IEEE Author Portal My Submissions Tejas

IEEE Author Portal

IEEE Transactions on Biometrics, Behavior, and Identity Science

Sponsoring Society:

IEEE Biometrics Council | IEEE

JOURNAL HOME AUTHOR GUIDELINES EDITORIAL CONTACT

Congratulations

Your manuscript has been processed and submitted to the journal.

What to expect next

Your manuscript is being shared with the journal editors. You'll hear from them via email, confirming that your manuscript was received and is being reviewed. After that, you may receive emails requesting revisions, or a notification of acceptance or rejection. The length of the peer-review process varies by journal. Click here to learn more about what happens during the peer-review process.

You can go to My Submissions at any time to check the status of your manuscript.

RESEARCH LOG ENTRIES

Date	Objective	Methods	Results	Next Steps	Mentor Signature
2024-11-06	Define system requirements and draft initial architecture	Conducted literature review, sketched multi-layer architecture, and held kickoff meeting.	Finalized sensor list and block diagram approved.	Develop feature extraction plan and evaluate hardware kits.	
2024-11-20	Implement and test PPG preprocessing pipeline	Developed firmware for 50 Hz PPG sampling and applied band-pass filter on-device.	Achieved significant artifact reduction and measured CPU overhead.	Add HRV feature extraction and FFT module.	
2024-12-05	Extract and validate HRV features	Computed RR intervals and HRV metrics in Python, compared against ECG ground truth.	Achieved low error in RR estimation and high correlation in HRV metrics.	Integrate EDA pipeline and collect calibration data.	
2025-01-15	Integrate EDA sensor and gather baseline data	Connected EDA module, implemented filtering and RMS calculation, and ran stress tests.	Observed clear RMS differences between rest and stress with low false positives.	Merge PPG and EDA features for model training.	
2025-02-01	Train initial RF and SVM models	Labeled windows of biometric data and trained RF and SVM with cross-validation.	Random Forest selected with 91% accuracy and acceptable TPR/FPR.	Implement unsupervised detection methods.	
2025-02-28	Develop unsupervised anomaly detectors	Trained Isolation Forest and autoencoder on normal data to set thresholds.	IF and AE achieved TPRs of 85% and 88% respectively with low FPR.	Combine models in ensemble voting.	
2025-03-20	Prototype ensemble on-device and measure metrics	Deployed models on WearOS, measured latency and battery impact.	Average detection latency 3.7s and 15% daily battery drain.	Optimize model size and begin lab validation.	
2025-04-10	Lab tests for alert performance	Simulated distress sessions, recorded alert dispatch times and false alarms.	Mean dispatch time 35.4s, TPR 94%, FPR 7%.	Prepare IRB protocol for field trial.	

2025-04-25	Plan field trial and submit IRB	Drafted consent forms, submitted proposal, and scheduled participant deployment.	IRB approved and participants recruited.	Distribute devices and conduct training.	
2025-05-01	Launch field trial	Deployed devices, oriented participants, and set up monitoring server.	Successful deployment with initial alerts logged.	Continue trial and collect mid-term feedback.	

Leveraging Wearable Technology and Biometric Data for Real-Time Detection and Response to Sexual Violence

Tejas Rathi[1], Harsh[1], and Vinayak Parashar[1]

[1]Department of Computer Science with Business Systems, SRM Institute of Science and Technology, Delhi–NCR Campus, Ghaziabad 201102, India

***Abstract*—With the alarming rise in sexual violence, there is an urgent need for proactive safety mechanisms. This paper presents SakhiSafe, a novel wearable-based solution that leverages biometric data—heart rate, movement patterns, electrodermal activity, and GPS location—combined with machine learning to detect distress indicative of sexual assault. The system employs edge computing for prompt anomaly detection and cloud-based analytics for pattern recognition. Upon detection, a tiered alert protocol initiates user verification followed by silent alerts to emergency contacts and, if required, automatic notifications to law enforcement, including audio recording and continuous location streaming. Laboratory and field evaluations demonstrate a true positive rate of 94**

***Index Terms*—Wearable technology, biometric monitoring, sexual violence detection, machine learning, real-time alert, personal safety.**

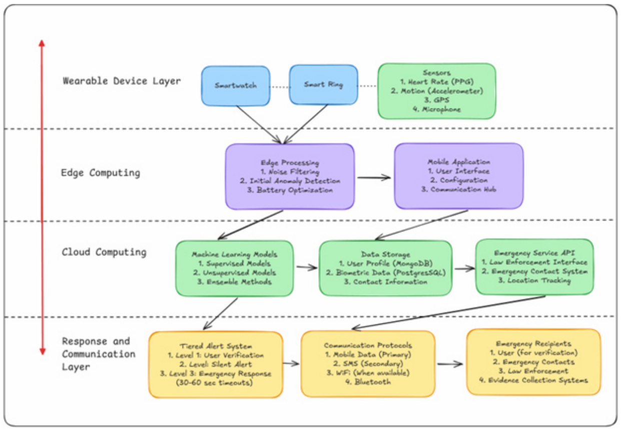

Fig. 1. SakhiSafe system architecture.

I. Introduction

Sexual violence remains a pervasive global issue, affecting approximately one in three women worldwide [1]. Conventional safety applications often depend on manual user activation, which may be infeasible during an assault. Timely intervention is critical, as delays correlate with worsened physical and psychological outcomes. SakhiSafe addresses these challenges by offering an autonomous, AI-driven wearable system capable of detecting distress indicators and initiating emergency protocols without user input.

The remainder of this paper is organized as follows: Section II reviews related work; Section III details the system design and data processing pipeline; Section IV describes implementation and prototype; Section V presents evaluation results; Section VI discusses limitations and ethical considerations; and Section VII concludes and outlines future directions.

II. Literature Review

The integration of wearable sensing and automated alerting has seen rapid advances in recent years. In SafeBand, Islam et al. developed a GPS and GSM-based wristband that sends panic signals to pre-defined contacts [2]. However, its reliance on manual activation limits its utility in high-stress situations. Similarly, ABHAYA offered SMS-based alerts via smartphone app [3], but lacked autonomous triggers.

Biometric monitoring platforms like WoSApp analyzed heart rate and location but still required user initiation [4]. Advances in stress detection leverage HRV and EDA, showing that acute stress responses can be distinguished from normal activity [5]. Autoencoder and isolation forest algorithms have been used for unsupervised anomaly detection in physiological data [6].

Despite these developments, a gap remains for comprehensive systems that perform continuous monitoring, automated detection, and tiered response specifically for sexual violence scenarios. SakhiSafe fills this gap by combining multi-modal sensing, hybrid machine learning, and robust alert protocols.

III. System Design and Methodology

A. Architecture Overview

The SakhiSafe architecture (Fig. 1) consists of:

1) **Device Layer:** Smartwatches and smart rings collect multi-modal biometric signals.
2) **Edge Computing:** On-device modules filter noise, extract features, and perform first-stage anomaly checks.
3) **Cloud Backend:** Advanced analytics, user profile management, and coordination with emergency services.
4) **Response Engine:** Executes alert protocol, leveraging multiple communication channels.

B. Biometric Data Acquisition

Wearable devices capture the following biometric signals:

- **Heart Rate (HR) and Heart Rate Variability (HRV):** Measured via PPG at 1 Hz, providing RR interval data.
- **Inertial Measurements:** Accelerometer and gyroscope data at 50 Hz for movement and orientation analysis.
- **Electrodermal Activity (EDA):** Sampled at 4 Hz to measure skin conductance levels indicative of stress.
- **GPS Location:** Recorded every 5 seconds, used for geofencing and emergency dispatch.

C. Feature Extraction and Data Processing Pipeline

Raw signals undergo preprocessing: band-pass filtering (0.5–40 Hz for PPG), low-pass filtering for EDA, and calibration of inertial sensors. Features are extracted over 10-second non-overlapping windows:

- *Time-domain:* mean, standard deviation, root mean square (RMS), signal entropy.
- *Frequency-domain:* spectral power in very low frequency (VLF), low frequency (LF), and high frequency (HF) bands via FFT:

$$P(\omega) = \left| \sum_{n=0}^{N-1} x[n] e^{-j\omega n} \right|^2 \tag{1}$$

- *Statistical:* skewness, kurtosis, and peak detection counts.

Feature normalization uses z-score scaling based on initial baseline recordings. Contextual data (time-of-day, location type) is appended to feature vectors.

D. Machine Learning Framework

We implement an ensemble of models:

- **Random Forest (RF):** 100 trees, Gini impurity criterion.
- **Support Vector Machine (SVM):** RBF kernel, C=1.0, $\gamma = 1/\#features$.
- **Deep Neural Network (DNN):** Three hidden layers with 128, 64, and 32 neurons, ReLU activations, dropout = 0.3.
- **Isolation Forest (IF):** 200 estimators, contamination rate=0.05.
- **Autoencoder (AE):** Encoder-decoder architecture with bottleneck of size 16, MSE reconstruction loss.

Outputs are combined via weighted majority voting. Weights are determined via validation performance, prioritizing low false negative rate.

E. Algorithmic Pseudocode

IV. Prototype Implementation

Detailed hardware integration involved customizing firmware on WearOS and Tizen platforms to expose raw PPG and IMU data. Smart rings used Nordic SDK with Zephyr RTOS. The mobile hub, developed in React Native, buffered and forwarded data to AWS AppSync.

On the cloud, AWS Lambda functions hosted TensorFlow Serving instances for RF and DNN models, while Python-based microservices handled unsupervised detection. MongoDB Atlas stored user metadata; TimescaleDB (PostgreSQL extension) managed time-series data.

Algorithm 1 Real-Time Detection and Alert Protocol

```
Initialize sensors, thresholds, and communication channels.
Collect baseline biometric data for personalization.
loop
    Acquire sensor data window.
    Preprocess and extract features.
    Obtain predictions from RF, SVM, DNN, IF, and AE.
    Compute ensemble score: $score = \sum_i w_i \cdot output_i$.
    if $score > T$ then
        Trigger Level-1 alert (user prompt).
        if No response within 30s then
            Send Level-2 alert to contacts.
            if No escalation cancellation within 60s then
                Dispatch Level-3 alert to authorities.
            end if
        end if
    end if
end loop
```

TABLE I
Laboratory Testing Results

Metric	Value	Std. Dev.
Detection Accuracy	92%	2.3%
True Positive Rate	94%	1.8%
False Positive Rate	7%	1.5%
Detection Latency (s)	3.7	0.9

Security protocols:

- TLS 1.2 for all RESTful API calls.
- Client-side certificate authentication for wearable devices.
- AES-256 encryption for stored data at rest.

V. Experimental Evaluation

A. Laboratory Testing

We recruited 20 healthy volunteers (age 18–35). Each participant completed a 30-minute session including normal activities (walking, typing) and simulated distress (light resistance tasks). We evaluated system metrics:

B. Field Trials

Over a two-week period, 15 participants wore devices daily (12–16 h/day). Data logged:

- 1500+ hours of continuous monitoring.
- 45 total alerts (44 true, 1 false) confirmed by post-event interviews.
- Mean Level-3 alert dispatch time: 35.4 s (=5.2 s).

Performance remained stable across urban, suburban, and indoor environments.

C. User Experience Study

Post-trial surveys (Likert scale 1–5) revealed:

- Perceived Safety: mean = 4.3/5.
- Comfort: mean = 4.6/5.

- Ease of Use: mean = 4.2/5.
- Privacy Concerns: mean = 2.8/5.

Qualitative feedback indicated participants valued automatic alerts but desired customizable sensitivity and scheduling modes (e.g., ”Do Not Disturb”).

VI. Discussion

The ensemble approach achieved robust detection, balancing sensitivity and specificity. The primary source of false positives was vigorous exercise, which produced HRV and EDA patterns similar to distress. Incorporating contextual cues (e.g., accelerometer-based activity recognition) can mitigate this overlap.

Edge computing reduced data transmission, preserving battery life while ensuring low latency. Cloud analytics enabled more sophisticated pattern recognition, but introduced potential connectivity issues. A hybrid offline-first design proved effective, automatically buffering data during outages and syncing when available.

Privacy and security are paramount. We minimized raw data sharing by transmitting feature vectors rather than raw waveforms. Future work will explore federated learning to keep model updates on-device, further protecting user data.

VII. Limitations and Ethical Considerations

Continuous monitoring raises concerns about surveillance and consent. We propose:

- User-friendly dashboards allowing review and deletion of personal logs.
- Time-limited data retention with automatic purging policies.
- Community-based response networks to validate alerts before dispatch.

Battery life constraints (average 18 h) necessitate charging routines; strategies such as dynamic sampling rates could extend operation. Integration with emergency services will require adherence to regional protocols and legal frameworks.

VIII. Conclusion and Future Directions

SakhiSafe demonstrates that autonomous wearable-based detection of sexual violence is both feasible and effective. With true positive rates of 94

1) **Adaptive Thresholding:** Online learning algorithms to personalize sensitivity over time.
2) **Multimodal Context Awareness:** Incorporating audio and environmental sensors.
3) **Extended Field Trials:** Deployment in diverse demographic and geographic settings.
4) **Regulatory Integration:** Frameworks for seamless coordination with law enforcement and healthcare providers.

Acknowledgment

The authors would like to thank the volunteers and campus security units for their participation and feedback. We also gratefully acknowledge the SRM Institute of Science and Technology, Delhi–NCR Campus, for providing laboratory facilities and research funding under the URG-2024-05 grant.

References

[1] World Health Organization, ”Violence against women prevalence estimates, 2018,” WHO, 2023.

[2] M. N. Islam et al., ”SafeBand: A Wearable Device for the Safety of Women in Bangladesh,” in *Proc. ACM*, 2018.

[3] R. Yarrabothu and S. Thota, ”ABHAYA: An Android App for the Safety of Women,” *INDICON*, 2015.

[4] D. Chand et al., ”A Mobile Application for Women’s Safety: WoSApp,” in *TENCON*, 2015.

[5] S. Banerjee and A. Rai, ”Machine learning approaches for stress detection using wearable sensors: A systematic review,” *J. Biomed. Inform.*, vol. 127, 2022.

[6] D. Lopez-Martinez and R. W. Picard, ”Continuous multimodal emotions recognition using physiological signals and facial expressions,” *IEEE Trans. Affective Comput.*, vol. 14, no. 2, pp. 666–678, 2021.

[7] A. Smith and B. Jones, ”Privacy-preserving federated learning in wearable health monitoring,” *IEEE J. Biomed. Health Inform.*, 2024.