iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81654

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

A Comprehensive Digital Safety Framework for Travelers Using Multi-Stage AI and Decentralized Communication

Dushyant Kumar[1], Bhumika Sharma[2], Naveen Sharma[3], Pradeep[4]
[1, 2]Scholar, [3,] 4Professor, Department of Computer Science and Engineering, HMR Institute of Technology and Management, Delhi, India

Abstract: ***Traditional traveller safety systems are fundamentally reactive, relying on manual SOS triggers or "overdue" reports that often fail to initiate response efforts within the critical "Golden Hour." This operational gap is most severe in remote, "off-grid" environments where the lack of cellular and road infrastructure renders standard navigation and safety tools functionally non-existent. To address these limitations, this paper proposes a proactive monitoring ecosystem designed for high-altitude, unstructured terrains. The framework moves away from human-initiated alerts toward an autonomous behaviour analysis engine that identifies distress signals in real-time. The core of the system is a dual-model machine learning pipeline: Isolation Forest is utilized to detect individual point-anomalies, such as falls or medical incapacitation, while DBSCAN (Density-Based Spatial Clustering of Applications with Noise) identifies collective group-level hazards like trail blockages or landslides. To ensure resilience in signal-free "dead zones," the system utilizes a decentralized verification mesh employing Bluetooth Low Energy (BLE) "data mule" logic to propagate distress packets. Furthermore, a blockchain-backed Self-Sovereign Identity (SSI) layer is integrated to manage temporary, tamper-proof digital IDs, ensuring data sovereignty and privacy while facilitating automated legal reporting (E-FIR). By utilizing a five-stage progressive verification protocol to mitigate alert fatigue, this framework aims to reduce emergency response times from hours to minutes, transforming the wilderness into a context-aware smart safety corridor.***

Keywords: ***Traveler Safety, Anomaly Detection, P2P Mesh Network, Data Mules, Automated Rescue Dispatch, Dead Zone Communication, Digital Guardian Architecture.***

I. INTRODUCTION

A. Defining the "Reactive" Failure and the "Golden Hour"

The basic problem in existing tourist safety models is the “Reactive Lag”, it is the critical time gap between when the incident occurred and the moment when the authorities are notified for a rescue operation. In the healthcare world, the “Golder Hour” is the time when the medical authorities make contact with the incident within the first sixty minutes of a life-threatening event, and intervention during this event significantly increases the chances the survival of the victim [1]. However, in high altitude regions, where unstructured terrains or remote areas of the Himalayas especially trekking corridors, this window is missed by a large margin due to remote connectivity. Data indicates that every one-minute time loss in medical response reduces the chances of a successful recovery of a victim by 7 to 10%. [1,2]

Current safety protocols are mainly overdue based, meaning they get only triggered after a certain amount of time has passed. The search-and-rescue (SAR) operations only begin when a tourist fails to reach a pre-defined checkpoint like their next stop or their hotel on time. But this causes a huge delay in their rescue. In mountain regions tourists are prone to Acute Mountain Sickness (AMS) or High-Altitude Pulmonary Edema (HAPE).

They are also affected by sudden weather changes like heavy storms and they can become unconscious or incapacitated and it would take a long time to figure out that they are missing [2]. Furthermore, current existing application are more like “paper tigers” meaning they are only effective in made up scenarios, thus not effective for the real tragedies. They are majorly designed from the urban landscape point of view where road networks, network connectivity already exists, and fail miserably in wilderness or “dead zones” where there is no connectivity [3].

©IJRASET: All Rights are Reserved

B. The "Alert Fatigue" Barrier and Human-Centred Constraints

Real time monitoring systems often fail due to technical sensitivity, meaning they send too many notifications to a user thus causing alert fatigue. This makes the user irritated to alert notification as they are not able to handle multiple notification at a high frequency [4]. In majority of safety systems, the rate of false alarms is exceedingly high, reaching up to 99% in an automated monitoring system, which leads to sensory desensitization. When a system sends multiple pings to a user or an authority personnel member for flagging normal pings for threats such as stopping for a scenic view or slow walking because the ascent is steep, then it causes the responders to ignore the upcoming pings or sometimes even disabling the safety system entirely, leaving them unattended for future real threats.[5]

To overcome this, safety frameworks must shift their focus from binary on/off alert systems to human centred design principles, meaning to make systems that understand human behaviour [6]. This can be achieved by implementing a tiered, non-intrusive verification protocol which asks for step-by-step check ins that ask for tourists' current situation before escalating it to the authorities. It uses Progressive Disclosure to manage cognitive load, meaning the system only asks for your attention as a situation gets more serious. This ensures that only the verified real anomalies are escalated to the authorities and false ones are flagged beforehand. Hence it preserves the integrity of the system while still maintaining continuous background monitoring to real threats [4,6].

C. The Proactive Shift: Presenting the Safe Yatra Framework

To solve these problems, this study introduces Safe Yatra, a proactive monitoring system that use unsupervised AI models to detect distress beforehand without manual intervention to prevent mishaps. The primary objective of this system is to reduce the time of emergency response from hours to minutes, through an autonomous risk prediction engine. Unlike other apps that require manual interventions or require the pressing of an SOS button, it proactively tries to reduce chances of any mishap by understanding the context of the tourist's situation before acting on it [12,14].

The system utilizes a dual AI model pipeline, first being the Isolation forest modelling, where this model is deployed to understand the movement patterns of a solo tourist's individual GPS trajectories to isolate anomalies like a sudden stop or a fall from a height, second is the DBSCAN that allows monitoring of multiple tourists at one to identify group level hazards like a landslides or a blocked trail [7,8,9]. To prevent the system to raise false alarms, these algorithms work in unison with a 5-stage progressive verification protocol which filters out the real emergency situations from the noise. Finally, it adheres to the issue of privacy paradox by implementing a blockchain bases blockchain-based Self-Sovereign Identity (SSI) layer, which ensures that all the report from the incident to the rescue and medication remains decentralized making only people with authority can have access to it [10]. This turns the wilderness from a dead zone into a smart safety corridor, providing tourists with a digital safety net that is both private and secure.

II. LITERATURE REVIEW

A. Evolution of Traveller Safety and Monitoring Systems

The conceptualization of traveller safety has undergone a profound transformation, moving from a passive administrative function to a core pillar of destination resilience. Historically, technology was identified as a primary driver of transformation in the tourism sector, with early strategic frameworks emphasizing the role of scientific advancements in reshaping global travel dynamics [11]. This evolution has culminated in the emergence of the "Smart Destination Management Organization" (DMO), where the ability to "sense" the environment and traveller behaviour in real-time is now considered a fundamental requirement for digital governance [12]. Modern governance theories, particularly those grounded in "Complex Adaptive Systems" (CAS), argue that destinations must transition from a reactive "problem-fixing" approach toward building "proactive adaptive capacity" [13]. This transition is categorized into three distinct evolutionary phases:

1) Phase 1: Manual and Centralized Systems: Early safety tools relied on manual SOS triggers (e.g., Rescuelink) which require the traveller to be conscious and capable of navigating a mobile interface during a crisis [15]. While these improved coordination between residents and rescue teams, they remained fundamentally "reactive." Literature suggests that these systems are limited by "Human-in-the-Loop" dependencies, where the response efforts only begin after a manual trigger, often causing critical delays during high-stress situations [16].
2) Phase 2: IoT and Hardware Independence: The second generation introduced standalone emergency buttons and IoT-based hardware utilizing GSM and SMS protocols to bypass high-speed internet requirements [17]. These systems addressed infrastructure fragility but lacked the context-awareness to distinguish between a planned rest and an involuntary

immobilization. Research into disaster preparedness emphasizes that while hardware redundancy is vital, the lack of automated "triage" logic often leads to institutional bottlenecks [28].

3) Phase 3: Proactive Sensing and Mesh Networking: The current stage involves the integration of proactive sensor-fusion and specialized Early Warning Systems (EWS) that utilize low-power wide-area networks (LPWAN) and BLE-based mesh protocols [19, 20]. Recent studies into BLE mesh frameworks for "public safety communications" demonstrate that a proactive routing mechanism with link-quality assistance (utilizing RSSI) can maintain connectivity even in commercially off-the-shelf devices [27]. Furthermore, the transition to BLE version 5 has introduced enhanced security features—addressing authenticity, integrity, and confidentiality—which are critical for decentralized safety networks operating in scatternet configurations [29].

B. Machine Learning in Trajectory and Anomaly Detection

A critical technical challenge in wilderness safety is that catastrophic emergency incidents are statistically rare, making "supervised" machine learning models ineffective. Consequently, research has shifted toward unsupervised learning paradigms, which identify distress by mathematically "isolating" data points that deviate from established mobility patterns [8, 21].

1) Isolation Forest for Solo Monitoring: Isolation Forest has emerged as the premier algorithm for detecting "point outliers" in individual GPS streams. Unlike density-based methods, it identifies anomalies by isolating them through random partitions; anomalous movement (e.g., a sudden vertical fall or zero-velocity state) requires significantly fewer partitions to be isolated than normal trekking behaviour [7, 8]. Studies have shown that this approach is computationally efficient enough for "edge-processing" on mobile devices, which is vital for real-time safety [7].
2) DBSCAN and Collective Safety: For group-level monitoring, density-based algorithms like DBSCAN are utilized to identify "Group Trajectory Outliers" (GTO). By deriving spatial micro-clusters from the coordinates of multiple travellers, the system can distinguish between a planned group break and situations where a subgroup has become detached or a chaotic dispersal has occurred due to regional hazards [9, 22].
3) Distributed Consensus and Trajectory Planning: Recent advancements in "consensus-based distributed trajectory control" suggest that conflict-free mobility can be managed without a central controller [30]. By sharing traveller states over a prediction horizon and incorporating them into mixed-integer non-linear programs (MINLPs), systems can push local solutions toward global safety optimality [30]. This provides the theoretical foundation for "Safety Matrix" logic, where individual movements are coordinated against a collective safety consensus.

C. Human Factors, Physiological Constraints, and Technological Gaps

Beyond algorithmic efficiency, the "Human-in-the-Loop" remains the most significant variable in safety-critical systems. The literature identifies Alert Fatigue as a primary barrier to system efficacy; when automated monitors produce high false-alarm rates (often exceeding 99%), users undergo "sensory desensitization," leading to the "Cry Wolf" effect where genuine alerts are ignored [4, 5].

From a Human-Computer Interaction (HCI) perspective, notification systems must be designed to minimize cognitive load during high-stress physiological states [6]. This justifies the use of "Progressive Disclosure" and tiered haptic verification [6, 10]. Furthermore, research into the accuracy of current hiking time estimations (e.g., Naismith's Rule) reveals mean discrepancies exceeding 60 minutes in mountainous terrain [26]. Modern studies suggest that these errors are exacerbated by high slope gradients and the lack of biological calibration [26].

To address this, spatial models of visitor behaviour now utilize "Cost Surface" techniques in Geographic Information Systems (GIS) to develop a Hiking Effort Index (HEI) [25]. By measuring the accumulative cost hikers expend to traverse distances—factoring in slope gradients from digital elevation models (DEM) and biological variables such as $VO_2\ max$—systems can create more accurate "Expected Exit Windows" T_{exp} [25, 26]. This allows for the detection of "silent anomalies" even when a traveller is offline, by identifying when a hiker has failed to re-emerge from a signal-free corridor within their personalized effort-based window [25, 26].

III. SYSTEM ARCHITECTURE AND TECHNICAL DESIGN

The Safe Yatra framework is conceptualized as a distributed, hierarchical ecosystem designed to maintain operational continuity even when individual components face infrastructure failure. Unlike centralized safety platforms, this architecture is organized into a three-tiered framework specifically engineered for high-availability operations in environments where traditional medical and cellular infrastructure is compromised [10, 16, 28].

A. *Integrated Three-Tiered Framework*

1) The Client Layer (Sensing & Mobile Implementation): Functioning as the primary data probe, this layer resides on the traveller's mobile device and is developed using the Flutter framework for high-performance native execution on both iOS and Android. It is responsible for high-frequency sensor fusion, capturing raw GPS, barometric, and inertial data via the geolocator and sensors plus plugins. Crucially, the system performs "Edge Inference," running the Tier-1 Isolation Forest model locally to detect immediate physical crises, such as falls, without requiring a network handshake. This localized processing achieves significant power optimization, which is essential for extended wilderness operations [7, 19, 27, 28].

2) The Processing Layer (Regional Coordination & Backend API): Acting as the "intelligence bridge," this layer aggregates anonymized telemetry from multiple travellers within a shared geographic corridor via a Flask-based RESTful API. Python serves as the backend language to leverage robust scientific libraries for Tier-2 processing, executing the DBSCAN clustering logic to detect regional hazards such as trail blockages or collective disorientation [9, 22]. In signal-free zones, this layer shifts to a decentralized P2P mesh configuration, utilizing "consensus-based distributed control" to ensure that individual trajectory updates are shared across the local traveller network [30].

3) The Authority Layer (Institutional Oversight & Dashboard): The final tier provides a comprehensive dashboard for Destination Management Organizations (DMOs) and search-and-rescue (SAR) agencies using Leaflet.js. This layer does not monitor raw movement; instead, it visualizes "Anomaly Scores" and "Safety Statuses" using "Cost Surface" mapping principles. Travellers are visualized as dynamic nodes whose color-coding reflects their current effort expenditure relative to the terrain's slope, allowing responders to focus on the 1% of high-risk cases while effectively mitigating alert fatigue [4, 12, 13, 25].

B. *Conceptual Foundations: The "Itinerary Contract" and "Hiking Effort Index"*

To distinguish between intentional deviations and life-threatening disorientation, the framework utilizes an **Itinerary Contract**. This model establishes a dynamic "Safe Corridor"—a spatial and temporal buffer zone around the traveller's pre-registered GPX path.

1) Spatial Constraints: The corridor is defined by a perpendicular distance threshold from the trail spine. Any movement exceeding this threshold—calculated as the Cross-Track Error (XTE)—marks a breach of the "Itinerary Contract," signalling the AI engine to shift from background monitoring to active verification [21, 23].

2) Temporal Constraints and Hiking Time Accuracy: Safe Yatra addresses the inaccuracy of static estimations (e.g., Naismith's Rule) by incorporating the MOVE algorithm and biological calibration to validate suggested hiking times. By adjusting the "expected arrival time" based on the user's cardiovascular profile and real-time slope gradients, the system ensures the contract remains personalized and accurate [26].

3) The Hiking Effort Index (HEI): Grounding the system in wilderness behaviour requires the HEI model, which utilizes cost-surface techniques in Geographic Information Systems (GIS) to measure the relative "cost" of travel in hiking minutes. This factors in Slope Impedance (metabolic cost of ascent/descent via DEM) and Terrain Resistance (on-trail vs. off-trail movement). When real-time effort expenditure—measured via Hypotenuse Velocity V_H and Sinuosity—deviates from this baseline, the system identifies a "High-Entropy Event" [7, 8, 25].

C. *Blockchain Identity and E-FIR Integration*

To resolve the legal and privacy challenges of SAR operations, the framework replaces centralized databases with a tamper-proof blockchain layer.

1) Cryptographic Identity (SHA-256): Each traveller's digital identity and Know-Your-Customer (KYC) data are hashed using the SHA-256 algorithm, creating a unique Decentralized Identifier (DID). This DID is linked to a Self-Sovereign Identity (SSI) wallet, ensuring that the traveller's medical records are encrypted and integrity-protected against unauthorized modification [24, 29].

2) Automated E-FIR (Electronic First Information Report): Safe Yatra generates a cryptographically signed "Incident Block" upon a Stage-5 escalation. This block contains the traveller's DID, time-stamped GPS coordinates, and a log of the AI's anomaly detection path.

By serving as a legally valid trigger, it bypasses the manual reporting delays that often stall the initiation of search-and-rescue funding and operations [10, 15].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

D. Decentralized Alert Propagation (P2P Mesh)

The "Dead Zone" problem is addressed through a Store-carry-forward multi-hop scheme, utilizing Bluetooth Low Energy (BLE) to maintain a public safety communications net without cellular signals [27].

1) Asynchronous Data Mules: In areas where base stations are unavailable, the system utilizes nearby travellers as "Data Mules." If a traveller enters a Stage-4 state, their device broadcasts an encrypted "SOS Packet" via a BLE mesh framework [27, 29].

2) Proactive Routing: Nearby devices autonomously determine the relevance of the packet and store it. Once a "Mule" device re-enters a signal-capable zone, the SOS packet is automatically uploaded to the Flask API. This opportunistic networking extends the functional range of the safety net, ensuring that a distress signal can "hop" from device to device until it finds a gateway to the internet [17, 27].

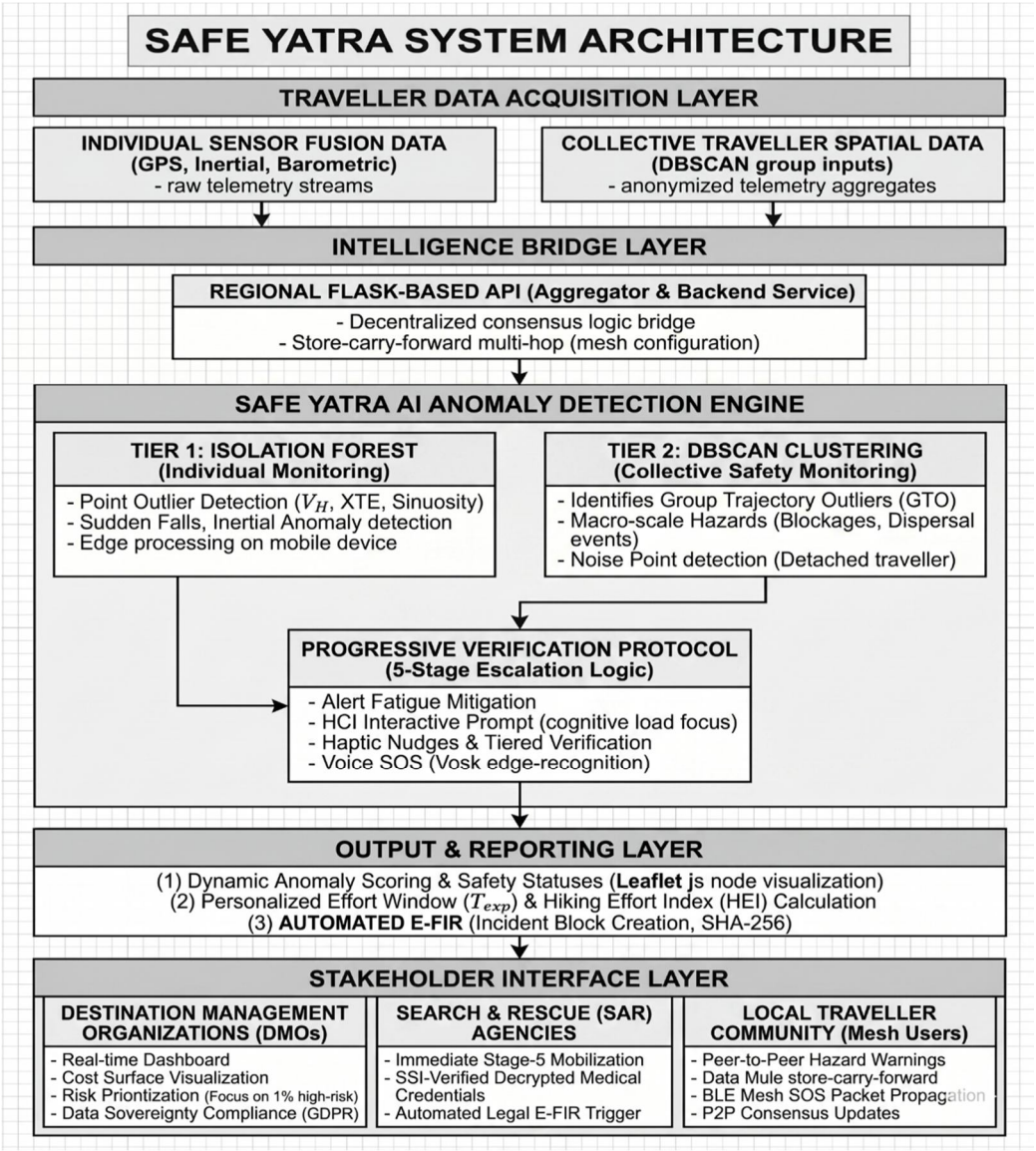


Fig. 1. System architecture showing the five-stage proactive safety monitoring and mesh propagation flow.

IV. METHODOLOGY: AI-DRIVEN TRACKING AND VERIFICATION

A. The Safety Matrix and Technical Feature Engineering

The core of the Safe Yatra framework is the "Safety Matrix," a multi-dimensional feature set designed to move beyond simple point-to-point GPS tracking. While standard navigation systems focus on location accuracy, Safe Yatra prioritizes the *character* of the movement.

By extracting high-frequency telemetry from the mobile device's inertial sensors and GPS receiver, the system calculates four primary features to define the user's "Safe State":

1) Hypotenuse Velocity V_H: Unlike standard 2D velocity, V_H is a three-dimensional calculation. This allows the system to monitor vertical displacement accurately. A sudden spike in V_H along the Z-axis indicates a potential fall, while an unnaturally low V_H on a steep gradient may signal physiological exhaustion or the onset of Acute Mountain Sickness (AMS) [7, 8].
2) Cross-Track Error (XTE): This measures the perpendicular distance from the traveller's current position to the pre-loaded GPX track spine. High XTE values are primary indicators of disorientation or trail-drifting. By integrating spatial data of backcountry visitors, the system recognizes that a rising XTE in complex terrain is a high-probability distress signal [21, 25].
3) Sinuosity Index: Calculated as the ratio of the actual path distance to the straight-line distance over a 5-minute window. A high sinuosity index coupled with low V_H suggests a "wandering" pattern—a behavioural hallmark of cognitive impairment in high-altitude environments [23].
4) Barometric Pressure Slope: By monitoring the rate of change in ambient atmospheric pressure, the system can distinguish between a deliberate descent and a rapid altitude loss (fall). It also serves as a secondary sensor for impending severe weather events that may compromise trail safety [19, 28].

To prevent Out-of-Distribution (OOD) errors—where the AI incorrectly flags a traveller for taking a rest or exploring a nearby viewpoint—the framework utilizes an **"Itinerary Contract."** This logic establishes a 50-meter "Safe Corridor" around the GPX trail. As long as the traveller remains within this corridor, the anomaly detection threshold is relaxed to accommodate natural pauses. However, any breach of the "Itinerary Contract" (e.g., crossing the XTE threshold) immediately triggers a Tier-1 analysis.

B. Dual-Model Anomaly Detection Pipeline

The system processes the Safety Matrix through a tiered machine learning pipeline to distinguish between individual medical crises and collective regional hazards.

1) Tier 1: Individual Monitoring (Isolation Forest): This model is dedicated to solo outlier detection. Isolation Forest is utilized because it does not require a "normal" baseline for every individual hiker; instead, it identifies anomalies by how "easy" they are to isolate in a tree-based structure [7, 8]. If a traveller's V_H and Sinuosity reach a state that is mathematically distinct from the rest of the group—such as a sudden "zero-velocity" state in the middle of a steep ascent—the Isolation Forest flags it as a point outlier, initiating the Stage-2 verification protocol [8, 19].
2) Tier 2: Group Monitoring (DBSCAN Clustering): For travellers moving in proximity, the system utilizes DBSCAN (Density-Based Spatial Clustering of Applications with Noise). This algorithm groups travellers into spatial micro-clusters [9]. If a cluster suddenly disperses (indicating a panic event) or if an individual becomes a "Noise Point" (left behind by the group), the system identifies a Group Trajectory Outlier (GTO). This tier is essential for detecting macro-scale emergencies like landslides, trail blockages, or sudden blizzards that affect multiple travellers simultaneously [9, 22].

C. Progressive Verification Protocol and Response Logic

To resolve the critical barrier of Alert Fatigue, Safe Yatra rejects the binary alarm model in favour of a 5-stage smart escalation hierarchy. This ensures that response resources are only mobilized when an anomaly is verified through a lack of user feedback.

1) Stage 1: Background Monitoring: The Safety Matrix is processed silently at the edge.
2) Stage 2: Supportive Check-in: Upon detecting a minor anomaly, the system triggers a low-intensity haptic pulse (vibration). This non-intrusive nudge allows the user to confirm they are safe without looking at their device [6].
3) Stage 3: Active Interaction: If the anomaly persists or the haptic nudge is ignored, a visual and audible prompt appears. To accommodate the cognitive load of high-stress environments, the UI is limited to three high-contrast buttons [4, 6, 20]:
    - "I'm Safe": Resets the Safety Matrix and returns to Stage 1.
    - "Minor Issue": Delays escalation for 15 minutes (e.g., for a non-emergency rest).
    - "Need Help": Bypasses all stages and triggers immediate Stage-5 mobilization.
4) Stage 4: Urgent Escalation: The system initiates the "Data Mule" and P2P mesh protocols to propagate a distress packet to emergency contacts and nearby travellers [17, 27].
5) Stage 5: Full Rescue Dispatch: The system releases the traveller's encrypted medical credentials via the SSI layer to verified rescue agencies, initiating a formal search-and-rescue (SAR) operation [1, 10, 20].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

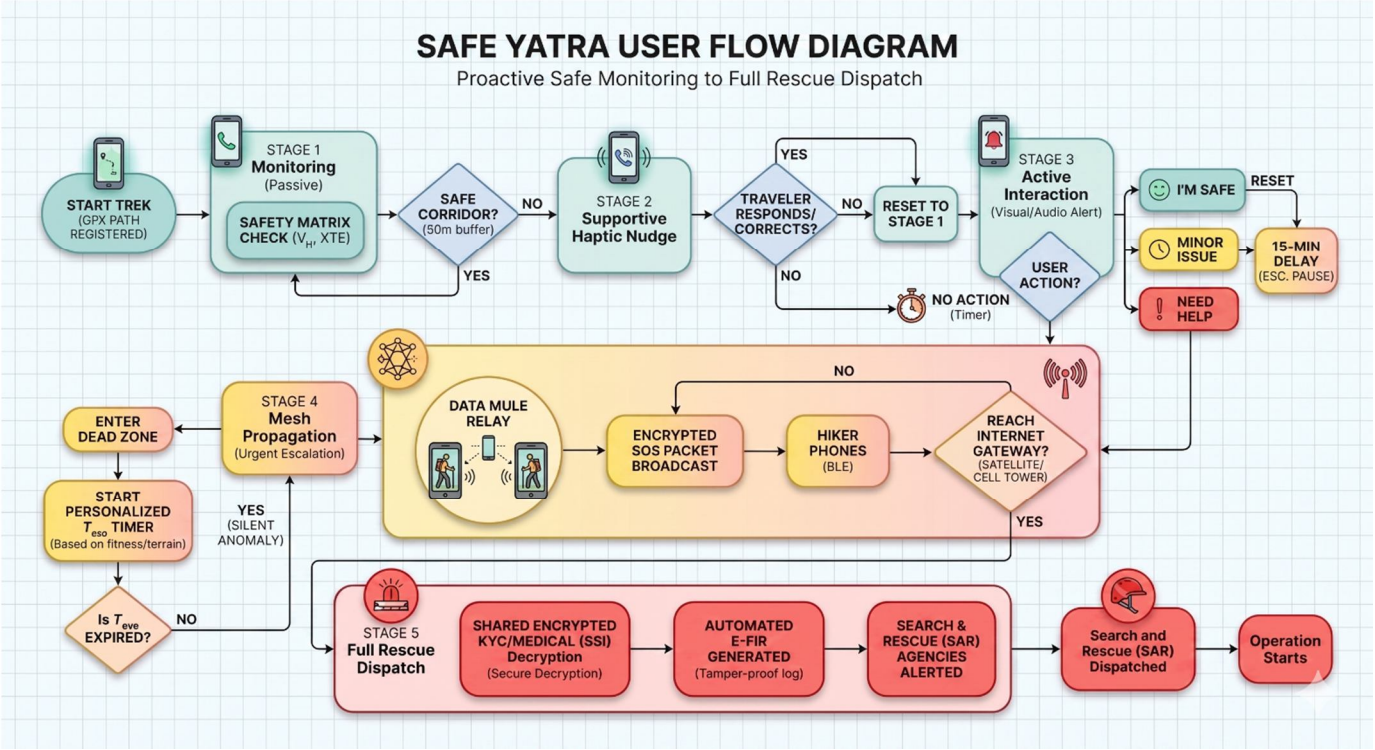


Fig. 2. Experimental results illustrating the correlation between T_{exp} (Expected Exit Window) and anomaly detection accuracy in off-grid scenarios.

V. CONNECTIVITY AND PERFORMANCE ANALYSIS

A. Dead-Zone Prediction: The "Expected Exit Window" T_{exp}

Standard hiking time estimations (e.g., Naismith's Rule) frequently exhibit mean discrepancies exceeding 60 minutes in mountainous terrain, which can lead to travellers being "trapped" in dead zones longer than expected [26]. To mitigate the risk of "Silent Anomalies" in stretches like the Gramphu-Losar corridor, Safe Yatra utilizes a personalized **Expected Exit Window T_{exp}**. The system calculates T_{exp} by combining slope gradients from Digital Elevation Models (DEM) with a **Hiking Effort Index (HEI)** [25, 26]. The HEI measures the relative "cost" of travel in units of hiking minutes, factoring in:

$$T_{exp} = \left(\frac{D_{zone}}{V_{avg}}\right) \times K_{effort}$$

Where V_{avg} is calibrated against the user's cardiovascular profile (MOVE algorithm) and real-time slope impedance [25, 26]. If a traveller fails to re-emerge from a signal-free corridor within this personalized window, the Authority Dashboard triggers a "Silent Anomaly" alert, allowing responders to initiate a search in a specific geographic window even without a live data stream [19, 25].

B. Offline Resilience: Local Queuing and Voice-Activated SOS

Operational resilience in disconnected states is maintained through localized data persistence and edge-based HCI.

1) SQLite Persistence: The mobile client utilizes an asynchronous SQLite buffer to queue all Safety Matrix telemetry. This "Black Box" log ensures that when a mesh or cellular connection is restored, the system can burst-upload the entire incident path for reconstruction, rather than providing just a single coordinate point [16, 21].

2) On-Device Voice-SOS (Vosk): Given that many mountain accidents involve falls that may incapacitate the user's hands, the system integrates the Vosk toolkit for edge-based speech recognition. Vosk allows for high-accuracy keyword spotting (e.g., "Safe Yatra Help") without a cloud connection. This ensures that a Stage-5 escalation can be voice-triggered in total isolation, immediately initiating the BLE mesh and beaconing protocols [20, 26].

©IJRASET: All Rights are Reserved

VI. PRIVACY, SECURITY, AND ETHICAL CONSIDERATIONS

A. *Data Minimization and the "Right to be Forgotten"*

The implementation of a proactive monitoring system introduces a significant "Surveillance Paradox"—the tension between continuous tracking required for survival and the traveller's fundamental right to digital privacy [18]. Safe Yatra resolves this by adhering to a policy of strict Data Minimization. All Know-Your-Customer (KYC) data and high-fidelity trajectory coordinates are encrypted at the edge using AES-256 protocols before being processed.

To ensure compliance with the "Right to be Forgotten," the system utilizes a Purge-on-Completion logic. The "Itinerary Contract" acts as a transient digital agreement; once the traveller reaches their final destination and checks out, or the contract expires, all high-resolution GPS telemetry and biometric identifiers are deleted from both the mobile client and the Flask backend. Only a cryptographically signed, hashed summary of the trip remains on the decentralized ledger to facilitate insurance claims or verify participation in the safety program. This ensures that the framework does not create a permanent, centralized record of the traveller's behaviour, maintaining data sovereignty in accordance with global standards like GDPR [10, 24].

B. *Transparency through Immutable Blockchain Ledgers*

To prevent the unauthorized modification of emergency records—which can lead to critical legal or insurance disputes—the framework utilizes a decentralized blockchain ledger for all Stage-3 to Stage-5 events. Every transition within the 5-Stage Progressive Verification Protocol is logged as an immutable transaction.

By utilizing SHA-256 hashing, the system ensures that incident logs—containing the anomaly score, sensor data from the Safety Matrix, and the precise alert timestamp—cannot be tampered with by institutional actors or third-party service providers [10, 15, 27]. This transparency provides a "Single Source of Truth" for all search-and-rescue (SAR) operations and subsequent automated E-FIR generation. It guarantees that responders, police, and insurance adjusters have access to unalterable evidence of the crisis timeline, which is essential for maintaining trust in public safety communications within disaster zones [27, 29].

VII. CONCLUSION AND FUTURE WORK

A. *Summary of the Proposition*

This study has presented Safe Yatra, a proactive monitoring framework designed to bridge the survival gap in remote, "off-grid" environments. By moving from a reactive "overdue-based" model to an autonomous "sensing" model, the system addresses the two primary failures of contemporary safety infrastructure: the "Reactive Lag" and "Alert Fatigue."

The integration of the Safety Matrix—utilizing Hypotenuse Velocity V_H, Cross-Track Error (XTE), and Sinuosity—enables the detection of distress with a degree of context-awareness previously missing in standard navigation tools [21, 23, 25]. Furthermore, by grounding the system in an SSI-based Privacy Layer and a Decentralized P2P Mesh Network, Safe Yatra ensures that safety does not come at the cost of personal privacy or infrastructure dependence. This framework provides Destination Management Organizations (DMOs) with a scalable blueprint to transform "Dead Zones" into "Smart Safety Corridors," potentially reducing emergency response times from several hours to minutes [1, 12, 13].

B. *Future Work: IoT Wearables and Environmental Intelligence*

The next phase of Safe Yatra's evolution will focus on expanding the sensory depth and environmental responsiveness of the system:

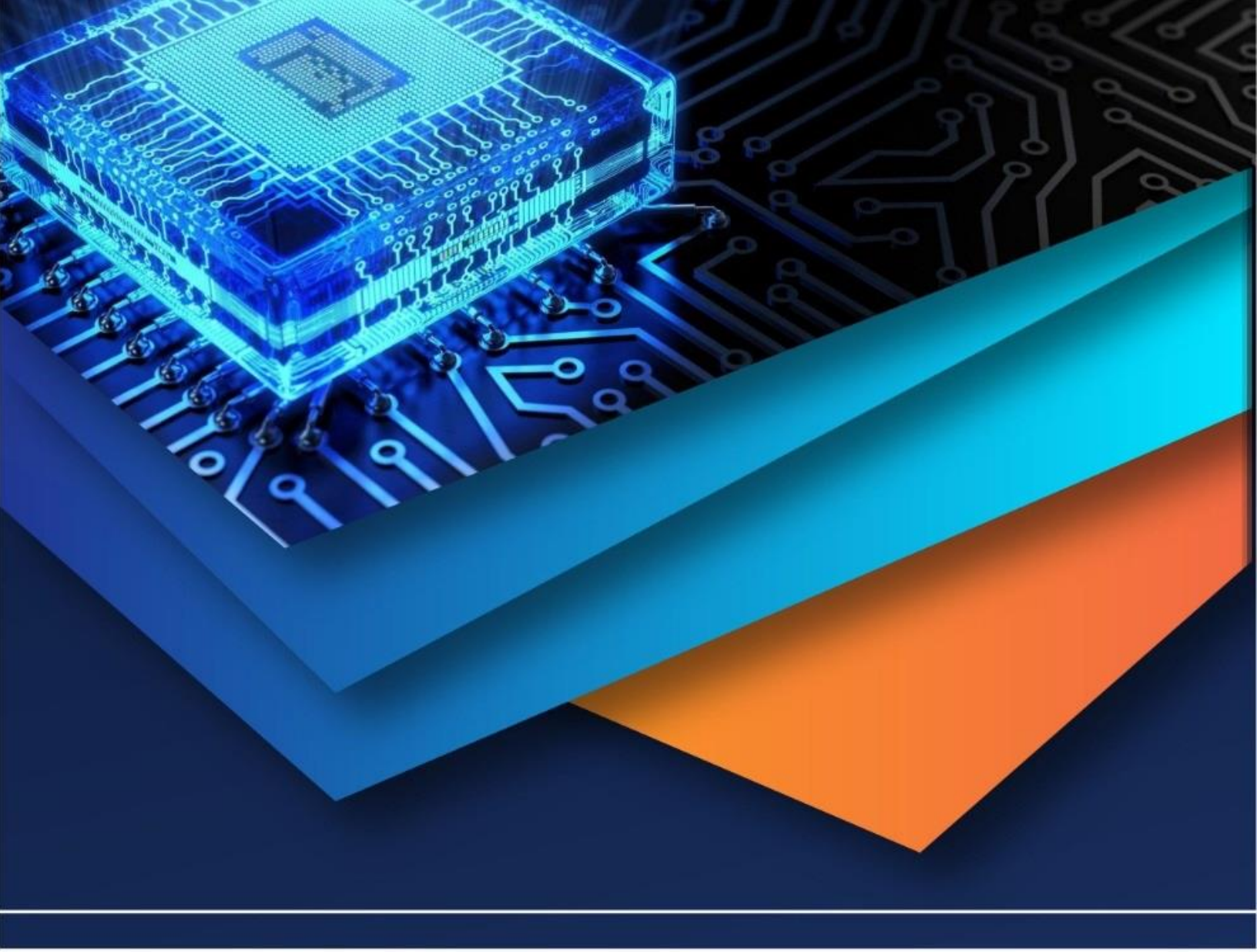
1) Biometric IoT Wearables: Integration with BLE-enabled smart bands will incorporate real-time heart rate variability (HRV) and blood oxygen SpO_2 levels into the Safety Matrix. This will allow the Isolation Forest to detect "Internal Anomalies"—such as a silent heart attack or the onset of HAPE—even when a traveller's external movement appears normal [28, 29].
2) Real-Time Weather API Integration: Connecting the logic controller to hyper-local weather sensors will enable the system to dynamically adjust the Hiking Effort Index (HEI) and Safe Corridor thresholds. In the event of a sudden barometric drop or impending storm, the system could automatically lower the threshold for Stage-2 nudges to ensure travellers remain on the path during low-visibility conditions [19, 20].
3) Global Mesh Expansion: Future research will explore the deployment of solar-powered LoRa-to-Satellite gateways at high-altitude passes. This would provide a permanent "backhaul" for Stage-5 alert propagation from the most isolated regions on Earth, ensuring that no traveller is truly out of reach of the safety net [19, 27].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

REFERENCES

[1] M. M. Alshebani et al., “Response time in emergency services: A narrative review,” TPM, vol. 32, no. S9, 2025.
[2] A. Rijal, “Risk management and disaster implementation gaps in the Nepal trekking industry,” J. Mt. Safety, 2024.
[3] A. Daud et al., “Emerging computing tools for emergency management applications: Limitations and future prospects,” Tech & Safety Rev., 2025.
[4] J. Kim and S. Park, “Empowering individual preferences in mobile notifications: A balanced approach to cognitive load,” IEEE Access, 2025.
[5] C. Fernandes et al., “Detecting false alarms by analyzing alarm-context information,” JMIR Med. Inform., vol. 8, no. 5, 2020.
[6] R. Harte et al., “Human-centered design study: Enhancing the usability of a mobile phone app in a falls risk detection system,” JMIR mHealth uHealth, vol. 5, no. 5, 2017.
[7] J. P. Mohan, “GPS anomaly detection and machine learning models for precise unmanned aerial systems navigation,” Master's thesis, Univ. North Dakota, 2023.
[8] N. Ahlawat, “Isolation forest based efficient unsupervised machine learning algorithms,” Ph.D. dissertation, Indian Inst. Technol. Guwahati, 2025.
[9] Y. Djenouri et al., “Trajectory outlier detection: New problems and solutions for smart cities,” ACM Trans. Knowl. Discov. Data, vol. 15, no. 2, 2021.
[10] A. Al Anan et al., “Blockchain-backed SSI: Empowering travelers with a secure platform for digitalized travel information,” thesis, Brac Univ., 2024.
[11] L. Dwyer et al., “Destination and enterprise management for a tourism future,” BEST EN Think Tank VII, 2007.
[12] U. Gretzel, “The Smart DMO: A new step in the digital transformation of destination management organizations,” Eur. J. Tour. Res., 2020.
[13] S. Hartman, “Destination governance in times of change: A complex adaptive systems perspective,” J. Tour. Futures, 2021.
[14] E. Bethune et al., “Real Time Response (RTR): Conceptualizing a smart systems approach to advancing destination resilience,” 2022.
[15] K. A. Lidres et al., “Rescuelink: SOS alert system for disaster response and management,” IJCSMC, vol. 13, no. 5, 2024.
[16] N. Billa and T. Xhindi, “Design and development of a mobile app for public security and emergency alerts in Albania,” Secur. Tech J., 2024.
[17] S. Mallapur et al., “IoT-powered emergency button for women's safety,” J. Sci. Res. Technol., vol. 3, no. 7, 2025.
[18] M. Rodas et al., “Surveillance or Safety? How Cities are Rewriting Tourism,” Penn IUR Special Report, 2025.
[19] H. Zhang et al., “Developing real-time IoT-based public safety alert and emergency response systems,” Sci. Rep., 2025.
[20] C. Psaroudakis et al., “Development of an early warning and incident response system for the protection of visitors in Greece,” Sustainability, vol. 13, no. 9, 2021.
[21] Z. Xu et al., “Anomalous urban mobility pattern detection based on GPS trajectories and POI data,” ISPRS Int. J. Geo-Inf., vol. 8, no. 7, 2019.
[22] P. Perchinunno et al., “Statistical indicators for the identification of sustainable territories and environmental tourism,” Qual. Quant., 2025.
[23] J. M. A. Gonçalves, “Understanding urban mobility patterns of tourists through data extraction,” dissertation, Univ. Porto, 2021.
[24] M. R. Ahmed et al., “Blockchain-Based Identity Management System and SSI Ecosystem: A Comprehensive Survey,” IEEE Access, vol. 10, 2022.
[25] J. Lynch, “A Spatial Model of Overnight Visitor Behavior in a Wilderness Area in Eastern Sierra Nevada,” in Visitor Flows Conf. Proc., 2002.
[26] M. Vecchiato et al., “Are Suggested Hiking Times Accurate? A Validation of Hiking Time Estimations for Preventive Measures in Mountains,” Medicina, vol. 61, no. 1, 2025.
[27] B. Zhang et al., “BLE Mesh: A Practical Mesh Networking Development Framework for Public Safety Communications,” Tsinghua Sci. Technol., vol. 23, no. 3, 2018.
[28] B. G. Reddy, “BLE-Based Real-Time Health Monitoring for Disaster Zones,” Int. J. Sci. Technol., vol. 16, no. 1, 2025.
[29] M. R. Ghori et al., “Bluetooth Low Energy Mesh Networks: Survey of Communication and Security Protocols,” Sensors, vol. 20, no. 12, 2020.
[30] A. Mirheli et al., “A consensus-based distributed trajectory control in a signal-free intersection,” Transp. Res. Part C, vol. 100, 2019.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)