

Smart Tourist Safety Monitoring and Incident Response System Using AI

Dr. V. Janani¹, Aditya², Niharika Jena² & Rushikesh S²

¹Associate Professor & Head, Department of Information Science and Engineering
Sri Sairam College of Engineering, Bangalore

²Final Year BE (Information Science and Engineering), Sri Sairam College of Engineering, Bangalore

DOI: doi.org/10.34293/iejcsa.v4i4.161

Abstract - Tourists travelling through remote, forested, hilly, wildlife, and adventure destinations may encounter disorientation, restricted areas, accidents, health emergencies, crime, or communication failure. Conventional mechanisms often separate location tracking, emergency reporting, identity verification, and authority coordination, which can delay intervention when a tourist cannot communicate or when a location signal lacks behavioural context. This paper proposes a unified Smart Tourist Safety Monitoring and Incident Response System that combines a mobile application, GPS tracking, geo-fencing, artificial-intelligence and machine-learning analytics, blockchain-based digital tourist identity, authority monitoring, and optional IoT wearable devices. After registration, a tourist receives a Digital Tourist ID associated with the mobile application or wearable. Location, movement, activity, and optional health signals are processed to identify unsafe-zone entry, route deviation, prolonged inactivity, fall-like events, and explicit SOS requests. Alerts are delivered to an authority dashboard for verification, prioritisation, escalation, and response recording. The paper presents the research foundation, system architecture, operational methodology, implementation plan, and evaluation framework. It does not claim completed experimental results; accuracy, latency, scalability, privacy, and field effectiveness remain evaluation objectives.

Keywords—smart tourism, tourist safety, artificial intelligence, blockchain, GPS tracking, geo-fencing, IoT, emergency response, anomaly detection.

INTRODUCTION

Tourism increasingly depends on digital maps, smartphones, positioning services, online platforms, and sensor-enabled devices. These technologies provide the possibility of observing tourist movement with greater spatial and temporal detail than manual check-posts or periodic reporting. Geoinformatics research identifies GPS, mobile positioning, smartphones, Bluetooth, geocoded social media, and wearable or ambulatory sensing as important sources for understanding tourist mobility [1]. The same capabilities can support safety operations when they are connected to clear risk rules and an emergency-response process.

Safety challenges become more serious in remote or high-risk destinations. A tourist may leave a planned route, enter a restricted or hazardous region, become immobile after an accident, suffer a medical emergency, or lose connectivity. A GPS coordinate alone does not indicate whether the person is safe. Similarly, an SOS button is valuable but depends on the tourist being conscious, able, and willing to activate it. Geo-fencing can identify entry

into a defined area, but it does not by itself understand behaviour or coordinate responders. Blockchain can improve credential integrity and auditability, but it is not a complete monitoring or dispatch system.

This paper proposes an integrated safety platform that connects these functions rather than presenting them as isolated features. The system uses a Digital Tourist ID for controlled identity representation, GPS and geo-fencing for spatial context, AI/ML for movement and event analysis, SOS for direct reporting, optional IoT wearables for additional sensing, and an authority dashboard for operational response. The contribution is an evidence-bounded system design and evaluation plan; the paper does not claim that a field-validated implementation or universal novelty has already been established.

LITERATURE REVIEW

The literature relevant to the proposed system can be grouped into five related areas: digital tourist mobility, location-based and geo-fenced services, movement anomaly detection, blockchain identity and secure data exchange, and wearable or IoT emergency monitoring.

A. Digital Mobility and Location-Based Tourism Services

Tourist mobility research demonstrates that GPS, mobile positioning, smartphones, Bluetooth, and related sensing can capture detailed movement patterns [1]. Such data can support route reconstruction, destination analysis, and location-aware services. However, mobility observation is not equivalent to safety monitoring. A safety system must interpret a location against planned routes, destination rules, time, terrain, connectivity, and the person's current state.

Contextual geofencing and location-based tourism services provide a foundation for delivering notifications or services when a user enters a defined area. These approaches are useful for safe-zone, restricted-zone, hazard-zone, and assembly-point policies. Their limitation for the present project is that tourism information and notification are usually the primary purpose; verified emergency detection, identity verification, responder acknowledgement, and incident closure are not necessarily integrated into the same workflow [2]–[4].

B. Anomaly Detection from Movement and Sensor Data

Trajectory-anomaly research provides candidate methods for the analytical layer. Studies have investigated probabilistic mobility models, n-gram representations, context-aware detection, neural collaborative filtering, uncertainty-aware modelling, and privacy-preserving analysis [6]–[13]. These methods suggest that an abnormal event should be evaluated using more than a single coordinate. Useful features include distance from the expected route, speed, direction change, time spent in an area, sequence of visited locations, motion state, and contextual points of interest.

Wearable-sensor research also shows how motion and location context can be combined to detect spatial, timing, duration, and sequence anomalies [14]. This is relevant to fall-like events, prolonged inactivity, and unusual movement. Nevertheless, much of the existing work uses urban mobility, transport, generic trajectory, or assisted-living data rather than labelled tourist incidents in remote environments. Model transfer should therefore be treated as an engineering hypothesis that requires destination-specific validation.

C. Blockchain, Identity, and Data Protection

Blockchain has been considered in tourism for digital identity, trusted transactions, traceability, and smart-tourism services [15], [16]. Tourism identity research is relevant because a responder may need to verify a tourist without exposing more personal information than necessary. A permissioned or otherwise governed ledger can record credential status, consent events, hashes, and audit events while sensitive profile and location data remain in controlled off-chain storage.

Blockchain and distributed-ledger approaches have also been proposed for IoT access control using pseudonymous identities, policy enforcement, and smart contracts [17]. These ideas can support role-based sharing between tourists, operators, and authorities. They do not eliminate privacy risk: continuous location and health data remain sensitive, and immutable records require careful retention, consent, correction, and governance policies. Differential privacy, trajectory protection, and cybersecurity studies emphasise the trade-off between analytical utility and location privacy [11], [18], [19].

D. Wearables, Edge Processing, and Emergency Communication

Optional wearables can provide motion, heart-rate, fall, or location signals when a smartphone is unavailable or when additional context is needed. Edge or store-and-forward processing is especially relevant to remote destinations where cellular coverage is intermittent. Recent tourist-safety architectures illustrate combinations of mobile applications, offline maps, fall detection, long-range SOS communication, geo-fencing, blockchain logging, and edge intelligence [20]. Such work is closely related to the proposed direction, but it should not be treated as validation of the specific platform described in this paper.

RESEARCH GAP

The main gap is not the absence of individual technologies. Existing studies demonstrate location-aware services, geo-fenced notifications, movement anomaly detection, privacy protection, blockchain identity or access control, IoT data exchange, and wearable emergency communication. The gap is the limited evidence for an evaluated end-to-end workflow that integrates these components for tourist safety.

In particular, the reviewed evidence does not establish a single validated platform combining a Blockchain Digital Tourist ID, GPS tracking, AI anomaly detection, geo-fencing, SOS, tourist safety scoring, an authority dashboard, and optional IoT wearables with measurable emergency-response performance. This is a bounded conclusion from the retrieved literature and should not be written as a claim that no comparable system exists anywhere. The proposed research addresses the gap by treating detection and response as one operational cycle.

The research is also motivated by evaluation gaps. A component may work in isolation while the complete system fails because of false alarms, poor connectivity, battery limitations, privacy leakage, delayed authority acknowledgement, or unclear escalation responsibility. Therefore, integration, privacy, robustness, and response workflow must be evaluated together rather than reporting only model accuracy or successful application screens.

PROBLEM STATEMENT

Tourists in remote and high-risk destinations require timely assistance, but existing safety practices often depend on manual monitoring, user-initiated reporting, fragmented applications, or delayed communication. GPS tracking provides position but limited interpretation; SOS mechanisms may fail when a tourist cannot act; geo-fencing detects boundary events but does not necessarily predict risk; identity systems secure credentials without completing the monitoring loop; AI depends on representative and labelled data; and IoT devices depend on battery, device availability, and network connectivity.

The problem addressed by this research is to design and evaluate a privacy-aware system that can continuously receive tourist location and optional sensor data, identify explicit and implicit safety events, verify the relevant identity, notify authorised personnel, and preserve a controlled incident record. The system must support both direct SOS and passive detection while remaining usable, secure, explainable, and resilient under intermittent connectivity.

PROPOSED SYSTEM

The proposed platform is organised around a tourist mobile application, an optional IoT wearable, a secure identity service, a location and geo-fencing service, an AI/ML analytics service, an SOS and escalation service, a safety-score service, controlled storage, and an authority dashboard.

A. Digital Tourist ID and Identity Verification

During registration, the system creates a Digital Tourist ID linked to the tourist's consent choices, emergency contacts, travel information, and selected credentials. The identifier should be pseudonymous in operational telemetry wherever possible. Identity verification can use signed credentials and a permissioned ledger to confirm credential

status and record consent or audit events. Raw identity, health, and continuous location histories should not be placed on a public ledger.

B. Mobile Application and Geo-Fencing

The mobile application provides registration, consent management, map and route information, location sharing, safety status, emergency contacts, and SOS activation. Geo-fences define restricted, hazardous, safe, assembly, and service areas. A geo-fence event is enriched with time, speed, route context, connectivity, and the tourist's current monitoring state before an alert priority is assigned.

C. AI-Based Anomaly Detection and Safety Score

The analytics layer evaluates route deviation, prolonged inactivity, unexpected entry, unusual oscillation, abnormal speed, loss of expected movement, and optional wearable signals. A hybrid design is appropriate: deterministic rules handle high-confidence events such as SOS and restricted-zone entry, while ML models estimate the likelihood that a movement pattern is unusual in its destination and context. The safety score should be explainable and should indicate the contributing factors rather than presenting an opaque number.

D. Authority Dashboard and Emergency Response

The dashboard displays verified alerts, last known position, identity token, event type, confidence, time history, communication state, and escalation status. An operational workflow should include event creation, authentication, prioritisation, acknowledgement, responder assignment, communication with the tourist, escalation when acknowledgement is delayed, and closure with an audit trail. The goal is to connect an alert to an accountable action, not simply to display a point on a map.

SYSTEM ARCHITECTURE

The proposed data flow is: Tourist or wearable → mobile application and gateway → GPS and sensor data → communication layer → rules and AI/ML analytics → risk or anomaly event → controlled database and ledger records → authority dashboard → acknowledgement and emergency response.

The sensing layer receives GPS coordinates, motion observations, device status, and optional health data. The mobile device can perform basic local checks to reduce communication dependence. The communication layer uses cellular or Wi-Fi when available and can support buffering or store-and-forward transmission during outages. The backend normalises events and applies authentication, rate limits, and data-quality checks.

The analytics layer combines trajectory history, planned route, geo-fence policy, time, terrain or point-of-interest context, connectivity, and user-defined emergency information. High-risk events are sent to the response service. Operational records are stored in a conventional geospatial or time-series database for rapid queries. The ledger

stores only appropriate hashes, credential status, consent records, and audit events. The dashboard presents the minimum information required by each authority role.

Security and privacy are cross-cutting architecture requirements. Data should be encrypted in transit and at rest, access should be role-based, identity and telemetry should be logically separated, retention should be limited, and consent withdrawal should be supported. The design should also document what happens when the ledger, dashboard, mobile device, or network is unavailable.

A. Data Flow and Event Processing

The system processes information as a sequence of authenticated events rather than as an unrestricted stream of personally identifiable data. A mobile application or wearable first collects a signal and attaches a timestamp, device identifier, approximate quality indicator, and consent context. The gateway validates the event format, applies basic filtering, and queues the event when connectivity is unavailable. On reconnection, queued events are transmitted with their original timestamps and a delivery status so that delayed information is not mistaken for a live observation.

Events are classified into informational, warning, high-risk, and emergency categories. An informational event may represent routine movement or a successful arrival. A warning may represent a minor route deviation or entry into a monitored zone. A high-risk event may combine prolonged inactivity with an unexpected location or loss of the planned route. An emergency event includes a direct SOS, a confirmed fall-like event, or a critical health threshold. The classification should remain configurable because destination authorities may define different risk levels.

Operational telemetry requires fast retrieval for maps, timelines, and route analysis, so it should be maintained in a controlled database with retention limits. The ledger should not become a repository for raw GPS histories or health records. Instead, it can store a pseudonymous credential reference, consent status, event hashes, and selected audit information. This separation reduces unnecessary disclosure and allows authorised services to apply retention or deletion policies to sensitive data.

Figure 1 illustrates the proposed movement of data from tourist devices through secure communication and analytics to controlled storage and authority response. The architecture separates sensing, processing, storage, and operations so that a failure in one layer can be detected and handled without silently invalidating the entire safety workflow.

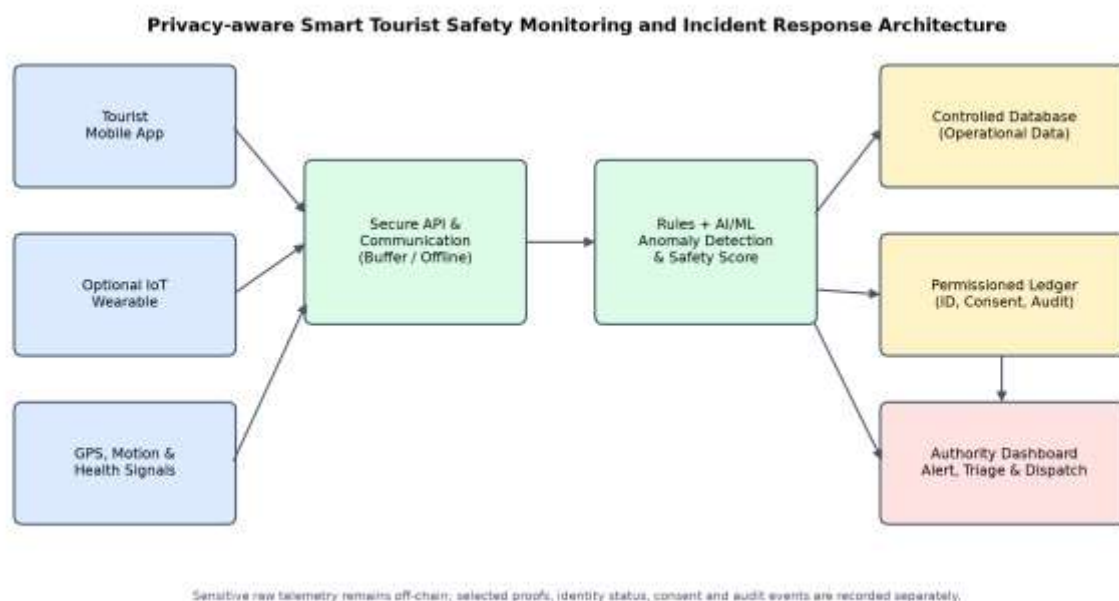


Figure 1 Proposed layered architecture for smart tourist safety monitoring and incident response.

The research methodology follows a design-and-evaluation sequence. First, requirements are collected from tourists, guides, destination operators, and response authorities. Requirements should cover incident types, response roles, connectivity conditions, consent, accessibility, and acceptable alert frequency. Second, a threat model and privacy-impact assessment identify risks involving identity theft, location exposure, spoofed GPS, unauthorised dashboard access, malicious alerts, and compromised devices.

Third, the architecture and protocols are designed, including the Digital Tourist ID, authentication, event schema, geo-fence rules, alert priorities, ledger transactions, data-retention policy, and escalation workflow. Fourth, a minimum viable prototype is implemented with a mobile client, backend, analytics service, storage layer, dashboard, and optional wearable gateway. Fifth, de-identified mobility traces and simulated incident scenarios are prepared. Scenarios should include normal tourism, route deviation, restricted-zone entry, prolonged inactivity, loss of connectivity, explicit SOS, and wearable fall-like movement.

For anomaly detection, data should be separated chronologically into training, validation, and test periods to reduce leakage from future behaviour. Evaluation should compare rule-only detection, conventional supervised or unsupervised models, and at least one privacy-preserving configuration. Thresholds should be selected using validation data and then fixed for the test set. The study should report false alarms by context because an unusual route may be benign in one destination and dangerous in another.

Finally, controlled experiments evaluate geo-fencing, alert delivery, authority acknowledgement, offline buffering, system availability, energy use, security controls, and usability. Field testing should begin with simulated or supervised scenarios before any live safety dependence. Since the current project material does not report a completed experiment, all performance values in this paper are evaluation targets rather than results.

B. Alert Classification

The system classifies incoming safety reports according to their urgency and potential impact on tourists. Each report is evaluated using the information available, such as its category, reported severity, location, time, and whether similar reports have been received nearby. Based on this assessment, the system assigns an alert level: **low**, **moderate**, or **high**.

Low-level alerts describe situations that may affect travel but do not indicate an immediate threat. Moderate alerts indicate a developing or localized concern for which travelers should exercise caution. High-level alerts represent a credible and time-sensitive risk that may require immediate action, such as avoiding an area or contacting local emergency services. The assigned level determines how the alert is presented to users and whether it is prioritized for review.

Classification supports timely communication; it does not establish that a report is verified. Where report reliability is uncertain, the system should communicate that uncertainty and avoid presenting an unconfirmed report as an official warning. Authorized reviewers can assess reports and update their status or classification as additional information becomes available.

C. Data Storage and Privacy Boundary

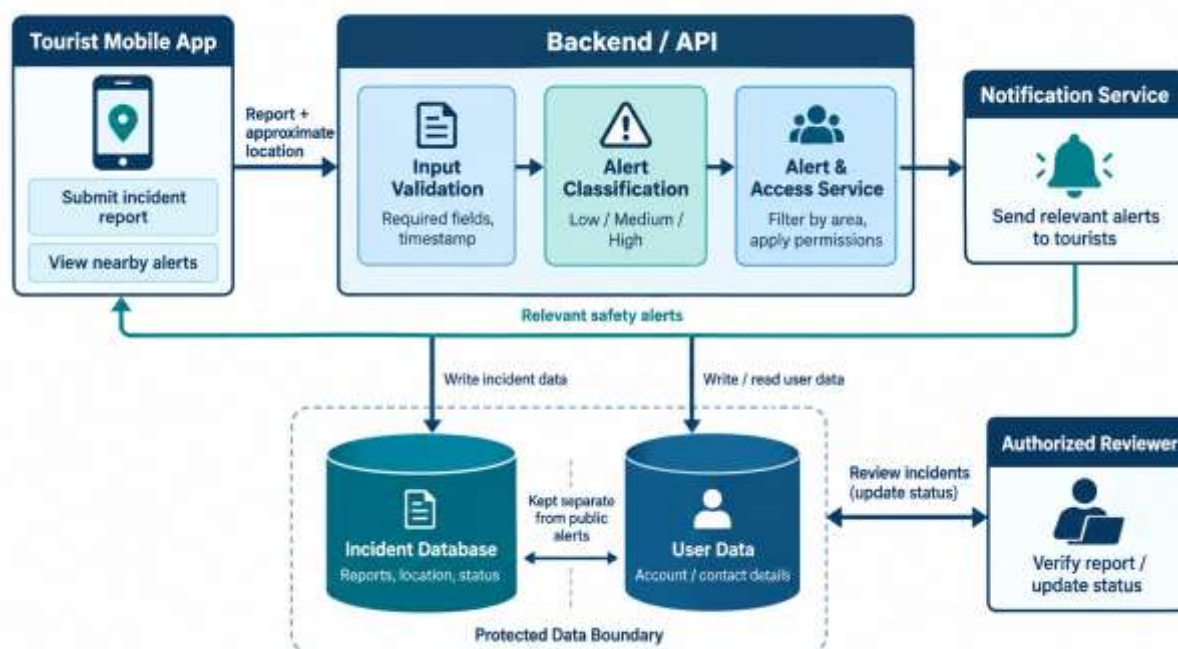
The system stores only the information needed to receive, assess, and communicate safety alerts. Report records may include the reported event category, description, approximate location, timestamp, alert level, and review status. Account or contact details, when collected, should be stored separately from public alert information and accessed only when needed to provide the service.

The privacy boundary separates information used for internal processing from information shown to other users. Public alerts should contain enough context to support safe decisions while excluding direct identifiers and unnecessary personal details. Location should be collected and retained at the level of precision required by the feature; precise or historical location data should not be exposed in public views.

Access to stored information should follow role-based permissions, with administrative and review functions limited to authorized personnel. Data should be protected during transmission and storage, and retained only for a defined operational period. These measures reduce unnecessary exposure while allowing the system to

maintain a useful record of reported incidents. The design should also provide a process for correcting or removing information when it is inaccurate or no longer required.

D. Architecture Diagram



METHODOLOGY

The proposed smart tourist safety system follows a user-centered, report-based methodology to collect safety information, assess its urgency, and communicate relevant alerts to tourists. The process consists of report submission, validation, classification, storage, review, and alert delivery.

First, a tourist submits an incident report through the mobile application. The report may include an incident category, a short description, the approximate location, and the time of occurrence. The application checks that required information is present before sending the report to the backend system.

Next, the backend validates the submitted data and assigns an alert level based on the reported severity and available context. Alerts are grouped into low, medium, and high levels to help prioritize information. This classification supports consistent processing, but it does not by itself confirm that an incident has occurred. Where review is available, an authorized reviewer can assess a report and update its status or classification.

The system stores incident information in a protected database. Account or contact details are kept separate from report information wherever practical. Access controls limit

who can view or modify stored data, and alerts shown to tourists contain only the information needed to communicate the reported risk.

Finally, the alert service selects relevant alerts for display in the application, for example based on the area a tourist is viewing. The tourist can review nearby safety information and make informed travel decisions. Thus, the methodology provides a structured flow from report submission to alert delivery while incorporating report review and privacy safeguards.

IMPLEMENTATION & EVALUATION

A. Implementation Plan

A practical prototype can use an Android or cross-platform mobile application with GNSS/GPS and native geo-fencing APIs. A REST or message-based backend can receive signed location and incident events. A geospatial or time-series database can support route and alert queries, while a Python-based service can host feature extraction and ML inference. A permissioned blockchain or distributed-ledger layer can manage credential status, consent, and audit hashes. A web dashboard can provide map-based monitoring, alert triage, acknowledgement, dispatch, and closure.

The implementation should favour reliability and maintainability over unnecessary technological complexity. Raw continuous location should remain in controlled storage; ledger writes should be limited to records that benefit from tamper evidence. The mobile client should cache critical configuration and queued events. Wearables should be optional so the core system remains useful when a tourist has only a smartphone.

B. Evaluation Parameters

The evaluation should include the following measures:

- Anomaly detection: accuracy, precision, recall, F1-score, false-positive rate, false-negative rate, calibration, and detection delay.
- Geo-fencing: boundary error, correct-entry and correct-exit detection, missed events, false alerts, and performance under noisy GPS.
- Emergency response: SOS delivery time, anomaly-to-alert time, authority acknowledgement time, escalation delay, and incident closure completeness.
- System performance: availability, throughput, concurrent users, backend latency, offline queue recovery, battery impact, and communication overhead.
- Security and privacy: authentication failures, unauthorised-access resistance, integrity of audit records, re-identification or privacy leakage risk, and effectiveness of role-based disclosure.
- Usability: task completion, alert comprehension, registration time, perceived burden, accessibility, and dashboard operator workload.

Results should be stratified by terrain or destination context, connectivity condition, device type, and incident class. A high overall F1-score would not be sufficient if

performance collapses during network outages or if false alarms overload authorities. The study should clearly distinguish experimentally measured results from expected outcomes and design objectives.

CONCLUSION

The evaluation should use repeatable scenarios rather than only screenshots or demonstrations. A normal-tour route can establish baseline location and battery behaviour. A restricted-zone scenario can measure boundary detection and alert generation. A route-deviation scenario can test whether the model distinguishes a genuine deviation from a permitted detour. A prolonged-inactivity scenario can test the interaction between motion signals, time thresholds, and user confirmation. SOS, loss of connectivity, delayed delivery, device restart, and authority acknowledgement scenarios should test the complete operational chain.

To determine whether integration adds value, the prototype should be compared with simpler configurations. A rule-only baseline can use geo-fence and fixed inactivity thresholds. A location-only model can exclude wearable or contextual signals. An AI configuration can use movement features without blockchain or dashboard integration. Ablation tests can then remove one feature at a time, such as route context, device-health status, or offline buffering. This approach helps identify whether a feature improves safety performance or only increases system complexity.

Synthetic incidents may not represent the full variety of real emergencies, and labelled tourist anomalies may be scarce. A model trained on one destination may not generalise to another because terrain, trails, transport patterns, and connectivity differ. GPS errors can be larger near dense vegetation, steep terrain, or buildings. User studies may also under-represent children, older travellers, people with disabilities, or visitors using low-end devices. These limitations should be reported with the evaluation rather than hidden behind a single aggregate score.

The expected contribution is a tested reference architecture and an evidence-based evaluation of the detection-to-response workflow. The work should demonstrate which components can operate together, quantify the cost of privacy and connectivity controls, and identify the conditions under which alerts are reliable enough for operational use. The contribution is not a claim that every emergency can be predicted automatically; direct SOS, human verification, and established emergency-service procedures remain important parts of the system.

This paper presented a proposed Smart Tourist Safety Monitoring and Incident Response System that integrates mobile sensing, GPS, geo-fencing, AI/ML anomaly detection, blockchain-based digital identity, optional IoT wearables, an authority dashboard, and an emergency-response workflow. The literature supports the feasibility of these component technologies, but the reviewed evidence is distributed across different

application domains and does not establish a single field-validated platform containing all functions with a common evaluation.

The proposed contribution is therefore an integrated, privacy-aware architecture and a methodology for testing whether integration improves detection-to-response performance under realistic conditions. The design must be evaluated for accuracy, false alarms, latency, connectivity resilience, privacy, scalability, usability, and operational workload. No quantitative performance result is claimed until the prototype and evaluation are completed.

REFERENCES

- [1] N. Shoval, "Sensing tourists: Geoinformatics and the future of tourism geography research," *Tourism Spaces*, 2018, doi: 10.1080/14616688.2018.1437768.
- [2] D. Martín, A. Alzua, and C. Álvarez Lamsfus, "A contextual geofencing mobile tourism service," Springer book chapter, 2011, doi: 10.1007/978-3-7091-0503-0_16.
- [3] R. Sood, "Intelligent mobile based tourist assistance system," *Proc. IEEE I2CT*, 2017, doi: 10.1109/I2CT.2017.8226211.
- [4] A. Nait-Sidi-Moh et al., "On the use of location-based services and geofencing concepts for safety and road transport efficiency," *MobiWIS*, 2013, doi: 10.1007/978-3-319-03737-0_14.
- [5] V. Patil, P. Singh, S. B. Parikh, and P. K. Atrey, "GeoSClean: Secure cleaning of GPS trajectory data using anomaly detection," *IEEE MIPR*, 2018, doi: 10.1109/MIPR.2018.00037.
- [6] D. Zhang et al., "iBAT: Detecting anomalous taxi trajectories from GPS traces," *UbiComp*, 2011, doi: 10.1145/2030112.2030127.
- [7] S. Buthpitiya et al., "n-Gram geo-trace modeling," *Pervasive Computing*, 2011, doi: 10.1007/978-3-642-21726-5_7.
- [8] 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, doi: 10.3390/ijgi8070308.
- [9] M. T. Datlıca and E. Demir, "Anomaly detection in location and trajectory datasets," *IEEE SIU*, 2021, doi: 10.1109/SIU53274.2021.9477872.
- [10] Y. Liu et al., "Neural collaborative filtering to detect anomalies in human semantic trajectories," *GeoAnomalies@SIGSPATIAL*, 2024, doi: 10.1145/3681765.3698463.
- [11] P. Singh, J. Rathi, and P. B. Patel, "SADHE: Secure anomaly detection for GPS trajectory based on homomorphic encryption," *ACM conference publication*, 2024, doi: 10.1145/3605098.3636165.
- [12] H. Wen, S. Cao, and L. Akoglu, "Uncertainty-aware human mobility modeling and anomaly detection," *arXiv:2410.01281*, 2024.