American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Encrypted Forest Trekking Ticket Booking And Real-Time Validation Platform

Manubothula Suprathika, Karramareddy Sharmila*
Vaagdevi Engineering College, Warangal, 506005, Telangana, India.
*Correspondence: Karramareddy Sharmila (sharmilakreddy@gmail.com)

ABSTRACT

With the rapid growth of digital tourism and forest-based adventure activities, managing trekking permissions, ticket reservations, and visitor information has become increasingly complex and security-sensitive. Traditionally, trekking bookings and validations were maintained using manual registers or semi-digital systems that relied on paper records or unsecured databases. These approaches often resulted in delayed booking confirmation, inaccurate slot availability, unauthorized record modifications, lack of transparency, poor audit capabilities, and difficulty in preventing duplicate bookings and overbooking. Furthermore, the absence of secure data management mechanisms exposed sensitive user information to potential security threats, creating the need for a reliable and automated trekking management solution. The proposed system introduces a secure web-based trekking ticket booking and real-time validation platform that integrates role-based authentication, automated slot verification, encrypted document management, and controlled information sharing within a unified framework. Advanced Encryption Standard (AES) encryption and RACE Integrity Primitives Evaluation Message Digest-160 (RIPEMD-160) hashing are employed to ensure the confidentiality, integrity, and protection of sensitive booking records and user data. The platform is developed using the Flask framework with TinyDB as the database and supports secure user registration, online route exploration, automated booking confirmation, schedule management, administrative monitoring, and encrypted file handling. Real-time validation prevents overbooking and scheduling conflicts, while role-based access control restricts unauthorized activities. The research enhances operational transparency, strengthens data security, improves booking efficiency, and provides a scalable foundation for secure smart tourism and digital forest management.

Keywords: Trekking Ticket Booking System, Role-Based Access Control (RBAC), Advanced Encryption Standard (AES), RIPEMD-160 Hashing, Real-Time Booking Validation, Smart Tourism

1. INTRODUCTION

Ecotourism is considered as the cornerstone of sustainable tourism due to its heightened emphasis on environmental protection. As defined by the Quebec Declaration on Ecotourism (2002), ecotourism not only strives to minimise negative impacts on nature but also actively promotes nature conservation and adopts an educational character, as some participants may undertake or join in specific conservation activities. Ecotourism is most commonly practised in areas of exceptional natural value, such as forests. When organising ecotourism activities, particular attention is paid to minimising the negative impact on the environment and meeting the expectations of tourists, who are primarily interested in interacting with natural values [1]. According to, ecotourism is understood as a purposeful journey to areas of natural value for cognitive, inspirational, and self-realisation purposes, without compromising the integrity of the environment. Ecotourism encompasses all forms of tourism (adventure and mass tourism) and some forms of recreation (hunting, fishing, and gathering). Rural areas, often associated with agriculture, hold a special place for ecotourism [2]. However, beyond their typically agrarian function, rural areas also

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

contribute to the ecological, social, and economic integrity of regions. Tourism in rural areas is undergoing a constant transformation in both demand and supply. The reference literature [3] mentions various classifications of tourism in rural areas, increasingly highlighting the significance of tourism forms based on specific destinations. One of them is forest tourism practised in forested areas. According to, "it is a peculiar unique type of tourism activity with a characteristic destination, that is, forested areas. Considering other components of travel, forest tourism comprises residential tourism and touring, as well as other types of tourism where forested areas are the destination". Therefore, the literature also mentions forest recreation [4], "which is a term generic to forest tourism, similar to how recreation is to tourism and all its forms can be classified as tourism activities consistent with the principles of sustainable development in rural areas and urban forests and forest parks". "Therefore, activities taking place in the forest include active leisure (such as cycling, running, and walking) and new outdoor activities such as bushcraft and geocaching. The above-mentioned elements, combined with an improvement in the living standard and ecological awareness, make the social function of the forest more significant to people than its productive function" [5].

1.1 RESEARCH MOTIVATION

The rapid digital transformation of industries such as tourism, travel services, eco-adventure management, and public sector forest administration has resulted in the continuous generation of large volumes of operational and user-centric data. Real-time companies managing trekking services and tourism platforms rely heavily on data analysis to understand booking patterns, seasonal demand, user behaviour, and resource utilization across different routes and schedules. Analysing this data enables organizations to optimize capacity planning, improve safety management, reduce operational bottlenecks, and enhance customer experience. Additionally, data-driven insights help organizations identify irregular activities, fraudulent bookings, and abnormal access behaviour, which are critical for maintaining system reliability. As digital interactions increase, the dependency on accurate, timely, and trustworthy data analysis becomes essential for informed decision-making.

1.2 PROBLEM DEFINITION

Modern trekking and tourism management systems face significant challenges related to data security, access control, and operational accuracy. Many existing platforms store sensitive user information, booking details, and operational documents without adequate protection, making them vulnerable to data breaches and unauthorized access. The absence of strong integrity verification mechanisms allows data tampering, which can lead to incorrect booking records and administrative disputes. Additionally, real-time booking systems often struggle with synchronization issues, resulting in overbooking or inconsistent slot availability. Limited role separation further increases the risk of internal misuse or accidental data modification. These issues collectively reduce system reliability, compromise user trust, and create operational inefficiencies for organizations managing large-scale trekking and tourism activities.

2. LITERATURE SURVEY

Yonghua Zhan, et al. [6] proposed a blockchain-enhanced privacy-preserving electronic ticketing system named PriTKT for Internet of Things (IoT) environments. The framework integrated blockchain technology with Structure-Preserving Signatures (SPS), Unlinkable Redactable Signatures (URS), and Zero-Knowledge Proofs (ZKP) to provide secure and privacy-aware ticket management. The proposed system supported flexible policy-based ticket purchasing while ensuring user anonymity and preventing unauthorized tracking of user activities. By utilizing blockchain, the platform maintained immutable transaction records, improved transparency,

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

and eliminated the need for trusted third parties. Sheng-Hui Chai, et al. [7] developed an online bus ticket booking system where tickets were automatically generated as encrypted Quick Response (QR) codes after successful reservation. The study aimed to reduce physical contact, minimize waiting time, and eliminate the need for printed tickets, particularly during the COVID-19 pandemic. A cryptographic mechanism was incorporated into the QR code to prevent unauthorized access and information leakage, thereby improving ticket security and user convenience. Giovanni Tuveri, et al. [8] investigated technologies supporting automatic ticket validation for public transportation systems. The study introduced the Beep4Me platform, which extended an existing mobile ticketing solution by incorporating automated validation mechanisms to record passenger entry and exit information accurately. The proposed architecture improved ticket verification efficiency, enhanced service monitoring, and supported additional intelligent functionalities for modern transportation systems. Yunlin Guan, et al. [9] focused on optimizing transportation operations by considering passengers with multiple-trip requests, homogeneous vehicle fleets, pickup and delivery time constraints, and mixed passenger loads. The study proposed a Genetic Algorithm (GA)-based optimization model that maximized operational profit while minimizing service costs. The implementation improved scheduling efficiency, optimized resource allocation, and enhanced overall transportation service effectiveness.

Robert Goecke, et al. [10] examined browser-based online booking systems as self-service platforms that transformed business-to-customer (B2C) travel services. The study highlighted the role of the Internet and World Wide Web as fundamental technologies supporting electronic tourism applications, online reservation systems, and Central Reservation System (CRS) web interfaces. The proposed architecture simplified online booking processes, improved customer accessibility, and supported efficient travel service distribution through web-based technologies. Kaluza, et al. [11] evaluated several appointment scheduling strategies and analysed their effectiveness under different operational scenarios. The study demonstrated that offering every available appointment option does not always produce optimal outcomes due to quality inference effects influencing customer decisions. The findings provided valuable management insights for selecting suitable appointment allocation strategies that balance operational efficiency and customer satisfaction. Paola Noemi San Agustin-Crescencio, et al. [12] proposed a three-layer security mechanism for protecting QR-code-based information. The first layer employed Advanced Encryption Standard (AES) encryption to ensure data confidentiality, while the second layer integrated two independent dichromatic QR codes into a single chromatic structure using multiplexing techniques. The third layer introduced wavelength-controlled recovery, which functioned both as a secure decoding mechanism and a physical access control system. This multi-layered approach significantly enhanced information security and protected QR code data from unauthorized access. Keattikorn Samarnggoon, et al. [13] investigated the implementation of a metaverse-based ticketing and educational environment by evaluating its architecture, usability, and effectiveness. The study assessed user experience through questionnaires and qualitative feedback collected during field experiments, demonstrating that immersive virtual environments can improve user interaction and support customized digital service delivery.

Sina Rafati Niya, et al. [14] proposed DeTi, a decentralized electronic ticketing platform developed using Ethereum smart contracts for secure event ticket distribution. The platform provided dedicated service management

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

capabilities while enabling users to verify ticket authenticity and regulate ticket resale within secondary markets. The decentralized architecture improved transparency, prevented fraudulent ticket duplication, and eliminated dependence on centralized authorities. Amjad Aldweesh, et al. [15] introduced a blockchain-based electronic ticketing framework that eliminated the need for third-party intermediaries during ticket issuance and validation. By leveraging blockchain technology, the proposed model enhanced transaction transparency, reduced the possibility of data leakage, strengthened user privacy, and improved the overall security of electronic ticket management systems. Abdullah Aljuffri, et al. [16] evaluated lightweight implementations of AES encryption against both profiled and non-profiled side-channel attacks. The study compared an unprotected AES implementation with a Domain-Oriented Masking (DOM)-based protected implementation to analyse their resistance against cryptographic attacks. Experimental results demonstrated that the protected implementation significantly improved security while maintaining computational efficiency, highlighting its suitability for lightweight and resource-constrained environments requiring secure encryption mechanisms.

3. PROPOSED SYSTEM

The proposed methodology as shown in Fig. 1 adopts a structured and secure approach for managing trekking ticket booking, operational coordination, and real-time validation in a multi-user environment. The study focuses on handling sensitive user information, booking records, route schedules, and administrative data while ensuring confidentiality, integrity, and controlled access. It integrates authentication mechanisms, encrypted data handling, role-based authorization, and real-time validation into a unified operational workflow. User interactions are carried out through a web-based interface and processed by a centralized server that enforces access control and coordinates backend operations. TinyDB maintains consistency across all operational records, while cryptographic techniques protect stored and transmitted data. Real-time validation mechanisms ensure accurate slot allocation, prevent overbooking, and support reliable system behaviour even under high user load.

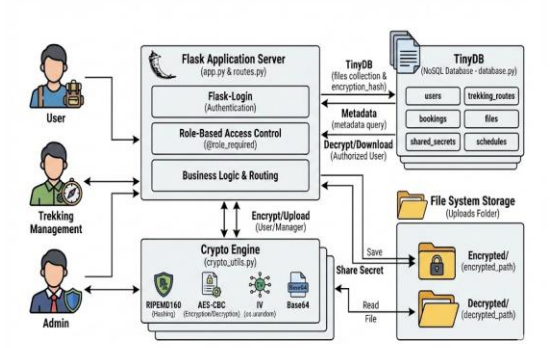

Fig. 1: Proposed system architecture for ticket booking and real-time validation platform

User Interaction and Request Initiation: Users such as general users, trekking management staff, and administrators interact with the system through a web-based interface. Actions like login, booking requests, file uploads, and data access are initiated from the client side and converted into HTTP requests sent to the backend server.

Authentication and Role Validation: The Flask application server processes incoming requests using Flask-Login to authenticate users. Once authenticated, role-based access control ensures that each request is permitted only if the user's role matches the required authorization level, preventing unauthorized operations.

Business Logic Processing and Routing: After access validation, the server executes the appropriate business logic related to bookings, schedules, file handling, or data sharing. Routing mechanisms direct requests to specific backend functions that coordinate database access, encryption tasks, and operational workflows.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

Cryptographic Processing and Secure Data Handling: Sensitive files and textual data are passed to the cryptographic engine, where RIPEMD-160 hashing is used for integrity and key derivation. Encryption and decryption operations are performed using AES, supported by random initialization vectors and encoding techniques to ensure secure data protection.

Persistent Storage and Metadata Management: Operational data such as users, routes, bookings, schedules, encrypted file paths, and shared secrets are stored in a TinyDB database. The database maintains structured metadata while the actual encrypted and decrypted files are stored separately in the file system.

Secure Retrieval, Validation, and Response Delivery: When authorized users request data access, the system verifies permissions, retrieves metadata, and performs decryption if required. Integrity checks are applied before delivering responses back to the user, ensuring accurate, secure, and reliable system interaction.

3.1 AES Encryption

AES is a symmetric block cipher as shown in Fig. 2 used to securely encrypt and decrypt data using a single shared secret key. It operates on fixed-size data blocks and applies multiple transformation rounds to achieve strong confidentiality. AES is designed for high performance and is suitable for encrypting large volumes of data efficiently. The encryption process combines substitution, permutation, and key mixing operations to resist cryptographic attacks. Due to its speed and security, AES is widely adopted in secure storage and data transmission systems. Proper key handling and mode selection are critical to maintaining AES security.

Plain Data and Key Input: AES encryption begins with fixed-size plaintext blocks along with a secret symmetric key. The same key is later required for decryption, making secure key handling essential.

Key Expansion: The original AES key is expanded into multiple round keys using a deterministic key schedule. Each round key is unique and strengthens resistance against brute-force and cryptanalysis attacks.

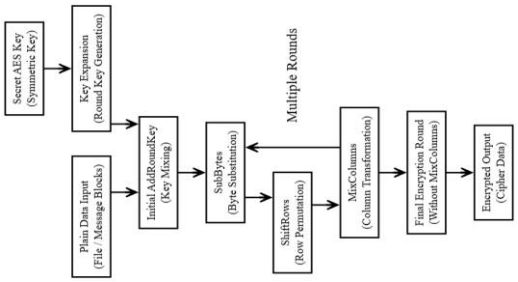

Fig. 2: Internal Workflow of AES encryption

Initial Add Round Key Operation: The plaintext block is combined with the first-round key using a bitwise XOR operation. This step immediately binds the data to the encryption key.

Core Transformation Rounds: Each encryption round applies Sub Bytes, Shift Rows, and Mix Columns operations to introduce confusion and diffusion. These transformations obscure statistical patterns in the original data.

Final Encryption Round: The final round performs substitution and permutation without the Mix Columns step. This ensures proper alignment for secure ciphertext generation.

Ciphertext Generation: After completing all rounds, the transformed data becomes ciphertext. The encrypted output is unintelligible without the correct AES key.

3.2 AES Decryption

AES decryption is the symmetric process of converting encrypted ciphertext back into its original readable form using the same secret key used during encryption. It applies a series of inverse mathematical transformations to undo the effects of encryption rounds. The decryption process as depicted in Fig. 3 follows the reverse order of encryption operations, ensuring accurate data recovery. Each round reverses substitution, permutation, and mixing applied during encryption. AES decryption guarantees data confidentiality by ensuring that

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

only entities possessing the correct key can reconstruct the original data. Secure and correct key usage is essential for successful decryption.

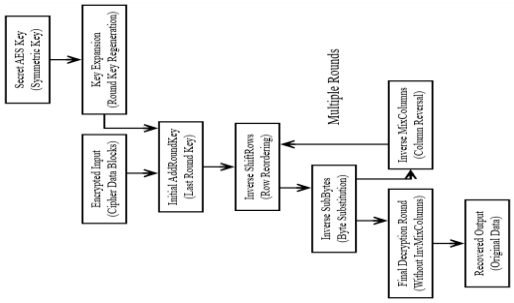

Fig. 3: Internal Workflow of AES decryption

Ciphertext and Key Input: AES decryption starts with the encrypted ciphertext, and the same secret key used during encryption. Without the correct key, decryption is computationally infeasible.

Key Expansion: The AES key is expanded into a set of round keys identical to those generated during encryption. These round keys are applied in reverse order during decryption.

Initial Add Round Key Operation: The ciphertext block is combined with the final round key using a bitwise XOR operation. This step initiates the reversal of encryption transformations.

Inverse Transformation Rounds: Each round applies inverse operations Inverse Shift Rows, Inverse Sub Bytes, and Inverse Mix Columns to systematically undo encryption effects. These steps restore the original data structure gradually.

Final Decryption Round: The final round excludes the Inverse Mix Columns operation and applies only inverse substitution and permutation. This completes the reversal process accurately.

Plaintext Recovery: After all rounds are executed, the original plaintext data is recovered. The output matches the original input provided before encryption.

3.3 RIPEMD-160 Hashing

RIPEMD-160 is a cryptographic hashing technique as shown in Fig. 4 designed to generate a fixed-length 160-bit hash value from input data of arbitrary size. It is widely used for data integrity verification due to its resistance to collisions and preimage attacks. The hashing process transforms input data into a unique digest that cannot be reversed to obtain the original data. Even a small change in the input produces a completely different hash, ensuring strong integrity protection. RIPEMD-160 operates through multiple rounds of nonlinear operations, bitwise functions, and modular additions. Its deterministic and lightweight nature makes it suitable for secure systems requiring reliable integrity checks and key derivation support.

Message Preparation and Padding: The input data is first converted into a binary stream and padded to meet the required block size. Padding ensures that the total length of the message is aligned to the algorithm's processing structure. The original message length is appended to preserve data completeness.

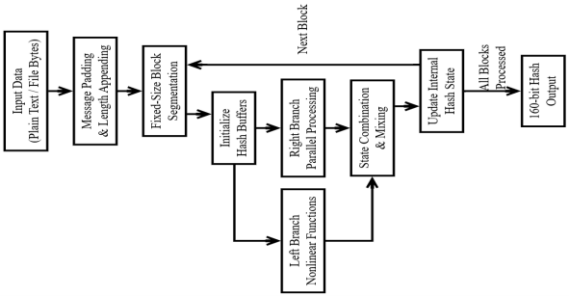

Fig. 4: Internal Workflow of RIPEMD-160.

Block Segmentation and Initialization: The padded message is divided into fixed-size blocks for sequential processing. Initial hash buffers are set with predefined constants that serve as the starting state. These buffers are used to accumulate transformations across all message blocks.

Parallel Compression Processing: Each data block is processed through two parallel computation paths known as the left and right branches. Nonlinear functions, bitwise operations, and modular additions are applied in multiple rounds. These parallel paths enhance resistance to cryptographic attacks.

State Combination and Update: The outputs from both parallel branches are combined using arithmetic and logical operations. The internal

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

hash state is updated by mixing previous values with newly computed results. This chaining process ensures dependency across all processed blocks.

Final Hash Generation: After all message blocks are processed, the final internal state is concatenated to produce a 160-bit hash value. This hash serves as a compact and irreversible representation of the input data. The output is used for integrity validation or cryptographic key derivation.

9.4 Results Description

Fig. 5 illustrates the Manage Trekking Routes Screen designed for configuring and maintaining trekking route information. The interface supports route creation, modification, and activation based on difficulty, duration, capacity, and pricing parameters. It enables administrators to dynamically control trekking availability while preventing overbooking scenarios. The screen plays a critical role in operational planning and resource allocation. It ensures structured route management aligned with system-wide booking and validation processes.

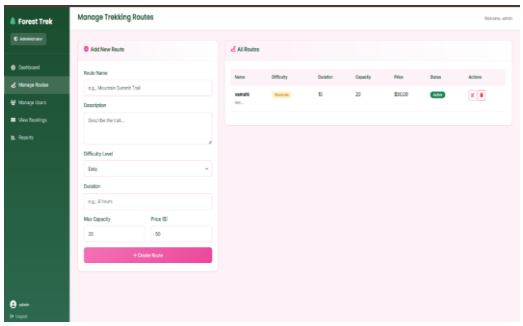

Fig. 5: Manage Trekking Routes Screen

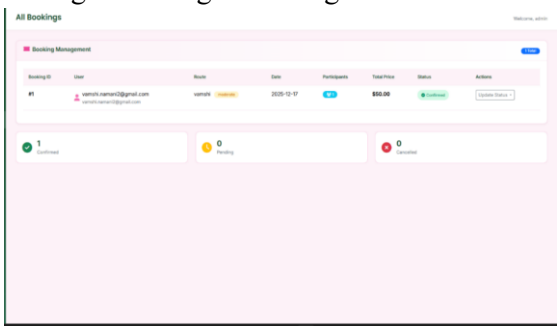

Fig. 6: Viewing Bookings Screen

Fig. 6 illustrates the Viewing Bookings Screen, which presents detailed records of trekking reservations within the system. It enables administrators to track booking identifiers, participant details, route selections, and booking status in a centralized view. The interface supports booking lifecycle management including confirmation, pending review, and cancellation handling. It facilitates transparency and auditability of trekking transactions. This screen is essential for enforcing real-time validation and secure booking control.

Fig. 7 illustrates the Trail Schedules Screen used for planning and managing trekking schedules across defined routes. The interface allows authorized personnel to create, update, and monitor trekking schedules based on date, time, and participant availability. It ensures controlled allocation of slots to prevent overcrowding and scheduling conflicts. The screen supports operational transparency by maintaining a centralized view of all active schedules. This module is critical for synchronizing route availability with booking and validation processes.

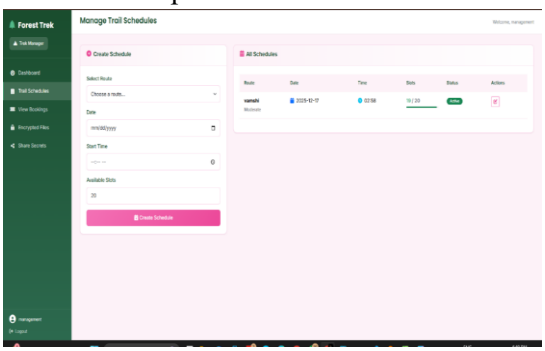

Fig. 7: Trail Schedules Screen

Fig. 8 illustrates the Booking Ticket Screen that facilitates the reservation of trekking routes by authenticated users. The interface supports selection of available treks, schedule confirmation, and participant allocation within predefined limits. It integrates booking validation logic to ensure consistency with route capacity and scheduling constraints. The screen forms a critical link between user intent and system-level booking enforcement. It ensures that trekking reservations are processed securely and systematically.

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

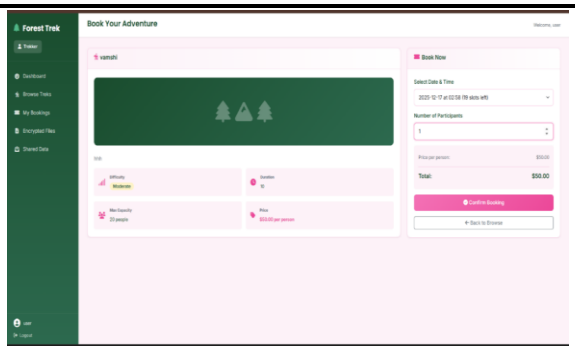

Fig. 8: Booking Ticket Screen

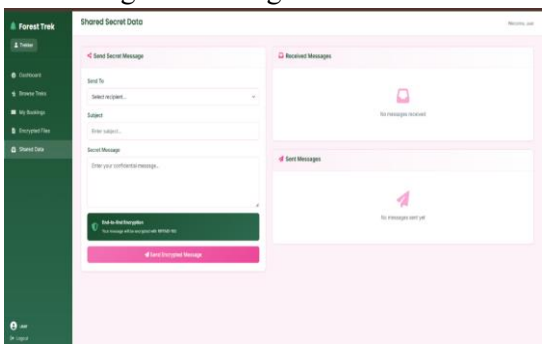

Fig. 9: Sharing Data Screen

Fig. 9 illustrates the Sharing Data Screen designed for secure exchange of confidential messages and information between system users. The interface supports end-to-end encrypted communication to protect sensitive operational and personal data. It enables controlled data dissemination while maintaining message confidentiality and access accountability. The screen separates sent and received data streams to improve traceability and auditing. This module reinforces secure collaboration within the trekking management ecosystem.

5. CONCLUSION

This research successfully demonstrates the design and implementation of a secure and efficient trekking ticket booking and real-time validation platform using a Flask-based web framework. The system integrates role-based authentication, real-time slot validation, encrypted file management, and controlled data sharing into a unified operational environment. By applying AES encryption and RIPEMD-160 hashing, the platform ensures strong confidentiality and data integrity for sensitive user records and operational documents. Performance improvements were achieved through lightweight TinyDB storage, optimized routing logic, and session-based request handling, which reduced response latency and improved concurrency handling during multiple booking requests. Real-time schedule verification effectively minimized overbooking and eliminated manual reconciliation delays. Modular architecture and separation of frontend, backend, cryptographic, and database layers enhanced maintainability and system stability. The system demonstrated reliable performance under concurrent user access and consistent booking workloads.

REFRENCES

[1] Weaver, D.; Lawton, L.J. Twenty years on: The state of contemporary ecotourism research. Tour. Manag. 2007, 28, 1168–1179.

[2] Saidmamatov, O.; Matyakubov, U.; Rudenko, I.; Filimonau, V.; Day, J.; Luthe, T. Employing ecotourism opportunities for sustainability in the Aral Sea Region: Prospects and challenges. Sustainability 2020, 12, 9249.

[3] Gonia, A.; Jezierska-Thöle, A. Sustainable Tourism in Cities—Nature Reserves as a 'New' City Space for Nature-Based Tourism. Sustainability 2022, 14, 1581.

[4] Bunruamkaew, K.; Murayama, Y. Land use and natural resources planning for sustainable ecotourism using GIS in Surat Thani, Thailand. Sustainability 2012, 4, 412–429.

[5] Krzymowska-Kostrowicka, A. Turystyka jako wędrówka po śladach zamierzchłego świata. Tourism 2005, 15, 29–39.

[6] Zhan, Y.; Yuan, F.; Shi, R.; Shi, G.; Dong, C. PriTKT: A Blockchain-Enhanced Privacy-Preserving Electronic Ticket System for IoT Devices. Sensors 2024, 24, 496. https://doi.org/10.3390/s24020496

American Journal of
AI Digital Transformation and Regenerative Pharmacist
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0418 www.zesterapublications.com Original Research Paper

[7] Chai, Sheng-Hui & Chong, Lee-Ying & Chin, Chong & Goh, Pey Yun. (2023). Bus Ticket Booking System using QR Code with AES Encryption. International Journal of Membrane Science and Technology. 10. 1854-1871. 10.15379/ijmst.v10i3.1846..

[8] Tuveri, G.; Garau, M.; Sottile, E.; Pintor, L.; Atzori, L.; Meloni, I. Beep4Me: Automatic Ticket Validation to Support Fare Clearing and Service Planning. Sensors 2022, 22, 1543. https://doi.org/10.3390/s22041543

[9] Guan, Y.; Wang, Y.; Yan, X.; Guo, H.; Zhao, Y. The One E-Ticket Customized Bus Service Mode for Passengers with Multiple Trips and the Routing Problem. Sustainability 2022, 14, 2124. https://doi.org/10.3390/su14042124

[10] Goecke, R. (2022). The Evolution of Online Booking Systems. In: Xiang, Z., Fuchs, M., Gretzel, U., Höpken, W. (eds) Handbook of e-Tourism. Springer, Cham. https://doi.org/10.1007/978-3-030-48652-5_27

[11] Kaluza, I., Voigt, G., Haase, K. et al. Control of Online-Appointment Systems When the Booking Status Signals Quality of Service. Schmalenbach J Bus Res 76, 397–432 (2024). https://doi.org/10.1007/s41471-024-00188-0

[12] San Agustin-Crescencio, P.N.; Hernandez-Gonzalez, L.; Guevara-Lopez, P.; Juarez-Sandoval, O.U.; Ramirez-Hernandez, J.; Estevez-Encarnacion, E.S. A Comprehensive QR Code Protection and Recovery System Using Secure Encryption, Chromatic Multiplexing, and Wavelength-Based Decoding. Appl. Sci. 2025, 15, 9708. https://doi.org/10.3390/app15179708

[13] Samarnggoon, K.; Grudpan, S.; Wongta, N.; Klaynak, K. Developing a Virtual World for an Open-House Event: A Metaverse Approach. Future Internet 2023, 15, 124. https://doi.org/10.3390/fi15040124

[14] Rafati Niya, S., Bachmann, S., Brasser, C. et al. DeTi: A Decentralized Ticketing Management Platform. J Netw Syst Manage 30, 62 (2022). https://doi.org/10.1007/s10922-022-09675-3

[15] Amjad Aldweesh, BlockTicket: A framework for electronic tickets based on smart contract PLOS ONE, 18(4), e0284166 - April 2023 https://doi.org/10.1371/journal.pone.0284166