IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 08, November 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.06

Women Safety Application Using One-Touch SOS, Real-Time GPS Alerting, Audio–Video Evidence Capture, and Voice-Based Complaint Filing with Multilingual Support

Dr.Manjushree C V
Associate Professor, Department of Information Science and Engineering
Vemana Institute of Technology, Bangalore, India
manjushree.cv@vemanait.edu.in
https://orcid.org/0009-0002-3099-2437
Meghana T, Pavani Priya, Sushmitha A, Udaya Shree
Department of Information Science and Engineering,
Vemana Institute of Technology, Bangalore, India
meghanat.is2023@vemanait.edu.in, pavanipaiya.is2023@vemanait.edu.in
sushmithaa.is2023@vemanait.edu.in , udayashree.is2023@vemanait.edu.in

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.12/Issue08/NVIS10085
Research Article | Open Access | Double-Blind Peer-Reviewed| Article ID: IJIRAE/RS/Vol.12/Issue08/NVIS10085
Received: 02,October 2026, Revised: 14,October 2026, Accepted: 29,October 2026, Published Online: 25,November 2026 https://www.ijiris.com/volumes/Vol12/iss-08/06.NVIS10085.pdf
ArticleCitation: Dr.Manjushree,Meghana,Pavani,Sushmitha,Udaya(2026),Women Safety Application Using One-Touch SOS, Real-Time GPS Alerting, Audio–Video Evidence Capture, and Voice-Based Complaint Filing with Multilingual Support. IJIRIS: International Journal of Innovative Research in Information Security, Volume 12, Issue 08 of 2026 pages 411-418 https://doi.org/10.26562/ijiris.2026.v1208.06 **BibTeX Key: Dr.Manjushree@2026Women**
IJIRIS papers should be cited as IJIRIS(International Journal of Innovative Research in Information Security, AM Publications, India 2026, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2026.v1208.06 The journal's official abbreviation is IJIRIS. **ORCiD:** https://orcid.org/0009-0004-9398-7488 About the License: Copyright©2026 copyright by the authors. This article is an open access and license under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/)

Abstract: Personal-safety emergencies are time-critical, and a person in danger may be unable to type, unlock a phone, or place a call. A useful safety application must therefore deliver a prompt alert with location, preserve evidence, and state its limits honestly, without presenting an automated alert as a guarantee of rescue. This paper presents Women Safety, a proposed Android-oriented application that combines a one-touch SOS alert with real-time GPS location sharing, automatic audio and video evidence capture, voice-based complaint filing with speech-to-text and multilingual translation, an offline SMS fallback, a safety timer, and a legal-awareness module, organized as a three-tier architecture (presentation, application, database). Voice triggering and an AI/ML distress-detection component are treated as extensions. The paper presents the architecture, methodology, implementation specification, threat model, and evaluation protocol. The available project report contains design descriptions, block diagrams, and a composite illustration of intended screens, but does not provide test counts, device matrices, latency logs, speech-recognition error rates, or user-study data. Accordingly, the results are presented as qualitative observations rather than validated performance claims. The framework establishes a basis for evaluating emergency-alert reliability, evidence capture, and complaint support while making its evidence limitations and safety boundaries explicit.
Index Terms: Women safety, emergency alert system, SOS, GPS tracking, Android application, evidence recording, speech-to-text, multilingual translation, safety timer, privacy

I. INTRODUCTION

Personal-safety applications matter wherever people travel, work, or move through public places and cannot rely on reaching help in time. In many emergencies, the person affected cannot seek immediate help because of fear, lack of communication, or delay in contacting family members and authorities. A Smartphone is almost always within reach, which makes it a practical device for sending an alert, sharing a location, and recording what is happening. Building such an application is different from claiming that it keeps its user safe: an alert that is sent is not an alert that is delivered, and a delivered alert is not help that has arrived. The Women Safety project addresses this distinction through a modular emergency workflow. The proposed system lets a registered user trigger an SOS through an on-screen button and, as extensions, a voice phrase, repeated power-button presses, or an expired safety timer. On a trigger, it captures the device location, starts audio and video recording, retrieves the saved emergency contacts, and sends an alert containing a location link. A separate voice-based complaint feature converts speech to text and can translate it, and a legal-awareness module presents laws, rights, and helpline numbers. A backend and database store users, contacts, alerts, media metadata, and complaints. The central research question is whether these complementary functions can be integrated into a dependable emergency workflow without conflating four different states: an alert triggered on the device, an alert dispatched to the network, an alert delivered to a contact, and an alert acknowledged by a person.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.06

The system therefore treats each of these as a separate status and treats every optional component, such as police integration or AI/ML distress detection, as conditional on its own evidence. This manuscript develops the architecture described in the project report into a research-oriented specification. It preserves the principal modules while distinguishing documented design choices from proposed evaluation refinements. It does not claim a new alerting protocol, a new speech-recognition or translation model, or experimentally established superiority over existing applications. Its contribution is the integration specification and the explicit separation of what each module does, what evidence is available, and what must be measured before real-world use.

II. RELATED WORK

A. Mobile SOS and location-sharing applications

The literature survey in the project report examines applications that send an emergency alert with a live location to pre-registered contacts. Rescue Now [6] is described as supporting activation by a single touch or a voice command, sharing the real-time GPS location with contacts and nearby police stations, recording audio and video silently, and adding an AI-based crime-prediction model that warns users about unsafe areas. Safe Her [1] is a progressive web application for real-time SOS alerting and live GPS tracking, and Abhaya [2] is an Android application for women's safety. A GPS and SMS alert system is reported in [4]. These works motivate the present design, but their reported behavior is not a measurement of this project. Entries [1], [2], [4], [5], and [8] are characterized here only from their titles and their listing in the project report, because their full texts were not part of the supplied material.

B. Voice-activated and sensor-based triggering

Dhivya *et al.* [3] describe a voice-recognition application in which predefined words such as "Help" or "Emergency" activate the SOS, which is useful when the user cannot reach the phone. Sinha *et al.* [7] describe an Android application that adds shake detection and voice activation, shares the location with contacts and nearby police stations, and helps users find nearby hospitals and police stations. These studies support treating the trigger as a separately evaluated component. They do not establish a false-trigger rate or a missed-trigger rate under noise, in a pocket, or with a locked screen.

C. Evidence capture and complaint support

Rescue Now [6] is described as recording audio and video silently to collect evidence. The present project adds a voice-based complaint feature that converts speech to text and translates the text. The cited works do not establish that speech recognition is accurate for distressed speech, for the languages used by the intended users, or in noisy surroundings, so complaint transcription and translation are treated as separately evaluated language tasks.

D. Security foundations

The project report lists data encryption, JWT-based sessions, HTTPS, permission management, and secure cloud storage. JSON Web Tokens [9] and TLS 1.3 [10] are established mechanisms for session claims and transport protection. They protect data in transit and the integrity of a session, but they do not decide who may see a user's location or recordings, which is a policy question addressed in Section VIII. Table I summarizes the connection between these foundations and the proposed framework. The comparison concerns task relevance rather than a numerical ranking across incompatible systems.

Table I – Literature Foundations and Their Role in the Proposed Framework

Work	Established contribution and role here	Boundary of applicability
Rescue Now [6]	One-touch or voice SOS, GPS sharing, silent recording, crime prediction. Motivates the alert and evidence branches.	Described behavior is not evidence of this system's performance.
Sinha et al. [7]	Shake and voice activation, safe-place finder. Motivates optional triggers.	No trigger error rates are established.
Dhivya et al. [3]	Voice-command SOS. Motivates hands-free triggering.	Recognition accuracy in this setting is not established.
SafeHer [1]	Web application with real-time SOS and live tracking (from title). Motivates cross-platform delivery.	Not reviewed beyond title.
Abhaya [2]; Sakure [4]	Android and GPS-plus-SMS alerting (from titles). Motivate the SMS fallback.	Not reviewed beyond title.
JWT [9]; TLS [10]	Session claims and transport security. Support the security components.	Do not define data-access policy.

III. RESEARCH GAP AND CONTRIBUTIONS

The project-level gap is the absence of an explicitly defined meaning for the states of an emergency alert, and of a defined behavior when part of the workflow fails. Simply listing features such as SOS, recording, voice complaint, and legal awareness leaves important questions unanswered: what the interface should show when the location is unavailable, what happens when the network is down, how accidental triggers are handled, who may see recorded media, and how any of these claims would be measured. The proposed framework makes four design contributions. First, it separates the trigger event from delivery status, using the four states triggered, dispatched, delivered, and acknowledged. Second, it runs location, evidence, and notification as independent branches so that the failure of one does not block the others. Third, it defines optional components (voice trigger, AI/ML distress detection, police integration) as conditional, so that their absence is reported rather than hidden. Fourth, it specifies an evaluation plan that separates alert delivery, location

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.06

accuracy, evidence capture, speech and translation quality, and interface behavior. These are integration and evaluation contributions, not claims of a first-of-its-kind system or of improved response time over existing applications. Demonstrating an empirical contribution requires the experiments described later in the paper.

IV. SYSTEM ARCHITECTURE

A. Triggers and input handling

The principal trigger is an on-screen SOS button placed on the home screen. The report also describes a voice phrase, repeated power-button presses, and a timer-based automatic SOS that fires if the user does not confirm safety within a chosen time. Each trigger should create a record containing the trigger type, a timestamp, the user identifier, and the state of the required permissions (location, camera, microphone, notifications). A trigger that cannot proceed because permission is missing should report which capability is unavailable rather than failing silently. A short, configurable cancel window for accidental triggers is a proposed refinement; the supplied material does not specify one.

B. Alert branches

After a trigger, three branches run in parallel, as in Fig. 1. The location branch obtains a GPS fix and records its accuracy, falling back to the last known location with a clear label when no fix is available. The evidence branch starts audio and video recording and stores timestamps. The notification branch sends the alert and a location link to the saved contacts, by push notification or backend-sent SMS when the network is available and by SMS from the device when it is not. The report's flowchart presents these steps in sequence; treating them as parallel branches, with separate statuses, resolves that difference without requiring one step to wait for another.

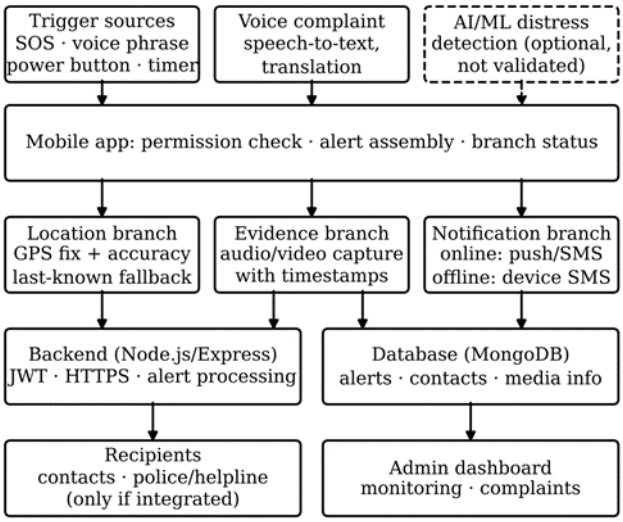


Fig.1. Proposed alert architecture. After a trigger, location, evidence and notification run as independent branches, each with its own status. The dashed elements (AI/ML distress detection) are optional extensions that are not demonstrated by the supplied material.

Keeping the branches separate makes partial failure observable. A location may be unavailable while the notification still goes out, and recording may be blocked by permission while the alert is still delivered. In each case the interface should show what succeeded and what did not, instead of a single success message.

C. Complaint and awareness branch

The voice complaint branch converts spoken input to text, optionally translates it into another language, and stores both versions with a timestamp. The legal-awareness module displays women's-safety laws, rights, and helpline numbers from a content store. Both are non-emergency functions and should not delay the SOS path.

D. Aggregation and presentation

The interface aggregates the status of each branch and displays alert history. The intended output comprises the trigger state, the location and its accuracy label, the recording state, the delivery status for each contact, and any processing limitations. An administrator dashboard is described for monitoring alerts, active users, and complaints; its access rules are not specified in the supplied material.

V. METHODOLOGY

A. Development approach and feature scope

The report describes an agile, user-centric process of requirement analysis, system design, modular implementation, testing, and deployment with continuous monitoring. Key features identified in the requirement analysis are one-touch SOS, live location tracking, automatic audio and video recording, emergency-contact management, and notifications. Each feature is developed as an independent module and later integrated, with APIs connecting location services, messaging, and cloud storage.

B. Data model

The report proposes MongoDB, accessed through Mongoose from a Node.js and Express backend, with seven collections: users; emergency contacts; SOS alerts and GPS records; audio and video records; complaints; legal-awareness content; and AI/ML analysis results.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.06

The media collection stores file paths, timestamps, duration, and user details rather than the media itself, which is held in local or cloud storage. Records should carry a user identifier and a creation time, and media records should carry an integrity digest so that later changes to a recording can be detected; the digest is a proposed addition.

C. Alert workflow and status model

The alert state is tracked per contact. A contact's alert is triggered when the user acts, dispatched when it leaves the device or backend, delivered when a delivery receipt or equivalent confirmation exists, and acknowledged when the contact responds. SMS and push delivery receipts are not guaranteed on every network, so delivered may be unobservable; in that case the interface should say that delivery is unconfirmed instead of reporting success. The end-to-end alert latency is defined as

$$T_{alert} = t_{deliver} - t_{trigger} \qquad (1)$$

where $t_{trigger}$ is the time the user action is registered and $t_{deliver}$ is the time delivery is confirmed at the recipient. The report describes delivery "within seconds"; no distribution of T_{alert} is supplied.

D. Offline fallback and safety timer

When the device has no data connection, the system should send SMS directly from the device, carrying the user's identity and a location link or coordinates. SMS needs only the mobile network, which is why the report describes it as a fallback for remote or low-network areas. The safety timer is set by the user before a journey; if it expires without confirmation, the same alert workflow runs. The timer needs a visible countdown and a clear way to confirm safety so that expiry is not mistaken for an emergency.

E. Voice complaint and translation

The complaint pipeline records speech, produces text with a speech-recognition service, and optionally translates it. The report presents an English-to-Hindi example. The language set, the recognition and translation services, and the handling of low-confidence transcripts are not specified. A transcript should be shown to the user for review before it is stored or submitted, because a recognition error in a formal complaint could change its meaning.

F. AI/ML distress detection

The report describes an AI/ML component that analyzes voice input to estimate distress and stores the results. It does not identify a model, features, training data, labels, or an operating threshold. This paper therefore treats distress detection as an optional extension whose output may inform the interface but should not trigger an alert on its own until it has been evaluated. A distress score shown without such evaluation is an illustration, not a measurement.

VI. IMPLEMENTATION

A. Proposed software organization

The report lists Android Studio, React Native, or Flutter for the mobile interface; Node.js and Express for the backend; MongoDB with Mongoose for storage; Python libraries for AI/ML; and JWT, HTTPS, and encryption for security. The component figure additionally names Google Maps for location display, Twilio for SMS, Firebase for push notifications, and Amazon S3 for media storage. These alternatives describe a development plan rather than a fixed, versioned stack, and the abstract's reference to Android is therefore read as the principal target platform. A practical implementation can separate trigger handling, location, recording, notification, complaint processing, and presentation into modules with explicit input and output contracts, each returning a status alongside its data. Table II distinguishes supplied artifacts from work still required.

Table II – Implementation Evidence in the Supplied Project Report

Component	Available material	Missing evidence
SOS and alert	Flowchart and narrative workflow.	Source code, API specification, delivery logs, tests.
Location	Description of GPS capture and map display.	Accuracy measurements, fallback behavior tests.
Recording	Description of automatic audio/video capture.	OS-version, locked-screen and permission tests.
Voice and translation	Narrative and one illustrative example.	Services used, languages, error rates.
AI/ML	Narrative role and database collection.	Model, data, labels, metrics.
Backend and security	Component descriptions.	Deployed configuration, security assessment.
Interface	Screen descriptions and composite illustration.	Running build, request traces, user tests.

B. Scope of the supplied material

The project report supplies design descriptions, block diagrams, a flowchart, and a composite results illustration, but it does not supply source code, a build, an API specification, or recordings of the application running on a device. The results illustration is therefore treated as a depiction of intended behavior. The report states that recording can start secretly in the background, but mobile operating systems restrict background access to the camera and microphone, so the feasibility and the required user disclosure of covert capture must be verified per platform version before it is described as supported. Direct police integration likewise depends on agreements with the relevant agencies and is not demonstrated.

C. Interface behavior

The interface should confirm that the trigger was registered and report the status of each branch. It should distinguish "not available" (for example, no GPS fix) from "not attempted" and from a processing error, and it should distinguish dispatched from delivered. An illustrative template is: "SOS triggered.

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 08, November 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.06

Location shared with your contacts by SMS; delivery is not yet confirmed. Recording started." This is a proposed message, not an output observed from a deployed system, and no message should imply that help is on its way unless a recipient has acknowledged the alert.

VII. EVALUATION METHODOLOGY

A. Alert metrics

Evaluation should treat each trigger as an event with a known outcome. Let N_{trig} be the number of triggers, N_{del} the number with confirmed delivery to at least one contact, N_{ft} the number of triggers during non-emergency use, and H_{use} the observed hours of use. The proposed measures are

$$DSR = N_{del} / N_{trig} \quad (2)$$

$$FTR = N_{ft} / H_{use} \quad (3)$$

where DSR is the delivery success ratio and FTR is the false-trigger rate. Latency T_{alert} from Eq. (1) should be reported as a distribution (median and upper percentiles) rather than a single average. Location error is measured against a surveyed reference point as

$$e_{loc} = d(p_{rep}, p_{ref}) \quad (4)$$

where p_{rep} is the reported coordinate, p_{ref} is the reference coordinate, and d is the great-circle distance. Results should be reported separately for indoor, outdoor, and moving conditions, and for the first fix versus a last-known location.

B. Speech and language metrics

Complaint transcription is assessed with the word error rate

$$WER = (S + D + I) / N \quad (5)$$

where S, D, and I are the numbers of substituted, deleted, and inserted words relative to a reference transcript of N words. Test speech should include each supported language, calm and stressed delivery, and background noise. Translation adequacy should be rated by bilingual reviewers on a stated scale, since a single automatic score does not establish that a complaint's meaning is preserved.

C. Voice trigger and distress detection

For the voice trigger and for any distress classifier, a positive event is a genuine trigger phrase or a genuine distress sample. Recall,

$$Recall = TP / (TP + FN) \quad (6)$$

Measures missed events and should be reported with precision, the confusion counts, and the false-trigger rate per hour of ordinary use. Distress-detection data should come from consented, ethically collected recordings, and results should state the languages, speakers, and noise conditions covered.

D. Comparison and ablation design

The proposed comparison starts from a baseline that sends location by SMS only, then adds backend notification, evidence recording, voice triggering, and the complaint features one at a time, using the same devices and conditions. Battery drain, alert latency, and false-trigger rate should be reported for each configuration. The complete application should not be assumed to be better because it has more features: each added feature can cost battery, increase false triggers, or delay the alert, and the evaluation should show whether it does.

Table III - Proposed Experiments and Required Measurements

Experiment	Required evidence and output
Alert delivery	Trigger log with timestamps; DSR; T_alert distribution by network condition; SMS fallback results.
Location	Surveyed reference points; error e_loc by setting; first-fix time; fallback labeling.
Evidence capture	Device and OS matrix; recording start time; success with locked screen and denied permissions.
Voice and complaint	Reference transcripts; WER by language and noise; reviewer ratings for translation.
Trigger and distress	Labeled samples; recall, precision, confusion counts; FTR per hour of use.
Usability and battery	Task-completion under stress simulation; battery drain per configuration.

VIII. SECURITY AND PRIVACY CONSIDERATIONS

The application is intended as one aid to personal safety, not as a mechanism that guarantees protection. It handles unusually sensitive data: precise location, recordings of a person and of others nearby, contact details, and complaint text. The proposed threat model covers accidental or malicious triggers, loss of connectivity or GPS, an unreachable contact, a lost or seized device, unauthorized access to stored media or location, misuse of location sharing to track a person, and exposure through logs or the administrator dashboard. Table IV summarizes these cases and the limits of the proposed response.

Table IV - Proposed Threat Model and Limits of the Workflow

Threat or failure	Proposed response	Residual limitation
Accidental SOS	Cancel window; clear trigger confirmation.	Not specified in the report; false-trigger rate unmeasured.
No network	Device SMS fallback.	Needs mobile coverage; delivery may be unobservable.
No GPS fix	Last-known location with a clear label.	Stale location may mislead contacts.
Contact unreachable	Multiple contacts; acknowledgment status.	Number of contacts and escalation not specified.

Device lost or locked	Session expiry; server-side revocation.	Not demonstrated.
Media or location exposure	Encryption, access control, retention limits.	Proposed controls; no security assessment supplied.
Tracking misuse	Consent, visible sharing indicator, easy revocation.	Requires policy and user-interface design.

The report lists encryption, JWT authentication, HTTPS, permission management, and secure cloud storage. These are requirements for implementation rather than measured outcomes, because no configuration or security assessment is supplied. Recording laws and consent rules differ between settings, and the legal weight of a recording depends on how it was made and kept; this paper makes no claim about admissibility. Stored recordings should carry an integrity digest and an access-controlled audit trail, retention should be limited and delectable by the user, and any test involving real people should use consenting volunteers and test endpoints rather than real emergency services.

IX. EXPERIMENTAL SETUP

The supplied report does not identify the devices, Android versions, network conditions, number of test runs, or participants used in any test. It provides no figures for alert latency, delivery, location error, recognition accuracy, or battery use. These omissions prevent reconstruction of a completed experimental setup. The proposed evaluation begins by fixing a device matrix covering several manufacturers and Android versions, and a condition matrix covering good, weak, and absent data connectivity; screen on, screen locked, and app in the background; and high and low battery. Test contacts and test endpoints replace real emergency recipients. Each run records the trigger, the status of each branch, and the timestamps needed to compute Eq. (1) to (4). The experiment record should freeze the application build, library versions, services used, language set, and the content version of the legal-awareness module. Latency measurements should be decomposed into trigger handling, location acquisition, dispatch, and delivery, because the largest delay is likely to differ between networks. Because no such measurements were supplied, this paper does not describe the system as real-time. Table III lists the evidence needed for the planned experiments.

X. RESULTS

A. Qualitative material in the project report

The source report's results chapter lists ten statements, including that the SOS feature sends the real-time location to saved contacts "within seconds," that audio and video capture start automatically, that voice-to-text and translation work accurately, and that the interface is easy to use under stress. It also presents a composite illustration of twelve panels showing the intended screens: SOS and location alert, audio and video capture, voice-to-text, English-to-Hindi translation, distress detection, a legal-awareness list, a fast-response screen, a user-friendly interface, an integrated platform, a workflow strip, a sample SOS message, and an overall-impact panel. Table V records what can be concluded from these without converting illustrations into measurements. The panels are not accompanied by build identifiers, device details, test logs, or reference data. Some panels display example values, such as an elapsed time on the fast-response screen and a percentage on the distress-detection screen. Without a test protocol these are illustrative screen content and are not treated as measured latency or detection accuracy. The architecture diagram in this paper is a newly drawn schematic, not an experimental result.

Table V - Qualitative Observations from the Source Report and their Evidence Limits

Reported item	Observation described	Interpretation supported
SOS and location	Location sent to saved contacts within seconds.	Intended behavior; no delivery counts or latency distribution.
Audio/video capture	Recording starts automatically on SOS.	Intended behavior; no locked-screen or OS-version test.
Voice-to-text	Spoken complaints converted accurately.	No reference transcripts or error rates.
Translation	One English-to-Hindi example panel.	A single example; no reviewer rating.
Distress detection	Panel shows a distress percentage.	Illustration only; no model, data, or metrics.
Legal awareness	Panel lists laws and helplines.	Content not verified here; currency not assessed.
Fast response	Panel shows an elapsed alert time.	Not a measurement; no protocol.

B. Quantitative result status

No numerical delivery ratio, latency distribution, location error, word error rate, translation score, distress-detection recall or precision, or battery measurement is available in the supplied material. There is no test denominator from which to derive such values. The report's statements that the application was "successfully developed" and works reliably are insufficient to establish those outcomes quantitatively. This paper makes no claim of superiority over existing safety applications; those comparisons remain experiments to be performed.

C. Functional evaluation status

The available evidence supports an architectural description and an illustration of intended screens. End-to-end behavior remains to be verified. Table VI defines functional tests for the implementation; all entries are proposed tests, not recorded passes.

Table VI - Proposed Functional Tests; Execution Evidence is not Supplied

Test case	Expected behavior
Trigger with GPS off	Send alert with a "location unavailable" or last-known label; do not block the alert.

No data connection	Send SMS from the device; mark delivery unconfirmed if no receipt.
No emergency contact	Do not report success; prompt the user to add a contact.
Permission denied	Name the unavailable feature; run the remaining branches.
Accidental trigger	Allow cancellation within the cancel window; record the event.
Timer expiry	Run the alert workflow only if safety was not confirmed.
Locked screen	Trigger and send the alert as designed; report recording status.
Invalid session token	Reject the request; do not expose stored data.
Low-confidence transcript	Show the text for review before storing or submitting.

XI. DISCUSSION

The principal value of the architecture is that it makes different kinds of evidence visible within one workflow. A trigger record shows what the user did, a location branch shows where the device was and how reliable that fix was, an evidence branch shows what was recorded, and the notification branch shows what reached whom. None of these outputs should silently substitute for another, and none should be summarized as "help is coming." Their usefulness depends on communicating what was done and what remains uncertain. The most consequential design issue is the boundary between alerting and rescue. The application can inform contacts and, where integrated, authorities; it cannot ensure that anyone responds. Interface language should reflect this, and on boarding should ask users to agree with their contacts on what an alert means and what to do when one arrives. Trigger design involves a trade-off. A sensitive trigger reduces missed emergencies but increases false alarms, which can erode contacts' willingness to respond. Voice and shake triggers are especially sensitive to noise and movement, so their thresholds should be set from validation data and reviewed against the intended use. An AI/ML distress detector should not trigger an alert on its own until its error rates are known. Privacy and evidence also pull in different directions: more recording and more sharing give contacts and investigators more information but increase the harm if the data are exposed or misused. Defaults should favor limited sharing, clear indicators, and easy revocation. Finally, legal-awareness content goes out of date. The illustrative panel cites the Indian Penal Code, which has since been replaced by the Bharatiya Nyaya Sanhita for offences after 1 July 2024, so the content store needs a named source, a version date, and a review process.

XII. LIMITATIONS

The first limitation is evidential: the available artifact is a project report, not a reproducible experimental package. Source code, a build, test logs, device matrices, and reference data were not supplied. The manuscript therefore describes a proposed framework with qualitative supporting material rather than a validated application. Second, several choices remain open, including the mobile framework, the speech-recognition and translation services, the AI/ML method, the set of supported languages, and the cloud provider. The report's mention of Android, React Native, and Flutter as interface options means the platform behavior of recording, background execution, and power-button triggers is not settled. Third, claims about response time, recognition accuracy, and ease of use under stress are unsupported by measurement, and the cancel window, escalation policy, and access rules for the administrator dashboard are not specified. Fourth, no user study, field trial, security assessment, legal review, or collaboration with emergency services is documented. These limitations preclude claims of readiness for deployment, protection of users, or real-time reliability.

XIII. FUTURE WORK

The immediate priority is a runnable, versioned build with logging of every trigger and branch status, followed by the experiments in Table III on a defined device and network matrix. A baseline of location-by-SMS should precede the evaluation of voice triggering, recording, and complaint features. Subsequent work should specify and test the cancel window, contact escalation, and the delivery-status model; evaluate speech recognition and translation for the supported languages with consented, stressed-speech data; and assess any distress detector independently before connecting it to the alert path. The legal-awareness content should be tied to official sources with version dates. Future studies can then assess battery cost, behavior under different Android versions and manufacturer power-saving settings, and usability with target users, and can examine privacy controls, data retention, and integration with emergency services with the necessary institutional approvals and ethics review.

XIV. CONCLUSION

This paper presents Women Safety as an integrated framework for emergency alerting that combines one-touch SOS, real-time GPS sharing, audio and video evidence capture, voice-based complaint filing with translation, an offline SMS fallback, and legal awareness. The architecture separates trigger, location, evidence, and notification, and it distinguishes triggered, dispatched, delivered, and acknowledged alerts so that the interface does not overstate what has happened. The project report provides design descriptions, diagrams, and an illustration of intended screens, but not the artifacts needed to verify quantitative performance. Accordingly, this manuscript reports qualitative evidence and specifies the experiments required to evaluate the framework. Its outcome is a structured, testable research design rather than a validated safety system. A reproducible build, measured alert reliability, evaluated speech and language components, and privacy-preserving defaults are the next requirements for establishing practical effectiveness.

ACKNOWLEDGMENT

The authors thank Dr.Manjushree CV, Associate Professor, Department of Information Science and Engineering, Vemana Institute of Technology, for her continuous support, guidance, and supervision during the project. The authors also thank the project coordinators Prof. Jyothi M and Dr. Aruna Reddy H, the Head of the Department Dr. Rajanna M, and the Principal Dr. Vijayasimha Reddy B G for their support, and acknowledge the department and institution for supporting the project work.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1208.06

AUTHOR CONTRIBUTION STATEMENT

Conceptualization: Dr.Manjushree C V
Literature Review and Methodology design: Meghana T, Pavani Priya
Validation: Sushmitha A, Udaya Shree
Investigation: Dr.Manjushree C V
Resources: Meghana T, Pavani Priya
Writing original draft preparation: Sushmitha A, Udaya Shree
Writing review and Editing: Meghana T, Pavani Priya
Supervision: Dr.Manjushree C V
Conflict of interest: The authors declare no conflicts of interest.

Data availability statement: Data supporting these findings are available within the article, at https://doi.org/10.26562/ijiris.2026.v1208.06, or upon request.

Supplementary materials: The supplementary materials are available at https://doi.org/10.26562/ijiris.2026.v1208.06

Publisher's note: AM Publications, India. IJIRIS (International Journal of Innovative Research in Information Security) Journals stays neutral with regard to jurisdictional claims in published maps and institutional affiliations. All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher. https://ampublications-india.com/

REFERENCES

1. S.Gautami et al., "SafeHer: A progressive web application for women safety with real-time SOS alerting and live GPS tracking," Int. J. Eng. Res. Technol. (IJERT), 2026.
2. R.S.Yarabothu and B.Thota, "Abhaya: An Android app for the safety of women," IEEE Conf. Publication, 2015.
3. S.Dhivya et al., "Voice recognition powered women safety app," Int. J. Comput. Sci. Eng., 2022.
4. K.Sakure et al., "Women safety app using GPS and SMS alert system," ResearchGate publication, 2022.
5. S.Verma and S. Singh, "Surakshit: Women safety Android application," J. Mobile Comput. Commun., 2022.
6. S.S.Pawar, R.Roy, K.V.Sawant, R.B.Singh, and M.Navale, "RescueNow: Real-time SOS and predictive women's safety system," Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET), 2025.
7. A.K.Sinha, A.V.Kumar, R. Saha, and K. J. Kadel, "Women security application using smart emergency response system and real-time location tracking," research publication, 2025.
8. M.Sharma et al., "Android-based women safety app," Int. J. Res. Appl. Sci. Eng. Technol. (IJRASET), 2023.
9. M.Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," IETF RFC 7519, 2015.
10. E.Rescorla, "The Transport Layer Security (TLS) protocol version 1.3," IETF RFC 8446, 2018.
11. Ashwini,Viraj,Sajeev (2025). BlogGen AI: An AI-Powered Blogging Platform for Automated Content Creation. International Journal of Innovative Research in Information Security, Volume 11, Issue 01, Pages 59-69 https://doi.org/10.26562/ijiris.2025.v1102.01
12. Varsha,Varun,JaykanthmShreya,Sneha(2025). Hybrid Fire Fighting Robot. International Journal of Innovative Research in Information Security, Volume 11, Issue 01, Pages 70-76 https://doi.org/10.26562/ijiris.2025.v1102.02
13. Vennela,Shivani,Vaishnavi,Dr.Rachitha(2025). Automated Lumbar Spine Object Detection. International Journal of Innovative Research in Information Security, Volume 11, Issue 01, Pages 77-86 https://doi.org/10.26562/ijiris.2025.v1102.03
14. Manaswi,Mirza,Vijayshree(2025). Smart Template Mapping and Fraud Detection. International Journal of Innovative Research in Information Security, Volume 11, Issue 01, Pages 87-96 https://doi.org/10.26562/ijiris.2025.v1102.04
15. Sneha,Meenakshi,Thejaswini (2025). Fresh Roots - Mobile Application. International Journal of Innovative Research in Information Security, Volume 11, Issue 02, Pages 97-101 https://doi.org/10.26562/ijiris.2025.v1102.05