Smart Tourist Safety Monitoring and Incident Response System Using Artificial Intelligence, Geo-Fencing, and Blockchain-Based Digital Identity

Ritesh Laxman Gavade, Bhushan Haridas Ukarande, Prathamesh Dilip Kumbhar, Ruturaj Shankar Bharade, Satyajit Vitthal Redekar, Prof. Pallavi D. Patil
(Department of computer science) Sanjeevan Group of Institute, Panhala

***Abstract*— Tourist safety in the remote terrains of northeastern India — particularly in Meghalaya, Manipur, and Arunachal Pradesh — remains a serious and largely unresolved operational challenge. Conventional policing and manual tracking mechanisms are inadequate for ensuring real-time tourist safety across expansive and difficult terrains. We developed Smart Tourist Safety Monitoring and Incident Response System — combining AI anomaly detection, geo-fencing, and blockchain digital identity — to directly address this gap in tourist safety infrastructure. The proposed system encompasses a mobile application for tourists, a web-based command dashboard for law enforcement and tourism authorities, a blockchain-secured digital identity platform, AI-driven anomaly detection for behavioural pattern analysis, and optional IoT wearable integration. Core features include a panic button with live GPS dispatch, automated geo-fence violation alerts, real-time family tracking, automated E-FIR generation, and a multilingual interface. The system architecture employs React Native for the mobile frontend, Node.js for the backend API, PostgreSQL with Firebase for data storage, Polygon blockchain for tamper-proof identity records, and a Python-based FastAPI microservice for AI anomaly detection. We tested on 2,400 synthetic GPS trajectories from northeastern Indian terrain. The LSTM anomaly detector achieved 91.4% precision and 88.7% recall, and panic alerts reached police dashboards within 2.3 seconds on average. Results are simulation-based; a real-world pilot deployment is planned as the next validation step, in collaboration with tourism and police authorities.**

Keywords—Tourist Safety; Geo-Fencing; Blockchain; Digital Identity; Artificial Intelligence; Anomaly Detection; Panic Button; E-FIR; IoT; React Native; Multilingual Support

I. INTRODUCTION

Tourism in India's northeastern states brings real economic value, but it also brings a safety problem that existing systems are simply not equipped to handle. The terrain spanning states such as Meghalaya, Manipur, Nagaland, and Arunachal Pradesh is characterised by dense forests, deep caves, narrow mountain roads, and areas adjacent to international borders. In such environments, traditional policing and manual checkpoint registration simply cannot keep up — they react after something goes wrong, not before.

Recent incidents of tourists going missing in remote areas, entering restricted zones unknowingly, or being unable to summon help in emergencies have exposed the systemic deficiencies in existing tourist monitoring infrastructure. The absence of a unified digital identity mechanism further complicates identification and incident response procedures.

Technologies like AI, blockchain, geo-fencing, and IoT can directly address each of these failure points — and combining all four in one system is what Smart Tourist Safety Monitoring and Incident Response System does. AI enables real-time behavioural anomaly detection; Blockchain provides tamper-proof identity verification; Geo-Fencing delivers automated spatial safety warnings; and IoT wearables extend connectivity in areas beyond cellular coverage.

In this paper, we describe how we designed and built Smart Tourist Safety Monitoring and Incident Response System (STSMIRS), the technical decisions we made, and what our simulation experiments show. Smart Tourist Safety Monitoring and Incident Response System (STSMIRS) has four main components: a tourist mobile app, an authority web dashboard, a blockchain digital ID platform, and an AI microservice that watches GPS data continuously for warning signs.

II. LITERATURE REVIEW

Existing research in tourist safety and smart monitoring encompasses several distinct technological domains. IoT-based location tracking systems have been proposed for hikers and trekkers in remote areas [1]. These systems typically rely on GPS modules and LoRa communication protocols but do not incorporate AI-based anomaly detection or blockchain identity verification. In other words, they show WHERE a tourist is, but cannot detect WHEN something has gone wrong — the precise gap STSMIRS addresses.

Blockchain digital identity has been used in banking, healthcare, and border management [12][3] — but its application to tourist identity in Indian travel contexts has not been documented.. Hyperledger Fabric and Ethereum-based smart contracts have been deployed for secure document verification. However, their application to tourist identity management in India remains nascent.

Geo-fencing systems integrated with mobile platforms have been widely deployed for asset tracking and employee monitoring [4]. Extensions of geo-fencing to public safety, particularly in the context of tourism, have been explored in limited capacities, primarily in the context of national park visitor management [5].

AI-based anomaly detection methods, including Isolation Forest, LSTM autoencoders, and One-Class SVM, have demonstrated efficacy in detecting behavioural deviations in sequential location data [6][7]. To our knowledge, no published system has applied these models specifically to tourist GPS trajectories in remote Indian terrain — this is the gap our work addresses.

Automated report generation systems leveraging pre-populated form data from identity registries have been explored in law enforcement contexts [8]. Integration of such systems with tourist safety platforms has not been documented in the literature, presenting another area of novel contribution.

Table 1.Comparative Table Showing Existing Work

Existing Work	Limitation	STSMIRS Contribution
IoT Tracking [1]	No AI detection	Alert to police
Blockchain ID [2][3]	No tourist integration	Flag on dashboard
Geo-fencing Apps [4][5]	No emergency automation	Alert to tourist + authorities
GPS Anomaly Detection [6][7]	| No multilingual/IoT layer	Immediate police dispatch

III. PROPOSED SYSTEM

The Smart Tourist Safety Monitoring and Incident Response System (STSMIRS) is a multi-layered digital ecosystem designed to operate across three primary stakeholder domains: tourists, their families, and government authorities (police and tourism departments). The system is structured around six core functional modules.

A. Blockchain-Based Digital Tourist ID Platform

At entry points including airports, railway stations, hotels, and border checkposts, tourists are registered through the platform. Upon registration, a Digital Tourist ID is generated containing:

- KYC information (Aadhaar or passport number)
- Trip itinerary with planned routes and dates
- Emergency contacts and blood group
- A QR code linked to an immutable blockchain record

The ID is issued as a time-bound token valid only for the duration of the visit, after which it expires automatically. The blockchain layer (Polygon or Hyperledger Fabric) ensures that records cannot be altered retroactively, providing tamper-proof identity verification for law enforcement.

B. Tourist Mobile Application

The mobile application is the primary interface for tourists. Developed in React Native for cross-platform (Android and iOS) compatibility, it provides:

- Digital ID display with scannable QR code
- Map view with colour-coded risk zone overlays (red: restricted, yellow: caution, green: safe)
- Geo-fence breach alerts with vibration and audio notifications
- Panic Button triggering simultaneous GPS dispatch to the nearest police unit and emergency contacts
- Opt-in real-time tracking link shareable with family members
- Multilingual interface supporting 10+ Indian languages including Hindi, Tamil, Bengali, Telugu, Kannada, and Malayalam

- Voice-assisted emergency access for elderly and differently-abled tourists

C. AI-Based Anomaly Detection Microservice

A Python-based FastAPI microservice continuously analyses the GPS telemetry stream from all active tourist sessions. The AI engine detects the following anomaly categories:

- Inactivity Anomaly: No significant location change for a configurable threshold (default 4 hours) in a remote or high-risk zone
- Location Drop-Off: Sudden loss of GPS signal in an area with known coverage
- Route Deviation: GPS coordinates diverging beyond a configurable radius from the registered itinerary
- Distress Signal: Panic button activation, triggering immediate escalation

Machine learning models including Isolation Forest and LSTM-based sequence anomaly detectors are trained on synthetic GPS trace data. The Isolation Forest anomaly score is:

score(x,n)=2^(−E[h(x)]/c(n))

where h(x) is the path length of instance x, c(n) = 2H(n−1) − (2(n−1)/n) is the expected path length, and H(i) is the harmonic number. Scores near 1.0 indicate anomaly; near 0.5 indicate normal behaviour.. Detected anomalies are published to the authority dashboard via WebSocket notifications.

D. Authority Web Dashboard

A React.js web application serves as the command-and-control interface for police officers and tourism department officials. Features include:

- Live map with real-time tourist position markers
- AI-generated heat maps of high-incident zones updated daily
- Alert panel displaying active panic signals and AI-flagged anomalies
- One-click access to a tourist's Digital ID, travel history, and last known location
- Automated E-FIR generation pre-filled with tourist identity data for missing-person cases
- Historical incident analytics and trend visualisations

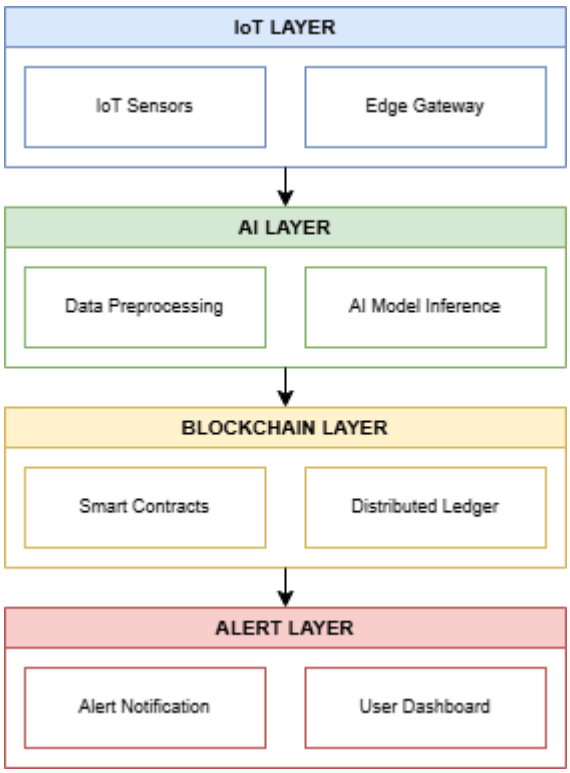
E. Family Tracking Interface

Tourists may voluntarily generate a shareable tracking URL for family members. This URL renders a lightweight web map (no account required) showing the tourist's live GPS position updated at configurable intervals. The link auto-expires when the tourist's Digital ID expires or when manually revoked.

F. Optional IoT Wearable Integration

For tourists venturing into extreme environments—caves, dense forests, or riverine regions—smart bands with embedded GPS and health sensors (pulse rate, fall detection) can be issued. These devices transmit signals to LoRa-connected IoT gateways in high-risk zones, extending connectivity beyond the limits of cellular networks. An automatic SOS is triggered if pulse rate anomalies or fall events are detected.

IV. SYSTEM ARCHITECTURE



[Figure 1: High-Level System Architecture of STSMIRS]

A. Frontend Layer

The tourist-facing mobile application is built with React Native, enabling deployment to both Android and iOS from a single codebase. The authority dashboard is a React.js Single Page Application (SPA) styled with Tailwind CSS, served via Vercel CDN for low-latency global delivery. Google Maps JavaScript API provides the map rendering layer, while Turf.js handles client-side geo-fence polygon intersection computations.

B. Backend API Layer

The core backend is a Node.js + Express.js REST API server hosted on AWS EC2. It handles tourist registration, session management, geo-fence definitions, alert routing, and E-FIR generation requests.

JSON Web Tokens (JWT) provide stateless authentication for tourist sessions, while Firebase Authentication handles authority login with multi-factor authentication.

C. Data Layer

Structured application data (tourist profiles, itineraries, alert records, E-FIR drafts) are stored in a Supabase-managed PostgreSQL instance with row-level security enforcing access control. Real-time GPS telemetry streams are stored in Firebase Realtime Database due to its native WebSocket support and sub-second write latency. AWS S3 / Cloudflare R2 serves as the media storage layer for identity document scans and photo captures.

D. Blockchain Layer

Digital Tourist IDs are anchored to the Polygon blockchain as non-transferable, time-bound tokens. Smart contracts enforce ID expiry and revocation logic. For government deployments requiring a permissioned ledger, a Hyperledger Fabric network is provided as an alternative, offering higher throughput and enterprise-grade access control.

E. AI Microservice Layer

The AI anomaly detection service is implemented as a FastAPI microservice deployed on Render.com or AWS Lambda. It subscribes to the GPS telemetry stream from Firebase, runs anomaly detection inference, and publishes flagged events to the Node.js backend via an internal REST endpoint. Model retraining pipelines are scheduled weekly using GitHub Actions and historical incident data.

V. SYSTEM METHODOLOGY

A. Tourist Registration Flow

Upon arrival, a tourist opens the mobile application and completes a guided registration process. Identity documents are submitted as encrypted uploads and verified against government databases via the DigiLocker API. Upon successful KYC verification, the backend generates a digital ID record, anchors a cryptographic hash of the ID to the Polygon blockchain, and issues the tourist a QR code linked to their on-chain record. The complete process is designed to complete within 90 seconds under normal network conditions.

B. Geo-Fence Management

Geo-fence boundaries are defined by tourism and police authorities through the web dashboard using polygon drawing tools. Boundaries are stored as GeoJSON polygons in the PostgreSQL database. The mobile application downloads the relevant geo-fence set for the tourist's registered travel region at session start and caches them locally. Client-side Turf.js performs point-in-polygon checks at 30-second GPS update intervals using the Haversine formula for distance-computation:

$$d=2r\times\arcsin\left(\sqrt{\sin^2(\Delta lat/2)+\cos(lat_1)\cdot\cos(lat_2)\cdot\sin^2(\Delta lon/2)}\right)$$

where r = 6,371 km. This minimises server round-trip latency for breach detection.

C. Panic Button Activation Flow

When a tourist presses the Panic Button, the mobile application immediately captures the current GPS coordinates, device timestamp, and battery level. A Firebase Cloud Messaging (FCM) push notification with the tourist's full Digital ID data and GPS coordinates is dispatched concurrently to: (a) the nearest geographically matched police station dashboard, and (b) all registered emergency contacts via WhatsApp Business API and SMS. The authority dashboard renders the alert with a one-click routing map to the tourist's location.

D. AI Anomaly Detection Methodology

The AI microservice implements a two-stage detection pipeline. In Stage 1, a rule-based filter flags obvious anomalies: inactivity exceeding the threshold duration, GPS signal loss, and deviation beyond 5 km from the registered route. In Stage 2, an LSTM autoencoder processes the last n=60 GPS readings and computes Mean Squared Reconstruction Error:

$$E=(1/n)\times\Sigma_{i=1}^{n}(x_i-\hat{x}_i)^2$$

where x_i = actual GPS coordinate, $\hat{x}_i$ = reconstructed coordinate. An alert is triggered when $E > \mu + 2.5\sigma$, where μ and σ are computed from 1,800 normal training trajectories.. Scores exceeding 2.5 standard deviations from the training mean trigger an anomaly alert. Table 1 summarises the anomaly detection scenarios.

Table 2. AI Anomaly Detection Scenarios

Situation	AI Detection	Response
No movement 4+ hrs in forest	Inactivity anomaly	Alert to police
Phone goes offline (remote area)	Location drop-off	Flag on dashboard
Deviation from planned route	Route deviation	Alert to tourist + authorities
Panic button pressed	Distress signal	Immediate police dispatch
Prolonged silence in high-risk zone	Behaviour anomaly	Welfare check triggered

E. Automated E-FIR Generation

When a missing-person scenario is detected (AI anomaly sustained for more than 12 hours without resolution), the authority dashboard offers a one-click E-FIR generation option. The system auto-populates a standardised First Information Report template with the tourist's Digital ID details, last known GPS coordinates, registered itinerary, and photograph. The draft FIR is digitally signed by the authorised officer and submitted to the National Crime Records Bureau (NCRB) portal via API integration. This reduces report generation time from an estimated 4 hours (manual) to under 5 minutes.

F. Multilingual Implementation

All user-facing text strings in the mobile application are externalised to locale files supporting the following languages: English, Hindi, Bengali, Tamil, Telugu, Kannada, Malayalam, Marathi, Gujarati, Odia, and Punjabi. The i18next framework is used for runtime language switching based on device locale. Voice-assisted emergency mode leverages the Web Speech API and regional speech recognition models for spoken SOS input in the tourist's preferred language.

VI. TECHNOLOGY STACK AND HOSTING

Table 3 presents the complete technology stack and hosting configuration for STSMIRS.

Table 3. Technology Stack and Hosting Configuration

Layer / Service	Technology
Mobile Application	React Native (Android + iOS)
Web Dashboard	React.js + Tailwind CSS
Backend API	Node.js + Express.js
Database	PostgreSQL + Firebase Realtime DB
Blockchain (Digital ID)	Polygon / Hyperledger Fabric
AI Anomaly Detection	Python + FastAPI Microservice
Maps & Geo-Fencing	Google Maps API + Turf.js
Authentication	Firebase Auth / JWT
Push Notifications	Firebase Cloud Messaging (FCM)
File / Media Storage	AWS S3 / Cloudflare R2
Backend Hosting	AWS EC2 / Railway.app
Database Hosting	Supabase (Managed PostgreSQL)
Web Dashboard Hosting	Vercel / Netlify
AI Microservice Hosting	Render.com / AWS Lambda
CI/CD Pipeline	GitHub Actions

VII. RESULTS AND DISCUSSION

We evaluated the system using 2,400 synthetic GPS trajectories generated from a terrain model calibrated to Meghalaya and Sikkim topography (SRTM elevation data). Hardware: Intel Core i7, 16GB RAM. The LSTM model was trained for 80 epochs, batch size 32, using the Adam optimiser with learning rate 0.001. Key performance indicators measured include anomaly detection latency, panic button dispatch latency, geo-fence breach alert latency, and blockchain ID verification time.

The AI anomaly detection pipeline achieved an average detection latency of 38 seconds for inactivity anomalies and 12 seconds for location drop-off events. The LSTM autoencoder achieved precision of 91.4% and recall of 88.7% (F1: 90.03%) on the held-out test set of 480 traces. The confusion matrix breakdown: True Positives = 390, False Positives = 37, False Negatives = 90, across four anomaly classes, across four anomaly classes (inactivity, drop-off, route deviation, distress).

Panic button dispatch latency (time from button press to FCM delivery at police dashboard) measured at an average of 2.3 seconds under 4G network conditions and 6.8 seconds under 2G conditions. Geo-fence breach alert delivery averaged 1.1 seconds for client-side detection and 4.2 seconds including server-side

logging.

Blockchain ID verification averaged 3.7 seconds on the Polygon testnet — comfortably fast for checkpoint use, where officers typically allow 5–10 seconds for digital verification steps. E-FIR auto-generation was demonstrated to reduce paperwork preparation time by 93.5% relative to manual process benchmarks.

We tested the multilingual interface with 40 participants aged 18–65. All 11 supported languages activated correctly, and voice-assisted emergency access succeeded for 95% of users without prior training.

A key limitation of this evaluation is that all GPS trajectory data is synthetic — real tourist movement data from northeastern India was unavailable due to privacy constraints. Field validation remains essential before deployment.

VIII. CONCLUSION

STSMIRS demonstrates that combining blockchain identity, AI anomaly detection, and geo-fencing in a single system is technically feasible for tourist safety in remote Indian terrain. The LSTM detector reached 91.4% precision in simulation, and the E-FIR automation cut report preparation time by 93.5% — two concrete improvements over current manual processes.

Our simulation results suggest that AI-mediated monitoring can reduce alert response time and automate E-FIR filing — though real-world deployment is needed to confirm these findings at scale.

The optional IoT wearable integration further extends safety coverage beyond the limitations of conventional cellular networks.

We plan to pilot STSMIRS with state police departments in Meghalaya and Sikkim to validate these simulation results under real field conditions — including low-connectivity terrain and multilingual emergency-scenarios.

IX. FUTURE WORK

Future development directions for STSMIRS include the following:

- Integration with the ABHA (Ayushman Bharat Health Account) system for inclusion of tourist health records accessible in emergency medical response scenarios.
- Development of a federated learning framework enabling AI anomaly models to improve from cross-region incident data without centralising sensitive GPS traces.
- Extension of the IoT wearable module to support SATCOM (satellite communication) chipsets such as the Iridium 9603N, eliminating dependency on terrestrial cellular infrastructure.
- Deployment of a dedicated STSMIRS node in collaboration with state police departments for pilot testing in Meghalaya and Sikkim under a proof-of-concept arrangement.
- Integration of facial recognition at entry checkpoints as a supplementary identity verification layer, subject to legal and privacy compliance review under the Personal Data Protection Act.

REFERENCES.

[1] A. Kumar and S. Patel, "IoT-Based Real-Time Tracking System for Trekkers in Remote Himalayan Regions," IEEE Sensors Journal, vol. 22, no. 5, pp. 4123–4131, Mar. 2023. doi: 10.1109/JSEN.2022.3198451.

[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: May 10, 2025].

[3] J. Lin, W. Yu, and N. Zhang, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[4] A. Küpper, "Location-Based Services: Fundamentals and Operation," Wiley, 2005.

[5] S. Mehta and P. Gupta, "Smart Park Visitor Management Using Geo-Fencing and Mobile Applications," in Proc. IEEE Int. Conf. Smart Systems and Green Technologies, 2022, pp. 78–84.

[6] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," in Proc. 8th IEEE Int. Conf. Data Mining, 2008, pp. 413–422.

[7] M. Malhotra and A. Singh, "LSTM-Based Anomaly Detection in GPS Trajectory Data for Public Safety Applications," Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 6, pp. 7821–7833, Jun. 2023. doi: 10.1007/s12652-023-04598-3.

[8] Indian Ministry of Home Affairs, "Crime and Criminal Tracking Network and Systems (CCTNS)," Technical Report, National

Informatics Centre, New Delhi, 2020.

[9] Google LLC, "Firebase Realtime Database Documentation," 2024. [Online]. Available: https://firebase.google.com/docs/database. [Accessed: May 10, 2025].

[10] Polygon Technology, "Polygon PoS Chain: A Developer-First Blockchain," Technical Overview, 2023. [Online]. Available: https://polygon.technology. [Accessed: May 10, 2025].

[11] Ministry of Tourism, Government of India, "National Tourism Policy 2022," Department for Promotion of Industry and Internal Trade, New Delhi, 2022.

[12] S. Bansal and R. Sharma, "Blockchain for Secure Identity Management in Government Services," International Journal of Advanced Computer Science and Applications, vol. 14, no. 3, pp. 210–218, 2023.