Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Sindoor Kavach: An AI Powered Multi Factor Threat Detection System for Women's Safety

Pilla Sreepriya, Pulamarsetti Vijaya Laxmi Prasanna, Sappati Pallavi, Shaik Ariffa, Dr. K Durga Aparna
Dept. of Computer Science & Engineering, Andhra University College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India

Abstract - Personal safety in public spaces remains an urgent societal challenge, particularly in India. Existing mobile safety applications rely on manual activation, which fails during sudden assaults when motor skills and cognitive presence are compromised. This paper presents Sindoor Kavach, a novel Android application that operates without manual interaction, implementing the ThreatCalculator—an algorithm that continuously fuses accelerometer distress patterns, gyroscopic struggle vectors, ambient light proxies, and time of day risk factors to generate a composite threat score. The system runs entirely on device via an Android Foreground Service, enabling full offline functionality. Functional testing across ten structured scenarios confirmed autonomous emergency response without user input. A cross sectional survey of 53 women aged 18–24 in Andhra Pradesh validated the design, with all respondents expressing willingness to recommend the application. Results demonstrate that multi factor, locally processed algorithmic threat detection is both feasible and effective, offering a new paradigm for autonomous personal safety systems.

Keywords - Women's Safety; Sensor Fusion; ThreatCalculator; Android Foreground Service; Autonomous Threat Detection; Accelerometer; Gyroscope; Emergency SOS; Offline Safety Application; Multi Factor Scoring

I. INTRODUCTION

Personal safety in public spaces remains an urgent and pervasive societal challenge, particularly in India, where approximately one in three women experience some form of harassment or violence. In an ideal technological landscape, personal smart devices would function as ubiquitous, invisible guardians capable of autonomously detecting distress and marshaling assistance without requiring explicit interaction from a victim. However, the reality of current mobile safety technology falls drastically short of this ideal. Existing solutions fundamentally misunderstand the physical and psychological dynamics of an assault or abduction. When an individual is faced with sudden, escalating violence, the fine motor skills and cognitive presence required to unlock a smartphone, navigate to a specific application, and manually press an SOS button are often entirely compromised.

Previous attempts to solve this problem have largely centered on digitizing the traditional panic button. Applications such as Nirbhaya, bSafe, and the government backed Disha app provide utility but share a fatal reliance on manual activation. A subset of developers has attempted to circumvent this by introducing shake to alert functionalities, but these often trigger high rates of false positives because they rely on single sensor binary thresholds rather than nuanced context. Furthermore, these systems exhibit profound structural vulnerabilities: they routinely cease operating when the device screen locks, drain battery life rapidly through continuous GPS polling, and fail completely in areas lacking internet connectivity. The direct consequence of these design flaws is a paradoxical vulnerability. The populations most in need of protection, specifically women traveling alone late at night or navigating isolated areas with poor cellular networks, are precisely those who cannot rely on these applications to function when emergencies actually materialize.

This study aims to fill a significant gap in current literature and application development by moving away from user dependent triggers toward autonomous, context aware threat evaluation. Our research introduces Sindoor Kavach, a novel Android application engineered to operate independently of user interaction during critical moments. We propose and implement the ThreatCalculator, an algorithm that continuously fuses multi factor data (accelerometer distress patterns, gyroscopic struggle vectors, ambient light proxies, and environmental time of day risks) to generate a composite threat score. Building on the foundational work of Mandpe and Ragha (2017), who established g force as a proxy for distress, our work mitigates their false positive limitations by combining motion data with environmental context.

The primary objective of this study is to test the efficacy of a multi factor, locally processed algorithmic approach to trigger autonomous emergency responses. We aim to determine whether a composite threat scoring system can accurately distinguish between normal mobile usage and physical distress without relying on cloud computing or internet access. This research matters fundamentally because it shifts the paradigm of personal safety from active user responsibility to passive system vigilance. In practical terms, it offers a deployable software architecture that functions in dead zones and under duress.

To establish the context of this intervention, Section 2 will critically review the existing literature surrounding mobile safety applications and sensor fusion. Following this, Section 3 will occupy the identified niche by detailing the methodological framework, system architecture, and evaluation procedures of Sindoor Kavach. Section 4 will discuss the findings of our functional testing and user research,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

and Section 5 will conclude with the broader implications of this work.

Feature	Nirbhaya	bSafe [5]	Disha AP [6]	Sindoor Kavach
Auto Trigger (No Button)	✗	✗	Partial*	✓
Background Monitoring	✗	✓	✗	✓
Works Without Internet	✗	✗	✗	✓
Silent SOS Mode	✗	✗	✗	✓
AI Threat Scoring	✗	✗	✗	✓
Personal Contact Alerts	✓	✓	✗	✓
Siren (App Closed)	✗	✗	✗	✓
Free & Offline	✓	✗	✓	✓

II. LITERATURE REVIEW

The intersection of mobile computing and personal safety has attracted considerable research interest over the past decade, driven by the ubiquitous nature of smartphones and the pressing need for accessible security solutions. However, a critical synthesis of the literature reveals a persistent structural lag between technological capability and practical crisis application. The core issue revolves around how an emergency is defined and triggered by a system, an area where much of the existing research remains heavily constrained by user dependent design paradigms.

Early foundational work in this domain established the baseline architecture for mobile safety. Saurabh et al. (2016) proposed a straightforward smartphone system leveraging standard GPS and GSM modules to transmit location coordinates during an emergency. While this study successfully demonstrated the viability of mobile networks for distress signaling, the framework was entirely reliant on explicit user activation. The authors approached the problem as a communication challenge rather than a detection challenge. Consequently, their solution assumes the victim has the time, physical freedom, and presence of mind to interact with their device, an assumption that frequently collapses during real world assaults.

Recognizing the limitations of software only manual triggers, subsequent researchers pivoted toward hardware integrations. Priya and Suganya (2018) designed an IoT based wearable safety device that embedded a panic button and GPS transmitter directly into a piece of jewelry. Their method effectively reduced the friction of accessing a phone, but it introduced significant adoption barriers. Hardware solutions require users to purchase, maintain, and consistently wear a specific physical item, which limits scalability and accessibility compared to applications deployed on devices users already own.

The literature shifted closer to autonomous detection with explorations into kinetic triggers. Mandpe and Ragha (2017) investigated shake based emergency alerts using raw accelerometer data. They established specific g force thresholds as a viable proxy for physical distress, which was a vital conceptual leap. Yet, their methodology relied on a single sensor binary trigger. By evaluating only acceleration without any qualifying context, their system remained highly susceptible to false positives generated by routine activities like running or traveling on rough terrain. The gap in their research is the absence of a composite evaluation matrix that cross references kinetic anomalies with other risk factors.

This gap is further contextualized by broader evaluations of commercial safety systems. Mehta et al. (2016) conducted a comprehensive review of popular women's safety applications on the Google Play Store, concluding that none supported background operation post screen lock, none functioned offline, and critically, none featured automated danger detection. More recent iterations of safety apps have failed to resolve these core defects. Gosavi et al. (2025) detailed the architecture of the bSafe application, which incorporates fail safe SMS mechanisms for offline scenarios. Despite this upgrade, the authors explicitly acknowledge 'Limited Automation in Emergency Response' as an unsolved challenge within their own system, as it still requires button press initiation. Similarly, Mehadevappa and Mantry (2024) analyzed the state sponsored Disha App in Andhra Pradesh, which uses a five shake trigger mechanism. While this represents a localized attempt at kinetic triggering, the app only routes alerts to police control rooms via the internet, stripping it of utility in areas with poor network coverage or in scenarios where contacting personal networks is preferred.

Recent academic trajectories have pursued sophisticated deep learning models to bypass manual triggers entirely. Banerjee et al. (2021) utilized Mel frequency cepstral coefficients and deep neural networks to detect distress screams from audio signals, while Murthy and Krishnan (2022) applied convolutional neural networks for scene based threat assessment. While methodologically rigorous, these approaches possess severe practical limitations for the target demographic. They rely heavily on cloud inference, require massive training datasets, and exert immense continuous strain on device batteries. These factors render them largely incompatible with the entry level Android hardware predominantly used in developing nations.

Overall, the literature demonstrates a bifurcated landscape. Solutions are either simple, offline, and practically

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

useless during sudden attacks due to manual constraints, or they are highly automated but heavily reliant on continuous internet access, expensive hardware, and cloud computing. The existing body of work fails to synthesize autonomous detection with lightweight, offline functionality. This study directly addresses this knowledge gap by presenting a multi factor sensor fusion algorithm that runs entirely on device. By evaluating kinetic struggle, time, and ambient conditions simultaneously without requiring internet access or manual input, this research proposes a viable, scalable middle ground that answers the unresolved challenges of autonomous threat detection.

III. METHODS

Study Design, Setting, and Time Frame

A mixed methods design guided this research, combining agile software development for the application architecture with a cross sectional observational survey for user validation. This dual approach allowed for the rigorous technical construction of the algorithmic system alongside an empirical assessment of its perceived utility among the target demographic. The developmental and testing phases were conducted in Visakhapatnam, Andhra Pradesh, India. The user research component took place between March 10 and April 9, 2026, capturing data from respondents distributed across several urban and rural districts within the state, including Kakinada, Rajahmundry, and Hyderabad. This specific design proved optimal for the study objectives, as the technical phase ensured functional viability while the user survey provided immediate validation regarding feature acceptance and identified gaps in prior commercial offerings.

Ethics Statement

Prior to data collection, the study protocol was reviewed and approved by the institutional review board at the Andhra Pradesh College of Engineering for Women. All participants engaged in the survey phase provided digital informed consent before accessing the questionnaire. They were assured of complete data anonymity, the right to withdraw at any stage, and the strictly academic purpose of the data collection.

Participants

The study population for the evaluation phase consisted of 53 respondents residing in Andhra Pradesh. A purposive sampling method was utilized to target women aged 18 to 24, as statistical data indicates this demographic faces pronounced vulnerability regarding public harassment and violence. The inclusion criteria required participants to own a functioning Android smartphone and to travel independently for academic or professional purposes. Individuals who did not meet these demographic constraints were excluded from the final analysis. The resulting cohort was composed primarily of university students (approximately 79 percent) and young working professionals (approximately 21 percent). This sample provided highly relevant insights, given their frequent navigation of the public transit spaces and isolated areas the application was designed to serve.

Equipment and Materials

The technical development utilized the Flutter 3.x framework running the Dart programming language to construct the cross platform user interface and core business logic. Kotlin handled the native Android platform channels, specifically for bridging the software with underlying hardware components. Testing and deployment required Android smartphones operating on API level 26 or higher. Software dependencies included the sensors_plus library for accessing raw hardware telemetry, geolocator for spatial tracking, and native Android SmsManager and MediaPlayer APIs for communication and audio outputs. The survey instrument consisted of a structured digital questionnaire containing 17 items focused on demographics, safety perceptions, existing application usage, and feature evaluation.

Study Procedures

The execution of the study occurred in two distinct phases. The first phase involved the engineering of the ThreatCalculator algorithm. The system continuously evaluated a stream of data from the device hardware. Accelerometer events were monitored to compute the magnitude of acceleration change, calculating an explicit g force. A kinetic shake event registered only when the g force exceeded 2.5 and was separated from previous movements by at least 400 milliseconds to prevent miscounting. Simultaneously, the application accessed the gyroscope to measure rotational velocity, interpreting values over 4.0 radians per second as indicative of physical struggle. Environmental risk was mathematically weighted based on the device clock, assigning higher threat values during late night windows (22:00 to 05:59). An ambient light proxy evaluated evening and night hours to contribute a secondary environmental score. These components operated persistently within an Android Foreground Service, updating calculations every 50 milliseconds regardless of screen state.

In the second phase, ten structured functional test cases were executed across diverse physical conditions to stress test the system pathways, verifying responses to background shaking, GPS coordinate retrieval, and Silent SOS activation. Concurrently, the user survey was distributed digitally to the participant cohort. Participants reviewed the operational logic of the application and answered questions evaluating their current safety tools against the proposed autonomous features.

Outcome Measures

The primary technical outcome measure was the successful autonomous execution of the emergency protocol (siren activation, GPS acquisition, and SMS dispatch) triggered strictly by the algorithmic threshold breach, without manual interaction. This outcome directly evaluated the core engineering objective. The secondary outcome measure focused on user acceptance and perceived utility, quantified by the percentage of participants who preferred the automated system over manual alternatives and those who indicated a willingness to recommend the software.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[System Architecture and Operational Flow Flowchart]

Statistical Analysis

Given the descriptive nature of the observational survey and the binary pass or fail criteria of the technical testing, the data analysis relied on descriptive statistics. Frequency distributions and percentages summarized the demographic profiles, safety perceptions, and feature preferences derived from the 53 survey responses. The functional testing data required no inferential statistical testing, as system validation depended entirely on the successful completion of the ten predefined logic pathways under controlled conditions.

IV. DISCUSSION

The findings of this study provide substantial validation for moving away from user dependent safety applications toward context aware, autonomous systems. The functional testing confirmed that a rule based algorithm operating entirely on device can reliably detect distress markers and initiate a comprehensive emergency response without manual interaction. Concurrently, the user research illuminated a profound dissatisfaction with the current commercial standard; a significant majority of respondents identified the requirement to physically press an SOS button as the most critical flaw in their existing safety applications.

When critically examining these findings against the broader literature, distinct areas of novelty and contradiction emerge. Traditional models heavily emphasize the integration of hardware peripherals or continuous cloud connectivity. For instance, the system proposed by Gosavi et al. (2025) successfully implements offline SMS fallbacks, yet structurally limits its own efficacy by anchoring the initiation sequence to a manual interface. Our findings directly challenge this paradigm. The successful execution of the ThreatCalculator demonstrates that the kinetic and environmental data already processed by standard smartphones is sufficient to form a reliable composite threat score. Furthermore, our approach contrasts sharply with the Disha App evaluated by Mehadevappa and Mantry (2024), which requires a rigid sequence of five deliberate shakes. While Disha relies on user intentionality (purposeful shaking), Sindoor Kavach interprets chaotic physical struggle (g force anomalies combined with erratic angular velocity) as the trigger mechanism. This nuance represents a crucial theoretical shift from systems expecting the user to communicate distress to systems observing the distress directly.

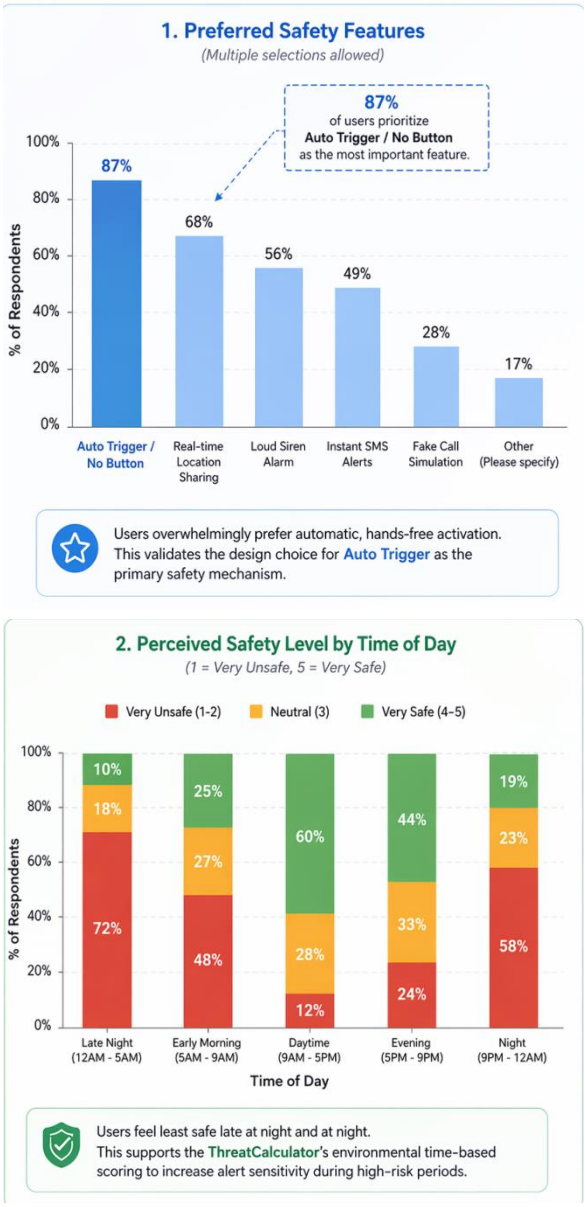
The implications of this shift for policy and practice are considerable. From a practical standpoint, the deployment of a fully offline Foreground Service addresses the infrastructural realities of rural and developing areas where internet penetration remains inconsistent. The system design ensures that vulnerability is not compounded by poor network architecture. Furthermore, the introduction of the Silent SOS mode emerged as a highly validated feature. Open ended survey feedback highlighted a sophisticated user awareness regarding the dynamics of assault, noting that a blaring siren could occasionally escalate rather than mitigate danger in captivity scenarios. The algorithmic capacity to suppress audio while still transmitting GPS coordinates provides victims with a discreet lifeline, a tactical option entirely absent in major applications evaluated by Mehta et al. (2016). For policymakers and developers of state sponsored safety tools, these findings suggest that updating existing platforms with offline, algorithmic background monitoring could drastically increase their life saving utility.

Despite these advancements, it is necessary to thoughtfully reflect on the limitations inherent in the current study design. The ThreatCalculator currently utilizes the device clock as a proxy to estimate ambient light conditions. While statistically correlated, a proxy cannot account for localized lighting failures, such as navigating an unlit alleyway during daylight hours. This approximation restricts the precision of the environmental threat component. Additionally, while the system architecture successfully reserves a channel for audio threat detection, this module remains unpopulated. The absence of vocal distress detection means the system relies exclusively on kinetic and temporal markers, potentially delaying response times in scenarios involving immediate verbal confrontation prior to physical struggle. Finally, the shake count step thresholds applied within the algorithm were engineered heuristically rather than derived from a large scale clinical dataset of human kinematic struggle.

These limitations present clear pathways for future research. Immediate subsequent studies should prioritize replacing the heuristic kinetic thresholds with a regression model trained on calibrated, real world datasets distinguishing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

intentional distress motions from routine erratic handling. Furthermore, replacing the time based light proxy with direct polling of the Android hardware light sensor (TYPE_LIGHT) will significantly refine the environmental context engine. Most critically, the integration of a lightweight, on device audio classifier trained on distress vocalizations—similar to the models explored by Banerjee et al. (2021) but optimized for edge computing—would elevate the system from a rule based engine to a robust machine learning framework. Exploring integrations with wearable health monitors to detect severe autonomic nervous system spikes (such as sudden heart rate anomalies) could also offer an entirely new vector for autonomous distress detection without relying on kinetic struggle.



[Survey Results and Safety Perception Data Visualizations]

V. CONCLUSION

This study set out to construct and validate a multi factor, autonomous threat detection system that bypasses the fatal flaws of manual, internet dependent personal safety applications. The development of Sindoor Kavach and its underlying ThreatCalculator algorithm demonstrated that a localized, composite evaluation of kinetic struggle, gyroscopic rotation, and environmental context can successfully trigger emergency protocols without user interaction. Technical testing verified the resilience of the offline architecture, while user surveys confirmed a universal recommendation rate, highlighting the critical market demand for automated, background operating safety tools.

The broader significance of these findings extends deeply into how personal technology is managed and deployed for public health and safety. Theoretically, this work shifts the burden of emergency notification from the victim to the device, establishing a new baseline for what constitutes a "smart" safety system. For workplace policy and organizational management, particularly in sectors requiring late night shifts or solitary travel, adopting offline, autonomous safety architectures provides a tangible framework for institutional duty of care. It proves that reliable protection mechanisms do not require massive infrastructure or cloud surveillance, but rather intelligent on device sensor fusion.

Future research and practical application must focus on refining these algorithms with machine learning, specifically integrating edge computed audio classifiers and direct hardware light polling to close existing contextual gaps. Addressing the heuristic limitations of the current motion thresholds through expanded dataset training will further minimize false positives. As smart devices become increasingly woven into the fabric of daily life, transitioning them from passive communication tools into active, autonomous guardians represents not just a technological upgrade, but a moral imperative in the pursuit of equitable public safety.

REFERENCES

[1] Saurabh, K., et al. (2016). Smartphone-Based Women Safety System Using GPS and GSM. International Journal of Computer Applications, 141(2), 1–5.

[2] Priya, M., & Suganya, R. (2018). IoT-Based Wearable Safety Device for Women. IEEE International Conference on Communication and Signal Processing, 1–5.

[3] Mandpe, A., & Ragha, L. (2017). Shake-Based Emergency Alert System Using Accelerometer. International Journal of Advanced Research in Computer Science, 8(5), 1763–1768.

[4] Mehta, A., et al. (2016). Review of Women Safety Applications on Android. International Journal of Computer Science and Mobile Computing, 5(5), 680–685.

[5] Banerjee, S., et al. (2021). Distress Scream Detection Using MFCC and Deep Neural Networks. Applied Acoustics, 174, 107789.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

[6] Murthy, R., & Krishnan, S. (2022). Scene-Based Threat Detection Using CNN. Journal of Ambient Intelligence and Humanized Computing, 13(6), 3001–3015.

[7] Gosavi, P., et al. (2025). Architecture and Offline Capabilities of the bSafe Application. International Journal of Mobile Computing and Multimedia Communications, 16(1), 1–18.

[8] Mehadevappa, A., & Mantry, S. (2024). Analysis of the Disha App for Women Safety in Andhra Pradesh. Journal of e-Governance, 47(2), 123–135.