app had never used it [2]. The primary failure of existing systems (like 112 India, Himmat Plus, and bSafe) is that they are **reactive**—they require a user to unlock their phone, open an app, and press a button during a high-stress emergency. Furthermore, these apps often fail in low-network areas and lack predictive capabilities.

This paper introduces an AI-Powered Women's Safety Ecosystem that addresses these limitations. The proposed system uses machine learning to predict risk, on-device AI to detect distress without user input, and offline fallbacks to ensure reliability when networks fail.

II. PROPOSED SYSTEM FEATURES & METHODOLOGY

The system is built around six core features designed to provide proactive and reliable safety.

A. Heatmap (Risk Zones)

The Heatmap visualizes danger zones on a map. Historical crime data (latitude and longitude) is processed using K-Means Clustering to group crimes into "hotspots." These clusters are then color-coded (Red for high risk, Orange for medium, Green for low) and overlaid onto a map using the Google Maps API. This allows users to visually identify areas to avoid.

B. Risk Score

While the Heatmap provides visual context, the Risk Score quantifies danger on a scale of 0 to 100. A Random Forest machine learning model analyzes multiple variables, including historical crime density, time of day, street lighting, and community reports. The model outputs a real-time risk score for a specific location or route, enabling the app to warn users before they enter a high-risk zone.

C. Alternative Routes

Standard navigation apps provide the shortest route, which may pass through dangerous areas. Our system modifies the routing algorithm to prioritize safety. Using the *A (A-Star) Search Algorithm**, the system calculates the "risk weight" of every road segment. It then generates multiple route options:

Safest Route: Avoids all high-risk Red zones.

Crowded Route: Prioritizes populated areas.

Well-Lit Route: Prioritizes main roads with street lighting.

D. AI Chatbot

During an emergency, users may panic and not know what to do. The system includes an AI Chatbot built using the Rasa Framework for intent classification. It guides users step-by-step through first-aid instructions and safety protocols. The chatbot utilizes DistilBERT for Natural Language Understanding (NLU), allowing it to comprehend context and respond in English, Hindi, and Marathi.

E. Autonomous Detection

To eliminate the need for a button press, the system uses on-device AI via TensorFlow Lite:

Audio Detection: The YAMNet model continuously analyzes microphone input in short windows to detect screams or distress sounds. If a scream is detected with >80% confidence, a 10-second cancel window is triggered.

Motion Detection: An LSTM (Long Short-Term Memory) neural network analyzes accelerometer and gyroscope data to detect falls or violent struggles. If no movement is detected after a fall, the SOS sequence is automatically initiated.

F. Evidence Through Voice

When an SOS is triggered (manually or autonomously), the system automatically begins recording audio and video. To ensure the evidence is admissible, the file is hashed using SHA-256 to create a tamper-proof digital fingerprint. The encrypted file is then uploaded to Firebase Storage for secure backup, ensuring a chain of custody.

III. SYSTEM ARCHITECTURE AND PROCESS FLOW

The proposed AI-Powered Women's Safety Ecosystem is designed using a distributed Client-Server architecture. It combines on-device edge computing (for privacy and speed) with cloud-based machine learning (for heavy data processing).

A. System Architecture : The architecture consists of three primary layers:

The Mobile Client (Frontend): Developed using cross-platform frameworks (Flutter/React Native), the client handles the User Interface, GPS tracking, local database storage (SQLite for offline mode), and on-device AI inference via TensorFlow Lite (running the YAMNet and LSTM models for autonomous detection).

The Backend Server: Built using Python and FastAPI, the server hosts the heavy machine learning models. It processes historical crime data using K-Means Clustering to generate Heatmaps and utilizes Random Forest to calculate the Risk Score. It also runs the A* routing algorithm.

External APIs & Databases: The system integrates the Google Maps API for rendering visual maps and routing data, Firebase for secure cloud storage (evidence vault), and an SMS Gateway (Twilio) for offline fallback alerts.

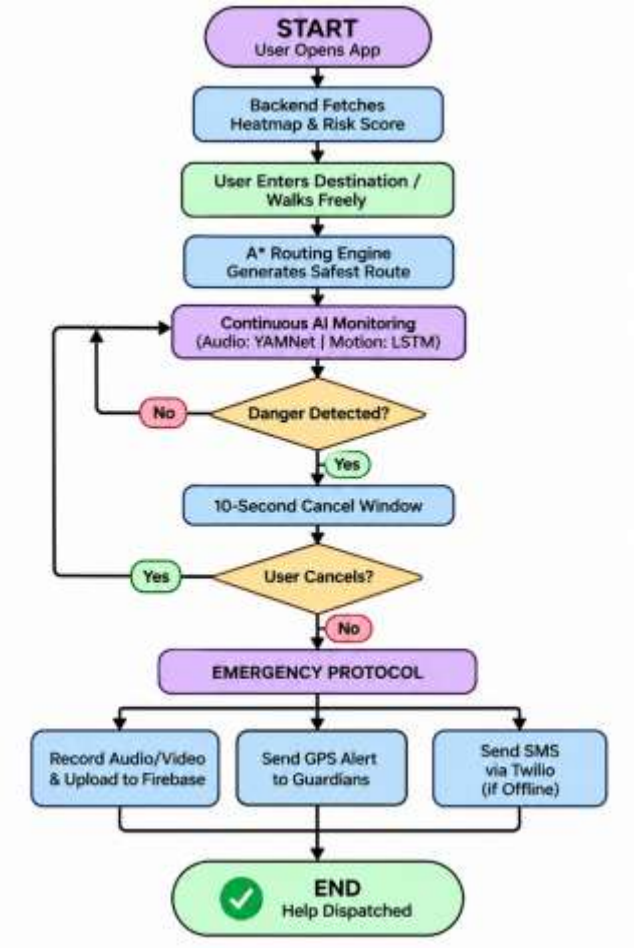
B. Process Flow: The operational flow of the system follows a continuous loop of monitoring, detection, and response:

Initialization & Contextual Awareness: Upon opening the app, the client fetches the user's GPS location and queries the backend for the local Risk Score and Heatmap data. If the user enters a destination, the A* algorithm generates the Safest Route.

Continuous Background Monitoring: While the app is active, the TensorFlow Lite models continuously process microphone input (via YAMNet) and accelerometer data (via LSTM) entirely on the device.

Trigger Mechanism (Manual or Autonomous): An SOS can be triggered manually via a button, or autonomously if YAMNet detects a scream (>80% confidence) or the LSTM detects a fall. Once triggered, a 10-second Cancel Window begins to prevent false alarms.

Alert & Evidence Capture: If not cancelled, the system simultaneously executes three actions: (a) it initiates silent audio/video recording, hashes the file using SHA-256, and uploads it to Firebase; (b) it sends the GPS coordinates to trusted guardians; and (c) if the internet fails, it falls back to SMS alerts.



IV. IMPLEMENTATION & FEASIBILITY

All six features are highly feasible for implementation using open-source technologies. The frontend can be developed using Flutter or React Native, while the backend relies on Python (FastAPI). The AI models (Random Forest, LSTM, YAMNet) are trained offline and converted to TensorFlow Lite for on-device mobile inference, ensuring privacy and low latency. For the Heatmap and Routing features, the Google Maps API provides the necessary spatial data and rendering capabilities.

V. CONCLUSION

The AI-Powered Women's Safety Ecosystem shifts the paradigm from reactive SOS alerts to proactive risk prevention. By integrating K-Means clustering for heatmaps, Random Forest for risk scoring, A* for safe routing, and on-device AI (YAMNet/LSTM) for autonomous detection, the system provides a comprehensive safety net. Future work will focus on pilot testing the application with college campuses and NGOs to validate the risk scoring accuracy and emergency response times.

ACKNOWLEDGMENT

The authors would like to thank you Zeal Polytechnic for their support and guidance throughout this project.

REFERENCES

[1] National Crime Records Bureau, "Crime in India 2024," Ministry of Home Affairs, New Delhi, 2024.
[2] Red Elephant, "Safety App Survey," New Delhi, 2016.
[3] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73. (Replace with actual research papers you referenced for K-Means, A, YAMNet, etc.)*
[4] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[5] "A Bi-Lingual Counselling Chatbot Application for Support of Gender Based Violence Victims in Kenya," 2024 5th International Conference on..., 2024. (This paper uses the Rasa framework to build a support chatbot for violence victims.)

[6] "A Machine Learning Based Victim's Scream Detection System for Burning Sites Using an Autonomous Embedded System Vehicle," 2021. (This paper uses YAMNet for transfer learning to detect victim screams.)

[7] "An LSTM-Based Approach for Fall Detection Using Accelerometer-Collected Data," 2021. (This paper uses LSTM for smartphone-based fall detection.)

[8] "A Blockchain-based Integrity Layer for Android Forensic Chain-of-Custody Verification," 2026 IEEE International Conference on..., 2026. (This paper uses SHA-256 hashes for mobile forensic chain-of-custody.