Deore Adarsh Sunil, 2026, 14:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Smart Tourist Safety Monitoring Using Iot And Artificial Intelligence: A Review Of Location Tracking, Risk Detection And Emergency Response

Deore Adarsh Sunil[1] Prof. M. A. Auti[2]; Prof. M. C. Kolse[3]; Prof. S. K. Said[4]
Department Of Artificial Intelligence And Data Science Jaihind College Of Engineering Pune, Maharashtra, India

Abstract—The rapid growth of digital documents creates a need for systems that can find relevant information and answer questions accurately. Traditional question-answering systems rely on predefined knowledge bases or keyword search and may fail to understand the meaning of complex questions, while large language models alone can produce fluent but unsupported answers. Retrieval-Augmented Generation (RAG) combines information retrieval with the generation abilities of large language models. This paper reviews RAG for document question answering. It explains sparse retrieval with BM25, dense retrieval with dual encoders and sentence embeddings, approximate nearest-neighbour vector search, re-ranking, and the integration of retrieved passages into generation, including fusion-in-decoder and self-reflective retrieval. Practical issues such as chunking, context length and the tendency of models to overlook information in the middle of long contexts are discussed, together with evaluation of faithfulness and relevance. A five-layer system is proposed in which users upload PDF documents that are extracted, cleaned and chunked, embedded with a sentence-transformer model and stored in a vector database; queries retrieve relevant chunks that are passed to an LLM to generate grounded answers through a Streamlit interface. Research gaps, objectives and a comparison of retrieval methods are presented.

Keywords—Retrieval-augmented generation, question answering, large language models, semantic search, vector database, text embeddings, document retrieval

I. INTRODUCTION

India receives millions of domestic and international tourists every year at hill stations, beaches, forts, wildlife sanctuaries and religious gatherings. Many of these places are remote or extremely crowded. Tourists may lose their way on trekking routes, enter areas closed due to landslides or tides, be separated from their group in a crowd, or need medical help where they cannot easily describe their location.

Smartphones and low-cost wearables now carry GPS, motion sensors and connectivity, and AI can analyse their data in real time. Urban computing, as described by Zheng *et al.* [1], uses such data to tackle city challenges, and the same ideas can be applied to visitor safety.

This paper reviews the technologies for a smart tourist safety monitoring system and proposes an architecture that balances protection with privacy.

II. BACKGROUND AND FUNDAMENTAL CONCEPTS

1. Safety Risks For Tourists

Fig. 1 classifies the main risk categories (environmental, crowd-related, personal security and health) and the technologies that address each.

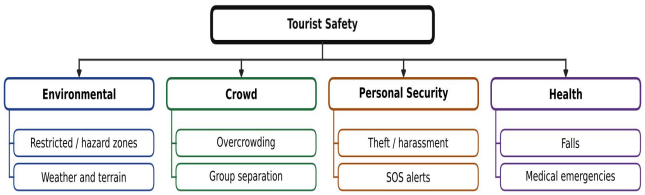


Fig. 1. Tourist safety risks and supporting technologies.

© 2026 Deore Adarsh Sunil This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

Ref.	Author(s) / Year	Technique / Approach	Key Contribution	Limitation / Gap
[2]	Zheng, 2015	Trajectory data mining overview	Methods for GPS trace analysis	General, not tourism-specific
[1]	Zheng et al., 2014	Urban computing framework	Data-driven city problem solving	Conceptual
[3]	Chandola et al., 2009	Anomaly detection survey	Taxonomy of techniques	No tourist data
[4]	White et al., 2011	Smartphone accident detection	Automatic responder notification	Vehicle accidents only
[5]	Bourke et al., 2007	Accelerometer fall detection	Low false-alarm thresholds	Laboratory falls
[7]	Li et al., 2018	CSRNet crowd counting	Accurate density in dense crowds	Needs camera coverage
[8]	Ganti et al., 2011	Mobile crowdsensing	Collective sensing via phones	Participation incentives
[10]	Beresford and Stajano, 2003	Location privacy techniques	Pseudonyms and mix zones	Utility trade-off

2. Geofencing And Location Services

A geofence is a virtual boundary around a real area. When a tracked device crosses the boundary, the system can send an alert, for example when a tourist approaches a cliff edge, a restricted forest zone or a beach with dangerous currents.

III. LITERATURE SURVEY

Zheng [2] reviewed trajectory data mining, covering preprocessing, map matching, pattern mining and anomaly detection on GPS traces. These techniques allow a system to learn normal routes at a destination and recognize unusual movement, such as a hiker leaving marked trails.

Chandola *et al.* [3] surveyed anomaly detection methods and their assumptions, which guide the choice of models for detecting unusual location, speed or inactivity patterns. For personal emergencies, White *et al.* [4] used smartphone accelerometers and acoustic data to detect vehicle accidents and notify responders automatically, and Bourke *et al.* [5] showed that accelerometer thresholds combined with posture checks detect falls reliably.

Crowd safety relies on estimating density from video. Zhang *et al.* [6] proposed a multi-column CNN for crowd counting from single images, and Li *et al.* [7] introduced CSRNet with dilated convolutions for highly congested scenes, enabling authorities to detect dangerous crowding.

Ganti *et al.* [8] described mobile crowdsensing, in which many users' phones collectively report conditions, a model for tourists reporting hazards. Long-range low-power networks [9] can carry alerts where cellular coverage is weak. Beresford and Stajano [10] analysed location privacy and proposed techniques such as pseudonyms and mix zones to reduce tracking risks. Table I summarizes these works.

TABLE I Summary of Literature Survey

IV. RESEARCH GAP

- **G1:** Existing tourist apps mostly provide information rather than active safety monitoring.
- **G2:** Remote destinations often lack mobile coverage, limiting real-time alerts.
- **G3:** Anomaly detection for tourist movement has little labelled data.
- **G4:** Integration with local police, rescue teams and the 112 emergency service is limited.
- **G5:** Privacy protection and consent for continuous tracking are often unclear.

V. OBJECTIVES

- **O1:** To identify safety risks faced by tourists and relevant technologies.
- **O2:** To review location tracking, geofencing, anomaly detection and crowd monitoring methods.
- **O3:** To propose a five-layer smart tourist safety monitoring architecture.
- **O4:** To compare positioning and communication technologies.
- **O5:** To discuss challenges, especially privacy and connectivity.

VI. PROPOSED SYSTEM ARCHITECTURE

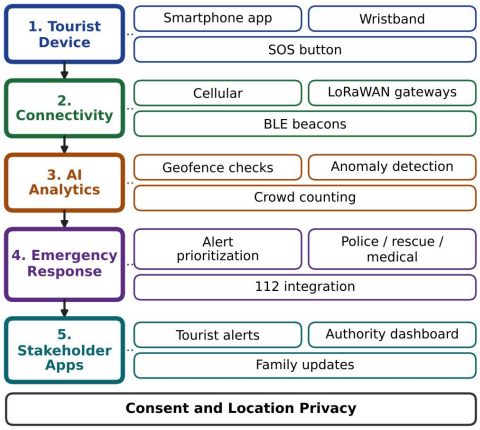


Fig. 2 shows the proposed architecture.

Fig. 2. Proposed five-layer smart tourist safety monitoring architecture.

1. Tourist Device Layer

A smartphone app or wristband provides GPS location, motion sensing, an SOS button and optional heart-rate monitoring. Tourists register voluntarily and give consent for tracking during the visit.

2. Connectivity Layer

Data is sent over cellular networks where available, and over LoRaWAN gateways installed along trekking routes or beaches in remote areas.

3. Ai Analytics Layer

The platform checks geofences, detects anomalies such as sudden stops, long inactivity, falls or deviation from planned routes, and estimates crowd density from cameras at key spots.

4. Emergency Response Layer

Alerts are prioritized and sent to the nearest police, rescue or medical team with the tourist's last known location, language and medical notes.

5. Stakeholder Application Layer

Tourists receive warnings and guidance in their language; authorities see a live dashboard; families can receive updates if the tourist permits.

VII. METHODOLOGY AND WORKING

Fig. 3 describes the monitoring workflow. A tourist at position p is inside a circular danger zone with centre c and radius r if

$$\|p - c\| < r \quad (1)$$

and an inactivity alert is raised when movement remains below a threshold for a time T while the device is outside a known resting place. Crowd density D in an area A is estimated as

$$D = \hat{N} / A \quad (2)$$

where $\hat{N}$ is the person count estimated by the crowd-counting model; densities above a safe limit trigger crowd-control measures.

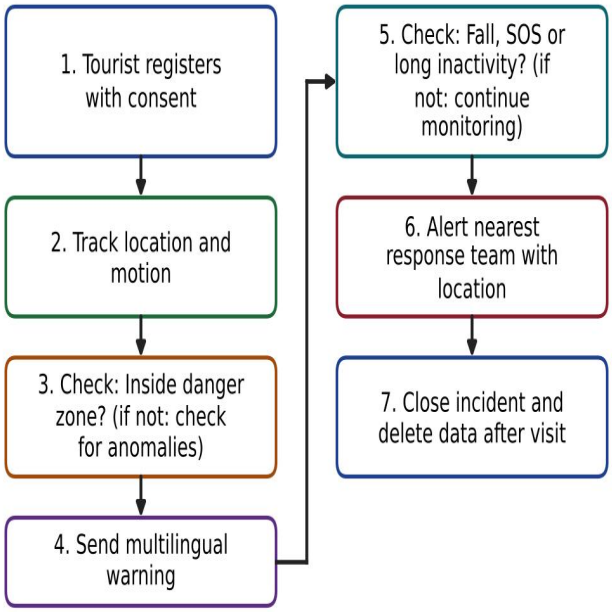


Fig. 3. Tourist safety monitoring workflow.

VIII. COMPARATIVE ANALYSIS

Table II compares positioning and communication options. GPS is accurate outdoors, BLE beacons work indoors and in caves, LoRaWAN extends coverage at low power and satellite messaging works almost anywhere at higher cost.

Technology	Coverage	Accuracy / Rate	Cost
GPS + cellular	Where network exists	~5–10 m	Low
BLE beacons	Indoor / short range	Zone level	Low
LoRaWAN	Several km, low data	Low data rate	Medium
Satellite messaging	Near global	Low data rate	High

TABLE II Comparison of Positioning and Communication Options

IX. CHALLENGES AND FUTURE SCOPE

Table III summarizes challenges. Future work includes drone-based search for missing tourists, integration with weather and landslide warning systems, AI chatbots that answer safety questions in many languages, and privacy-preserving analytics that work on aggregated rather than individual data.

Challenge	Mitigation
Poor connectivity	LoRaWAN; store-and-forward alerts
Battery life	Adaptive GPS sampling
False alarms	Multi-signal confirmation; user check-in
Privacy	Opt-in, minimal retention, anonymization
Language barriers	Multilingual alerts and voice

TABLE III Challenges and Mitigation

X. CONCLUSION

Tourists are especially vulnerable because they are unfamiliar with their surroundings. The reviewed technologies, namely geofencing, trajectory anomaly detection, fall detection, crowd counting and crowdsensing, can together form a smart tourist safety monitoring system that warns visitors early and speeds emergency response. Such a system must operate in areas with poor connectivity, avoid excessive false alarms and, above all, protect tourists' privacy through consent and minimal data retention.

1. Acknowledgment

The authors express their sincere gratitude to the Department of Artificial Intelligence and Data Science, Jaihind College of Engineering, Pune, for providing the facilities, guidance and encouragement needed to carry out this work. The authors also thank the faculty members and colleagues whose valuable suggestions helped improve the quality of this review.

REFERENCES

1. Y. Zheng, L. Capra, O. Wolfson, and H. Yang, "Urban computing: Concepts, methodologies, and applications," ACM Trans. Intell. Syst. Technol., vol. 5, no. 3, Art. no. 38, 2014.
2. Y. Zheng, "Trajectory data mining: An overview," ACM Trans. Intell. Syst. Technol., vol. 6, no. 3, Art. no. 29, 2015.
3. V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Comput. Surv., vol. 41, no. 3, Art. no. 15, 2009.
4. J. White, C. Thompson, H. Turner, B. Dougherty, and D. C. Schmidt, "WreckWatch: Automatic traffic accident detection and notification with smartphones," Mobile Netw. Appl., vol. 16, no. 3, pp. 285–303, 2011.
5. A. K. Bourke, J. V. O'Brien, and G. M. Lyons, "Evaluation of a threshold-based tri-axial accelerometer fall detection algorithm," Gait Posture, vol. 26, no. 2, pp. 194–199, 2007.
6. Y. Zhang, D. Zhou, S. Chen, S. Gao, and Y. Ma, "Single-image crowd counting via multi-column convolutional neural network," in Proc. IEEE CVPR, 2016, pp. 589–597.
7. Y. Li, X. Zhang, and D. Chen, "CSRNet: Dilated convolutional neural networks for understanding the highly congested scenes," in Proc. IEEE/CVF CVPR, 2018, pp. 1091–1100.
8. R. K. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: Current state and future

challenges," IEEE Commun. Mag., vol. 49, no. 11, pp. 32–39, 2011.

9. U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," IEEE Commun. Surveys Tuts., vol. 19, no. 2, pp. 855–873, 2017.
10. A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," IEEE Pervasive Comput., vol. 2, no. 1, pp. 46–55, 2003.