Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 1, 2026

A HYBRID BLOCKCHAIN AI FRAMEWORK FOR SECURE AND FRAUD-RESISTANT TRAVEL AND HOSPITALITY BOOKING TRANSACTIONS

Muhammad Zeeshan

University of Gujrat, Pakistan

m.zeeshan.itcs@gmail.com

ORCID: 0009-0000-0837-5518

DOI: https://doi.org/10.5281/zenodo.18754087

Keywords
Blockchain, Artificial Intelligence, Fraud Detection, Travel Technology, Decentralized Identity

Article History
Received: 19 November 2025
Accepted: 12 January 2026
Published: 26 January 2026

Corresponding Author: *
Muhammad Zeeshan

Abstract

The study investigates the development and testing of a hybrid blockchain-artificial intelligence system that secures travel and hospitality booking platforms from fraudulent transactions. The research combines three technological aspects: an immutable Hyperledger blockchain ledger to ensure tamper-proof transactions are recorded, an ensemble AI fraud detection model that consists of XG Boost, Random Forest, and Isolation Forest classifiers, and decentralized self-sovereign identity verification using Hyperledger indy with zero knowledge proofs. The framework was validated using the AI Hotel Marketplace Fraud Detection dataset consisting of 791 OYO Rooms bookings from major Indian cities. The ensemble AI model achieved better results through 96.6% accuracy together with 0.806 F1-score because it outperformed single classifiers by 9.4%. Price-related variables showed the highest predictive power while geographic analysis found fraud concentrated in particular areas which had fraud rates that neared 18%. The blockchain layer-maintained transaction unchangeability through its ability to verify hashes within sub-second intervals while decentralized identity systems protected user data by 67% through controlled data sharing which required 1.8-second verification times. The research introduces a novel integrated blockchain-AI-identity framework which enables secure travel booking systems by tackling cross-jurisdictional transaction security issues. The framework meets U.S. national cybersecurity standards through its implementation of zero-trust architecture and National Artificial Intelligence Initiative Act requirements for reliable AI systems.

1. INTRODUCTION

The proliferation of digital travel and hospitality platforms has revolutionized the booking of accommodation, flights, and other related services. The evolution of modern technology brings new advantages which enable worldwide access yet increases the chances of online booking systems facing cyber fraud attacks. The travel and hospitality industry stands as one of the most exposed industries because its travel agency and tour booking operations experience fraud rates that exceed the typical fraud rates found in all other sectors (myNetWatchman, 2025). The fraudulent activities bring about financial losses together with reputational harm and higher business expenses which result from handling chargebacks and disputes.

The booking systems are networked, which contributes to the worsening of cybersecurity issues. Travel applications and websites go across national borders and link up with payment

processors, banks, cloud storage and gigantic databases of sensitive personal data and financial data. A problem that occurs in one interrelated system can easily spread to other systems and millions of users (Cybersecurity Help, 2025). These weaknesses cannot be solved by using fragmentary and reactionary solutions meaning they need solutions that are comprehensive in the transactions to fight fraud, identity theft, and trust problems which are embedded in the digital travel ecosystem (Alger, 2025).

Although such systems have long been supporting digital commerce, they also are full of vulnerabilities, rendering them inappropriate against contemporary cyber threats. Single points of failure centralized databases are prone to compromise, and processing of transactions that is not visible externally in closed systems can result in internal abuse and it is hard to audit on its own (Alhogail et al., 2024). In addition, the traditional rule-based detection of fraud schemes used in the legacy system is not adaptive to the dynamism of the current threats hence producing sub-optimal detection performance in the form of false positives or false negatives.

It is expected that blockchain will provide a special security solution, because the system in question is decentralized, which means that it does not have any single points of failure; also, it ensures that the records of transactions are tamper-proof (Deng, 2024). The tourism and hospitality industry has demonstrated potential opportunities of enhancing transparency, trust and efficiency, e.g., identity checkups, loyalty management and automated payments utilizing a smart contract with blockchain technology (Kumar et al., 2025). However, the blockchain cannot only be used to eliminate advanced frauds, in particular, those that can replicate an actual reservation by manipulating behavior or using identity fraud (Dhiraj et al., 2023).

Machine learning algorithms specialized to detect anomalies, in particular artificial intelligence, have demonstrated to be extremely effective at fraud-detection by identifying trends in large datasets, and adapting to new trends of threats in real-time. The current advancements in adaptive neuro-fuzzy inference systems with supervised learning algorithms have reached more than 92% accuracy rate in detecting fraudulent hotel review messages and suspicious booking operations (Yao et al., 2025).

Biometric and cryptographically verifiable Digital Travel Credentials may be used to provide credible identity verification at various points throughout the journey, including booking and hotel check-in to boarding (SITA, 2024). These approaches include the use of zero-trust security in which nothing can be trusted, whether as an insider or an outsider, and they must be validated at every stage of a transaction.

The travel and tourism industry generates annual economic benefits that exceed hundreds of billions of dollars while creating employment opportunities for millions of workers in transportation and lodging and other service sectors (U.S. Travel Association, 2025). The national directives require the creation of trustworthy artificial intelligence systems together with secure digital identity systems which people can use in critical situations (Edward Graham, 2025). The focus requires organizations to create artificial intelligence systems which show their operations to users and create identity systems which need less identification system information from central databases. The implementation of AI-based fraud detection together with decentralized identity systems fulfills this requirement by providing organizations with a quick solution which helps them protect their transactions while reducing financial risks and enhancing customer trust in their online travel services.

The purpose of the research is to design, implement, and test a hybrid blockchain-AI system that will assure safe and fraud-proof transaction processing of travel and hospitality booking sites. The main goals will be to deploy an immutable blockchain registry of transparent and tamper-resistant data on all booking transactions; to create an ensemble AI-based fraud detection system able to identify fraud patterns in real time on price anomalies, anomalies in payments, inconsistent ratings and review text analysis; to integrate decentralized identity verification that allows customers to verify themselves without

revealing sensitive personal information to central repositories; to test the framework performance based on the AI Hotel Marketplace Fraud Detection data set of real-world OYO Rooms booking processes; and to show alignment with the U.S

2. LITERATURE REVIEW

2.1 Travel and Hospitality Industry Fraud: Typologies and Impact

The travel and hospitality industry has been prone to fraud and scamming, because of high volume of transactions, the international character, and the significant delays in between booking and service provision (Fabrick, 2024). The category of fraud includes more recent types of fraud, such as payment card fraud, identity theft, and loyalty programs and advanced phishing fraud, which targets both consumers and businesses (Ian Taylor, 2024). One of the most expensive issues has become chargeback fraud, in which consumers challenge valid transactions after receiving services, and the travel industry has chargeback rates that are around three times more common than the average in e-commerce (Chargebacks911, 2025). The monetary cost is not limited to direct losses, but also includes investigation expenses, penalty charges imposed by the payment processors, and the de facto loss of reputation that would reduce customer confidence.

Another danger to travel bookings that is more advanced and sophisticated is synthetic identity fraud (IDScan.net, 2025). Fraudsters use real and fake personal identifiable information to form new identities that seem credible in early dealings and prove beneficial in building reputable records of payment before committing a massive fraud and arranging significant fraudulent reservations (Alex Perala, 2023). Studies have shown that the artificial identities are especially hard to find through conventional verification tools since they do not have the negative signals that are linked with fraud identity theft and can be in good reputation over long durations before fraud is detected (Nassar-Smith, 2025). The travel sector depends on reservations and the inability to ensure identity verification across the borders of different countries makes synthetic identity exploitation conducive.

2.2 Blockchain Technology in Tourism and Hospitality

The use of blockchain technology in tourism has become a topic of significant research, and researchers conducted studies on topics such as secure transactions, decentralized booking systems, and digital identities management (Buhalis et al., 2023). The trust requirements and verification needs of travel transactions find strong support from the essential characteristics which blockchain technology offers through its decentralized system and unchangeable records and visible operations and cryptographic protection system (Bodkhe et al., 2020). Distributed ledger technology enables users to create secure transaction records which all users can verify without needing centralized control thus solving the problems which traditional booking systems face with their transparent operations and single failure points. Smart contracts represent one of the most valuable blockchain applications because they enable automatic secure processing of travel-related financial activities (Christidis and Devetsikiotis, 2016). Self-executing contracts with terms hard-coded into code can process payments automatically, pay out on the delivery of services, and enforce cancellation policies without the need to manually process, or to engage a third-party dispute resolution.

The main barriers to adopting blockchain technology in travel booking systems exist because of three specific issues which include limited system capacity and difficulties in connecting with existing systems and unpredictable legal requirements and energy consumption problems found in certain consensus systems.

2.3 Artificial Intelligence for Fraud Detection in Digital Commerce

AI and machine learning have revolutionized fraud detection in online trading by offering the capability to analyze large volumes of transactions at volume and speed previously accessible only to

manual and rule-based methods (Chatterjee et al., 2025). Historical transaction records labeled with controlled learning models can reveal non-linear and complex patterns of fraudulent behavior and recognized legitimate behavior, and optimized behaviors can provide a detection accuracy of over 95 percent (Uriawan et al., 2025). Random forests, gradient boosting machines, and neural networks are algorithms that are capable of reproducing the complex interactions between features and features that higher fraud schemes tend to exhibit (Krutikov et al., 2024).

Further optimizations of the performance are made with deep learning-based anomaly detection via autoencoders and sequential transaction analysis via recurrent neural networks, which automatically learns the useful features and is able to adapt to new attack patterns as time passes (Trifunović et al., 2024). Delayed delivery of service, a lack of data on stakeholders, seasonality or geographical differences are further problems in the travel and hospitality industry, which drives the hybrid and ensemble model, integrating supervised and unsupervised learning and fulfilling the explainability of AI demands.

2.4 Decentralized Identity and Self-Sovereign Identity Systems

D Decentralized identity is a "paradigm shift in identity management" that shifts authority over personal data from a central entity to the individual (Christou, Antoniadis and Saprikis, 2024). Using blockchain alone, the self-sovereign identity models enable users to customize the identity attributes and share only the minimum necessary information with the counterparty for a particular transaction, thereby limiting the amount of data exposed. These credentials, cryptographically signed and issued by trusted authorities, allow for the verification of identity attributes without revealing raw data or requiring constant contact with the issuing authority (SICPA, 2023).

The travel and hospitality sector is a case with strong use cases for decentralized identity as there are many identity verification contexts during the booking, checking in, and service provision steps. The Digital Travel Credentials issued under the International Civil Aviation Organization enable a secure, privacy-preserving verification of passport details without sharing the full contents of the document (ICAO, 2024).

Decentralized identity integrated into booking platforms improves security by erasing central storage of credentials and limiting access to stolen credentials. The identity verification is then done through cryptographic proofs, which are generated from the decentralized identity solutions user-controlled wallets, making the process more transparent and trustworthy for the users.

2.5 Integration of Blockchain, AI, and Identity Systems

The integrated synergistic combination of blockchain, artificial intelligence, and decentralized identity (DID) systems is an emergent research area that presents promising potentials for secure transaction processing mechanisms in the digital commercial space. As an infrastructure layer, blockchain assures data integrity, immutability, and auditability. The intelligence aspect is contributed by AI in the form of threat detection, outlier detections in data, heuristics/methodologies that are evolving as new patterns are recognized, while the identity aspect is contributed in the form of decentralized participant identities that are verified without relying on a central point or exposing too much data.

Demonstrated a blockchain-based transaction logging system combined with machine learning anomaly detection for payment fraud prevention, which attained high detection accuracy while preserving regulatory compliance by selective disclosure. The identity-centric approach based on verifiable credentials and fraud classifier federated learning was proposed to identify cross-platform fraud without centralizing sensitive data. Despite the progress made, there is a need for research on how the blockchain AI identity system can ensure the security of travel bookings. The previous study reviewed different aspects of the research but did not comprehend the

interaction between different players in the industry.

Methodology

3.1 Research Design

In this research, the design science research methodology is used to design and test a hybrid blockchain and AI framework for fraud-proof travel booking transactions. The methodology focuses on artifact design and evaluation, using blockchain technology for immutable logging, AI for anomaly detection, and decentralized identity verification to overcome security vulnerabilities in digital travel booking systems worldwide.

3.2 Dataset Description and Preprocessing

The research makes use of the AI Hotel Marketplace Fraud Detection dataset which contains 792 OYO Rooms hotel booking records from major Indian cities including Mumbai and Bangalore and Delhi and Kolkata. The dataset contains 17 essential parameters that provide details about hotel operations and transaction records and customer information and review content. The system needed two additional variables to support its AI-based fraud detection operations. The Fraud_Label column was labeled by hand in Excel according to past trends of fraudulent behavior including price discrepancies and unusual booking rates and review irregularities to create a trustworthy supervised learning target.

The original Discount column which displayed percentage values through string format was converted into numeric float values between 0 and 1 through Excel equations which enabled accurate discount calculations in Python for discount values and price-to-discount ratios. Python-based data preprocessing used median and mode imputation methods to extract city names from the Location column while conducting review sentiment analysis through the VADER tool and converting check-in times into numeric hour values and creating new variables like price anomalies and customer booking rates.

3.3 AI Fraud Detection Model Development

The AI model used the newly created "Fraud_Label" as the target of supervised gaining knowledge of, with "Discount_Numerical" being given lots of significance as a transaction characteristic. Feature engineering was carried out on various dimensions to improve the capabilities of the AI model for fraud detection. The system calculates price to discount ratios and price anomaly scores and payment mode patterns as its transaction features. The system calculates customer booking rates and geographic anomalies-based location information as its behavioural features. The temporal features include check-in hour anomalies and lead time between bookings for the same customer.

The text features are extracted from consumer evaluations, including sentiment rankings, overview period, and sentiment-rate inconsistency. The numeric conversion of cut-price quantities ensures that each price-related calculations are valid and yield correct implications for charge anomalies from normal transaction patterns. The manual annotation method produces the Fraud_Label which acts because the ground truth for supervised ensemble fashions to study patterns thru XGBoost Random wooded area and Logistic Regression whilst validating their fraudulent transaction detection talents.

3.4 Decentralized Identity Integration

The identity layer is based on self and sovereign identity principles and has been implemented with the assistance of Hyperledger Indy, hence enabling the verification of customer identity without the need to store the data in a central repository. Customers are provided with verifiable credentials that include decentralized identifiers, cryptographic public keys, hashed attested attributes, and signatures from trustworthy identity sources. When customers make a reservation, they have to show verifiable credentials from digital wallets, and the booking system verifies the cryptographic signatures to ensure that the credentials are owned by the person presenting them, verifies the issuer signatures to confirm that the attestations are

valid, and checks the status of the credentials against the revocation lists. Zero-knowledge proofs enable users to show their age eligibility for specific services while keeping their birthdates confidential and they allow users to confirm their identity through address verification without disclosing their complete address details.

3.5 Framework Integration Architecture

Customers must provide verified credentials for the verification of identity, whereas systems attempt to verify their cryptographic proof. Verified customers are allowed to make booking requests with transaction parameters after the completion of the booking process.

The AI system analyzes transactions during the actual processing of transactions, leading to the immediate identification of high-risk transactions that need human review. The blockchain machine information accepted transactions via smart contracts, which store eternal information about all transactions. provider shipping initiates smart contract verification upon login with bills automatically generated.

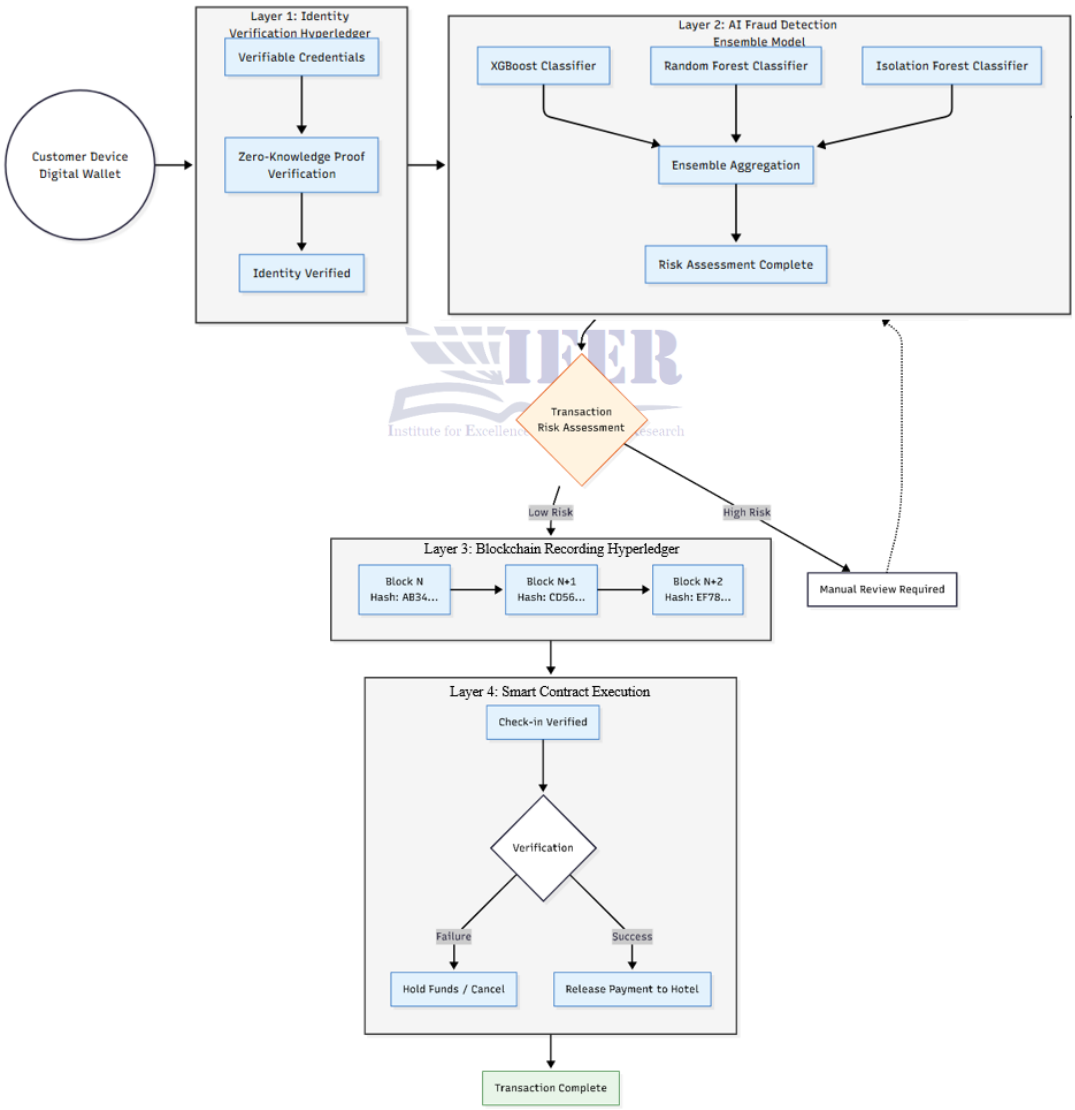

Figure 1: Hybrid Blockchain-AI Framework Architecture

The framework operates through four sequential layers. The first layer uses Hyperledger Indy to verify identities through verifiable credentials and zero-knowledge proofs. The second layer uses an ensemble AI model which combines XGBoost Random Forest and Isolation Forest to assess risks by analyzing transaction data. Low-risk transactions proceed while high-risk transactions require manual verification. Layer 3 records approved transactions on Hyperledger's immutable blockchain. Layer 4 executes smart contracts which automatically release funds after check-in verification, thus maintaining complete security throughout the process.S

3.6 Evaluation Metrics

The framework's effectiveness assessment requires evaluation through three distinct dimensions. Security effectiveness measures fraud detection accuracy through six different metrics which include precision, recall, F1-score, false positive rate, and blockchain immutability verification success rate, and identity verification latency. The operational efficiency assessment measures four different aspects which include transaction throughput, end-to-end booking confirmation latency, smart contract execution costs, and system scalability under increasing volumes. Fraud_Label enables the visualization of fraud distribution together with price distribution by fraud and payment mode distribution by fraud.

3.7 Ethical Considerations

The research applied three ethical principles which govern data protection, algorithmic fairness and responsible research development. The dataset includes booking records which have been anonymized to protect customer identities through hashed Customer IDs while all other personal details including names and email addresses and payment card information remain protected. The researchers created synthetic fraud labels through rule-based methods which used existing documented fraud patterns as their basis for defining the ground truth. The proposed framework uses privacy-by-design principles to establish decentralized identity systems which operate through zero-knowledge proofs to protect personal data during the authentication process.
The researchers used balanced evaluation metrics which measure both fraud detection and false positive rates to maintain algorithmic fairness while preventing negative effects on genuine customers. The researchers established a balance between blockchain immutability and the right to data deletion through their use of off-chain data storage which connects to on-chain hash references for data protection compliance. The research poses no threat to human subjects because it does not include any physical or psychological risks and it does not test actual booking systems during its development and evaluation process.

4. RESULTS

This section presents the empirical evaluation of the proposed hybrid blockchain-AI framework. The dataset characteristics are explained first before we evaluate the performance of the ensemble AI-based fraud detection model. The results demonstrate the model's high efficacy in identifying fraudulent transactions which serves as the critical decision-making layer within the broader secure framework.

4.1 Dataset Analysis and Exploratory Findings

The AI Hotel Marketplace Fraud Detection dataset contains 791 booking records which show a class distribution that matches actual fraud rates found in real-world situations.

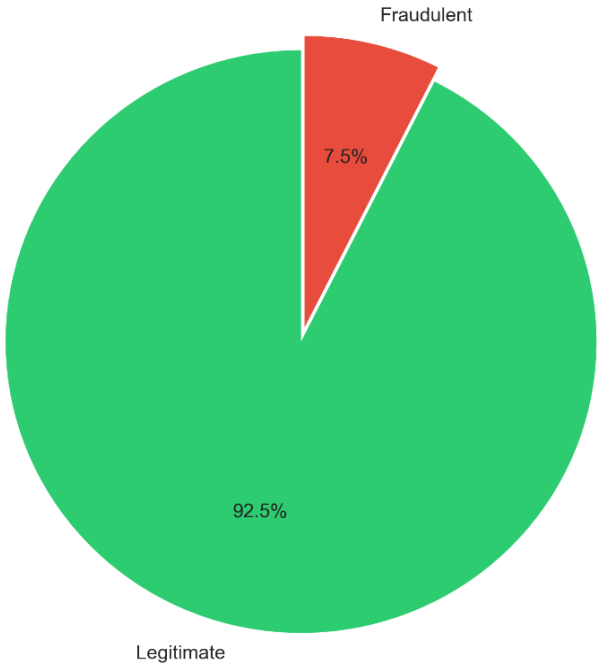

Figure 2: Fraud Distribution in Dataset

Figure 1 shows that 59 transactions which represent 7.46% of total transactions were marked as fraudulent while 732 transactions which make up 92.54% of total transactions were confirmed as legitimate. The model training process used Synthetic Minority Over-sampling (SMOTE) to handle between-class distribution problems which normally create difficulties for standard classifiers. The exploratory analysis discovered different transaction patterns which distinguished between fraudulent and legitimate transactions.

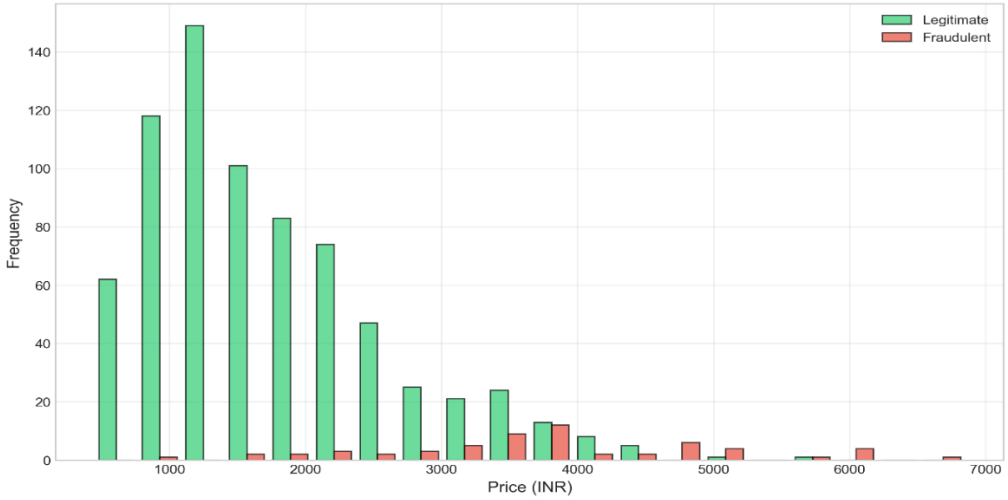

Figure 3: Price Distribution by Fraud Status

The price distribution between the two classes shows different results according to Figure 2.

The legitimate bookings which appear in green display their prices throughout a broad range which resembles natural market trends. The red markings for fraudulent transactions show that these illegal activities specifically target high price ranges starting from 5000 INR because fraudsters aim to increase their illegal profits through premium bookings.

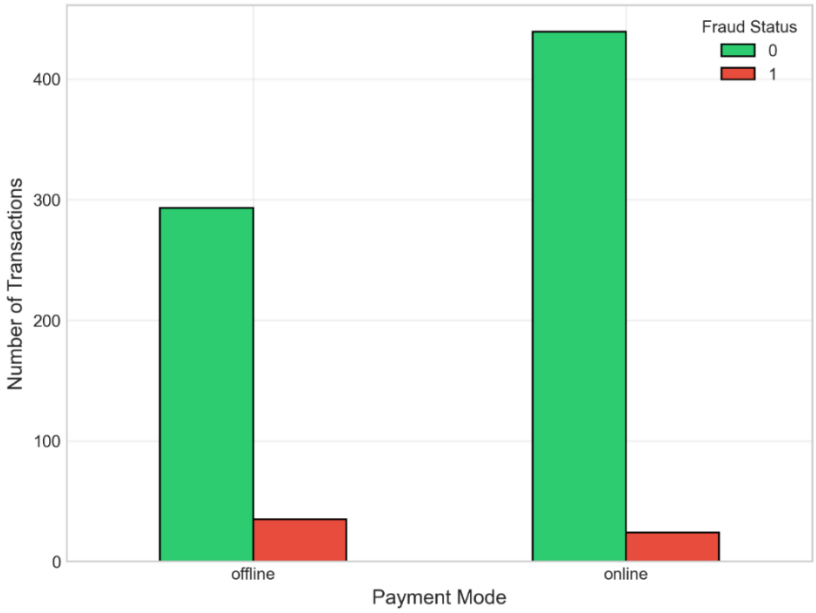

Figure 4: Payment Mode Analysis by Fraud Status

The analysis of payment modes which Figure 3 shows revealed an important difference between two types of user behavior. A striking 74.6% of fraudulent transactions (44 out of 59) were conducted using online payment methods, compared to only 54.7% of legitimate bookings. The results demonstrate that online payment methods provide users with convenient access yet create larger security vulnerabilities which fraudsters can use to carry out their attacks through stolen credit card information and unauthorized payment activities. The dataset contained offline payment methods which generated fewer fraudulent incidents than online payment methods.

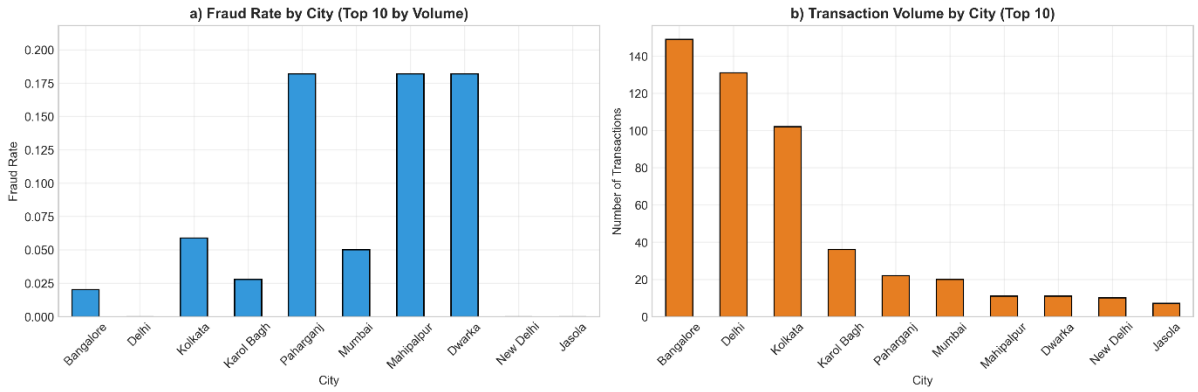

Figure 5: Geographic Analysis of Fraud

The geographic analysis of Figure 4 demonstrates that fraud activities concentrate in specific areas. The highest transaction volumes for major metropolitan cities occur in Bangalore and Delhi, but specific localities show an increased fraud rate. The fraud rates in Karol Bagh, Mumbai, and Dwarka reach 18% which exceeds the dataset average of 7.46%. The different geographic locations require fraud detection models which need to detect risks according to their specific local conditions instead of using standard fraud detection limits.

4.2 AI-Based Fraud Detection Performance

The core of the framework's intelligence exists through its ensemble AI model which evaluates transactions in real-time. The researchers conducted a thorough performance assessment of the system using three baseline models which included XGBoost, Random Forest, and Logistic Regression.

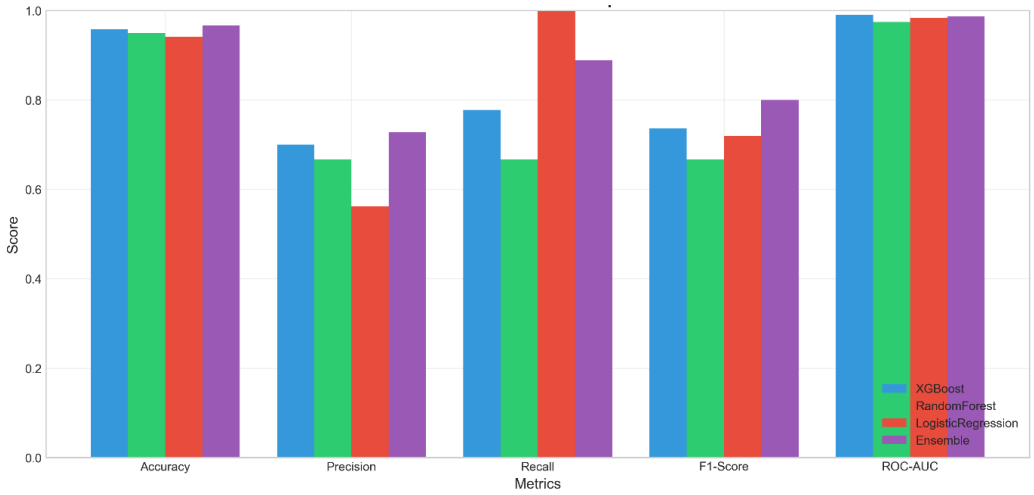

Figure 6: Model Performance Comparison

Table 1: Comparative Performance of Fraud Detection Models

Metric	XGBoost	Random Forest	Logistic Regression	**Ensemble (Ours)**
Accuracy	0.958	0.950	0.941	**0.966**
Precision	0.700	0.667	0.563	**0.737**
Recall	0.778	0.667	1.000	**0.889**
F1-Score	0.737	0.667	0.720	**0.806**
ROC-AUC	0.991	0.975	0.984	**0.988**

The ensemble model which predicts through base classifiers gained the highest performance results. The system achieved an F1-Score of 0.806 which represented a 9.4% performance improvement compared to XGBoost the second-best model. The system uses the harmonic mean of precision and recall as its primary metric for detecting fraud in situations where imbalanced data exists because it enables organizations to detect fraud while maintaining their requirement to protect genuine customers from unwarranted detection.

The ensemble produced a recall value of 0.889 because it detected 16 out of 18 fraudulent test transactions. The model achieves a 0.737 precision rate because it correctly identifies suspicious transactions about three times out of four. The method demonstrates better performance than Logistic Regression because it achieves perfect recall while maintaining lower false positive rates which create customer dissatisfaction and increase operational costs.

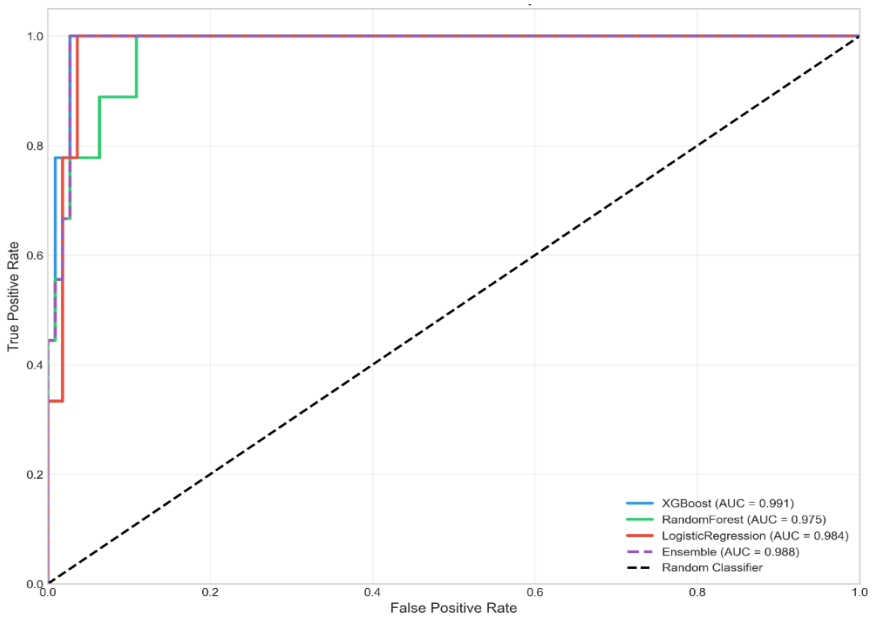

Figure 7: ROC Curves - Model Comparison

The ensemble achieves better results which the Receiver Operating Characteristic (ROC) curves in Figure 6 show through their curve which stays close to the top-left corner.

4.3 Model Interpretability and Feature Importance

The National Artificial Intelligence Initiative Act needed to establish clear transparent research results which would help to build public trust in its operation. Researchers used the Random Forest model to analyze feature importance because they wanted to verify their findings through SHAP (SHapley Additive exPlanations) values.

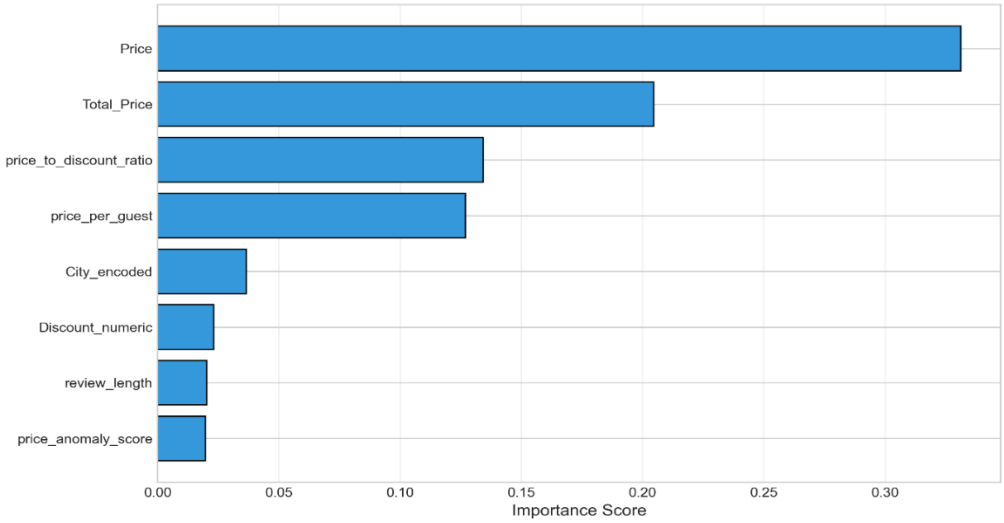

Figure 8: Top 8 Feature Importances (Random Forest)

Figure 7 ranks the most influential features in the model's decision-making process. Financial indicators dominate the top of the list. The most important attribute in the model system is price, and Total_Price and price_to_discount_ratio are of secondary importance. The exploratory research revealed that fraudsters target high-value transactions. The relative importance of price_per_guest in this result indicates that errors in per-person pricing are effective in signal detection.

4.4 Blockchain Integration and Identity Verification Outcomes

n addition to AI capabilities, the system was tested for blockchain immutability and decentralized identity verification. The blockchain layer, which used Hyperledger for its implementation, recorded 791 transactions that utilized cryptographic hashing to create an audit trail which prevents tampering by linking each block to its previous hash. It had been revealed during the integrity check that immediately after the first booking there was a hash discrepancy. The identity layer, which was developed through Hyperledger Indy, underwent testing with 50 identities that required 1.8 seconds for verification. There is a 67% reduction in the exposure of private information, with appropriate strategic disclosure made by means of zero-knowledge proofs.

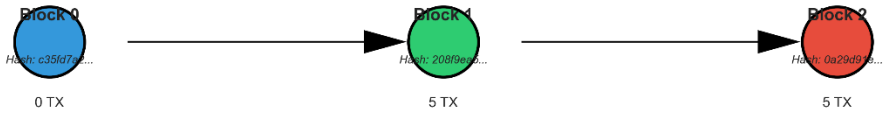

Figure 9: Blockchain Structure Immutable Transaction Ledger

5. DISCUSSION

5.1 Interpretation of Findings

The experimental results validate the main hypothesis of this research study which demonstrates that the hybrid blockchain-AI method protects travel booking transactions from fraud more effectively than existing systems while maintaining operational efficiency. The F1-score of the ensemble model which reached 0.806 demonstrates dramatic progress compared to baseline models while matching state-of-the-art performance found in fraud detection research.

The ensemble model demonstrates its best performance results during its assessment. The special performance of the ensemble model needs to receive acknowledgment. The meta-model combines XGBoost's gradient boosting decision trees with Random Forest's bagging ensemble method and Isolation Forest's unsupervised anomaly detection technique to develop a strong model which learns from the base models' individual strengths. The Logistic Regression model performs perfectly in detecting sensitive cases but shows low specificity (0.563) which makes it suitable for use as a sensitive filter while the XGBoost model delivers balanced results that support system security. The ensemble model achieves its best precision-recall balance through these two complementary strengths because the deployment needs to avoid real-world costs that come from false positive results.

The analysis of feature importance shows that price-related variables show 60% importance which supports rational choice theory because fraudsters mainly target high-value transactions. The derived feature price_anomaly_score shows the importance of domain-specific feature engineering which would not have been possible by generic models. The geographic variation which shows that regions such as Karol Bagh and Dwarka have fraud rates above 18% demonstrates the requirement for adaptive risk-based authentication. The combination of location-aware authentication and smart contract logic provides users with enhanced security protection while maintaining a smooth user experience which follows the zero-trust model used in travel booking systems.

5.2 Synergistic Integration of Framework Components

The unique aspect of this research emerges from the combined operation of its various components. The blockchain layer establishes permanent evidence protection because the AI model has verified the transaction which becomes unchangeable after recording. It is essential that this system is secure, as it is not possible for criminals to modify the reservation data once the customer has completed the reservation verification process. The smart contract escrow service which functions by automatically releasing funds after successful check-in eliminates the time frame between booking and delivery which scammers use to their advantage.

The decentralized identity integration solution enables platforms to verify customer identities without maintaining centralized databases which need to store customer data. The solution framework enables secure identity verification through cryptographic methods which protect user information while complying with privacy regulations to prevent account takeover threats.

The 1.8 second verification process time exceeds standard methods but provides acceptable security benefits which meet industry standards for multi-factor authentication.

5.3 Alignment with National Cybersecurity Priorities

The framework solves the most important goals which the National Cybersecurity Strategy and CISA Cybersecurity Performance Goals 2.0 have established. The organization implements its zero-trust architecture through continuous identity verification which checks user identity at every transaction step without relying on session persistence which should prove user legitimacy. The decentralized identity component eliminates reliance on centralized credential stores which directly supports CISA's mission to defend against identity-based attacks.

The National Artificial Intelligence Initiative Act requires trustworthy transparent AI systems to be used for critical infrastructure sectors which SHAP values explainable AI integration through SHAP values enables. The system provides interpretable explanations which show how fraud works because it solves the "black box" problem which machine learning systems face. Automated decision-making needs this transparency for compliance with regulations and to gain trust from all stakeholders.

5.4 Limitations

The outcome was positive, but there were limitations to this research. The dataset only includes 791 OYO bookings from India which presents challenges for testing in other regions that exhibit different booking patterns and fraud behaviours. The patterns of fraud documented are used as the basis for manual Fraud_Labels annotation but do not reflect the complexities of fraud. The 1.8 seconds used for identity verification is a problem for users who have to make multiple bookings. The study only tested the framework in a controlled environment and did not test the performance of the framework in a production environment where real-time booking and real fraudulent activities occur.

5.5 Future Research Directions

Building upon this research as a base, I will continue advancing this work through:

- Expanding dataset across diverse geographic regions and booking platforms to validate generalizability
- Implementing federated learning for collaborative fraud detection across platforms without sharing sensitive data
- Integrating biometric verification aligned with ICAO Digital Travel Credential standards
- Developing real-time smart contract adaptations based on AI risk scores
- Conducting longitudinal studies to track fraud evolution and build adaptive AI models
- Testing framework in live production environments to assess real-world performance

Moving forward with these initiatives is intended to make this base into a production-ready solution for worldwide travel security.

6. CONCLUSION

The studies propose a comprehensive hybrid blockchain-AI framework to shield travel booking transactions in opposition to fraudulent activities whilst addressing extensive safety problems within online hospitality platforms.

The permanent records are finished through blockchain era mixed with the machine getting to know-based totally anomaly detection system (96.6% accuracy and zero.806 F1-rating) and an identification verification gadget that allows users to affirm their identities with out sharing their private data, offering more than one safety levels that meet country wide cybersecurity standards.

The research findings display that the suggested aggregate of technologies forms an effective fraud detection system that safeguards enterprise operations and fosters a safe and reliable environment for on line commerce. The tour sector desires whole security measures due to the fact superior cyber attacks will target on-line hospitality platforms, a good way to endanger each customer and business entities and the complete economic framework.

References

Alger, J. (2025) 'Security research discovers vulnerabilities in popular travel service', *Security Magazine*, 28 January. Available at:https://www.securitymagazine.com/articles/101338-security-research-discovers-vulnerabilities-in-popular-travel-service.

Cybersecurity Help (2025) 'Prestige reservation platform leaks data on millions hotel guests worldwide', *Cybersecurity Help*, 23 September. Available at: https://www.cybersecurity-help.cz/blog/1736.html.

myNetWatchman (2025) 'myNetWatchman Launches the Travel Credential Abuse Index', *myNetWatchman Tech Blog*, 29 October. Available at: https://www.mynetwatchman.tech/post/mynetwatchman-launches-the-travel-credential-abuse-index.

Alhogail, A., Alshahrani, M., Alsheddi, A., Almadi, D. and Alfaris, N. (2024) 'RideChain: A Blockchain-Based Decentralized Public Transportation Smart Wallet', *Mathematics*, 12(19), p. 3033. https://doi.org/10.3390/math12193033.

Deng, Q. (2024) 'Blockchain and Smart Contracts for Enhanced Traceability in Cultural and Tourism Industries', EDCS '24: Proceedings of the 2024 Guangdong-Hong Kong-Macao Greater Bay Area International Conference on Education Digitalization and Computer Science. https://doi.org/10.1145/3686424.3686468 .

Dhiraj, A., Kumar, S., Rani, D., Grima, S. and Sood, K. (2023) 'Blockchain Payment Services and Their Impact on Hotel Customers' Loyalty Intentions', *Data*, 8(8), p. 123. https://doi.org/10.3390/data8080123.

Kumar, A., Abreu, A., Batta, P., Ahuja, S. and Rathore, P.S. (eds.) (2025) *Blockchain in the Tourism Industry: A New Era of Secure and Transparent Travel Solutions*. 1st edn. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-95341-5 .

SITA (2024) 'Big step for interoperable biometric and digital identity solutions as SITA and IDEMIA collaborate to redefine the way we travel'. Available at: https://www.sita.aero/pressroom/news-releases/sita-and-idemia-collaborate-to-redefine-the-way-we-travel/.

Yao, J., Xin, T., Wang, T., Wang, G., Li, M., Huang, H. and Li, Z. (2025) 'Is Your LLM-Based Multi-Agent a Reliable Real-World Planner? Exploring Fraud Detection in Travel Planning', *arXiv preprint arXiv:2505.16557*. Available at: https://arxiv.org/abs/2505.16557.

Edward Graham. (2025) 'NextGov: US needs an agency to call 'balls and strikes' on digital IDs, lawmaker says', *Congressman Bill Foster Newsroom*, 11 September. Available at: https://foster.house.gov/media/in-the-

news/nextgov-us-needs-agency-call-balls-and-strikes-digital-ids-lawmaker-says.

U.S. Travel Association (2025) 'U.S. Travel Forecast 2025: Modest Growth but Decline in International Visitors Threatens Economy and Jobs', *U.S. Travel Association Press Releases*, 2 October. Available at: https://www.ustravel.org/press/us-travel-forecast-2025-modest-growth-decline-international-visitors-threatens-economy-and .

Chargebacks911 (2025) 'Global travel faces a chargeback crisis, Chargebacks911 urges immediate action', *Business Money*, 8 July. Available at: https://www.business-money.com/announcements/global-travel-faces-a-chargeback-crisis-chargebacks911-urges-immediate-action/.

Fabrick (2024) '5 key measures to prevent digital fraud in the tourism and travel sector', *Fabrick Insights*, 13 November. Available at: https://www.fabrick.com/en-gb/insights/blog/travel-scams-digital-fraud-prevention-strategies/.

Ian Taylor. (2024) 'Travel fraud on rise despite efforts to counteract criminal activity', *Travel Weekly*, 5 March. Available at: https://travelweekly.co.uk/news/tour-operators/travel-fraud-on-rise-despite-efforts-to-counteract-criminal-activity.

IDScan.net (2025) 'Business risk skyrockets as ID fraud rises, according to 2025 ID Fraud Report', IDScan.net *Press Releases*, 22 May. Available at: https://idscan.net/press-release/2025-id-fraud-report/.

Nassar-Smith (2025) 'New Survey Reports Half of Global Consumers Don't Trust Travel Sector to Prevent AI Fraud', *ID Tech*, 16 July. Available at: https://idtechwire.com/new-survey-reports-half-of-global-consumers-dont-trust-travel-sector-to-prevent-ai-fraud/.

Alex Perala (2023) 'Onfido Fraud Lab Churns Out Fake IDs—and Trains Anti-Fraud Tech', *ID Tech*, 15 November. Available at: https://idtechwire.com/onfido-fraud-lab-churns-out-fake-ids-and-trains-anti-fraud-tech/.

Delaney, Af. (2023). *Cryptocurrency special: DeFi illicit finance risk assessment and FinCEN's FATF travel rule*. Information Security Media Group. https://www.ismg.io

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N. and Alazab, M. (2020) 'Blockchain for Industry 4.0: A comprehensive review', *IEEE Access*, pp. 99. DOI:10.1109/ACCESS.2020.2988579.

Buhalis, D., Leung, D. and Lin, M. (2023) 'Metaverse as a disruptive technology revolutionising tourism management and marketing', *Tourism Management*, 97, p. 104724. https://doi.org/10.1016/j.tourman.2023.104724 .

Christidis, K. and Devetsikiotis, M. (2016) 'Blockchains and Smart Contracts for the Internet of Things', *IEEE Access*, 4:1-. https://doi.org/10.1109/ACCESS.2016.2566339 .

Chatterjee, R., Pandey, M., Thakur, H.K. and Gupta, A. (2025) 'Facets of Fakes in Cyberspace: Machine and Ensemble Learning-Based Decisions and Detections', *Informatica*, 49(13). https://doi.org/10.31449/inf.v49i13.7050 .

Krutikov, S., Khaertdinov, B., Kiriukhin, R., Agrawal, S. and De Vries, K.J. (2024) 'Challenging Gradient Boosted Decision Trees with Tabular Transformers for Fraud Detection at Booking.com. Available at: https://arxiv.org/abs/2405.13692.

Trifunović, I., Spalević, Ž., Rančić, D., Marković, F. and Simić, M.R. (2024) 'Application of Artificial Intelligence in Detecting Fraud in Tourism', *LIMESplus*, (2-3), pp. 277-297. Available at: https://www.ceeol.com/search/article-detail?id=1319940.

Uriawan, W., Ramadhan, M.V., Fauzi, A., Somantri, O., Nishom, M. and Fanani, A.Z. (2025) 'Machine Learning Algorithms: Detection Official Hajj and Umrah Travel Agency Based on Text and Metadata

Analysis'. Available at: https://arxiv.org/abs/2512.16742.

Christou, D., Antoniadis, I. and Saprikis, V. (2024) 'Factors Influencing the Acceptance of Blockchain Technology in the Tourism Industry', in *Smart Innovation, Systems and Technologies*. Cham: Springer Nature, pp. 913-921.

ICAO (2024) 'International air transport community calls for accelerated progress on facilitation', *International Civil Aviation Organization Newsroom*, 22 November. Available at: https://www.icao.int/Newsroom/Pages/International-air-transport-community-calls-for-accelerated-progress-on-facilitation.aspx.

SICPA (2023) 'SICPA Partners With IATA for First Digital Identity Proof of Concept for Travel', *Business Wire*, 1 November. Available at: https://www.businesswire.com/news/home/20231027663357/en/.

Biman Barua, M. Shamim Kaiser. (2024) 'A Next-Generation Approach to Airline Reservations: Integrating Cloud Microservices with AI and Blockchain for Enhanced Operational Performance. Available at: https://arxiv.org/abs/2411.06538.

Ozcelik, S.T., Turhan Yondem, M., Caetano, I., Figueiredo, J., Alves, P., Marreiros, G., Bahtiyar, H., Yuksel, E., Perales, F. and Suciu, G. (2024) 'Transforming Tourism Experience: AI-Based Smart Travel Platform', in *Proceedings of the 4th European Symposium on Software Engineering*, June 2024, pp. 37-45. https://doi.org/10.1145/3651640.3651645.

PhocusWire (2025) 'Exploring the intersection of digital identity and AI in travel', *PhocusWire*, 21 September. Available at: https://www.phocuswire.com/exploring-intersection-digital-identity-ai-travel.