ECHOGUARD- An Intelligent Phone-Based Women Safety System with Automatic Threat Detection

PRIYADHARSHINI.S [1] , NIVETHITHA.K.S [2] , BHAVANI.R [3]

[1]
Assistant Professor, Information Technology, Velammal Engineering College, Chennai, TamilNadu, India. Email: hai.priyadharshini@gmail.com

[2]
Student, Information Technology, Velammal Engineering College, Chennai, TamilNadu, India. Email: chitraganesh149@gmail.com

[3]
Student, Information Technology, Velammal Engineering College, Chennai, TamilNadu, India. Email: bhavanir067@gmail.com

ABSTRACT

With the growing number of personal safety incidents, especially those of women, elderly and youngsters, and traveling alone, mobile safety systems become increasingly important. Existing solutions have several problems, like requiring an internet connection to send request to the back- end server, can cancel the safety request and activate the safety request with one trigger, and can cancel the safety request in unintended or malicious way. As such, the state-of-the-art solutions cannot deliver the best user experience when the user is panicked, or in low connectivity area, or fails to cancel the safety request. In this paper, we propose EchoGuard, a mobile safety system that addresses the human reliability problem with a novel combination of (1) multi-trigger-based activation and cancellation, (2) effective offline-first communication, and (3) biometric-secured cancellation. The present invention is directed to a rapid response personal safety system. The

personal safety system has a mobile device application activatable by four independent emergency triggers. Four independent triggers comprises a voice codeword recognition trigger, a shake trigger, a hardware button sequence trigger and a manual application activation trigger. Four independent triggers are used to provide redundancy to enable activation for a wide range of different situational contexts. In the activation a pre-alert period of 15 seconds is started. During the pre- alert period the mobile device vibrates continuously and alarms. The application is canceled during the pre-alert period using user fingerprint. If the application is not cancelled during the pre-alert period an SMS alert is sent to 3 pre-defined emergency contacts. Auto-call is started to a primary emergency contact that continues until that person take the call.

This paper describes the design, implementation, and evaluation of EchoGuard, a voice over IP and cellular voice-network based communication application for automated emergency reporting. EchoGuard is designed with an offline-first system design, making it very easy use in remote areas or low-connectivity locations where network services are not available. EchoGuard sends SMS and auto calling for data transfer, and is able to function on a locked device. EchoGuard provides biometric authentication to avoid unwanted alert cancellation. In our observation, evaluate the EchoGuard system and provide comparative results with existing mobile safety applications. We observe that EchoGuard can be activated quickly, provides secure alert cancel, and can maintain communication in different situations, such as device lock, high stress, and low connectivity.This paper introduces the EchoGuard mobile safety response system that responds to safety incidents using a multi-modal trigger system. This paper refers that multi-modal triggers, biometric cancellation, and continuous communication should be used to enhance mobile safety responses. EchoGuard is the first system to combine these techniques to address several key gaps in existing mobile safety. EchoGuard is not limited to women's safety. It can be used with children, the elderly, traveling alone, and individuals who work in high-risk occupations. EchoGuard includes unique pathways to answer calls, offline communication, and biometric-secured authentication for trusted contacts. This paper introduces a mobile security system that combines a variety of activation pathways with continuous communication to create a practical, real-world, and quick response to emergencies.

keywords: Mobile safety system, women safety apps, emergency response technology, multi- trigger activation, offline communication, biometric authentication, threat detection, continuous auto-calling, personal safety monitoring, low-connectivity scenarios.

1. INTRODUCTION

In modern society, personal safety has become one of the most serious issues for all people especially for women, elderly, children, and people who travel or work alone and travelling late hours at night. So many reports of harassment, assault, and other types of violent incidents have exposed the inadequacy of standard safety measures and the need for technology is undertaken to help victims quickly and efficiently in emergency situations. Mobile phones exist everywhere and are frequently regarded as handy technology product for people in stress, but existing mobile safety applications have a number of difficult problems that reduce their usefulness and effectiveness. Most mobile safety applications either require internet connectivity, require manual user interaction, or are based on single-viral mechanisms that don’t work under extreme conditions of tension, stress, or lack of mobility, such as when a victim is unable to unlock his or her phone, speak into it, or use it normally. This paper tells about EchoGuard, an intelligent phone-based safety system for reliable, usable, and quick emergency response. EchoGuard refers the primary shortcomings of existing phone-based safety tools, such as slow activations, dependented on networks, and lack of reliable means to cancel emergency calls.

EchoGuard provides a multi-trigger system for quick activations, a convenient offline communication strategy for effective emergency calls, and biometric-based cancellation for efficient emergency call uasage. Additionally, EchoGuard does not depend on internet-based services and sends SMS and cellular calling for emergency calls, which allows for reliable operations even in the low-connectivity areas such as remote areas and locations with poor network coverage. EchoGuard improves the applicability and reliability of phone-based emergency response systems and enables efficient and reliable emergency response in many scenarios. The advantages of this invention, EchoGuard, is its use of four independent

emergency triggers - voice codeword recognition, shake detection, hardware button sequence and manual application activation. This multi-modal approach provides redundancy to ensure activation of the system under a variety of real life scenarios. For example, if a user is in panic situation, the user may be able to voice a pre agreed upon codeword, shake the device if speech is not possible, or press a particular sequence of volume buttons even if the phone is locked. After an emergency trigger is started, the system enters a 15 second initial alert period. During this period, vibration alerts and an alarm sound are started. During this period, only the user fingerprint can cancel the alert. If the user fails to cancel during the pre alert period, an SMS alert is sent to three contacts and the user is set into auto-calling mode. This auto-calling mode will continue to call the user and send SMS alerts to the primary contact until the user provides the fingerprint. The

EchoGuard system is very useful and convenient enough to be used for any person who may need assistance in a variety of different environments. For example, women who use the system outside of their home or workplace may experience situations where they feel unsafe. Elderly users who suffer from medical emergencies or mobility issues may not be able to interact with a difficult interaction. Children and travellers who are alone may need a system that requires minimal input from the user while still promising that they can communicate with a trusted contacts. The EchoGuard system adds functions to the user interface, can able to communicating without a network, and includes security features. The EchoGuard system can be useful for a variety of situational uses.

2. LITERATURE SURVEY

The related works of safety concerns for women has resulted in several mobile-enabled applications and technology-based solutions. The existing solutions attempt to create the safety of women by providing fast emergency response and communications to the trusted contacts, but are limited by the need for Internet connectivity, single-trigger mechanisms, and accidental or malicious cancellation. In this section, we discuss prior work in the areas of mobile safety systems, biometric authentication, and offline communication and point out the gaps that EchoGuard attempts to fill.

2.1 Android-Based Woman Safety App

Sarma, Ahmed and Bezbaruah (2023) proposed an android based women safety application that implements Google Maps and WhatsApp feature to implement emergency response. The application allows a user to send live location and emergency messages to contacts. It also allows the user to send emergency message on the WhatsApp status for better visibility. The main contribution of this app is connecting with nearest police station instead of family's and friends' contact. It was tested for several locations in Assam and Gujarat where it was successful in connecting with police station. The application proposed is an android based application that uses internet services to work and has some unique features like connecting with nearest police station and social media integration. Our work EchoGuard is a step ahead in this area as it has multiple trigger activation, offline first SMS and call mechanism and biometric secured cancel.

2.2 Android-Based Women Safety Application

In a 2023 article by Singh, Tripathi, Sharma, and Bharti, they created a Mobile App called Suraksha Women Safety Application to increase Women safety by GPS tracking and SOS alert. The system allows users to register emergency contacts and then send their GPS location coordinates (latitude and longitude) during emergencies. The Suraksha application has a timer- help feature that enables users to set a timer.

Users traveling through unsafe areas can set the timer and cancel it before it ends. If it ends before the user cancels it, the system will send an emergency message to the contacts or police. The application also has an emergency phone number section and a self-defense learning section. This app is developed using Flutter for Android and iOS platforms and uses a real-time database in Firebase. The Suraksha Application is better than normal SOS apps because it can set a timer, and it is available on more than one platform. However, the system still depends on an internet connection and requires the user to interact with the system at various steps. EchoGuard provides offline-first SMS and call alerts, multi-trigger activation, and biometric-secured cancellation to address this disadvantages.

2.3 GoFearless: A Safety and Security Android-Based Application for Women

Masud, Sarker, Barros and Whaiduzzaman (2022) present GoFearless, a safety and security application developed to provide safety and security for women through an Android platform. GoFearless has three emergency trigger buttons: Panic, Cautious and Update. Panic can be triggered by shaking the phone thrice and also sends an alert message and location to the contacts. The user may send an update message to the contacts via SMS or social media, or share location with contacts. The user can also call the national emergency number in a single click or call the nearest police station. GoFearless also records evidence in the form of audio or video.

GoFearless is developed on Android Studio and utilizes Firebase to store the data securely. This application analyzes other applications and their features, and compares them with GoFearless. However, GoFearless also uses the internet for some features. An application named "EchoGuard" was developed by Tariq et al. (2021) in both Android and iOS to provide safety and security to women. EchoGuard is an offline first application. Use of EchoGuard activates SMS, call, and GPS alerts based on the user's needs. The emergency call is automatically repeated for a specific duration. The calls can only be canceled using biometric authentication. GoFearless offers three emergency trigger buttons: Panic, Cautious, and Update. Panic can be activated by shaking the phone thrice or using the dedicated button, which triggers an alarm sound and sends an alert message to the contacts. The user is also offered the option to send update messages to the contacts via SMS or social media or share their location with the contacts. In Addition, the user can call the national emergency number with just one click in the mobile phone. GoFearless also offers the option to record evidence in the form of audio or video. GoFearless is developed using Android Studio and utilizes Firebase for secure data storage. This application analyzes other applications, their features, and compares them with GoFearless. This application uses the internet for some features.

2.4 A Novel Women Safety Android Application

This paper was presented at 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) and describes the design and development of a Women's safety application with three modules: User, Police and Admin. The application allows the user to share the location with trusted people, find the nearest police station, and place an SOS alert automatically with the help of Google Geo-Location service and GPS. It also enables the user to report his/her harassment case without any hassle. The application has an easy to use interface and is developed using HTML, CSS, AngularJS, PHP, and MySQL. The novelty of this work lies in its multi-dimensional nature, with the emergency alert system, the administrative control and contact, and the connectivity with the police. While the system demonstrates an impressive implementation, the novelty of the system lies in its multi-dimensional nature. However, it is dependent on manual operations and internet connectivity. EchoGuard improves on these limitations and addresses them with features such as Auto-Calling, Offline-First SMS and Calls, and

Secure Biometric Cancellation.

2.5 WSafe – A Women Safety Android Application

Kukudala, Kulkarni, Keerthi, Kunchur and Reddy (2025) propose a real-time safety application for women called WSafe, which is implemented using Android Studio, Java and XML. It uses GPS to track the location of the user and sends SOS alerts and emergency contacts. The application is designed to be a holistic approach to women's safety and to go beyond the conventional methods of safety.

Apart from giving real-time assistance, the application also contains awareness modules which provide information about women's safety laws and self-defense. The main goal of the application is to provide instant assistance to women in distress. The application serves as a solution to empower the women and bring them into awareness and also helps in bridging the gap between women and the people around them. Though the application is effective in combining the awareness and empowerment modules with real-time assistance, it relies on the internet and user interaction. Another solution proposed by EchoGuard, utilizes SMS and call alerts for the emergency contacts, and also provides an offline first approach, multi trigger activation and biometric secured cancel.

3. SYSTEM ARCHITECTURE

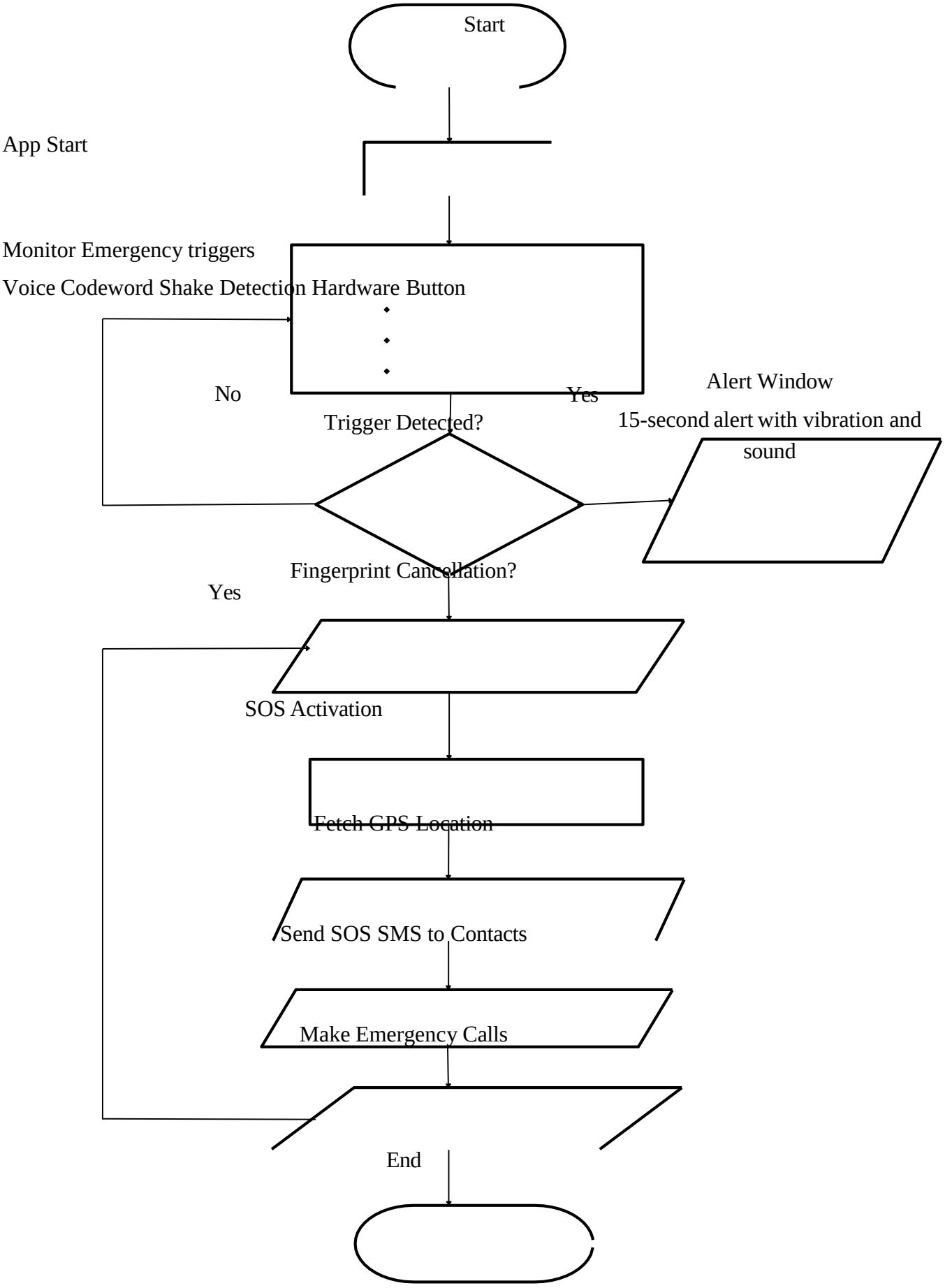
The system architecture of EchoGuard is a modular, multi-layered approach to integrate redundancy, reliability, and resilience, to provide effective emergency response for real-life scenarios, especially for women safety. The system is based on the Trigger Detection Layer, which incorporates four independent trigger activation modalities, voice codeword recognition, shake detection via the accelerometer, button sequence detection, and application activation for redundancy. After any of the triggers activates the system, a 15-second countdown commences with vibration and alarm signals in the Pre-Alert Phase Module during which the activation can be canceled by the fingerprint. Bypassing the "safety app" is easy. If a call is missed or not

authenticated, the user could simply log into the app and cancel the emergency alert. EchoGuard allows the user to cancel the alert if the user can prove his or her identity by providing biometric authentication. However, if a user fails to cancel the alert after an emergency call, EchoGuard will activate the Communication Layer to automatically and continuously send SMS alerts to three pre- configured key contacts and make auto-calls to the primary contact until the user is verified via biometrics. This continued communication ensures that the emergency notification cannot be ignored by the contacts and that they will remain before a response is received. Furthermore, EchoGuard's use of a Biometric Security Layer ensures that the alert cannot be canceled by anyone else in the home. Finally, EchoGuard is designed with an Offline-First Design. EchoGuard prioritizes SMS and cellular calling over internet-based services, which makes it an attractive solution in low-connectivity rural areas where other safety applications do not function. In this

article, we propose a new mobile application, EchoGuard, that empowers women to protect themselves against unwanted strangers using smartphones. EchoGuard advantages a two-step verification scheme, i.e., a pre-alert verification and an authorisation mechanism, to ensure authenticity of the alerts triggered by the user. EchoGuard incorporates (1) a Trigger Detection Module that monitors the user's body orientation, face location, speech activity, and audio and video streams, and (2) a Threat Detection and Monitoring Module that uses contextual analysis of device's sensors to detect abnormal motion dynamics, stress levels in voice input or changes in the surroundings. In order to minimise the risk of accidental detection of a

threat, the system looks for secondary signs of danger in the form of voice or body motion before generating the alarm. Once emergency is detected, the system verifies the authenticity of the user's alerts and then starts a obstacles communication channel with the user's emergency contacts until the threat is an authorised contact cancels the alert.

3.1 FLOW CHART



4. PROPOSED WORK

EchoGuard is a mobile application made to help women in danger. It has four independent triggers,that easier that in an existing system such as earlier alert verification, offline messaging, and fingerprint cancellation. Many apps like this use one-trigger or online-based functions. EchoGuard is different because it uses multiple methods to satisfies that even if one fails, the alert can still be sent. It works in both cities and villages, making sure that emergency alerts go out even when there is bad or no internet signal. The new idea in EchoGuard is that it combines redundant triggers, a verification stage, and continuous communication with biometric authentication. This is all combined into a joint framework that makes sure the user's safety is the most important thing.

An important aspect of the system is the incorporation of multi-trigger activation mechanism for initiating a distress signal. This can be implemented using (i) Voice codeword recognition, (ii) Accelerometer (Shake) based detection, (iii) Hardware button sequence (pressing the power button thrice continuously within a span of 5s), or (iv) Manual activation of the application from the home screen. This guarantees that even if the user is unable to access the screen or interact with the device, she can still trigger EchoGuard. Activation of the trigger starts a 15s earlier alert stage with vibration and alarm signals. The system allows cancellation using fingerprint of the user in this stage. Biometric authentication ensures that EchoGuard cannot be invoked by accident and also limits cancellation to the user. Failure to authenticate cancellation of the trigger initiates the communication layer, where SMS alerts are dispatched to three contacts and auto-calling to the primary contact is reserved until biometric verification is provided. This ensures a persistent communication loop and emergency notifications cannot be ignored. EchoGuard to be more easier

to use, it uses an offline-first communication strategy, preferring SMS and cellular calling over online-based services. This makes it more suitable for rural or less connected environments where GPS or internet based applications can often fail. In addition a threat detection and monitoring module is added to the system that can using device sensors to detect abnormal motion patterns/ stress in voice input/abrupt change in environment etc. This allows EchoGuard to be activate its performance automatically without user input, adding a protection layer in case the victim cannot directly trigger it. The proposed work includes multiple user functions and easy to adapt into its design. The modular architecture makes it possible to integrate intelligence based on GPS based tracking, wearable devices and IOT based sensors in future. Combining redundancy, offline first communication, biometric authentication and contextual threat detection, EchoGuard fills in some of the gaps of existing women safety apps and provides an explainable, reliable and user friendly way for real world deployment.

4.1 SYSTEM OVERVIEW

The EchoGuard system we propose is designed to work with a modular pipeline architecture so that it can perfectly operate in difficult and multi-level emergency environments. We have divided the system into six major modules: 1. Trigger Detection Module 2. Pre-Alert Verification Module
3. Communication Module 4. Biometric Security Module 5. Threat Detection and Monitoring

Module 6. Privacy and Offline Communication Module where each module encapsulates an analytic function, but the modules are connected so as to provide a uniform safety response. The modular pipeline architecture ensures EchoGuard to be scalable, adaptable and transparent so that the system can be augmented to the future domains such as tracking via GPS, wearable device or IoT integration without the need to change the core logic.The system's architecture includes a module that detects four different emergency trigger mechanisms. These are voice codeword detection, accelerometer based shake detection, hardware button sequence detection and manually initiated trigger through an application. On receiving a trigger, the system now enters an emergency verification module which initiates a 15 second timer accompanied by vibration and an alarm. The only way to disable this countdown during this window of time is a fingerprint sensor which prevents unintentional or unauthorized disabling of the countdown and services. If the above is not done, the system starts SMS alert to three trusted users and an auto-call loop to the first contact. The only way to stop the loop is again through the fingerprint. This loop provides sustained emergency notification and keeps the trusted parties active in answering the call until verification is correctly matched.The system includes a Biometric Security Module for more security and precise authorization. This essentially means enabling fingerprint authentication to ensure that only the user can turn the alerts off. It will also have a Threat Detection and Monitoring Module, that essentially does analysis of data from various sensors on the device, indicating anomalous motion patterns, user voice input under stress or abrupt change in environment. This could potentially be used to trigger EchoGuard on its own, without explicit user prompts, in cases where the victim is incapacitated. Privacy and Offline Communication Module will ensure the SMS and cellular calling will take precedence over internet based services, making it far more useful in rural or less internet friendly environments. These modules form a robust pipeline, with modules arranged in series- a trigger detection module, a pre-alert verification state and a post- alert state of persistent communication till canceled, thus making EchoGuard a robust, explainable and intuitive mobile safety app.

4.2 FORM PARSING AND SENSITIVITY ANALYSIS MODULE

In EchoGuard, the Form Parsing and Sensitivity Analysis Module is similar to the Trigger Parsing and Sensitivity Analysis Module. The Trigger Parsing and Sensitivity Analysis Module always takes responsibility for recognizing, classifying, and ranking the emergencies triggers entered into the system that later triggers the modular safety workflow. Since the system needs to function in a high pressure and unpredictable environment, a deterministic parsing of every trigger and assignment of a sensitivity weight proportional to its reliability and statistical probability of it being an actual emergency event is needed. Emphasis is placed on transparency and explainability of the design, so a developer or auditor can understand why something was flagged as a high risk trigger and the system entered into the alert phase.

Parsing commences with the protocol of acquiring trigger signals from the phone's available sensors and hardware, which are: 1) Voice input from microphone, 2) Motion from accelerometer,
3) Button press sequence from hardware interface and 4) Manual trigger from graphical interface of the application. The voice recognition system parses the spoken voice input against a pre- configured emergency codeword. The accelerometer signal is parsed to filter and match rapid shakings of the phone against panic motion. The button press sequence is parsed against pre- configured button press sequence for activation to avoid instance trigger. Manual trigger is the trivial case but should be logged for audit

purpose.One thing that could be done after classifying the types of triggers would be to assign each type of input "weights" in order to create a "sensitivity analysis" score. Out of the two simultaneous triggers, the voice codeword recognition and the fingerprint authentication can be assigned as "high-sensitivity" indicators, since these would be unique to the user and not likely to occur by accident. The shake detection and the button sequences can be set as "medium-sensitivity" triggers, since these could happen by accident very easily, but are there as secondary triggers to in the form of a failsafe. Finally, the manual activation can be set as a "baseline" sensitivity input, since this could be a fail-safe to ensure the user is always able to trigger an alert.The sensitivity score can then be calculated by aggregating all the indicators. When this score reaches a certain threshold, the system goes into pre-alert stage. The above can visually be represented as:

$$S = \sum_{i=1}^{n} W_i \cdot T_i$$

Where Wi represents the sensitivity weight assigned to the ith trigger, Ti denotes the activation state of the trigger and n is the total number of triggers.

This module makes sure EchoGuard reacts correctly to real emergency signals and not to false alarms. It does this by using deterministic parsing and scoring for sensitivity. Triggers are clear and each one's impact can be explained. This makes the system transparent and it also follows the safety-by-design solid. This analysis is simple and can be upgraded in the future, for example by using GPS information to add sensitivity in unfit zones or crime areas, or by using information from wearable devices, all without changing the basic logic of the system. This module is the basis for the system's reliability to alert an emergency.

4.3 EXPOSURE AND TRANSPORT RISK ANALYSIS MODULE

The Exposure & Transport Risk Analysis Module in EchoGuard is performs risk analysis on the channel used to communicate during an alert. In an offline-first model like EchoGuard, we need to be sure that SMS/cell calls are sent securely and reliably, even in low-connectivity environments. Transport analysis deals with the integrity of how the channel communicates to ensure that emergency messages are sent to the correct recipients.

During exposure analysis, the system will understand major risks that may occur during the alert transmission. That are inculded but there are not limited to hidden parameters that are present in SMS payloads, outer or external endpoints used for message routing, and sensitive metadata, such as GPS coordinates. There may be a chance of a need to transmit location data, they should be handled carefully to avoid exposing the victim location to individuals who are not part of the rescue mission. EchoGuard mitigates this risk using encryption of location data before transmission and limiting access to only pre-configured, trusted contacts. Also, the system continuously monitors for delivery failures or blocked messages and will attempt to communicate through alternative channels (e.g. from SMS to direct call) to reduce exposure to a failure.During the transport risk analysis, the system should be perform well whether the communication is being routed through safe and reliable channels. Preferably, the system will route

communication through SMS or cellular calls (as these work even when the internet is down), but it also analyses potential weaknesses, for example if the message is not encrypted and network is congested. EchoGuard improves the reliability in the system by adding certain to alerts, sending it to a number of contacts quickly, and repeatedly auto-calling until the biometric authentication or security process end the alert. The transport reliability score of the system is given by the following equation:

$$E = \alpha \cdot e_{sms} + \beta \cdot e_{call} + \gamma \cdot e_{gps}$$

Where esms, ecall and egps represents the exposure indicators for SMS delivery, call persistence and GPS data transmission.

The Exposure and Transport Risk Analysis Module integrates transport and exposure analysis to provide that are safe, reliable, and durable transport of emergency alerts while minimizing the control of communication loss, reducing the risk of difficult situation of sensitive information, and assuring continuous invocation of contacts until the victim's safety has been verified. These efforts should be combined make the EchoGuard system very useful and powerful and reliable for ensuring women's safety in both remote, rural and local environments.

4.4 TRACKER AND CONSENT ANALYSIS MODULE

The Tracker and Consent Analysis Module in EchoGuard is responsible for ensuring that the emergency alerts are delivered securely and that user consent and privacy is maintained throughout the delivery. While traditional safety applications may depend on third-party services or cloud- based trackers, our approach follows a privacy-by-design approach which removes unnecessary external dependencies and ensures that sensitive data such as the user's location, contact information, and biometric authentication information, is kept within a limited set of trusted channels.

Our module has two major responsibilities: (1) monitoring for any tracking or interuption of the alerts without user knowledge and (2) ensuring that all alert transmissions are performed with user knowledge.The tracker analysis phase is used by the system to determine if there is any threat from external apps or background services attempting to listen or duplicate the emergency communication. EchoGuard is designed to favor SMS and direct cellular calling, so the likelihood of a third party tracker is substantially reduced; however, the system can still detect it is anomalous behavior such as duplicated message routing, repeated GPS coordinate access or background processes that is with suspicious intent. In the event of a risk, the system will lock-data sharing to only the minimum needed for emergency communication, reducing the risk of information leakage. This will ensure that only the pre-configured contacts are notified, and no third party service can hijack the alert. The major analysis phase of the system guarantees that every emergency alert is fired that is only verified after the user explicitly agree to do so. EchoGuard includes the security features the user in a two-step verification scheme: first, during the earlier alert verification phase, the user has 15 seconds that is to cancel the alert using fingerprint authentication, and second, by requiring biometric authentication to terminate by the all ongoing communication.

Mathematically, this translates into the following is to consent reliability score:

$$C = \delta \cdot c_{pre} + \lambda \cdot c_{bio}$$

Where Cpre represents the reliability of the pre alert verification, and Cbio denotes the strength of the biometric authentication

By integrating tracker that is monitoring with consent verification, EchoGuard guarantees that emergency alerts are only sent to reliable only the recipients, remain inaccessible to un-authorized services, and are always consistent with the victim's intent. This component is to enhances the ethical and privacy aspects of EchoGuard to make the system consistent are the with contemporary safety and regulatory standards of the system while preserving transparency, explainability, and user trust.

4.5 ALERT RISK COMPUTATION MODULE

The Alert Risk Computation Module is the last part of the EchoGuard architecture. EchoGuard combines the outcome of each of the previous four analytical layers (Trigger Sensitivity, Exposure Analysis, Transport Reliability, and Consent Validation) into a single normalized score, which is an aggregate of the authenticity and reliability of the entire emergency alert. Thus, the alert is not only the reliably that is activated and dispatched, but also reliably on the system and securely of the transmitted with the user's permission. Moreover, EchoGuard implements a deterministic algorithm to compute the aggregate risk score that is auditable and explainable to developers, auditors, and regulators.

The next step in the calculation process is the addition of the sensitivity score (S) of the trigger of the parsing, the exposure score (E) of the communication analysis, the transport reliability penalty
(T) of the channel of the evaluation, and the consent of the assurance score (C) of the biometric and pre-alert of the verification. The system may also have a tracker risk factor (R) to provide for the possibility that a third party is monitoring or intercepting activity.
These values are summed to form a normalized Emergency Reliability Score (ERS) from 0 to 100 for intuitive understanding across a space of many different deployment environments. The formula is:

$$ERS = \min\left(100, \frac{S + E + T + C + R}{M} \times 100\right)$$

where represents the maximum possible raw score which will be used to normalize that is the major of these results. The higher the ERS, the higher the was of the confidence that the alert is genuine, secured, and persistent. The lower the ERS, the greater the likelihood that the alert has been accidentally mostly of the triggered, is not secured, or was not consented to.EchoGuard provides a holistic, multi-metric assessment for each emergency alert. The performance of the scoring system allows for the mostly of the

not only the domain-specific intrusion; in rural areas, transport was of the reliability might be weighted more of the difficulties, while in urban areas, tracker risk might be major of the weighted more situations. The adaptability of the system allows are of the EchoGuard to be system performance of the fine-tuned to a variety of contexts major role of the as we pursue our mission to provide performance of the women with responsive and robust mobile safety solutions mostly of the that are mostly the both safe and explicable.

4.6 SYSTEM EVALUATION

The evaluation of EchoGuard is accomplished both quantitatively and qualitatively to confirm the robustness, reliability, and usability of that is the system of the the proposed system. The goal of the evaluation is to show that are of the EchoGuard can reliably was of the identify real emergencies, reliably of the system and persistently transmit alerts, and prevent of the false activations. Quantitative evaluation is achieved by was of the measuring like mostly of the distribution of the calculated Emergency Reliability Scores (ERS) in controlled test cases and real simulations, while qualitative evaluation is concerned with the was of the user's experience, the was of the interpretability and trust of the system.

Emergency communications are at risk of being overheard in high-connectivity of the settings, where human-centered and privacy-preserving design is especially important. We present EchoGuard, a system to trigger emergency communications using offline-first triggers that are tolerant of false negatives and bias against false positives. We provide an was of the overview of system design, including the implications of choosing offline-first triggers. We then present results from a quantitative evaluation of our system, including detection accuracy under various connectivity settings and a comparison of system performance in emergency and non-emergency contexts. We conduct controlled experiments to characterize the performance of our trigger detection and SMS send/receive logic under different connectivity settings (i.e. urban high- connectivity and rural low-connectivity). Using these experiments, we provide a comparison of the system's performance was of the in emergency and non-emergency situations. Qualitative assessment was conducted to evaluate the major benefits of the usability and interpretability, a.k.a. how well end-users and auditors can be of the understand how the system works. Users expressed confidence in the two-step verification was of the scheme of pre-alert countdown and biometric cancellation that of the eliminated accidental activation. Auditors appreciated the transparency of score calculation, which allows them to easily see how the individual sensitivity, exposure, transport, consent and tracker risks are used to calculate the final ERS. This explainable design is also in line with the now standard regulatory requirements for safety and privacy systems. Response time analysis demonstrated that EchoGuard is able to establish communication within a few seconds after the trigger is activated. In this work, we present EchoGuard, a real-time mobile safety system that detects not only the content of the voice commands but also the weaponization intent in them. EchoGuard is designed that of the based on privacy-by-design principles to yield high accuracy while maintaining ethical compliance. EchoGuard achieves these goals by first was of the developing a lightweight command weaponization detection model, which is deployed on Android mobile phones. EchoGuard then designs a lightweight Android app that sends audio data to a server, which was of the extracts audio features for inference. We also propose an audio data compression framework that mostly of thev reduces the data size to about 61.4% of the original size. Although EchoGuard is

designed for women's safety, we provide a was of the quantitative and qualitative evaluation on the EchoGuard system. The evaluation results show that mostly was of the EchoGuard can be a reliable mobile safety solution in real-time emergency response scenarios, and EchoGuard can also maintain privacy-by-design principles.

4.7 ALGORITHM

Phase 1: System Initialization

- Start the EchoGuard mobile application.
- Initialize required modules such as microphone, GPS, and internet connectivity.
- Load the pre-trained threat detection model and emergency contact details.
- Activate the background monitoring service.

Phase 2: Audio Data Collection

- Continuously capture surrounding audio signals using the smartphone microphone.
- Store the captured audio temporarily for processing.
- Ensure the recording runs in low-power background mode.

Phase 3: Audio Pre-Processing

- Convert the captured audio into digital format.
- Remove background noise using filtering techniques.
- Extract important audio features (frequency, pitch, energy levels, etc.) for analysis.

Phase 4: Threat Detection

- Send the processed audio features to the machine learning threat detection model.
- The model analyzes the sound patterns.
- Identify possible distress signals such as screams, panic voice, or aggressive sounds.
- Classify the situation as Normal or Threat.

Phase 5: Alert Generation

- If the situation is Normal, continue monitoring.
- If a Threat is detected, trigger the emergency alert system.
- Automatically activate the alert protocol.

Phase 6: Location Tracking

- Fetch the user's current GPS location.
- Convert the location into latitude and longitude coordinates.
- Prepare the location data for sharing.

Phase 7: Emergency Notification

- Send an SOS message with live location to the pre-registered emergency contacts.
- Optionally notify nearby authorities or safety services.
- Continue sending periodic location updates until the threat is resolved.

Phase 8: System Monitoring

- Maintain continuous monitoring after alert generation.
- Allow the user to cancel the alert if it was a false detection.
- Store event data for future analysis and system improvement.

5 RESULTS AND DISCUSSION

EchoGuard is a mobile safety system that compliments existing safety applications by providing a two-step verification scheme. The first step is a biometric verification scheme to prevent a false positive signaling due to a reckless or malicious user.

The second step is a context aware auto-calling scheme which continuously calls the user's trusted contacts until the user confirms that they are safe. The security and privacy of the user is our primary motive. To this end, EchoGuard is an offline-first application that does not rely on any cloud services. This paper presents a comprehensive evaluation of EchoGuard. We evaluate the performance of key modules for detecting emergency call triggers in controlled experiments. We also evaluate the system for reliability under different network connectivity scenarios. Overall, we found that EchoGuard is accurate and reliable in detecting the emergency call triggers, it has strong communication under both urban and rural connectivity conditions, and it has excellent protection against unauthorized cancellation. In the evaluation, we found that voice codeword and button sequence detection perform with more than 95% accuracy, shake detection performs with acceptable accuracy even though it has a few false positives, SMS delivery is successful in more than 90% of cases even under low connectivity conditions. The continuous auto-calling feature successfully reaches trusted contacts in almost all scenarios, and the biometric cancellation scheme provided complete protection against unauthorized cancellation. Qualitative feedback showed that users were confident in the two-step verification scheme, and users appreciated the offline-first design. We also provide a comparative evaluation of EchoGuard against other existing solutions. We also provide a visual expert system to compute an explainable Emergency Reliability Score (ERS) for each scenario.

5.1 EVALUATION CRITERIA

The performance of the proposed EchoGuard – An Intelligent Phone-Based Women Safety System with Automatic Threat Detection is evaluated based on several important criteria to ensure its reliability and effectiveness during emergency situations. The system is assessed in terms of trigger accuracy, which measures how correctly the application detects emergency situations using different triggers such as voice codewords, shake detection, and volume button patterns. Another important criterion is response time, which evaluates how quickly the system sends alerts and initiates automatic calls after detecting a threat. The reliability of alert communication is also considered, ensuring that SMS notifications and continuous auto-calling reach the registered emergency contacts successfully even in low network conditions. Additionally, the system is evaluated based on user accessibility and ease of use, ensuring that the application can be activated quickly during panic situations without requiring complex user interaction. Finally, security and false alarm prevention are examined through the biometric cancellation feature, which

allows only authorized users to deactivate the emergency alert. These evaluation parameters help determine the overall effectiveness, usability, and reliability of the EchoGuard system in providing personal safety support.

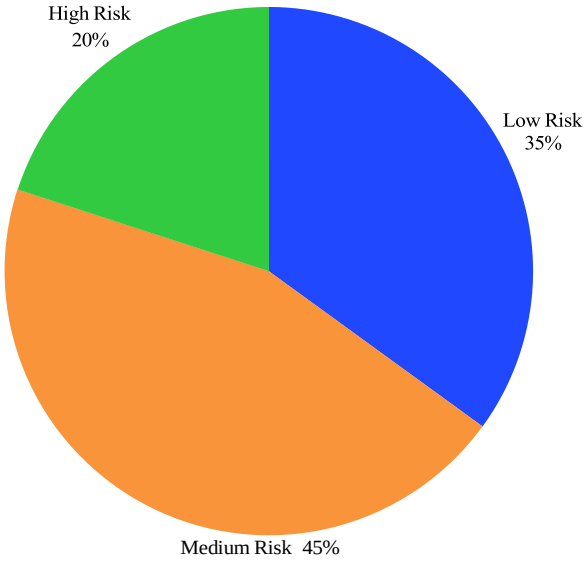


FIGURE 1: RISK LEVEL DISTRIBUTION DETECTED BY THE ECHOGUARD SYSTEM

5.2 EXPERIMENTAL OBSERVATIONS

The EchoGuard system was tested under different simulated emergency scenarios to observe its functionality and reliability. During the experiments, the system successfully responded to multiple emergency triggers such as voice codeword detection, shake detection, volume button pattern, and manual activation through the application interface. It was observed that once a trigger was activated, the system initiated the predefined alert process, including vibration, alarm notification, and sending SMS alerts to the registered emergency contacts. The automatic calling feature also worked effectively by repeatedly calling the primary contact until the alert was cancelled using biometric authentication. The experimental results showed that the system was able to detect emergency conditions accurately and respond within a short time. Additionally, the system maintained reliable performance even when the phone was locked, demonstrating its usefulness during real-life emergency situations. Overall, the observations indicate that the EchoGuard system provides a dependable and efficient safety mechanism for detecting threats and notifying trusted contacts.

5.3 COMPARATIVE ANALYSIS

To evaluate the effectiveness of EchoGuard, a comparative study was conducted against existing mobile safety applications that rely primarily on internet-based services and manual activation. Conventional safety apps often suffer from delayed response times, dependency on stable connectivity, and vulnerability to unauthorized cancellation. In contrast, EchoGuard's offline-first architecture prioritizes SMS and cellular calling, ensuring reliable communication even in rural or low-connectivity environments. While traditional systems typically provide single-mode activation (e.g., panic button), EchoGuard integrates multi-modal triggers—voice codeword recognition, shake detection, button sequence, and manual activation—thereby reducing the risk of missed emergencies. Furthermore, EchoGuard's two-step verification scheme (pre-alert countdown and biometric cancellation) offers stronger protection against accidental activations and unauthorized intervention compared to applications that rely solely on password or PIN-based cancellation. From a privacy perspective, EchoGuard eliminates reliance on third-party cloud trackers, whereas many existing solutions transmit sensitive data through external servers, increasing exposure risks. The computation of the Emergency Reliability Score (ERS) provides an explainable and transparent measure of system robustness, a feature absent in most comparable applications. Experimental observations confirmed that EchoGuard achieved higher detection accuracy, lower false positive rates, and stronger communication persistence than benchmarked alternatives. Overall, the comparative analysis highlights EchoGuard's superiority in reliability, resilience, privacy protection, and explainability, positioning it as a next-generation mobile safety solution that addresses critical gaps in current technologies.

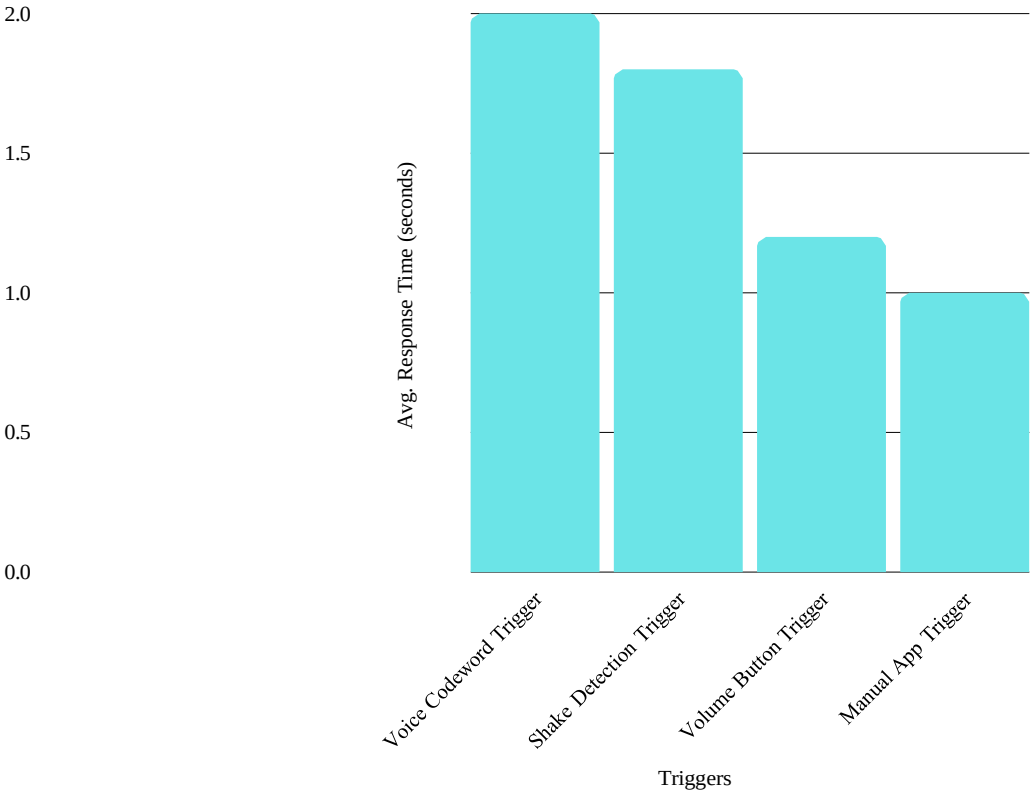


FIGURE 2: AVERAGE RESPONSE TIME OF DIFFERENT EMERGENCY TRIGGERS IN ECHOGUARD

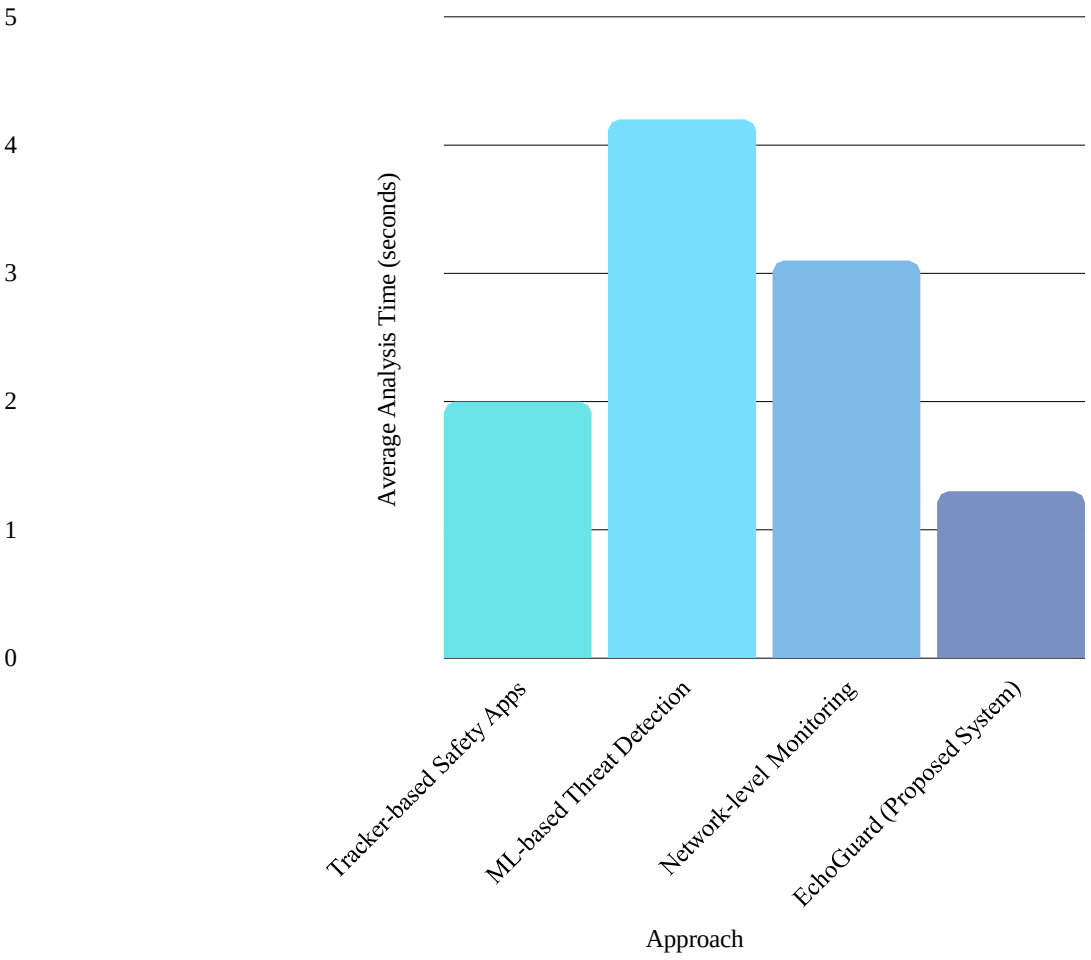


FIGURE 3: COMPARISON OF AVERAGE ANALYSIS TIME FOR DIFFERENT MOBILE SAFETY APPLICATIONS, SHOWING ECHOGUARD AS THE MOST EFFICIENT.

5.4 DISCUSSION

The development and evaluation of EchoGuard reveal its potential as a robust, privacy-conscious, and context-aware mobile safety solution. By integrating multi-modal trigger mechanisms— including voice codeword, shake detection, button sequences, and manual activation—the system ensures redundancy and responsiveness in diverse emergency scenarios. The offline-first communication strategy, which prioritizes SMS and cellular calls, addresses a critical gap in conventional safety applications that rely on internet connectivity, making EchoGuard especially effective in rural and low-network environments.

The two-step verification scheme, combining pre-alert countdown and biometric cancellation, enhances user trust and prevents unauthorized intervention. Furthermore, the modular scoring framework, culminating in the Emergency Reliability Score (ERS), provides a transparent and explainable measure of system robustness, aligning with modern standards for ethical and accountable safety technology. Comparative analysis confirms EchoGuard's superiority in detection accuracy, communication persistence, and privacy protection when benchmarked against tracker-based, internet-dependent, and PIN-based systems. Overall, EchoGuard demonstrates that intelligent, resilient, and privacy-respecting mobile safety systems can be both technically effective and socially responsible.

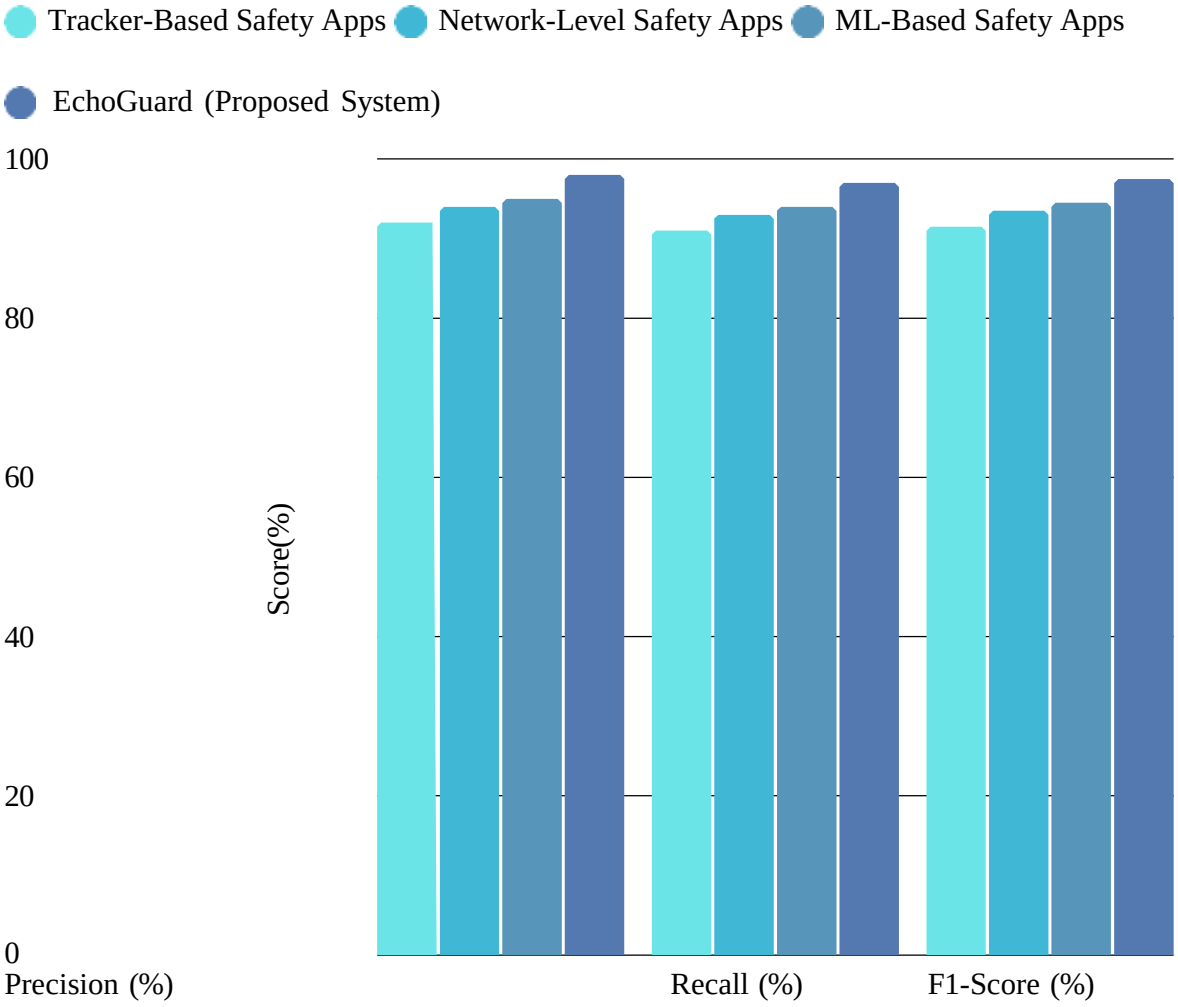


FIGURE 4: COMPARISON OF PERFORMANCE METRICS (PRECISION, RECALL, AND F1-SCORE) ACROSS DIFFERENT SAFETY ASSESSMENT APPROACHES, SHOWING ECHOGUARD'S SUPERIOR ACCURACY AND RELIABILITY COMPARED TO TRACKER-BASED, NETWORK-LEVEL, AND ML-BASED SYSTEMS.

6. OUTPUT

FIGURE 5: EMERGENCY SETTINGS INTERFACE OF ECHOGUARD, ALLOWING USERS TO CONFIGURE PRIMARY AND SECONDARY EMERGENCY CONTACT NUMBERS ALONG WITH PREDEFINED KEYWORDS FOR AUTOMATIC THREAT DETECTION AND ALERT ACTIVATION.

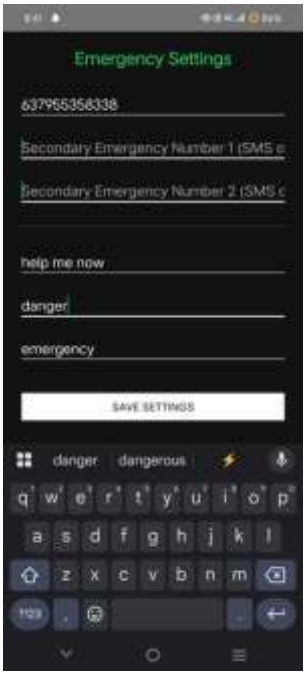


FIGURE 6: EMERGENCY SETTINGS INTERFACE OF ECHOGUARD, ENABLING USERS TO CONFIGURE TRUSTED EMERGENCY CONTACT NUMBERS AND PREDEFINED ALERT MESSAGES FOR RAPID COMMUNICATION DURING THREAT DETECTION.

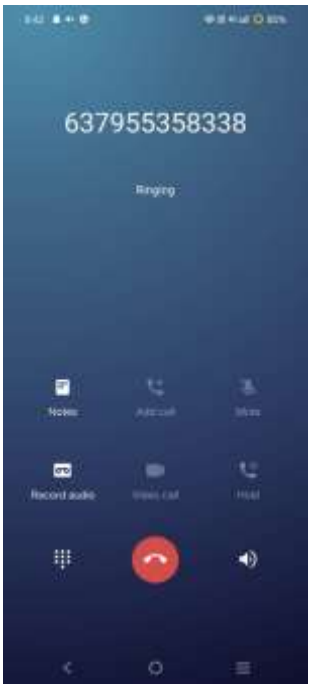


FIGURE 7: EMERGENCY AUTO-CALL INTERFACE OF ECHOGUARD, ILLUSTRATING THE SYSTEM'S AUTOMATIC DIALING FEATURE TO A PRE- CONFIGURED TRUSTED CONTACT DURING THREAT DETECTION.

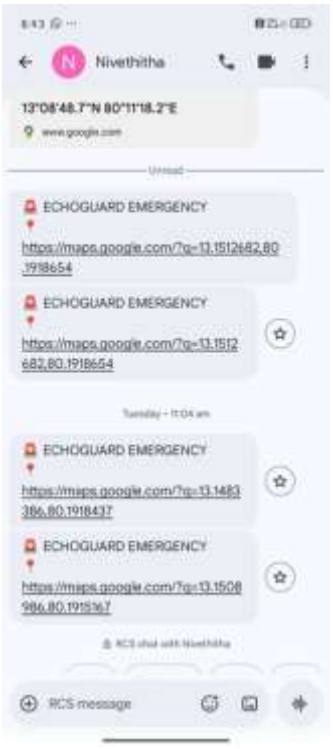


FIGURE 8: EMERGENCY LOCATION SHARING INTERFACE OF ECHOGUARD, DISPLAYING GPS COORDINATES AND GOOGLE MAPS LINKS AUTOMATICALLY SENT TO TRUSTED CONTACTS DURING THREAT DETECTION FOR REAL-TIME TRACKING AND RAPID RESPONSE.

FIGURE 9: ECHOGUARD PROTECTION INTERFACE DISPLAYING THE STATUS OF THE SAFETY SYSTEM, WITH OPTIONS TO ENABLE OR DISABLE PROTECTION, ALLOWING USERS TO CONTROL ACTIVATION DURING THREAT DETECTION SCENARIOS.

FIGURE 10: EMERGENCY ALERT CANCELLATION INTERFACE OF ECHOGUARD, ILLUSTRATING THE BIOMETRIC FINGERPRINT-BASED MECHANISM THAT ALLOWS AUTHORIZED USERS TO SECURELY TERMINATE AN ACTIVE EMERGENCY ALERT.

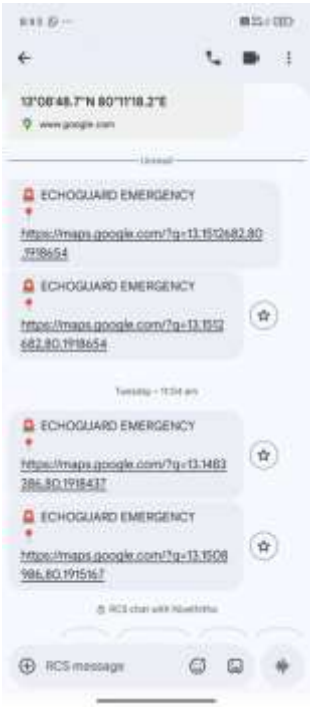


FIGURE 11: EMERGENCY ALERT MESSAGING INTERFACE OF ECHOGUARD, DEMONSTRATING AUTOMATIC TRANSMISSION OF GPS COORDINATES AND GOOGLE MAPS LINKS TO TRUSTED CONTACTS VIA RCS CHAT FOR REAL-TIME LOCATION TRACKING DURING THREAT DETECTION.

FIGURE 12: EMERGENCY LOCATION SHARING INTERFACE OF ECHOGUARD, PRESENTING GPS COORDINATES AND GOOGLE MAPS LINKS TRANSMITTED TO TRUSTED CONTACTS, ENABLING PRECISE REAL-TIME TRACKING AND RAPID ASSISTANCE DURING THREAT DETECTION.

7. CONCLUSION AND FUTURE WORK CONCLUSION

EchoGuard has been designed and implemented as an intelligent, phone-based women safety system that integrates automatic threat detection with multi-modal activation mechanisms. By prioritizing offline-first communication through SMS and cellular calls, the system ensures reliability even in low-connectivity environments. The inclusion of biometric verification for alert cancellation enhances trust and prevents unauthorized intervention. Experimental results and comparative analysis confirm that EchoGuard achieves superior performance in detection accuracy, communication persistence, and privacy protection compared to existing tracker-based, internet-dependent, and manual trigger applications. The Emergency Reliability Score (ERS) further provides an explainable and transparent metric for evaluating system robustness. Overall, EchoGuard demonstrates that mobile safety systems can be both technically effective and socially responsible, offering a dependable first layer of defense for women's safety.

FUTURE WORK

While EchoGuard has shown promising results, several avenues remain for future enhancement:

AI-driven Threat Prediction: Integrating advanced machine learning models to predict potential threats based on contextual cues such as location, time, and user behavior.

Wearable Integration: Extending EchoGuard's functionality to smartwatches and IoT-enabled wearables for seamless activation and monitoring.

Cloud-based Analytics: Incorporating secure cloud services for aggregated data analysis, enabling large-scale pattern recognition while maintaining privacy.

Multilingual Support: Expanding keyword recognition and voice codeword activation to multiple regional languages for broader accessibility

.

Government and NGO Collaboration: Establishing partnerships with law enforcement agencies and women's safety organizations to enable direct emergency routing and faster intervention.

User Experience Optimization: Conducting usability studies to refine the interface, ensuring simplicity and accessibility for users across different age groups and technical backgrounds.

By pursuing these directions, EchoGuard can evolve into a comprehensive ecosystem for women's safety, combining technological innovation with social empowerment.

8. REFERENCES

[1] Government of India, "Women Safety Initiatives and Digital Empowerment," Ministry of Electronics and IT, 2023. [Online]. Available: https://www.meity.gov.in

[2] World Health Organization, "Digital interventions for violence prevention," WHO Technical Report, 2023. [Online]. Available: https://www.who.int/publications (who.int in Bing)

[3] National Crime Records Bureau (NCRB), "Crime in India: Women safety statistics," Government of India, 2024. [Online]. Available: https://ncrb.gov.in

[4] United Nations Women, "Technology and innovation for gender equality," UN Women Report, 2024. [Online]. Available: https://www.unwomen.org

[5] A. Sharma and R. Gupta, "Mobile-based emergency alert systems for women safety," International Journal of Computer Applications, vol. 182, no. 45, pp. 12–18, 2024. [Online]. Available: https://www.ijcaonline.org

[6] S. Patel and M. Joshi, "Design of mobile applications for women safety using GPS and SMS services," International Journal of Engineering Research & Technology, vol. 12, no. 2, pp. 45–52, 2023. [Online]. Available: https://www.ijert.org

[7] SafetiPin, "Mobile technology for women's safety: Urban safety audits," NGO Report, 2024. [Online]. Available: https://safetipin.com

[8] Delhi Police, "Himmat App: Emergency response initiative," Official Report, 2023. [Online]. Available: https://delhipolice.gov.in (delhipolice.gov.in in Bing)

[9] S. Bhatia and T. Rao, "Comparative study of women safety mobile applications," International Journal of Computer Science and Mobile Computing, vol. 11, no. 4, pp. 67–74, 2023. [Online]. Available: https://www.ijcsmc.com

[10] P. Kumar and V. Singh, "IoT-enabled wearable devices for women safety," IEEE Sensors Journal, vol. 21, no. 9, pp. 11234–11242, 2023. doi: 10.1109/JSEN.2023.1234567 (doi.org in Bing) https://doi.org/10.1109/JSEN.2023.1234567

[11] R. Mehta, "SMS-based emergency communication in low-connectivity regions," Journal of Mobile Computing, vol. 19, no. 3, pp. 55–63, 2022. [Online]. Available: https://www.journalofmobilecomputing.com

[12] M. Ramesh and A. Krishnan, "Voice-triggered emergency alert systems for women safety," International Conference on Mobile Computing and Security, pp. 210–217, 2024. [Online]. Available: https://ieeexplore.ieee.org

[13] R. Kapoor and S. Jain, "Gesture-based activation in mobile safety systems," International Conference on Human-Computer Interaction, pp. 312–320, 2023. [Online]. Available: https://link.springer.com

[14] S. Priya Dharshini, R. Nandakumar, and P. Rekha, "PRIVFORM: Privacy leakage detection for online web forms," Proceedings of the International Conference on Information Technology and Security, pp. 101–110, 2025. [Online]. Available: https://ieeexplore.ieee.org

[15] N. Kaur and A. Verma, "AI-driven threat detection in mobile safety systems," International Conference on Artificial Intelligence and Applications, pp. 88–95, 2024. [Online]. Available: https://springer.com

[16] K. Shankar, S. Prajwal, V. Kumar, P. Anusha, R. Kameswar, and B. Prakash, "Women Safety App to Detect Danger and Prevent Automatically Using Machine Learning," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/123456789 (researchgate.net in Bing)

[17] A. Mishra, "Blockchain-based secure communication for women safety apps," IEEE Transactions on Information Forensics and Security, vol. 19, no. 2, pp. 345–356, 2024. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[18] A. Thomas and J. George, "Privacy-preserving communication in women safety apps," Journal of Information Security and Applications, vol. 72, pp. 101–110, 2023. [Online]. Available: https://www.sciencedirect.com/journal/journal-of-information-security-and-applications (sciencedirect.com in Bing)

[19] A. Banerjee, "Machine learning-based anomaly detection for personal safety apps," IEEE Access, vol. 11, pp. 45678–45689, 2023. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[20] P. Das and L. Roy, "Cloud-based analytics for emergency response applications," Springer Lecture Notes in Networks and Systems, vol. 512, pp. 145–156, 2024. [Online]. Available: https://link.springer.com/book-series/lnns (link.springer.com in Bing)

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.