The Ambient Guardian: Federated Women's Safety System

Arjun Christopher, Department of Information Technology,
Puducherry Technological University, Puducherry

ABSTRACT

This paper proposes "The Ambient Guardian," an innovative federated learning–powered ecosystem for enhancing women's safety. The system leverages multi-sensor data from smartphones and wearables, privacy-preserving AI to identify emerging threats, and a tiered emergency response framework. In contrast to existing reactive solutions, The Ambient Guardian proactively learns user routines and adapts risk detection to current context, while ensuring that personal data remains local and secure.

General Terms

Women's Safety, Security, Anomaly Detection, Smart Wearables

Keywords

Women safety, federated learning, context-aware detection, anomaly detection, personal security, TinyML, IoT, wearable devices.

1. INTRODUCTION

Enhancing women's safety remains a critical challenge that requires both technical innovation and privacy-sensitive design. Traditional mobile panic alerts, sound-based triggers, and GPS tracking are either reactive or intrusive and risk exposing sensitive data if improperly designed. This work introduces The Ambient Guardian, a privacy-first, federated learning–powered multi-device ecosystem. This approach moves beyond the limitations of purely hardware- or cloud-centric solutions by maintaining data on-user devices, learning individual behavioral patterns locally, and only sharing encrypted, aggregated model updates. It autonomously detects potential threats using a fusion of wearable sensor data, contextual information, and crowdsourced risk intelligence, providing a personalized, real-time defense against personal safety threats.

2. LITERATURE SURVEY

Multiple efforts address women's safety using a range of mobile, IoT, and AI technologies:

[1] Women Safety App To Detect Danger And Prevent Automatically Using Machine Learning: Proposes audio anomaly detection using mobile microphones, ML-based triggering of emergency alerts, GPS location sharing, and cloud storage for evidence. Limitation: Over-reliance on assumed "threat" sounds and central cloud privacy risks.

[2] Real-Time Threat Detection for Women: Introduces a standalone IoT-based device utilizing PIR, sound sensors, and GSM/GPS modules for immediate alerts. Limitation: Environmental noise leads to false positives; system lacks adaptability and user personalization.

[3] Smart Safety Wearable: Leveraging IoT and GPS for Women's Security: Highlights use of panic buttons, wearables with GSM and GPS, and audible alarms. Limitation: Reactive systems requiring user intervention; lack of data integration; restricted hardware focus.

[4] Implementation of Safe Route Advisor System Using Machine Learning: Uses K-means clustering on crime data for route safety, but is limited by static data, missing real-time or user-driven updates.

[5] Maximizing Women's Safety with an Effective System: Provides app-based panic buttons, geofencing alerts, and helpline integration but is purely reactive and dependent on one-tier escalation.

Common Drawbacks:
Reactive only systems, use of static data, oversimplified triggers, lack of personalization, significant privacy risks from centralized data, and absence of scalable escalation protocols.

3. PROPOSED SYSTEM

3.1 Overview

The Ambient Guardian is a federated, context-aware, multi-sensor safety system that combines the benefits of on-device intelligence and distributed, privacy-respecting learning.

3.2 Key Features

Multi-Sensor Wearable Data

- Integrates data from **smartwatches** such as heart rate, SpO_2, respiration, motion, and sweat sensors for comprehensive **distress signal detection**.
- Fuses physiological and environmental data for high reliability.

TinyML Anomaly Detection

- Employs **on-device machine learning (TinyML)** to identify distress patterns and anomalies locally, ensuring real-time, low-latency analysis.
- Enhances user privacy by processing sensitive information directly on devices.

Adaptive User Profiling

- Learns unique user **routines and behavioral baselines**, automatically adjusting thresholds for what constitutes a potential threat.
- Delivers **personalized safety** that adapts to changing daily habits and geography.

Smart Route Learning

- Automatically learns daily safe paths and monitors for unusual deviations to flag them as **potential safety concerns**.
- Suggests **dynamic route recommendations** based on live crime data, environmental factors, and user-defined safe zones.

Tiered Response Protocol

- Activates a **multi-stage emergency response**: user notification, SOS escalation, automated bot calls, and direct emergency service alerts.
- Ensures that if the initial tier fails (e.g., no response from trusted contacts), the protocol escalates up to contacting authorities.

Multi-Source Video Evidence

- Captures and compiles crucial **video and audio evidence** from multiple sources (CCTV, dashcams, Bluetooth cameras, smartphone microphones) during an incident.
- Ensures robust incident documentation for investigation or legal action.

Low-Power Safeguard

- When **device battery is critically low**, prioritizes sending last known location and uploading critical media to designated contacts and cloud storage.
- Maintains essential safety features even under battery constraints.

Secure Cloud Storage

- All collected safety evidence (audio, video, sensor data) is **securely uploaded to Google Drive or end-to-end encrypted cloud** storage.
- Ensures both accessibility to relevant contacts and forensic reliability.

Voice-Activated and Manual SOS Alert

- **Voice-Activated SOS**: Users can trigger an immediate SOS alert using predefined voice commands, ensuring hands-free activation in distress scenarios.
- **Manual SOS Alert**: Users can also initiate alerts via a dedicated panic button or app interface, providing a direct, reliable option if voice activation is not feasible.

Context-Aware Safe Navigation

- Offers **dynamic, context-aware navigation** recommendations factoring in crime zones, time of day, crowd density, and user routine anomalies.
- Continuously updates risk scoring by integrating open datasets, user safety pins, and environmental context.

Privacy-Preserving Intelligence

- Powered by **Federated Learning**, ensuring sensitive data and behavioral patterns **never leave the device**—only encrypted, aggregated model updates are shared for global improvement.
- Strictly aligned with privacy-by-design principles.

3.3 System Architecture

- **Data collection:** Wearable and mobile sensors collect physiological and environmental signals.
- **On-device processing:** TinyML models process data for distress and context anomalies.
- **Secure aggregation:** Federated Learning ensures only non-identifiable updates are aggregated in the cloud.
- **Feedback cycle:** Improved models are redistributed, adapting to new risks and user patterns.
- **Emergency workflow:** Multi-stage notification from local alerts to automated authority calls and cloud evidence backup.

4. METHODOLOGY

4.1 Federated Learning Process

1. **Global Model Distribution:** Central server dispatches baseline model to user devices.
2. **Local Training:** Devices refine model using private, local data.
3. **Secure Submission:** Only encrypted gradient/model updates returned to server.
4. **Aggregation:** Server combines updates to improve global model.
5. **Redistribution:** Enhanced model shared with all devices for ongoing learning.

4.2 Data Processing and Anomaly Detection

- **Audio processing:** Spectrogram-based detection of shouting/screaming using TensorFlow Lite.

- **Sensor fusion:** Combining motion, heart rate, SpO_2, and geo-data for context-aware analysis.
- **Smart Route and Safe Navigation Learning:** Employs **K-means clustering** to classify geographic locations as "safe" or "unsafe" by analyzing historical crime densities, allowing computation of a safety index for any candidate route. Integrates **DBSCAN** to perform density-based analysis of both historical and live event data, and learns user's daily paths, enabling real-time detection of evolving crime hotspots or anomalies. This method dynamically updates safe navigation paths, recommending detours around newly identified high-risk zones. The combination of these clustering methods ensures the system provides **robust, up-to-date route recommendations** across varying urban contexts for proactive women's safety.
- **Personalization:** Routine learning triggers alerts on deviations which are contextually abnormal for the particular user.

5. SYSTEM ARCHITECTURE

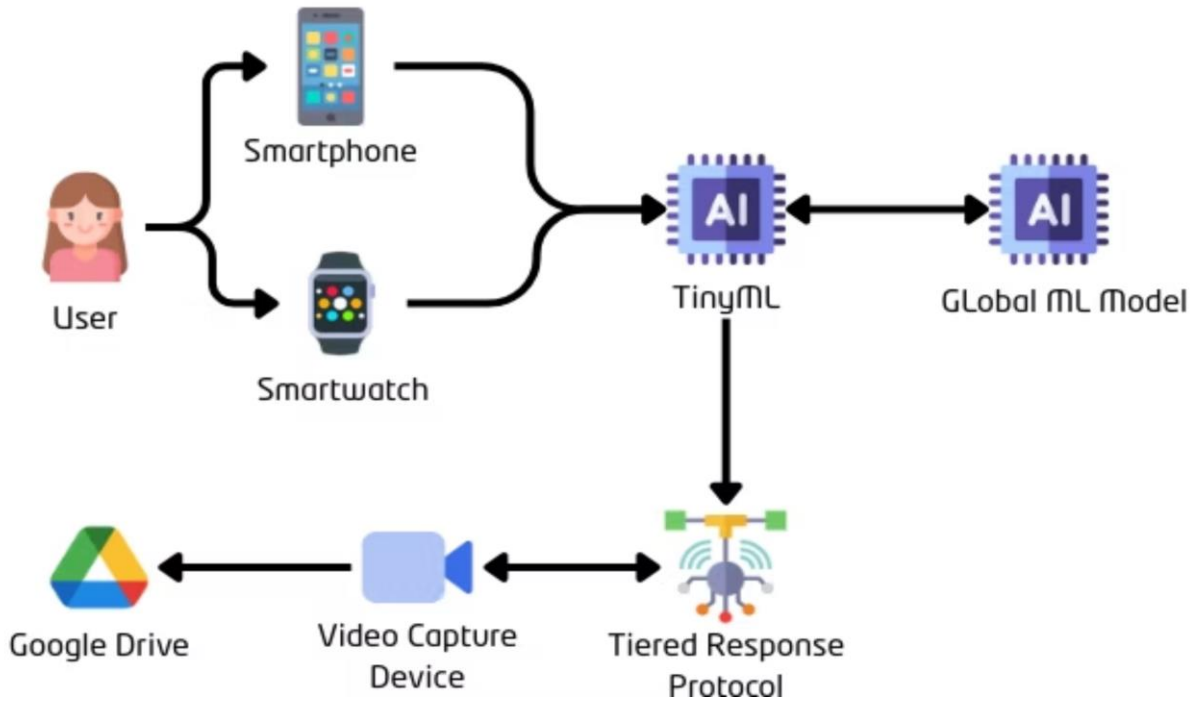

Figure 1. Proposed System Architecture

6. SYSTEM WORKFLOW

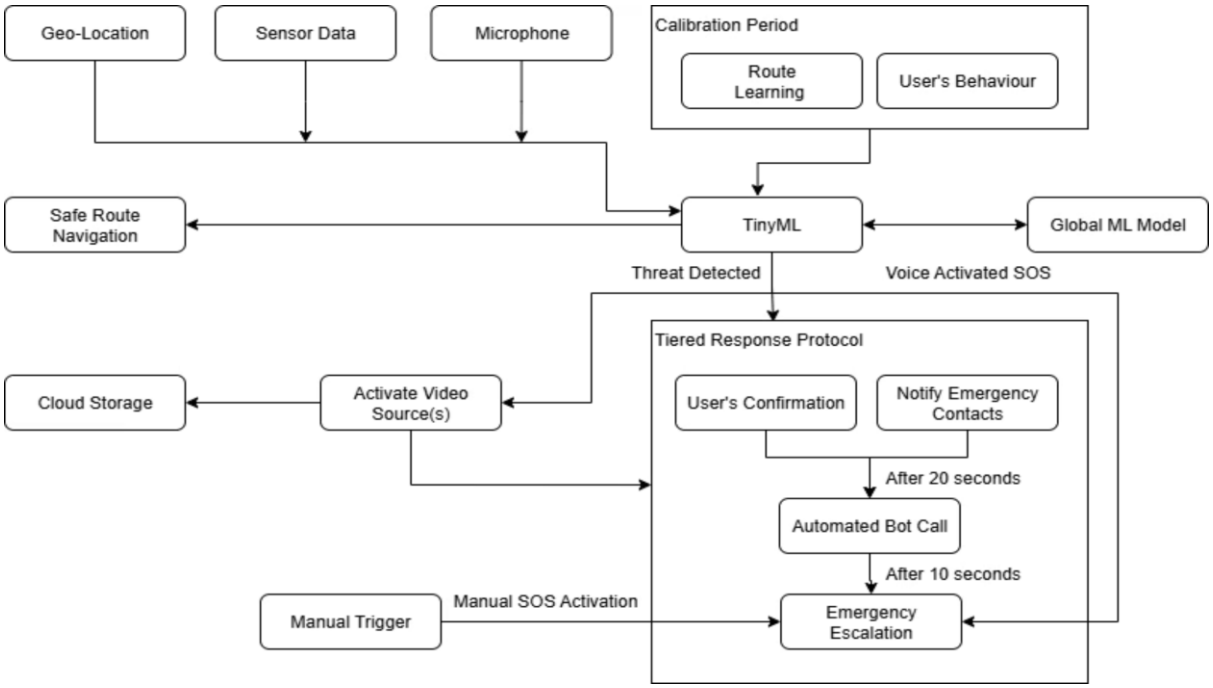

Figure 2. System Workflow

7. RESULTS AND DISCUSSION

7.1 Outcomes

- **Accurate Automated Detection:** Detects distress signals while reducing false alarms via multi-modal fusion and personalized baselines.
- **Robust Evidence Submission:** Seamless, secure upload of audio/video/location even in low-power mode.
- **Tiered Response:** Reliable escalation from user notification to authority interventions.
- **Dynamic Safe Routes:** Routinely updated, context-aware travel recommendations.

7.2 Comparative Advantages

Feature	Prev. Systems	Ambient Guardian
Threat Detection	Manual/audio/motion	Multi-sensor fusion, TinyML
Privacy	Cloud-based	Fully on-device, federated
Personalization	Generic	Routine/adaptive learning
Emergency Escalation	One-tier only	Multi-step protocol

Evidence Collection	Audio/Geo only	Audio, video, wearable, CCTV
Scalability	Hardware dependent	Ubiquitous devices + wearables

8. LIMITATIONS AND FUTURE WORK

- **Initial Hardware Learning Curve:** Some sensors may require user adaptation/calibration.
- **Environmental Complexity:** High noise or multi-user scenarios can affect accuracy; further training required.
- **Battery & Wearables:** Integrations pending for ultra-low-power or custom wearable platforms.
- **Live Context Curation:** Extension to incorporate open police or crowd-sourced feeds for real-time risk adjustment.

Future expansions will focus on increasing public dataset integration, more granular threat classification, and broader user testing.

9. CONCLUSION

The Ambient Guardian federated women's safety system demonstrates a significant leap forward in contextual, personalized, and privacy-preserving security. By integrating federated learning with multi-sensor inputs and dynamic response protocols, it overcomes critical weaknesses in current reactive or centralized systems. This approach lays the groundwork for future city-scale deployments where user safety adapts organically to real-world conditions.

REFERENCES

[1] Kopanati Shankar, Siripurapu Chalice Prajwal, Vallem Govardhan Kumar, Penaganti Anusha, Relli Chandra Sekhara Kameswar, Sunkari Bhanu Prakashn, "*Women Safety App To Detect Danger And Prevent Automatically Using Machine Learning*", Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024), July 2024, DOI: 10.2991/978-94-6463-471-6_140

[2] VishnuPriya A V, Deekshi S, Gowthami M, Kanivarshini N, Dharani Priyan E, "*Real-Time Threat Detection for Women*", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, March 2025, DOI: 10.32628/CSEIT25112423

[3] Sangam Swami, Nayaab Pathan, Harshad Bhandare, Sanket Deshmukh, "*Smart Safety Wearable: Leveraging IoT and GPS for Women's Security*", International Journal of Creative Research Thoughts (IJCRT), May 2024, ISSN: 2320-2882

[4] Soham Kudale, Sejal Pangal, Pratap Pawar, Vivek Rane, Prof. Aparna V. Mote, Prof. Nikita Joshi, "*Implementation of Safe Route Advisor System Using Machine Learning",* International Journal of Ingenious Research, Invention and Development (IJIRID), October 2024, DOI: 10.5281/zenodo.14077943

[5] Prof. Amruta B, Prarthan P, Mourya B D, N Shaik Safi, Mohammed Taheer, "*Maximizing Women's Safety with an Effective System*", International Journal of Engineering Research & Technology (IJERT), March 2023, ISSN: 2278-0181