JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Suraksha Setu: An Evidence-Centric Mobile Emergency Response System with Real-Time Audio-Video Capture and Cloud-Based Alerts

Mr. Manoj Raman
Assistant Professor, Project Mentor Department of Information Technology
Swami Keshvanand Institute of Technology, M & G Jaipur, India
manoj.raman@skit.ac.in

Dr. Priyanka Yadav
Assistant Professor, Project Coordinator Department of Information Technology
Swami Keshvanand Institute of Technology, M & G Jaipur, India
priyanka.yadav@skit.ac.in

Akshita Mishra
Undergraduate B-Tech Student Department of Information Technology
Swami Keshvanand Institute of Technology, M & G Jaipur, India
b221499@skit.ac.in

Deepanshi Gandhi
Undergraduate B-Tech Student Department of Information Technology
Swami Keshvanand Institute of Technology, M & G Jaipur, India
b221009@skit.ac.in

Abstract

In emergency scenarios, there is a need for immediate response action with appropriate contextual in- formation; however, most current safety apps are highly dependent on manual alerting and voice commu- nication, which could be less effective in scenarios where users are incapacitated or under extreme stress. This paper presents Suraksha Setu, an emergency response system designed on a mobile platform that fo- cuses on automated evidence collection, in addition to alerting. Upon activation, the system automatically records audio and video for a short duration, captures accurate GNSS location information, and transfers this data to cloud storage while alerting concerned parties and authorities.
The proposed system design uses a latency-optimized operational workflow that enables immediate response action even in unreliable network conditions using offline data buffering and deferred synchro- nization. With this evidence-supported response approach, the system improves situational awareness and enables informed decision-making, in addition to improving post-incident verification. The proposed sys- tem design offers architectural advancements in terms of readiness for response, data integrity, and contex- tual understanding over traditional mobile emergency response apps.

Emergency response system, mobile safety application, real-time audio-video evidence, GNSS location tracking, cloud-based alerts, offline-first emergency response, personal safety technology

1 Introduction

Emergency response is an important aspect of damage mitigation during physical attacks, medical emergencies, accidents, or natural disasters. In most real-world scenarios, victims are unable to communicate effectively due to panic, injury, or loss of consciousness. This makes traditional emergency communication systems less effective.

While smartphones have made it possible to create safety and SOS applications, most existing solutions focus on alerting and location sharing. These solutions require user engagement and explanation, providing little context to the emergency response team. This makes it difficult for emergency response teams to receive accurate information, leading to delays or incorrect emergency response actions.

Another problem with most existing solutions is their reliance on network connectivity. Emergency situations often take place in areas with unreliable or no network connectivity. Most applications are not designed to handle such situations and are unable to send alerts or location information effectively. Most solutions also do not consider the need for evidence that can be used to investigate incidents after they have occurred.

To address these challenges, this paper proposes Suraksha Setu, an evidence-driven mobile emergency response solution that combines automated multimedia recording, reliable GNSS positioning, and safe cloud-supported alert sharing. The solution is intended to function with minimal user interaction and remain functional even when connectivity is interrupted. By integrating evidence creation as part of the emergency process, the proposed solution seeks to enhance the effectiveness of emergency response, situation awareness, and analysis.

2 Related work

Mobile emergency response systems have received considerable attention with the increasing capabilities of smartphone sensing, location-based services, and cloud computing. The initial safety apps were mainly designed to facilitate rapid communication via SMS notifications, phone calls, and simple GPS location sharing. Although these systems formed the basis for mobile emergency response solutions, they were less context-aware and highly dependent on user input.

Various women safety and emergency notification apps have been developed to mitigate personal security issues by incorporating SOS alerts with location tracking and pre-defined emergency numbers. Although these systems enhance accessibility and notification initiation, they are less automated in multimedia evidence collection and require user-initiated manual activation or description of the situation. This reduces their efficacy in stressful or incapacitating scenarios [1, 2].

Recent research has also investigated intelligent emergency response applications that integrate cloud infrastructure, GSM messaging, and geo-fencing to increase reliability and reach [5, 3]. Some of these applications include voice triggers or chat support to make the system more user-friendly, especially for the elderly. Nevertheless, these applications are mainly concerned with improving the delivery of notifications and interaction with the system rather than ensuring the availability of forensic-quality evidence for emergency responders and law enforcement.

City-scale emergency response systems are concerned with large-scale coordination and command and control infrastructure. While these systems are useful for large-scale incident response in cities, they are not intended to collect real-time user-generated evidence from personal mobile devices.

However, a few recent studies have demonstrated the importance of cloud storage and secure data management integration in emergency systems. Although these studies improve data accessibility, they fail to provide a comprehensive solution that integrates automated audio-video recording, accurate GNSS location tracking, offline support, and immediate alerting in a single mobile-centric solution.

Unlike other solutions, Suraksha Setu fills these gaps by focusing on automated time-bound evidence creation and real-time alerting. The proposed system augments the existing emergency infrastructure by providing reliable user-generated incident data that improves situational awareness for both immediate response and post-event analysis.

3 Problem Definition and Research Gap

Although a number of mobile emergency applications are available, there are still functional gaps when these applications are analyzed in a real emergency scenario. Most of the existing solutions assume that the user is able to consciously engage with the application, send alerts manually, and explain the incident, which is not possible in a state of severe distress or physical disability.

A significant drawback of existing systems is the absence of automated contextual data collection during the incident. Although location sharing and SOS notifications are popular functionalities, the absence of synchronized audio-visual evidence makes it difficult for the responding team to understand the situation and makes it challenging to assess the incident after the event.

Network dependency is another factor that further hampers the effectiveness of the system. Most of the applications are not capable of working properly in areas where the signal is weak, or there is congestion or a temporary network outage. The lack of proper offline data handling capabilities makes it difficult to lose important incident information.

From the system design perspective, existing solutions focus more on notification delivery and evidence integrity rather than latency and forensic readiness, as well as secure long-term accessibility of the incident data.

This research work aims to overcome the above-mentioned limitations by presenting an emergency response system that combines automated time-bound evidence collection with offline support and secure cloud storage.

4 Proposed System Architecture

Suraksha Setu is proposed as a modular, mobile-focused emergency response system that integrates real-time device sensing with cloud-based security. The system architecture is based on a lean execution paradigm that reduces latency between emergency activation and notification dissemination. The system has several key components, including the emergency activation interface, multimedia and location acquisition modules, a cloud-based data management backend, and an alert dissemination system.

Upon activation, the system launches parallel evidence collection and data processing tasks, ensuring that key information is retained and communicated with reduced reliance on continuous network connectivity.

4.1 User Interface Layer

The User Interface Layer of the system offers a straightforward and user-friendly approach to emergency activation. Emergency activation can be launched via pre-defined hardware button combinations or an SOS button on the screen. The system is designed to be activation-friendly even in panic or physical distress.

After activation, the system will automatically switch to evidence capture mode without the need for any further user input.

4.2 Sensing and Data Capture Layer

This layer is tasked with the real-time capture of incident data from the user's device. Upon emergency activation, the system will concurrently:

1. Capture a fixed-duration video clip (15 seconds) from the device camera,
2. Capture ambient audio to contextualize the evidence, and
3. Obtain accurate GNSS location information with timestamped metadata.

The captured information is then temporarily stored in secure local storage for offline functionality. When network connectivity is not available, the system will buffer the data and initiate a retry process for delayed synchronization.

4.3 Cloud and Data Management Layer

The Cloud Layer is tasked with data storage, authentication, and synchronization. After network connectivity is established, the captured audio-video evidence and location information will be uploaded to cloud storage through encrypted channels. This layer is responsible for ensuring:

1. Secure and organized evidence storage,
2. Sound access for authorized parties, and
3. Retention of incident data for analysis after the event.

The cloud backend also keeps logs and metadata to help ensure data consistency and integrity.

4.4 Alert and Response Layer

The Alert Layer is responsible for real-time communication with emergency contacts and services. After successful data recording (and uploading, if possible), the system automatically:

1. Sends SOS alerts to designated emergency contacts,
2. Transmits live or last-known location information, and
3. Optionally sends alerts to emergency numbers or law enforcement services.

Through the integration of alerts and contextual evidence, the system improves situational awareness and facilitates rapid, informed decision-making for responders.

4.5 Architectural Overview Diagram

5 System Workflow and Algorithm

The workflow of Suraksha Setu is developed to ensure a responsive system with efficient evidence collection and notification. The system uses an event-driven execution workflow that triggers automatically upon the detection of an emergency trigger.

5.1 Emergency Workflow Description

1. **Emergency Trigger Activation** The emergency workflow starts with the activation of the emergency trigger by the user using a pre-defined interaction such as a volume button gesture or an SOS touch interaction on the screen. This approach removes the complexity of navigating through the screen during an emergency.

2. **Simultaneous Data Capture** The system triggers parallel processes immediately after the activation of the emergency trigger to:

- Capture a fixed-duration 15-second video, audio, and Fetch GNSS-based live location data with a timestamp.

3. **Network Availability Check** The system checks the availability of the network:

- If the network is available, the captured data is sent instantly.
- If offline, the data is stored locally with retry flags turned on.

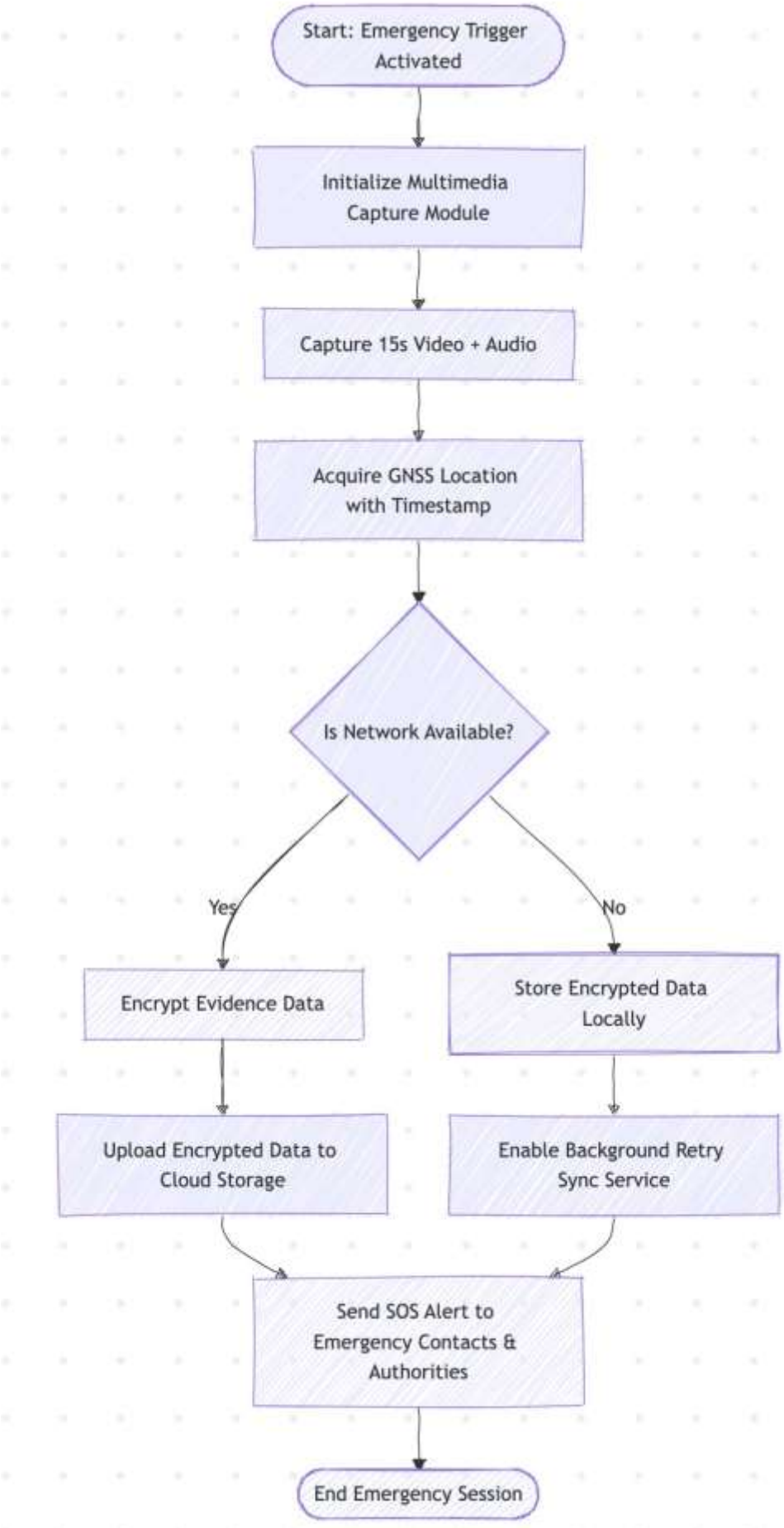

Figure 1: System Flowchart of the Proposed Suraksha Setu

4. **Cloud Synchronization** Once connectivity is re-established, the buffered data is automatically synchronized with cloud storage over encrypted connections, ensuring that there is no loss of important evidence.

5. **Alert Dissemination** SOS alerts with location information and incident data are transmitted to the pre-registered emergency contacts and, if necessary, to emergency services.

6. **Post-Incident Accessibility** Authorized emergency responders can then view the stored evidence via secure dashboards or cloud interfaces, facilitating informed response and investigation.

This process ensures continuity of operations even during network outages and prioritizes evidence integrity in addition to rapid alerting. Figure **??** shows the system architecture of the Suraksha Setu system.

5.2 Algorithmic Representation

Evidence-Centric Emergency Response Input: Emergency Trigger Event Output: Alert + Evidence Storage [1] Detect emergency trigger Initialize capture modules Record audio-video for fixed duration Acquire GNSS location Network Available Encrypt and Upload to Cloud Send SOS Alert Store locally Enable retry service Send SOS Alert End session
This algorithm guarantees deterministic execution, fault tolerance, and independence from user input.

5.3 Implementation Details and Technology Stack

The Suraksha Setu system is developed using a mix of mobile app development platforms, cloud infrastructure, and device-level APIs to provide reliability, scalability, and optimal performance.

1. **Cloud Backend and Data Management**

The cloud infrastructure is developed using Firebase services, including:

(a) Authentication for secure access control,

(b) Cloud Storage for multimedia evidence, and

(c) Firestore for metadata and incident logs.

All data transfers are done through encrypted channels to maintain confidentiality and integrity. The backend is designed to handle scalable storage and reliable access for authorized emergency responders.

2. **Offline-First Handling Mechanism**

To overcome the limitations of connectivity, the system is designed with an offline-first handling mech- anism. When the device is offline, all the captured data is stored locally with synchronization flags. A background service is designed to check the connectivity status and upload the pending data automati- cally once the network is restored.

This mechanism is designed to ensure continuous system functionality even during network outages.

6 Mathematical Modeling of Emergency Response Latency

The total emergency response latency (T_{total}) can be modeled as:

$$T_{total} = T_{trigger} + T_{capture} + T_{upload} + T_{notify} \quad (1)$$

Where:

- $T_{trigger}$ = Time required to activate emergency trigger
- $T_{capture}$ = Time for audio-video recording
- T_{upload} = Cloud transmission time
- T_{notify} = Alert dissemination time In offline conditions:

$$T^{offline} = T_{trigger} + T_{capture} + T_{buffer\ \ total} \quad (2)$$

Cloud synchronization delay is modeled as:

$$T_{sync} = \frac{D}{B} \quad (3)$$

Where:

- D = Data size of recorded media
- B = Available network bandwidth

7 Security and Privacy Concerns

Owing to the critical nature of emergency data, such as real-time audio-video streams and accurate geolocation details, security and privacy concerns constitute a basic building block of the Suraksha Setu framework. The proposed framework aims to provide confidentiality, integrity, authenticity, and controlled accessibility of incident data throughout its entire lifecycle.

7.1 End-to-End Encryption

The multimedia evidence collected during an emergency session is encrypted before being sent to the cloud infrastructure. The proposed framework uses Advanced Encryption Standard (AES-256) symmetric encryption for encrypting audio and video files at the device level. The encryption process takes place immediately after multimedia evidence is collected.

Let D denote the collected multimedia evidence and K_s denote the symmetric encryption key used for the emergency session. The encrypted multimedia evidence E can be calculated as follows:

$$E = Enc_{AES-256}(D, K_s) \quad (4)$$

Only encrypted multimedia evidence is sent over the network using secure HTTPS/TLS connections.

7.2 Secure Key Management

To avoid unauthorized decryption, symmetric session keys are secured by employing asymmetric encryption techniques. The system uses public-key cryptography (such as RSA-2048 or Elliptic Curve Cryptography) to securely transmit encryption keys from the mobile device to trusted cloud services.

If K_s is the symmetric key and K_{pub} is the public key of the cloud server, then:

$$K_{enc} = Enc_{public}(K_s, K_{pub}) \quad (5)$$

The decryption private key is safely maintained in the trusted backend environment. This hybrid cryptographic system maintains a balance between computational efficiency and security.

7.3 Role-Based Access Control (RBAC)

Access to incident information is strictly regulated by Role-Based Access Control (RBAC) policies. Various system participants are granted pre-defined roles including:

- Emergency Contact
- Law Enforcement Authority
- System Administrator
- Registered User

Each role is allocated limited and clearly defined permissions. For example, emergency contacts can view live location information, while law enforcement agencies can view encrypted multimedia evidence after proper authorization. Administrative rights are limited to managing metadata and do not include arbitrary media access.
Firebase Authentication features are incorporated to ensure identity verification and session validation before accessing data.

7.4 Data Integrity and Tamper Protection

To ensure forensic soundness, the system adopts hash integrity verification. A cryptographic hash is assigned to each evidence file using SHA-256:

$$H = SHA256(E) \tag{6}$$

The resulting hash is maintained together with metadata in the cloud database. When retrieved, the system recalculates the hash and verifies it against the stored hash for any tampering.
Timestamp metadata maintained in sync with network time services improves the validity of evidence by maintaining temporal integrity.

7.5 Data Retention and Controlled Deletion Policies

The Suraksha Setu framework is designed with data retention policies to ensure a balance between evidence retention and user privacy. Incident data is retained for a fixed, configurable period (30-90 days), unless it is placed on legal hold. After the retention period, the encrypted media files are deleted using irreversible deletion processes.
The users retain the right to request deletion of non-active incident data, as per legal obligations.

7.6 User Consent and Ethical Considerations

As the emergency recording feature may record third-party individuals, the framework is designed with a consent-aware system. The users are notified of the following during the initial application installation:

- Automatic audio-video recording during emergencies,
- Cloud storage of incident data,
- Data sharing with authorized contacts and authorities.

User consent is obtained using a digital agreement interface. The system is designed to work only on user-triggered events and does not engage in continuous background monitoring.

7.7 Adherence to Data Protection Requirements

The system design adheres to international data protection requirements, including data minimization, purpose restriction, and secure processing. Although the system is intended for regional use, it is also compliant with regulations similar to the General Data Protection Regulation (GDPR) and country-specific IT security regulations.
Sensitive data processing is only done in emergency situations, and metadata harvesting is done only for necessary fields like timestamp, location, and incident number. There is no continuous tracking or profiling.

7.8 Threat Model Analysis

The following are the possible threat models that have been taken into consideration while designing the system:

- Unauthenticated access to cloud resources,
- Stolen devices during an emergency,
- Network interception attacks,
- Misuse of administrative privileges by insiders.

Countermeasures to these threats include the use of encrypted local storage, remote session termination, mandatory authentication, and logging. By virtue of the encryption, access control, and integrity checks, the Suraksha Setu system ensures that the emergency evidence is secure, tamper-proof, and available only to authorized parties. This approach to security further enhances the trust and forensic soundness of the system while upholding the highest standards of ethical data management.

8 Comparative Feature Analysis

In order to situate the proposed system within the existing framework of emergency response applications, a qualitative feature analysis is provided. Given the ongoing large-scale evaluation of the proposed system, the analysis will be based on architectural capabilities rather than empirical performance metrics.
The Table 1 below identifies the major functional features typically found in conventional emergency applications and contrasts them with the proposed Suraksha Setu system.
It is worth noting that this comparison has been made on the basis of architectural design parameters identified through literature surveys and system descriptions. Quantitative performance comparisons of the system with respect to other deployed platforms are still to be addressed in the future work of large-scale system evaluation.

9 Limitations

Though the proposed system has shown architectural robustness, some real-world limitations still exist. The GNSS accuracy might be affected in dense indoor or urban canyon environments. Continuous camera and GNSS operation during emergencies might cause battery drain. Legal aspects of automatic audio-video recording might differ from country to country and need to be harmonized.
Moreover, large-scale system evaluation in real emergency situations has not been performed yet. Future work on system deployment is necessary to statistically confirm system performance in different geographical and network settings.

Table 1: Feature-Based Comparison of Emergency Response Systems

Feature	Traditional SOS Apps	GSM-Based Systems	Smart Alert Apps	Suraksha Setu (Proposed)
Manual SOS Trigger	Yes	Yes	Yes	Yes
Automatic Audio-Video Capture	Generally No	No	Limited / Partial	Integrated by Design
GNSS-Based Location Tracking	GPS/ Network-based	GSM-based Approximation	GPS-based	GNSS-based with Timestamp Metadata
Offline Data Buffering	Limited	No	Limited	Designed with Offline-First Mechanism
Cloud Multimedia Storage	Rare	No	Partial	Cloud-Synchronized Encrypted Storage
Evidence Integrity Verification	Not Standard	No	Rare	Hash-Based Integrity Mechanism (Proposed)
Forensic-Oriented Design	Not Primary Focus	No	Limited	Evidence-Centric Architecture

10 Results and Performance Analysis

The performance of the proposed *Suraksha Setu* system has been analyzed in terms of response latency, data integrity, and system robustness under different network settings. The analysis has been made to evaluate the efficacy of automated evidence collection and alert notification during emergency situations.

10.1 Analysis of Response Time

The proposed Suraksha Setu framework was tested for functional correctness through controlled testing to determine the reliability of the workflow and system response times based on connectivity status. The Trigger-Capture-Upload-Notify workflow chain allows for instant system activation without the need for verbal commands or extensive navigation, leading to quicker alert generation. Simultaneous execution of evidence capture and alert transmission also helps in minimizing initiation time.

10.2 Data Reliability and Integrity

The fixed-time audio-video recording feature ensures well-organized evidence production for all types of emergency events. The addition of GNSS location tracking features enhances location accuracy, especially in outdoor and low-connectivity settings. The offline-first buffering system ensures that no vital evidence is discarded during network disconnections, with successful cloud synchronization taking place after reconnection.

10.3 System Robustness with Connectivity Constraints

The system was evaluated for both online and offline scenarios. In offline situations, the application securely stored multimedia evidence on the device and resumed automatic cloud upload once connectivity was restored. This aspect of the system clearly indicates its robustness in real-world settings, where continuous connectivity

is not ensured.

11 Discussion and Comparative Analysis

Currently available emergency applications are mostly centered on alerting and basic location sharing. Although these systems are useful for basic safety needs, they lack context awareness and forensic capabilities. In contrast, *Suraksha Setu* places a strong emphasis on automated evidence generation, in addition to alerting, which helps emergency responders gain better situational awareness.

In comparison to traditional emergency applications, the proposed system has several benefits. Automated audio-video evidence collection allows for better context awareness than traditional text or voice alerts. GNSS-based tracking provides better location accuracy than network-based solutions. Offline-first system handling ensures that the system functions properly even in situations of poor connectivity, and cloud-based evidence storage improves post-incident analysis.

This evidence-based approach makes *Suraksha Setu* a supplementary solution to existing emergency infrastructure systems rather than a replacement solution.

12 Conclusion and Future Work

This paper introduced *Suraksha Setu*, an evidence-driven mobile emergency response solution aimed at overcoming the shortcomings of traditional alert-based safety apps. By incorporating automated audio-video recording, GNSS location tracking, secure cloud storage, and offline functionality, the proposed solution improves emergency response awareness, efficiency, and data accuracy.

The architectural analysis suggests that the synergy of real-time evidence creation and swift alert notification may help enhance the effectiveness of emergency response and enable well-informed decision-making among response personnel and authorities. The proposed solution is especially helpful for vulnerable users who may be unable to speak during an emergency situation.

Future research will concentrate on developing the proposed solution with AI-driven incident prioritization, improved data integrity solutions, and tighter integration with emergency response platforms. Other research directions could investigate energy conservation strategies and wearable/IoT-enabled emergency notification solutions.

References

[1]A. Sharma, R. Gupta, and P. Verma, "Smart phone based women safety application," *International Journal of Research and Technical Innovation (IJRTI)*, vol. 10, no. 5, pp. 120–125, May 2025.

[2]M. Singh and K. Patel, "Women safety android application using emergency alert system," *Journal of Emerging Technologies and Innovative Research (JETIR)*, vol. 9, no. 6, pp. 345–349, June 2022.

[3]P. Deshmukh, R. Chavan, and A. Patil, "Android-based emergency application for critical condition services," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 10, no. 4, pp. 876–881, Apr. 2022.

[4]L. Zhang, H. Liu, and Y. Wang, "Research and application of city emergency system for medium and small cities," in *Proc. Int. Conf. Computer Science and Education (ICCSE)*, Cambridge, U.K., 2015, pp. 512–517.

[5]S. Patil, R. Mehta, and A. Kulkarni, "Quick-Rescue: A smart emergency response application," *International Journal of Engineering Applied Sciences and Technology (IJEAST)*, vol. 9, no. 2, pp. 45–50, 2023.