Payment Method Selection: The system shall provide users with options to choose from multiple payment methods including credit/debit cards, digital wallets, and bank transfers during the checkout process.

UC Name	**Payment Method Selection (UC-301)**
Summary	Allows users to select a preferred payment method during the checkout process.
Dependency	Book Flight (UC-102)
Actors	Primary Actor: User (Passenger) Secondary Actor: System
Preconditions	User has initiated the checkout process and reached the payment step.
Description of the Main Sequence	1. System presents the available payment methods (credit/debit cards, digital wallets, bank transfers) to the user. 2. User selects a preferred payment method from the options provided. 3. System proceeds with the selected payment method for transaction processing.
Description of the Alternative Sequence	1a. If the user is not satisfied with the available payment methods, they can abort the transaction and can contact customer support if needed. 1b. If the selected payment method is unavailable or encounters an error, the system prompts the user to choose an alternative payment method. 1c. If the system fails to present the available payment methods due to technical issues, it displays an error message and prompts the user to try again later.
Non functional requirements	**Security**: The system must ensure that users' payment information is securely handled and transmitted during the payment method selection process. **Performance**: The payment method selection process should have low latency and high responsiveness to provide users with a smooth and efficient checkout experience, even during periods of high traffic. **Compatibility**: The payment method selection interface should be compatible with various devices and screen sizes, ensuring accessibility for users across different platforms.

Postconditions	User successfully selects a payment method, unless a problem occurred.

Payment Processing: The system shall securely process payments made by users through the selected payment method, ensuring accuracy and reliability of transaction data.

UC Name	**Payment Processing (UC-302)**
Summary	System securely processes payments made by users through the selected payment method, ensuring accuracy and reliability of transaction data.
Dependency	Payment Method Selection (UC-301)
Actors	Primary Actor: User (Passenger) Secondary Actors: Fraud Department, Finance Department
Preconditions	User has selected a payment method and initiated the payment process.
Description of the Main Sequence	1. User provides payment details through the selected payment method (e.g., card details, wallet information). 2. The Fraud Department will monitor for payment fraud. 3. The Finance Department **securely communicates** with the financial institution to authorize and process the transaction. 4. Upon successful authorization, the payment system updates the transaction status and records the payment details. 5. Confirmation of successful payment is displayed to the user. 6. The system delivers the E-ticket to the user through their preferred communication channel (e.g., email, website).
Description of the Alternative Sequence	2a.If the fraud department finds something suspicious they will not approve the transaction and the system will perform as described in UC-303 (Fraud Detection and Prevention) 3a. If the payment authorization fails, the payment system notifies the user and prompts for alternative payment details or methods. 4a. If the payment processing encounters an error after authorization, the payment system provides appropriate error messages and instructs the users to contact customer support.
Non functional requirements	**Security**: The payment processing system must adhere to strict security protocols to protect users' payment information during

	transmission and storage. **Performance**: The payment processing system should have low latency and high throughput to efficiently handle payment transactions, ensuring timely processing and responsiveness to user actions.. **Scalability**: The payment processing system should be scalable to accommodate increasing transaction volumes without degradation in performance, ensuring seamless operation during peak usage periods. **Reliability**: The payment processing system should be highly reliable, minimizing the risk of transaction failures or data inaccuracies to maintain trust and confidence among users.
Postconditions	Payment is successfully processed, and transaction data is accurately recorded.

Transaction history: The system should provide an easy way to review transactions made.

UC Name	**Reviewing transactions** (UC-303)
Summary	The system provides an easy way for users to review transactions made, allowing them to view details of past transactions.
Dependency	Payment Processing (UC-302)
Actors	Primary Actor: User (Passenger) Secondary Actor: System
Preconditions	User is logged into their account on the system.
Description of the Main Sequence	1. User navigates to the "Transactions" or "Order History" section within their account settings. 2. The system retrieves and displays a list of past transactions associated with the user's account. 3. User can select a specific transaction to review by clicking on it. 4. The system presents detailed information about the selected transaction, including date, time, payment method, amount, and

	any relevant order details. 5. User reviews the transaction details and can optionally print or save a copy for their records.
Description of the Alternative Sequence	
Non functional requirements	**Reliability**: The system's transaction review functionality should be reliable, ensuring that users can consistently access and review past transactions without errors or data discrepancies. **Usability**: The interface for reviewing transactions should be user-friendly and intuitive, providing clear navigation and presentation of transaction details to enhance the user experience. **Performance**: The performance impact of retrieving and displaying transaction data should be minimized to ensure fast and responsive access to transaction details, even for users with large transaction histories. **Security**: The system must ensure the confidentiality and integrity of transaction data during retrieval and display to prevent unauthorized access or tampering.
Postconditions	User successfully reviews transactions made.

Encryption of Sensitive Information:
The system shall encrypt all sensitive user data using industry-standard encryption algorithms such as AES (Advanced Encryption Standard) or equivalent. It must ensure that sensitive information, including user credentials, financial data, and personal details, are securely encrypted during storage and transmission.

UC Name	**Encryption of Sensitive Information UC-401**
Summary	The system encrypts all sensitive user data, including user credentials, financial data, and personal details, using industry-standard encryption algorithms such as AES (Advanced

	Encryption Standard) or equivalent, to ensure security during storage and transmission.
Dependency	User account creation (UC-201) , Payment Processing (UC-302)
Actors	Primary Actor: User (Admin) Secondary Actors: System, IT Department
Preconditions	Sensitive user data is collected or transmitted within the system.
Description of the Main Sequence	1. The system identifies sensitive user data that requires encryption, including user credentials, financial data, and personal details. 2. The system utilizes industry-standard encryption algorithms such as AES or equivalent to encrypt the sensitive user data. 3. Encrypted data is securely stored in the system's cloud database or transmitted over networks.
Description of the Alternative Sequence	None
Non functional requirements	**Security**: The encryption system must adhere to industry-standard encryption algorithms and practices to ensure the confidentiality and integrity of sensitive user data. **Reliability**: The encryption system should be reliable, ensuring that sensitive user data is consistently encrypted and protected from unauthorized access or tampering. **Performance**:The encryption system should have minimal impact on system performance, ensuring that encryption processes do not significantly degrade system responsiveness or throughput. **Compliance**: The encryption system must comply with relevant regulations and standards governing the protection of sensitive user data, such as GDPR, HIPAA, or PCI DSS.
Postconditions	Sensitive user data is securely encrypted and stored or transmitted.

Protection Against Cyber Threats:

The system must incorporate mechanisms to detect and mitigate various cyber threats such as malware, phishing attacks, SQL injection, cross-site scripting (XSS), and denial-of-service (DoS) attacks. It should implement intrusion detection and prevention systems (IDPS) to monitor and respond to suspicious activities in real-time.

UC Name	**Protection Against Cyber Threats**
Summary	The system incorporates mechanisms to detect and mitigate various cyber threats such as malware, phishing attacks, SQL injection, cross-site scripting (XSS), and denial-of-service (DoS) attacks. It implements intrusion detection and prevention systems (IDPS) to monitor and respond to suspicious activities in real-time.
Dependency	
Actors	Primary Actor: User (Admin) Secondary Actor: IT Department, Fraud Department
Preconditions	Ticket booking functionality is available, and users are making transactions.
Description of the Main Sequence	1. The system continuously monitors ticket booking transactions for suspicious payment transactions, multiple bookings from the same IP address, or anomalies in user behavior. 2. Upon detecting potentially fraudulent transactions, the system flags them for further investigation by the IT department and Fraud Department. 3. The flagged transactions are analyzed by the IT department and fraud detection algorithms or services to determine the likelihood of fraud. 4. Based on the analysis, the fraud department takes appropriate actions, such as reviewing transactions, contacting users for verification, or blocking suspicious accounts.
Description of the Alternative Sequence	**None**
Non functional requirements	**Reliability**:The system's fraud detection mechanisms should be reliable and accurate in identifying potentially fraudulent

	transactions to minimize false positives and negatives. **Performance**: The performance impact of fraud detection algorithms or services should be optimized to ensure timely analysis and response to potentially fraudulent transactions without significantly affecting system responsiveness or transaction processing times. **Security**: The fraud detection and prevention features implemented by the system must ensure the security and integrity of user transactions and sensitive information while minimizing the risk of fraudulent activities. **Compliance**:The system's fraud detection and prevention measures must comply with relevant regulations and standards governing fraud prevention, such as PCI DSS, GDPR, or industry-specific compliance requirements.
Postconditions	Potentially fraudulent transactions are flagged for further investigation, and appropriate actions are taken by the fraud department.

Fraud Detection and Prevention:

The system should include features to detect and prevent fraudulent activities related to ticket bookings, such as suspicious payment transactions, multiple bookings from the same IP address, or anomalies in user behavior.
Integration with fraud detection services or algorithms should be implemented to analyze booking patterns and flag potentially fraudulent transactions for further investigation by the fraud department.

UC Name	**Fraud Detection and Prevention (UC-303)**
Summary	The system includes features to detect and prevent fraudulent activities related to payment. It integrates with fraud detection services or algorithms to analyze booking patterns and flag potentially fraudulent transactions for further investigation by the fraud department.

Dependency	Payment Processing (UC-202)
Actors	Primary Actor: System Secondary Actor: Fraud Department
Preconditions	User has initiated the checkout process and reached the payment step.
Description of the Main Sequence	1. The system monitors ticket booking transactions in real-time for signs of fraudulent activity, such as unusual payment patterns, multiple bookings from the same IP address, or suspicious user behavior. 2. Upon detecting potentially fraudulent transactions, the system flags them for further investigation by the fraud department. 3. The flagged transactions are reviewed by fraud detection algorithms or services to assess the likelihood of fraud based on predefined criteria and thresholds. 4. Based on the analysis, the fraud department takes appropriate actions, such as contacting users for verification, blocking suspicious accounts, or initiating legal proceedings against perpetrators.
Description of the Alternative Sequence	1. If the fraud detection system encounters technical issues or errors, the system logs the incident and notifies administrators for resolution.
Non functional requirements	**Performance**: The performance impact of fraud detection algorithms or services should be optimized to ensure timely analysis and response to potentially fraudulent transactions without significantly affecting system responsiveness or transaction processing times. **Compatibility**: The system's fraud detection and prevention measures must comply with relevant regulations and standards governing fraud prevention, such as PCI DSS, GDPR, or industry-specific compliance requirements. **Reliability**: The system's fraud detection mechanisms should be reliable and accurate in identifying potentially fraudulent transactions to minimize false positives and negatives.
Postconditions	Potentially fraudulent transactions are flagged for further investigation.