Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

A Conceptual Framework for Proactive Tourist Safety Using AI-Based Risk Scoring and Blockchain Digital Identity

Manaswini Pola
Student, B. Tech AIML 4th Year
Holy Mary Inst. Of Tech. and Science
Hyderabad, Telangana, India

Rasabathula Abhilash
Student, B. Tech AIML 4th Year
Holy Mary Inst. Of Tech. and Science
Hyderabad, Telangana, India

Vempati Sharanya
Student, B. Tech AIML 4th Year
Holy Mary Inst. Of Tech. and Science
Hyderabad, Telangana, India

Dr. Sumithabhashini. P
Assoc. prof, AI & ML
Holy Mary Inst. Of Tech. and Science
Hyderabad, Telangana, India

Lagala Prithviraj
Student, B. Tech AIML 4th Year
Holy Mary Inst. Of Tech. and Science
Hyderabad, Telangana, India

Dr. Venkataramana. B
Assoc. prof, CSE
Holy Mary Inst. Of Tech. and Science
Hyderabad, Telangana, India

Abstract - **Tourist safety within smart tourism ecosystems continues to face significant challenges due to delayed incident detection, fragmented emergency response mechanisms, and increasing concerns related to data privacy and trust. Conventional safety systems largely operate in a reactive manner and depend on centralized monitoring or manual reporting, limiting their ability to anticipate and prevent potential threats. To address these limitations, this paper proposes a conceptual framework for proactive tourist safety that integrates AI-based risk scoring with blockchain-enabled digital identity management.**

The proposed framework conceptually incorporates continuous, context-aware risk assessment derived from environmental conditions, behavioral patterns, and device-level indicators to anticipate unsafe situations before incidents occur. To balance proactive safety monitoring with privacy preservation, a blockchain-based self-sovereign identity model is integrated to enable secure, decentralized, and controlled access to essential identity information exclusively during verified emergency scenarios.

Rather than focusing on implementation or empirical performance evaluation, this study emphasizes architectural design, functional workflows, and theoretical feasibility, offering a design-oriented blueprint for next-generation tourist safety systems. The proposed framework aims to serve as a foundational reference for future empirical research and real-world deployment of privacy-aware, proactive safety solutions in smart tourism environments.

Keywords - Tourist Safety; Conceptual Framework; AI-Based Risk Scoring; Blockchain Digital Identity; Self-Sovereign Identity; Smart Tourism; Privacy-Preserving Systems.

1. INTRODUCTION

1.1 Background & Motivation

The increasing adoption of smart tourism technologies has enhanced travel experiences but has also introduced new challenges related to tourist safety. Tourists often operate in unfamiliar environments, making them vulnerable to accidents, crime, and delayed emergency assistance. Existing tourist safety mechanisms primarily rely on reactive approaches such as emergency helplines and surveillance systems, which respond only after incidents occur. Recent advances in artificial intelligence (AI) enable real-time contextual analysis and predictive risk assessment, offering opportunities to anticipate unsafe situations through continuous monitoring of environmental and behavioral patterns [1], [2]. However, the use of continuous monitoring raises concerns related to data privacy, centralized control, and user trust.

Blockchain technology, particularly self-sovereign identity (SSI) models, has emerged as a promising approach to address these concerns by enabling decentralized and user-controlled identity management [8], [9]. By allowing selective disclosure of sensitive information, blockchain-based identity systems provide a potential pathway to balance proactive safety monitoring with privacy preservation.

1.2 Research Gap

Current research predominantly addresses AI-based safety monitoring and blockchain-based digital identity management as separate solutions. AI-driven systems often lack privacy-preserving mechanisms and rely on centralized data processing [1], [3], while blockchain-based identity frameworks focus on

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

secure authentication and access control without incorporating real-time risk awareness [6], [8]. In the tourism context, limited research has proposed an integrated conceptual framework that combines continuous AI-based risk scoring with decentralized identity management to support proactive and privacy-aware tourist safety.

1.3 Contributions of the Paper

This paper proposes a conceptual AI–blockchain framework for proactive tourist safety. The study presents a high-level architectural design and conceptual risk-scoring logic that integrates environmental, behavioral, and device-level indicators with blockchain-based self-sovereign identity management. The framework provides a design-oriented foundation for future empirical research and implementation of privacy-aware safety systems in smart tourism ecosystems.

2. LITERATURE REVIEW

2.1 AI-Based Safety and Risk Assessment

Artificial intelligence (AI) has been increasingly applied to safety-critical domains to enable predictive risk assessment, anomaly detection, and proactive decision-making. Prior studies demonstrate that machine learning and deep learning techniques can analyze multimodal data streams—such as behavioral patterns, contextual information, and sensor data—to identify abnormal situations and assess potential risks before incidents occur [1], [2]. In particular, predictive risk modeling and behavior-based anomaly detection have shown promise in improving situational awareness and reducing response latency in safety management systems [3], [5].

Within smart city and mobility contexts, AI-driven safety solutions primarily focus on event detection or post-incident analysis, often relying on centralized data processing infrastructures [1]. While these approaches enhance automation, they raise concerns related to scalability, privacy, and trust, especially when continuous monitoring of individuals is involved. In the tourism domain, the application of AI for continuous risk scoring remains limited, with most solutions lacking an integrated, privacy-aware design.

2.2 Blockchain and Digital Identity in Tourism

Blockchain technology has been widely explored as a mechanism for enhancing transparency, trust, and data integrity in tourism ecosystems. Existing studies highlight the role of blockchain in improving booking transparency, reducing fraud, and enabling secure information sharing among tourism stakeholders [6], [7]. Beyond transactional use cases, blockchain has gained attention for decentralized digital identity management, particularly through self-sovereign identity (SSI) models.

SSI frameworks leverage decentralized identifiers (DIDs) and verifiable credentials to enable individuals to maintain control over their personal data while allowing selective disclosure when required [8], [9]. Such identity models have been proposed for applications in education, healthcare, and smart cities, demonstrating their potential to address privacy and trust challenges. However, within tourism safety systems, blockchain-based identity solutions are primarily discussed in isolation, without integration into real-time safety monitoring or risk assessment workflows.

2.3 Limitations of Existing Approaches

Despite advancements in AI-based safety monitoring and blockchain-enabled identity management, existing approaches exhibit notable limitations. AI-driven safety systems often depend on centralized architectures and continuous data collection, which can undermine user privacy and reduce adoption due to trust concerns [1], [3]. Conversely, blockchain-based identity frameworks emphasize secure authentication and data ownership but lack mechanisms for contextual risk awareness and proactive safety response [6], [8].

In the tourism context, most existing solutions remain reactive, fragmented, and siloed, addressing either safety monitoring or identity management independently. There is a lack of unified conceptual frameworks that combine continuous AI-based risk assessment with decentralized, privacy-preserving identity control to support proactive tourist safety. This limitation underscores the need for an integrated, design-oriented approach that bridges predictive intelligence and trustworthy identity management within smart tourism ecosystems.

3. CONCEPTUAL FRAMEWORK OVERVIEW

3.1 Design Objectives and Assumptions

The primary objective of the proposed conceptual framework is to enable proactive tourist safety by anticipating potential risks before incidents occur, while simultaneously preserving user privacy and trust. Unlike conventional reactive safety systems, the framework is designed to support continuous situational awareness through intelligent risk assessment without requiring constant manual intervention.

The framework is guided by the following design objectives:

- To conceptually integrate AI-based risk scoring for continuous assessment of tourist safety,
- To ensure privacy-preserving identity management through decentralized digital identity mechanisms,
- To support timely and prioritized emergency response based on assessed risk levels
- To maintain scalability and adaptability across diverse tourism environments.

To support conceptual clarity, several assumptions are made. It is assumed that tourists interact with the system through personal smart devices capable of providing basic contextual and behavioral data, such as location and movement patterns. The framework also assumes the availability of external contextual information (e.g., environmental conditions or public safety indicators) and the participation of authorized emergency responders capable of accessing identity information during verified emergencies. These assumptions are intended to define the conceptual boundaries of the framework rather than prescribe implementation constraints.

3.2 High-Level System Architecture

The proposed framework follows a multi-layer conceptual architecture that integrates risk assessment, identity management, and emergency response workflows in a cohesive manner. At a high level, the architecture consists of four

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

interconnected layers: the data sensing layer, the AI-based risk assessment layer, the blockchain-based identity layer, and the application and response layer.

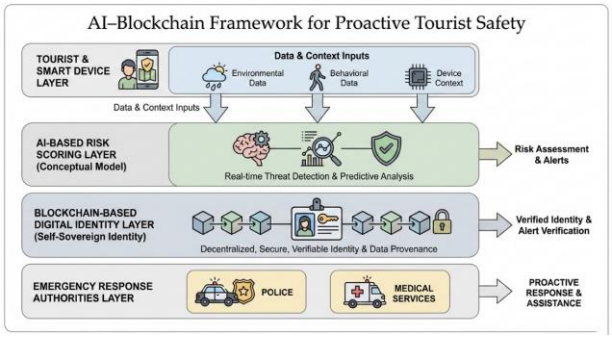

Figure 1: Overall Conceptual Framework Architecture

The data sensing layer conceptually represents the collection of contextual, behavioral, and device-related indicators generated through user interaction and environmental awareness. These inputs are logically forwarded to the AI-based risk assessment layer, where a conceptual risk-scoring logic evaluates the likelihood of unsafe situations based on predefined contextual and behavioral patterns.

The blockchain-based identity layer operates independently of continuous monitoring and is activated only when elevated risk levels are identified. This layer conceptually employs self-sovereign identity principles to enable secure, decentralized, and controlled access to essential identity information during emergency scenarios. By decoupling identity access from routine monitoring, the framework seeks to minimize privacy exposure while maintaining emergency readiness.

Finally, the application and response layer provides a unified interface for tourists and authorized responders. This layer supports conceptual alert generation, situational awareness, and coordinated response actions based on assessed risk levels. Together, these layers form a cohesive conceptual architecture that emphasizes proactive safety, privacy preservation, and trust within smart tourism ecosystems.

4. CONCEPTUAL METHODOLOGY

4.1 Data Dimensions and Contextual Inputs

The proposed framework conceptually relies on the fusion of multiple data dimensions to support continuous situational awareness and proactive risk assessment. Rather than depending on a single data source, the methodology assumes the availability of heterogeneous contextual inputs that collectively provide a holistic view of a tourist's safety state.

These inputs are broadly categorized into three dimensions.

- **Environmental context** includes location-based safety indicators, such as general area risk levels or adverse environmental conditions.
- **Behavioral context** represents movement patterns and temporal activity indicators that may signal abnormal or potentially unsafe situations.
- **Device-related context** captures system-level indicators, such as connectivity status or device availability, which may indirectly influence a tourist's vulnerability during emergencies.

These dimensions are conceptually treated as complementary inputs that, when combined, enable a more robust understanding of potential safety risks.

4.2 Conceptual AI-Based Risk Scoring Logic

At the core of the framework is a **conceptual AI-based risk scoring logic** designed to aggregate contextual inputs into a unified safety risk representation. The risk scoring mechanism is not intended as a trained or deployed predictive model but as a theoretical abstraction that illustrates how intelligent systems can support proactive safety assessment.

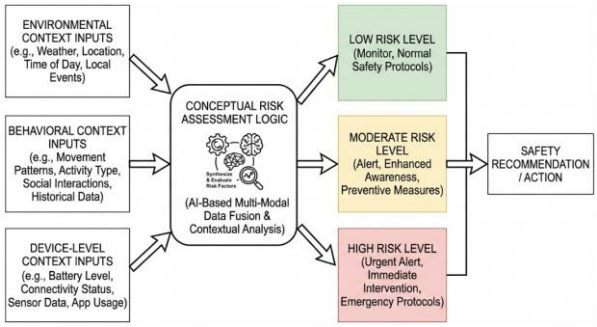

Figure 2: Conceptual AI-Based Risk Scoring Logic

In this conceptual model, contextual inputs are evaluated collectively to estimate the likelihood of unsafe situations. Environmental indicators provide situational awareness, behavioral patterns contribute temporal and movement-based insights, and device-related indicators reflect potential communication or accessibility constraints. These inputs are conceptually weighted and combined to produce a dynamic risk level, which may be categorized into qualitative states such as low, moderate, or elevated risk.

The primary purpose of this risk scoring logic is to demonstrate how AI-inspired reasoning can enable continuous risk awareness and prioritized response, rather than to specify algorithmic details or performance metrics.

4.3 Blockchain-Based Identity and Privacy Model

To address privacy and trust concerns associated with continuous monitoring, the framework conceptually integrates a **blockchain-based identity and privacy model** grounded in self-sovereign identity principles. In this model, tourists retain control over their digital identity credentials, which are securely stored and managed outside of routine monitoring processes.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

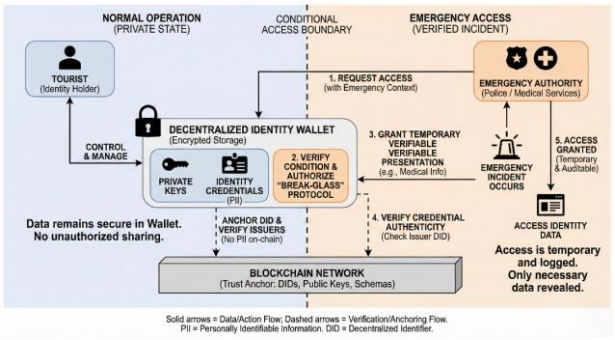

Figure 3: Blockchain-Based Identity & Privacy Workflow

The identity layer remains logically inactive during normal operation and is activated only when elevated risk levels are identified. During such scenarios, authorized entities may be granted controlled access to essential identity attributes required for emergency response. This selective disclosure mechanism ensures that sensitive personal information is shared only when necessary and under predefined conditions.

By decoupling identity management from continuous risk assessment, the framework conceptually balances proactive safety requirements with strong privacy preservation and user trust.

4.4 Emergency Decision and Response Workflow

The conceptual emergency workflow is driven by the assessed risk level rather than explicit user-initiated alerts. Under normal conditions, the system maintains passive monitoring without external intervention. When moderate risk levels are identified, the framework conceptually supports heightened situational awareness and preparatory actions without exposing personal identity information.

In cases where elevated risk thresholds are reached, the framework enables a coordinated response workflow. This includes conceptual alert generation, contextual information sharing, and controlled activation of the identity layer to support timely and informed intervention by authorized responders. The workflow emphasizes prioritization and responsiveness while minimizing unnecessary data exposure.

Overall, the methodology illustrates a structured, privacy-aware decision flow that aligns proactive risk assessment with responsible emergency response within smart tourism ecosystems.

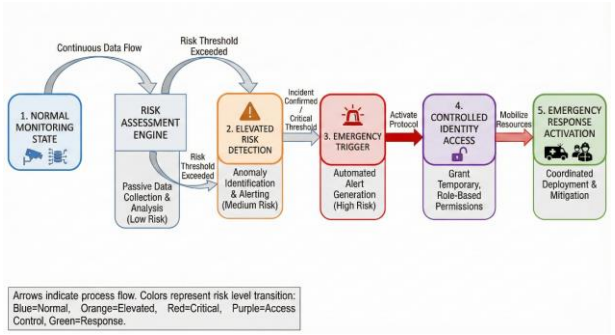

Figure 4: Emergency Decision & Response Workflow

5. Conceptual Validation and Expected Outcomes

5.1 Scenario-Based Reasoning

As this study adopts a conceptual and design-oriented approach, validation is performed through **scenario-based reasoning** rather than empirical experimentation. Scenario reasoning is used to logically examine how the proposed framework would behave under representative tourist safety situations and to assess the internal consistency of the framework's design.

In a typical low-risk scenario, such as routine tourist movement within familiar or well-monitored areas, the framework maintains passive situational awareness without triggering alerts or accessing identity information. This demonstrates that the system can operate unobtrusively during normal conditions. In moderate-risk scenarios, such as unusual activity patterns or entry into potentially unsafe environments, the conceptual risk scoring logic enables heightened awareness and preparatory monitoring while preserving user privacy.

In high-risk scenarios—such as prolonged inactivity in unsafe locations or abnormal movement patterns during vulnerable time periods—the framework conceptually activates prioritized response mechanisms. At this stage, controlled access to essential identity information supports informed and timely intervention by authorized responders. These scenarios illustrate how the framework logically transitions between safety states while maintaining alignment with privacy-preserving principles.

5.2 Expected Benefits Over Reactive Systems

Compared to conventional reactive safety systems, the proposed conceptual framework offers several expected advantages. First, continuous risk awareness enables earlier identification of potentially unsafe situations, allowing preventive or preparatory actions before incidents escalate. This proactive orientation reduces reliance on user-initiated distress signals and manual reporting.

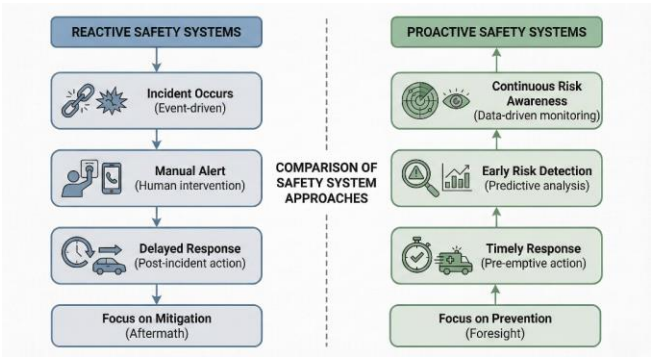

Figure 5: Proactive vs Reactive Safety Systems

Second, the integration of decentralized identity management conceptually addresses privacy and trust concerns that commonly limit adoption of real-time safety monitoring systems. By restricting identity access to verified emergency

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

conditions, the framework minimizes unnecessary data exposure while maintaining emergency readiness.

Finally, the layered and modular nature of the framework supports adaptability across diverse tourism contexts, including urban, rural, and international environments. By conceptually aligning predictive risk assessment with privacy-aware identity control, the framework provides a balanced alternative to existing reactive systems that often sacrifice either safety effectiveness or user privacy.

6. LIMITATIONS AND RESEARCH CHALLENGES

Despite its conceptual strengths, the proposed framework is subject to several limitations and research challenges that must be acknowledged.

First, as a design-oriented study, the framework does not include empirical implementation or experimental validation. The conceptual risk scoring logic and emergency workflows are derived from theoretical reasoning and prior literature, and their real-world effectiveness remains to be validated through practical deployment and quantitative evaluation.

Second, the framework assumes the availability of continuous contextual inputs and user interaction through smart devices. In real-world tourism environments, data availability may be constrained by network connectivity limitations, device heterogeneity, or user preferences related to data sharing. Such constraints may affect the reliability and completeness of risk assessment in practice.

Third, while the blockchain-based identity model conceptually enhances privacy and trust, its adoption may face practical challenges related to interoperability, governance, and regulatory compliance across different regions and tourism stakeholders. Establishing trust among multiple authorities and ensuring compliance with data protection regulations represent non-trivial challenges for decentralized identity systems.

Finally, user acceptance and trust remain critical factors influencing the success of proactive safety systems. Even with privacy-preserving mechanisms, tourists may be hesitant to participate in continuous monitoring due to perceived privacy risks or usability concerns. Addressing these challenges will require careful system design, transparent governance, and empirical studies focusing on usability and trust.

7. FUTURE RESEARCH DIRECTIONS

The conceptual framework presented in this study provides a foundation for several promising directions for future research. A primary avenue involves the **empirical validation** of the proposed architecture through pilot deployments or controlled simulations. Future studies can evaluate the effectiveness of AI-based risk scoring mechanisms using real-world or synthetic datasets to assess responsiveness, reliability, and scalability across diverse tourism contexts.

Another important direction concerns the **refinement of risk modeling techniques**. Future work may explore advanced machine learning approaches, multimodal data fusion strategies, or adaptive weighting mechanisms to improve contextual risk interpretation while maintaining transparency and explainability. Comparative evaluations of different risk modeling paradigms could further inform the design of proactive safety systems.

Research on **decentralized identity governance and interoperability** represents an additional opportunity. Future studies may examine cross-platform and cross-border interoperability of self-sovereign identity systems, as well as policy, regulatory, and ethical considerations related to privacy-preserving emergency access. Investigating governance frameworks that balance decentralization with accountability will be essential for real-world adoption.

Finally, **user-centric evaluations** focusing on trust, usability, and acceptance are critical. Future research should assess how tourists perceive proactive safety systems and privacy controls, and how interface design and transparency mechanisms influence participation. Such studies will be instrumental in translating conceptual frameworks into practical, user-trusted solutions within smart tourism ecosystems.

8. CONCLUSION

This paper presented a **conceptual framework** for proactive tourist safety that integrates AI-based risk scoring with blockchain-enabled digital identity management. By shifting the focus from reactive incident response to continuous, context-aware risk awareness, the framework addresses key limitations of existing tourist safety systems that rely on manual intervention and centralized monitoring.

The proposed design conceptually demonstrates how heterogeneous contextual inputs can be synthesized through AI-inspired risk assessment logic to anticipate potentially unsafe situations, while blockchain-based self-sovereign identity mechanisms ensure privacy-preserving and controlled access to sensitive information during emergency scenarios. Through a layered architectural approach, the framework balances proactive safety objectives with user trust, data minimization, and decentralized identity control.

Rather than offering empirical evaluation, this study contributes a **design-oriented blueprint** that clarifies how predictive intelligence and decentralized identity technologies can be cohesively aligned within smart tourism ecosystems. The framework lays a conceptual foundation for future empirical research, system implementation, and policy-aligned deployment, supporting the development of privacy-aware, trustworthy, and resilient tourist safety solutions.

9. REFERENCES:

[1] Tamascelli, N., et al. (2024). Artificial intelligence for safety and reliability: A descriptive, bibliometric and interpretative review on machine learning. Reliability Engineering & System Safety, 241, 109546.

[2] Armenteros-Cosme, P., et al. (2025). Advancements in artificial intelligence and machine learning for occupational risk prevention: A systematic review on predictive risk modeling and prevention strategies. Sensors, 25(17), 5419.

[3] Ahmed, N., et al. (2023). Cybersecurity risk assessment using AI-based predictive models. Journal of Information Security and Applications, 73, 103458.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

[4] Ordóñez, F. J., & Roggen, D. (2016). Deep convolutional and LSTM recurrent neural networks for multimodal wearable activity recognition. Sensors, 16(1), 115.

[5] Malekzadeh, M., Clegg, R. G., Cavallaro, A., & Haddadi, H. (2018). Protecting sensory data against sensitive inferences. Proceedings of the 1st Workshop on Privacy by Design in Distributed Systems, 1–6.

[6] Aghaei, H., Naderibeni, N., & Karimi, A. (2021). Designing a tourism business model on a blockchain platform. Tourism Management Perspectives, 39, 100845.

[7] Balasubramanian, S., Sethi, J. S., Ajayan, S., et al. (2022). An enabling framework for blockchain in tourism. Information Technology & Tourism, 24, 165–179.

[8] Grech, A., Sood, I., & Ariño, L. (2021). Blockchain, self-sovereign identity and digital credentials: Promise versus praxis. Frontiers in Blockchain, 4, 616779.

[9] Mazzocca, C., et al. (2024). A survey on decentralized identifiers and verifiable credentials. IEEE Communications Surveys & Tutorials.

[10] World Wide Web Consortium (W3C). (2022). Decentralized Identifiers (DIDs) v1.0.

[11] World Wide Web Consortium (W3C). (2022). Verifiable Credentials Data Model v1.1.