PASSVAULT - Multi-Pass Digital Wallet

PROJECT REPORT
for
21CSC205P – DATABASE MANAGEMENT SYSTEMS

Submitted by

Saumye Singh [RA2311033010049]
Vineet Sahoo [RA2311033010053]

Under the Guidance of
Dr. S. Sadagopan
(Associate Professor, Department of Computational Intelligence)

In partial fulfilment of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING
WITH SPECIALIZATION IN SOFTWARE ENGINEERING

DEPARTMENT OF COMPUTATIONAL INTELLIGENCE
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR- 603 203
FEBRUARY 2025

Project Report: PassVault - Multi-Pass Digital Wallet

1. Introduction

PassVault is a digital wallet application designed to centralize and manage various digital passes, such as event tickets, loyalty cards, boarding passes, and coupons, in one secure platform. It eliminates the need for multiple apps or physical cards, offering convenience, security, and intelligent features powered by a robust database management system (DBMS).

With the increasing reliance on digital transactions, users often struggle with managing different digital passes across multiple platforms. PassVault addresses this challenge by providing a single, unified solution where users can store, retrieve, and manage all their digital passes with ease. The platform ensures security through encryption, tokenization, and multi-factor authentication, preventing unauthorized access and data breaches.

---

2. Key Features

i. Centralized Storage

- Stores event tickets, boarding passes, loyalty cards, and discount coupons in a single platform.
- Eliminates the need for multiple physical cards or separate apps.
- Provides a categorized dashboard for easy access to different types of passes.

ii. QR/Barcode Integration

- Allows users to scan and store QR codes and barcodes for easy retrieval.
- Generates QR codes for digital passes to facilitate quick check-ins and transactions.
- Works seamlessly with third-party services such as airports, cinemas, and shopping centers.

iii. Expiration Alerts

- Notifies users about upcoming expirations of tickets, coupons, and memberships.
- Provides auto-renewal reminders and one-click renewal options where applicable.

iv. Transaction History

- Logs all pass-related transactions, including usage history, redemptions, and expiration dates.
- Allows users to filter and track spending habits and usage patterns.

v. Pass Transfers

- Enables secure transfer of passes, such as event tickets or gift coupons, to other users.
- Uses digital signatures and encryption to ensure authenticity and prevent fraud.

vi. Advanced Security

- Implements **end-to-end encryption** to protect stored passes.
- Uses **tokenization** to replace sensitive data with unique identifiers.
- Supports **multi-factor authentication (MFA)** for added security.
- **2.7 Smart Suggestions**
- Provides personalized recommendations based on user behavior and preferences.
- Uses AI-driven analytics to suggest relevant offers, event tickets, and discounts.

vii. Data Aggregation

- Syncs passes from multiple sources, including emails, user accounts, and third-party integrations.
- Uses API-based connectivity to ensure seamless integration with external platforms.

---

3. Technical Architecture

i. Frontend

- Developed using React Native or Flutter for cross-platform compatibility.
- Ensures a responsive UI for both Android and iOS users.
- Provides intuitive navigation, real-time updates, and smooth user experience.

ii. Backend

- Uses Python (Django/FastAPI) or Node.js (Express.js) for handling business logic and server-side operations.
- Ensures secure communication between the client and database.
- Implements RESTful API architecture for efficient data exchange.

iii. Database Management System (DBMS)

- **PostgreSQL** or **MySQL** is used to store:
    - User profiles and authentication data.
    - Digital pass details and metadata.
    - Transaction history and pass redemptions.
    - Security logs and access controls.

- Ensures ACID compliance and optimized indexing for fast queries.

---

4. Benefits

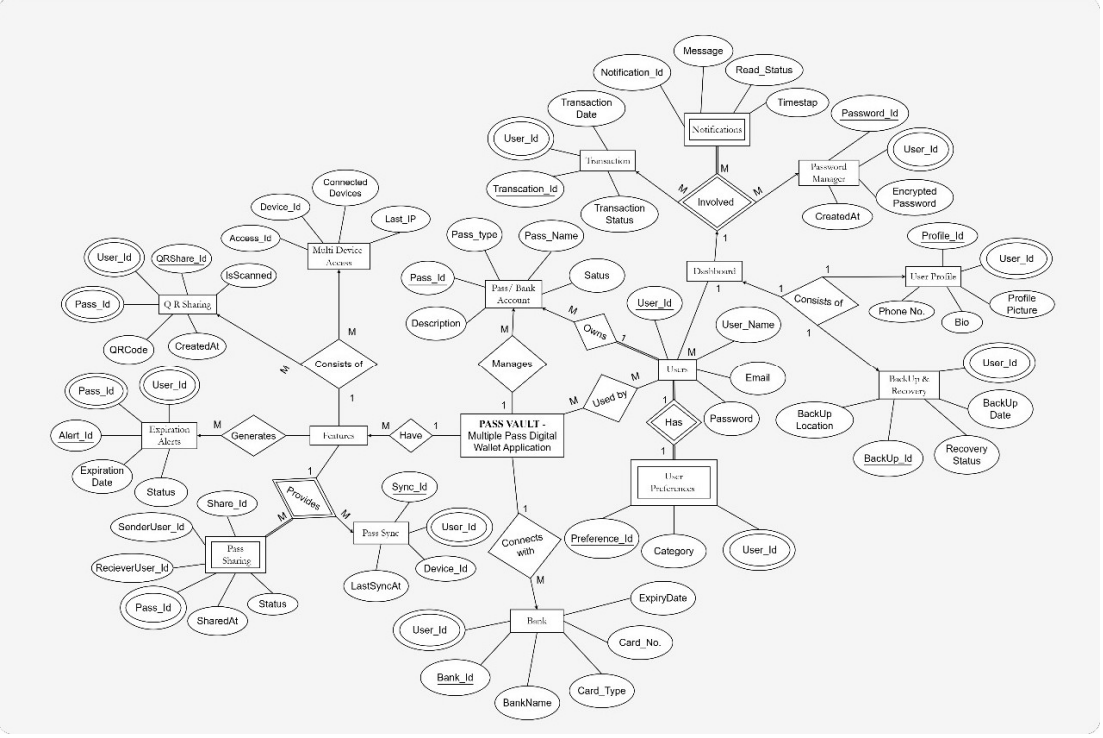
i. Benefits for Users

- **Convenience:** Stores all passes in one easily accessible location.
- **Security:** Protects sensitive data with high-end encryption and authentication measures.
- **Smart Suggestions:** Provides personalized recommendations for upcoming events and offers.
- **Sustainability:** Reduces paper waste by digitizing passes and tickets.

ii. Benefits for Businesses

- **Improved Customer Engagement:** Enhances loyalty programs and targeted marketing strategies.
- **Data-Driven Insights:** Provides analytics on customer behavior and preferences.
- **Cost Efficiency:** Eliminates the need for physical printing of passes and tickets.

5. Er Model Diagram:



6. Detailed Description

i. Pass Vault

- **Notation:** Rectangle (Entity)
- **Purpose**: Central entity managing multiple features like pass storage, synchronization, sharing, transactions, and notifications.
- **Relationships:**
    - **Manages** → *Pass/Bank Account* (1 - M) (One Pass Vault can manage multiple passes/bank accounts)
    - **Has** → *Features* (1 - M) (One Pass Vault has multiple features)
    - **Connects with** → *Bank* (1-M) – Total Participation
    - **Used By** → *Users* (M-M) – Total Participation

---

ii. Users

- **Attributes:**
    - User_Id (Primary Key) (Multivalued)
    - User_Name
    - Email
    - Password
- **Notation**: Rectangle (Entity)
- **Domain:** Represents individual users of the system.
- **Relationships:**
    - **Has** → *Dashboard* (1 - 1) (Each user has one dashboard) – Total Participation
    - **Used by** → *Pass Vault* (M - 1) (Multiple users can use one Pass Vault instance) – Total Participation
    - **Has (Weak Relationship)** → *User Preferences* (1 - 1) (Each user has one profile) – Total Participation

---

iii. User Profile

- **Attributes:**

    - Profile_Id (Primary Key)
    - User_Id (Multivalued)
    - Phone No.
    - Bio
    - Profile Picture
- **Notation**: Rectangle (Entity)
- **Domain:** Stores user-specific details for identity and personalization.
- **Relationships:**
    - **Belongs to** → *Dashboard* (1 - 1) (One user has one profile)

---

iv. Password Manager

- **Attributes:**
    - Password_Id (Primary Key)
    - User_Id (Multivalued)
    - Encrypted Password
    - CreatedAt
- **Notation:** Rectangle (Entity)
- **Domain:** Secure storage for user passwords.
- **Relationships:**
    - **Involved in** → *Dashboard* (M - 1) (One password manager per user)

---

v. BackUp & Recovery

- **Attributes:**
    - BackUp_Id (Primary Key)
    - User_Id (Multivalued)
    - BackUp Date
    - Recovery Status
    - BackUp Location
- **Notation:** Rectangle (Entity)

- **Domain:** Helps users recover lost or corrupted data.
- **Relationships:**
    - **Belongs to** → *Dashboard* (1 - 1) (One backup per user) – Total Participation

---

vi. Notifications

- **Attributes:**
    - Notification_Id
    - Message
    - Read_Status
    - Timestamp
- **Notation:** Concentric Rectangle (Weak Entity)
- **Domain:** Alerts users about transactions, expirations, and pass-sharing events.
- **Relationships:**
    - **Involved in (Weak Relationship)** → *Dashboard* (M - 1) (Multiple notifications for one transaction)

---

vii. Transaction

- **Attributes:**
    - Transaction_Id (Primary Key)
    - User_Id (Multivalued)
    - Transaction Date
    - Transaction Status
- **Notation:** Rectangle (Entity)
- **Domain:** Tracks pass purchases and bank transactions.
- **Relationships:**
    - **Involved in** → *Dashboard* (M - 1) (Multiple transactions per user) – Total Participation

---

viii. QR Sharing

- **Attributes:**

    - QRShare_Id (Primary Key)
    - Pass_Id (Multivalued)
    - User_Id (Multivalued)
    - QRCode
    - CreatedAt
    - IsScanned
- **Notation:** Rectangle (Entity)
- **Domain:** Allows users to share passes using QR codes.
- **Relationships:**
    - **Comprises** → *Features* (M - 1) (Multiple QR shares for one pass)

---

ix. Pass Sharing

- **Attributes:**
    - Share_Id
    - SenderUser_Id
    - ReceiverUser_Id
    - Pass_Id (Multivalued)
    - SharedAt
    - Status
- **Notation:** Concentric Rectangle (Weak Entity)
- **Domain:** Enables pass sharing between users.
- **Relationships:**
    - **Comprises (Weak Relationship)** → *Features* (M - M) (Multiple users can share passes**)**

---

x. Expiration Alerts

- **Attributes:**
    - Alert_Id (Primary Key)
    - Pass_Id (Multivalued)
    - User_Id (Multivalued)

    - Expiration Date
    - Status
- **Notation:** Rectangle (Entity)
- **Domain:** Notifies users about upcoming pass expiration.
- **Relationships:**
    - **Generated by** → *Features* (M - 1) (Multiple alerts for one feature)

---

xi. Pass Sync

- **Attributes:**
    - Sync_Id (Primary Key)
    - User_Id (Multivalued)
    - Device_Id
    - LastSyncAt
- **Notation:** Rectangle (Entity)
- **Domain:** Syncs passes across multiple devices.
- **Relationships:**
    - **Provided by** → *Features* (M - 1) (Multiple syncs per feature)

---

xii. Multi-Device Access

- **Attributes:**
    - Access_Id (Primary Key)
    - Device_Id
    - Last_IP
    - Connected Devices
- **Notation:** Rectangle (Entity)
- **Domain:** Manages device connectivity for users.
- **Relationships:**
    - **Consists of** → *Features* (1 - M)

---

xiii. User Preferences

- **Attributes:**
  - Preference_Id
  - User_Id (Multivalued)
  - Category
- **Notation:** Concentric Rectangle (Weak Entity)
- **Domain:** Stores customization settings for users.
- **Relationships:**
  - **Belongs to (Weak Relationship)** → *Users* (1 - 1) – Total Participation

---

xiv. Bank

- **Attributes:**
  - Bank_Id (Primary Key)
  - User_Id (Multivalued)
  - BankName
  - Card_No.
  - Card_Type
  - Expiry Date
- **Notation:** Rectangle (Entity)
- **Domain:** Stores banking information for transactions.
- **Relationships:**
  - **Connects with** → *PassVault* (M - 1) – Total Participation

---

xv. Pass / Bank Account

- **Attributes:**
  - Pass_Id (Primary Key) (Multivalued)
  - Pass Type
  - Pass_Name
  - Status

    - Description
- **Notation:** Rectangle (Entity)
- **Domain:** Manages user passes and linked accounts.
- **Relationships:**
    - **Managed by** → *Pass Vault* (M - 1) – Total Participation

---

xvi. Dashboard

- **Notation:** Rectangle (Entity)
- **Domain:** Provides users an interface to manage their passes.
- **Relationships:**
    - **Owned by** → *Users* (1 - 1)
    - **Involves (Weak Relationship) – Total Participation** → *Notifications* (1-M)
    - **Involves – Total Participation** → *Transaction, Password Manager* (1-M)
    - **Consists of** → *Backup and Recovery* (1-1) – Total Participation

---

xvii. Features

- **Notation:** Rectangle (Entity)
- **Domain:** Represents system functionalities.
- **Relationships:**
    - **Is part of** → *Pass Vault* (M - 1) – Total Participation
    - **Consists of** → *Multi Device Access* (1-M)
    - **Consists of** → *QR Sharing* (1-M)
    - **Generates** → *Expiration Alerts* (1-M)
    - **Provides (Weak Relationship)** → *Pass Sharing* (1-M)
    - **Provides** → *Pass Sync* (1-M)

7. Notations Used in ERD:

i. Basic Notations

- **Entities (Rectangles):** Represent main objects (e.g., Users, Bank, Pass Vault).
- **Attributes (Ellipses):** Linked to entities, including simple, multivalued (double ellipse), and derived (dashed ellipse) attributes.
- **Relationships (Diamonds):** Define connections between entities (e.g., *Owns*, *Manages*).

ii. Cardinality Notation

- **1..1 (One-to-One)** → 1 (e.g., One user has one profile).
- **1..M (One-to-Many)** → 1 - M (e.g., One user can have multiple bank accounts).
- **M..N (Many-to-Many)** → M - M (e.g., Users can share passwords with multiple users).

iii. Additional Notations

- **Weak Entity (Double Rectangle**): Lacks a unique key, depends on a strong entity (e.g., *Notifications*).
- **Weak Relationship (Double Diamond):** Links weak entities to strong ones (e.g., *BackUp & Recovery* to *Users*).
- **Multivalued Attribute (Double Ellipse):** Stores multiple values (e.g., *Connected Devices* in *Multi-Device Access*).
- **Keys (Underlined Attributes):** Primary Key uniquely identifies records (e.g., User_Id in *Users*), while Foreign Keys establish relationships.
- **Participation Constraints:**
    - **Total (Double Line):** Every instance must participate (e.g., *Users* in *Transactions*).
    - **Partial (Single Line):** Some instances may not participate (e.g., *Users* in *Pass Sharing*)

---

8. Extended Features in ERD

i. Specialization

- Specialization is the process of defining a **subclass** from a **superclass**, where the subclass inherits attributes from the parent entity but also has unique attributes.
- Example:
    - *Pass / Bank Account* can be specialized into:
        - **Pass** (e.g., Membership Cards, Coupons, Tickets)
        - **Bank Account** (e.g., Credit Cards, Debit Cards, Digital Wallets)
    - *Users* can be specialized into:
        - **Regular Users** (who store passes, manage transactions)
        - **Admin Users** (who manage security, user permissions)

ii. Generalization

- Generalization is the process of combining multiple entities into a **higher-level entity** based on shared attributes.
- Example:
    - *QR Sharing*, *Pass Sharing*, and *Pass Sync* can be generalized into **Pass Management**, as they all involve sharing, syncing, and scanning passes.
    - *Password Manager* and *BackUp & Recovery* can be generalized into **Security Management**, since both deal with securing user credentials and restoring data.

iii. Aggregation

- Aggregation represents a **"whole-part"** relationship where an entity is a component of a larger entity but still exists independently.
- Example:
    - *Transaction* involves both *Users* and *Bank*, meaning a transaction belongs to a bank and is performed by a user. Here, **Transaction is an aggregated entity** that connects *Users* and *Bank*.
    - *Notifications* can be aggregated with *Transaction*, as transactions generate alerts that are sent to users.

These extended features help in making the database **more structured, modular, and scalable**, improving efficiency in handling different user roles, security mechanisms, and transaction processes.

9. Challenges and Solutions

i. Data Integration

Challenge: Integrating multiple data sources and formats from different service providers. Solution: Using standardized APIs and middleware to facilitate seamless data aggregation.

ii. Security Concerns

Challenge: Preventing unauthorized access, data leaks, and fraudulent pass usage. Solution: Implementing encryption, tokenization, and multi-factor authentication.

iii. Cross-Platform Compatibility

Challenge: Ensuring consistent performance across various mobile devices. Solution: Using React Native or Flutter to maintain uniformity in UI/UX.

---

10. Potential Impact

- **Simplifies digital pass management**, reducing clutter and inconvenience for users.
- **Enhances business engagement**, allowing companies to leverage digital loyalty programs.
- **Promotes sustainability** by reducing reliance on paper-based systems.
- **Improves security and fraud prevention** through robust encryption and authentication mechanisms.

---

11. Conclusion

PassVault is set to **revolutionize digital pass management** by offering a **secure, centralized, and user-friendly** platform. By combining innovative features with **state-of-the-art security**, PassVault benefits both individual users and businesses. The platform enhances customer experiences, promotes sustainability, and ensures seamless digital transactions, making it a **standout solution in the digital wallet space**.
