ICT 3123- FISAC 1

CRED

Sai Charan - 220911638

Ayush – 220911632

Arnav - 220911476

DEPARTMENT OF I&CT, MIT, MAHE, MANIPAL

Introduction to the Work

The CRED Mobile Application is designed to provide users with a convenient and secure platform to manage their credit card transactions, payments, and rewards. With an increasing number of users relying on digital platforms for financial management, there is a growing need for robust, user-friendly applications that facilitate quick access to essential financial tools while maintaining high standards of security and data protection. This document outlines the requirements for the development of the CRED application to meet these needs.

Problem Statement

Managing credit cards and payments efficiently has become crucial for individuals looking to maintain financial health. Traditional banking and payment management systems often lack the user-friendly interfaces and seamless integration features that modern consumers expect. Additionally, the complexity of handling multiple credit cards, tracking payments, and accessing rewards often results in users missing payment deadlines, leading to penalties and increased financial stress.

The key problems addressed by the CRED application are:

- **Lack of a unified platform** for managing multiple credit cards and rewards.

- **Challenges with timely payment management**, leading to missed deadlines and penalties.

- **Inadequate user interfaces** that are not optimized for mobile use, causing frustration and a lack of engagement.

- **Security and data privacy concerns** associated with handling sensitive financial information online.

Scope

The CRED Mobile Application aims to solve these problems by providing a comprehensive, easy-to-use platform with the following scope:

1. **User Authentication and Security**: Implementing secure user authentication (e.g., OAuth) and role-based access controls to protect user data and comply with industry standards such as PCI-DSS.

2. **Credit Card Management**: Enabling users to add, remove, and manage multiple credit cards from various issuers on a single platform.

3. **Payment Processing and Scheduling**: Providing real-time payment processing capabilities and setting reminders for payment deadlines to help users avoid late fees and maintain a good credit history.

4. **Rewards Tracking and Redemption**: Allowing users to monitor, calculate, and redeem rewards and offers associated with their credit cards.

5. **User Notifications and Alerts**: Sending timely notifications about payment due dates, rewards expiration, and potential issues to improve financial awareness.

6. **Data Analytics and Insights**: Offering users insights into their spending patterns and personalized financial advice to help them make better financial decisions.

7. **Event-Driven Architecture**: Leveraging a microservices and event-driven architecture to allow real-time updates, scalability, and fault tolerance.

The application is intended for mobile use, supporting both Android and iOS platforms. It will be designed with a focus on usability, scalability, and security to meet the needs of a growing user base. The initial deployment will focus on core functionalities, with plans for continuous improvement based on user feedback and technological advancements.

Software Requirements Specification (SRS)
CRED Mobile Application

Contents

1 Introduction

1.1 Purpose

The purpose of this document is to present a detailed description of the CRED Mobile Application. It will outline the purpose and features of CRED, the interfaces it will provide, its functionality, and the constraints under which it must operate. Additionally, it will describe how the application will handle external inputs and interactions. This document is intended for both stakeholders and developers involved in the project and serves as a foundational reference for the development and deployment of the CRED system.

1.2 Scope

The CRED Mobile Application is a software system designed to help users manage credit card payments and earn rewards for timely payments. This application will streamline the process of tracking due dates, processing payments, and redeeming rewards, which can otherwise be complex and time-consuming for users. By improving user convenience and providing timely reminders, CRED aims to reduce missed payments and encourage better financial habits among users.

More specifically, CRED will enable users to manage multiple credit cards, track payment due dates, receive notifications, and earn reward points for on-time payments. The software will integrate securely with payment gateways to process transactions and maintain user data privacy through compliance with PCI-DSS and GDPR standards. Additionally, CRED will support a flexible rewards system, where users can redeem points for various offers available within the application.

The system's architecture will include a microservices-based backend and a relational database to manage user accounts, credit card details, transactions, and rewards. This approach ensures scalability and robust performance, meeting the needs of a growing user base while remaining user-friendly and secure.

1.3 Glossary

Term	Definition
Active Account	An account that is actively tracked by the system, with ongoing transactions and payment activity.
User	A registered individual using the CRED application to manage their credit card payments and earn rewards.
Payment Gateway	A third-party service that securely processes credit card transactions within the CRED application.
Reward Points	Points awarded to users for making timely payments. Points can be redeemed for various offers within the app.
Notification	A reminder or alert sent to users about upcoming payment due dates, successful payments, or available rewards.
Security Compliance	Adherence to regulations such as PCI-DSS and GDPR to ensure data security and privacy within the application.
Software Requirements Specification	A document that fully describes all of the functions of the CRED application and the constraints under which it must operate.
Stakeholder	Any person or organization with an interest in the CRED application, including developers, users, and business partners.
Transaction	A payment made through the CRED application. Each transaction records payment amount, date, and associated rewards.
Credit Card Management	The functionality that allows users to add, view, update, or delete credit card details within the CRED app.

1.4 References

- IEEE Std 830-1998 IEEE Recommended Practice for Software Requirements Specifications.

- PCI-DSS Compliance Documentation

- GDPR Documentation

1.5   Overview

This document outlines functional and non-functional requirements, user interfaces, and system interactions for CRED.

2   Overall Description

2.1   Product Perspective

The CRED Mobile Application is a standalone product focused on helping users manage credit card payments and earn rewards for timely payments. Unlike traditional banking apps, CRED emphasizes a reward-based approach to encourage responsible financial behavior. It operates independently but integrates with third-party payment gateways for secure transactions.

CRED's architecture is based on a microservices model, with modular components for user management, payment processing, and rewards. This approach allows seamless interactions between services, external APIs, and ensures scalability, security, and adaptability to a growing user base.

2.2   Product Functions

The CRED Mobile Application offers a range of features to enhance user experience in managing credit card payments and rewards. The following is a high-level overview of the core functions:

- **User Account Management**: Allows users to register, log in, and manage their profiles with secure authentication.

- **Credit Card Management**: Enables users to add, view, update, or delete credit card details.

- **Payment Tracking**: Provides tracking of due dates and a view of past payments.

- **Notifications and Alerts**: Sends reminders for upcoming payments, successful payments, and reward updates.

- **Rewards System**: Awards points for timely payments; points can be redeemed for offers within the app.

- **Payment History**: Displays a record of all past payments and transactions.

- **Transaction Summaries**: Summarizes spending patterns to help users understand their financial habits.

- **Credit Score Tracking**: Monitors and provides updates on users' credit scores.

- **Reward Redemption**: Allows users to redeem earned points for in-app offers or discounts.

- **Secure Payment Processing**: Provides secure credit card payment options through third-party payment gateway integrations.

- **Data Security and Compliance**: Ensures PCI-DSS and GDPR compliance to protect user data.

- **Multi-Factor Authentication**: Provides an optional additional security layer for user accounts.

- **Customer Support Access**: Enables users to reach customer support directly through the app.

- **User Feedback Collection**: Collects feedback on features, usability, and overall experience to guide improvements.

- **In-App Offers and Promotions**: Displays special offers or discounts based on user reward points and activities.

- **Analytics and Insights**: Provides users with insights into their spending and payment patterns.

- **User Settings Management**: Allows customization of notification preferences, privacy settings, and profile information.

- **App Updates and Notifications**: Notifies users about new features, app updates, and improvements.

2.3   User Classes and Characteristics

The CRED Mobile Application has three primary user classes with varying levels of interaction and responsibility within the system.

- **Individual Users**

  - **Description**: General users managing personal credit card payments, tracking due dates, and earning rewards.
  - **Characteristics**:
    * Moderate to high frequency of use.
    * Utilizes features like payment reminders, transaction history, credit score monitoring, and reward redemption.
    * Basic to moderate technical expertise.
  - **Importance**: High, as they make up the primary user base.

- **Customer Support Representatives**

  - **Description**: CRED's support staff assisting users with technical and account-related issues.
  - **Characteristics**:
    * Frequent access to backend systems for troubleshooting.
    * Permissions for account management with limited access to sensitive data.
    * Skilled in customer service and technical support.
  - **Importance**: High, critical for maintaining user satisfaction and app reliability.

- **System Administrators**

  - **Description**: Responsible for backend infrastructure, security, and overall system health.
  - **Characteristics**:
    * Full access to system configuration, data management, and security settings.
    * High technical expertise and familiarity with the system's architecture.
  - **Importance**: High, essential for maintaining operational stability and security.

2.4   Operating Environment

The CRED Mobile Application is designed to function efficiently across a range of modern devices and software environments. The following are the specifications for the operating environment:

- **Hardware Platforms**:

  - Compatible with smartphones running Android and iOS.
  - Minimum hardware requirements: 2GB of RAM, Dual-core processor, and Internet connectivity for real-time updates and data synchronization.

- **Operating Systems**:

  - **Android**: Version 8.0 (Oreo) and above.
  - **iOS**: Version 12.0 and above.

- **Software Dependencies**:

  - **Payment Gateways**: Integration with third-party payment processors to enable secure transactions.
  - **Notification Services**: Utilizes push notification services to send reminders and alerts.
  - **Database Systems**: Cloud-based database (e.g., AWS or Google Firebase) for secure data storage and retrieval.
  - **APIs**: Utilizes RESTful APIs for data exchange between client and server components, and integration with third-party services like credit score monitoring.

2.5 Design and Implementation Constraints

The development of the CRED Mobile Application must consider the following constraints:

- **Regulatory Compliance**: Adhere to PCI-DSS for payment security and GDPR for data privacy.

- **Hardware Limitations**: Optimized for devices with at least 2GB RAM and dual-core processors.

- **External Integrations**: Requires integration with payment gateways and credit score APIs.

- **Security Standards**: Use SSL/TLS encryption and multi-factor authentication.

- **Technology Stack**: Backend to use scalable microservices, ideally with Node.js or Python.

- **Design Standards**: Follow mobile UX best practices and coding conventions for maintainability.

2.6 User Documentation

The following user documentation will be provided with the CRED Mobile Application:

- **User Manual**: A comprehensive guide covering app installation, features, and usage.

- **Online Help**: Context-sensitive help available within the app for quick assistance.

- **Tutorials**: Step-by-step tutorials for key functions, such as payment tracking and reward redemption.

All documentation will be delivered in digital format, optimized for both desktop and mobile viewing.

2.7 Assumptions and Dependencies

The development of the CRED Mobile Application is based on the following assumptions and dependencies:

- **Third-Party Integrations**: Reliant on external payment gateways and credit bureau APIs for transaction processing and credit score updates.

- **Platform Dependencies**: Assumes compatibility with the latest versions of Android and iOS.

- **Cloud Infrastructure**: Dependent on reliable cloud services (e.g., AWS or Firebase) for data storage and user authentication.

- **Regulatory Compliance**: Assumes all third-party components meet PCI-DSS and GDPR standards.

3 External Interface Requirements

3.1 User Interfaces

The CRED Mobile Application includes the following main screens to facilitate secure and user-friendly interactions:

- **Login and Verification Screen**:
  - Users are prompted to enter their PAN (Permanent Account Number), phone number, and email address during account setup.
  - Verification is completed through a one-time password (OTP) sent to the registered phone number, ensuring secure access.

- **Home Dashboard Screen**:
  - Displays a summary of due payments, reward points, available offers, and the user's credit score.
  - Allows quick access to recent transactions and important notifications.

- **Payments Screen**:
  - Displays upcoming payment dues for each linked credit card.
  - Allows users to initiate payments, schedule payments, and enable auto-pay.

- **Rewards Screen**:
  - Shows accumulated reward points and available offers or discounts for redemption.
  - Enables users to redeem points or view their redemption history.

- **Credit Score Screen**:
  - Displays the user's current credit score with a breakdown of factors affecting it.
  - Provides insights and tips to help users improve their score.

- **Notifications Screen**:
  - Lists all recent notifications, including payment reminders and rewards updates.
  - Users can customize notification preferences from this screen.

- **Profile Screen**:
  - Provides access to account settings, linked cards, and security options.
  - Allows users to update their personal information, notification preferences, and privacy settings.

- **Help and Support Screen**:
  - Provides access to FAQs, contact options for customer support, and troubleshooting guides.
  - Users can initiate a chat or call support directly from this screen.

3.2   Hardware Interfaces

The CRED Mobile Application interfaces with hardware through the following characteristics:

- **Supported Devices**:
  - Smartphones and tablets running Android (version 8.0 and above) and iOS (version 12.0 and above).
  - Minimum device specifications: 2GB RAM and a dual-core processor.

- **Data and Control Interactions**:
  - Real-time data retrieval from the device's internet connection for transaction updates, notifications, and credit score tracking.
  - Utilizes device storage for caching recent transactions and rewards history for offline viewing.

- **Communication Protocols**:
  - Secure communication over HTTPS with SSL/TLS encryption for data exchanges.
  - Push notification protocol (e.g., Firebase Cloud Messaging or Apple Push Notification Service) for alerts and reminders.

3.3   Software Interfaces

The CRED Mobile Application interacts with several external software components to ensure smooth functionality and secure data handling:

- **Operating Systems**:
  - Compatible with Android (version 8.0 and above) and iOS (version 12.0 and above) for optimal performance across mobile platforms.

- **Database System**:
  - A cloud-based database (such as AWS RDS or Google Firebase) stores user information, transaction history, and reward data.
  - Ensures secure storage with encryption and supports real-time data updates for seamless user experience.

- **Payment Gateway Integration**:
  - Interfaces with third-party payment gateways to process credit card payments securely.
  - Sends payment data and receives transaction confirmations; all data exchanges are encrypted to comply with PCI-DSS.

- **Credit Bureau API**:
  - Integrates with external credit bureau APIs to fetch and update user credit scores periodically.
  - Requests user credit data and receives score information to display within the app.

- **Notification Service**:
  - Uses Firebase Cloud Messaging (FCM) or Apple Push Notification Service (APNS) to send push notifications for reminders and alerts.
  - Sends messages to the user's device, enabling real-time updates on payments, rewards, and credit score changes.

- **APIs and Data Exchange**:
  - RESTful APIs facilitate secure data exchange between the client (app) and backend server, including payment transactions, account updates, and rewards.
  - All communication is conducted over HTTPS with SSL/TLS encryption to ensure data security.

3.4 Communications Interfaces

The CRED Mobile Application uses several communication interfaces to ensure secure and efficient data transfer, notifications, and user verification.

- **Network Communication Protocols**:

  - All data exchanges between the app and backend server use HTTPS with SSL/TLS encryption for security.
  - Compliant with PCI-DSS and GDPR standards for data privacy.

- **Push Notifications**:

  - Uses Firebase Cloud Messaging (FCM) for Android and Apple Push Notification Service (APNS) for iOS to deliver real-time notifications, including payment reminders, rewards updates, and credit score alerts.

- **Data Synchronization**:

  - Real-time synchronization between the device and server for accurate information on payments, rewards, and credit scores.
  - Supports push or polling-based updates based on connectivity.

- **Email Communication**:

  - Sends account verification emails, alerts, and updates to the user's registered email in HTML format, ensuring compatibility with most email clients.

- **Phone Communication**:

  - Uses SMS-based OTP (One-Time Password) for secure user verification during login and critical actions.
  - SMS messages are sent over secure channels to prevent interception and enhance security.

4 System Features

4.1 User Registration and Verification

4.1.1 Description and Priority

This feature allows users to register an account by entering PAN, phone number, and email, with OTP-based verification. It is of **High Priority** as it is essential for user onboarding and security.

4.1.2 Stimulus/Response Sequences

- **User Action**: User enters PAN, phone, and email, then submits the registration form.

- **System Response**: System sends an OTP to the user's phone number.

- **User Action**: User enters the OTP and submits.

- **System Response**: System verifies the OTP. If correct, it creates the account; if incorrect, an error message is displayed.

4.1.3 Functional Requirements

- **REQ-1**: The system shall allow users to input PAN, phone number, and email for registration.

- **REQ-2**: The system shall send an OTP to the phone number for verification.

- **REQ-3**: The system shall verify OTPs and allow users to proceed upon successful verification.

- **REQ-4**: If OTP validation fails, the system shall show an error message and an option to resend OTP.

4.2 Payment Tracking and Management

4.2.1 Description and Priority

This feature enables users to view upcoming payments, schedule payments, and manage credit card payments. It is of **High Priority** due to its core role in payment management.

4.2.2 Stimulus/Response Sequences

- **User Action**: User views upcoming payments on the dashboard.

- **System Response**: The system displays payment amounts, due dates, and allows the user to initiate payments.

4.2.3 Functional Requirements

- **REQ-1**: The system shall display all upcoming payments, amounts, and due dates.

- **REQ-2**: The system shall allow users to initiate payments for selected credit cards.

- **REQ-3**: The system shall support scheduling payments and show confirmations or errors.

4.3 Rewards and Points Redemption

4.3.1 Description and Priority

Users earn reward points for timely payments, which can be redeemed within the app. This feature is of **Medium Priority** as it enhances user engagement.

4.3.2 Stimulus/Response Sequences

- **User Action**: User views reward points and selects an offer for redemption.

- **System Response**: System deducts points and confirms redemption.

4.3.3 Functional Requirements

- **REQ-1**: The system shall display users' total reward points and available offers.

- **REQ-2**: The system shall allow points redemption and provide a confirmation upon successful redemption.

4.4 Credit Score Monitoring

4.4.1 Description and Priority

Allows users to monitor their credit score with updates from credit bureaus. This is a **Medium Priority** feature that supports financial awareness.

4.4.2 Stimulus/Response Sequences

- **User Action**: User checks the credit score section.

- **System Response**: System retrieves and displays the latest credit score.

4.4.3 Functional Requirements

- **REQ-1**: The system shall retrieve and display the user's credit score.

- **REQ-2**: The system shall provide tips for improving the user's credit score.

4.5 Notifications and Alerts

4.5.1 Description and Priority

This feature sends timely notifications about payments, rewards, and important updates. It is of **High Priority** to ensure user engagement and prevent missed payments.

4.5.2 Stimulus/Response Sequences

- **User Action**: Payment due date approaches.

- **System Response**: System sends a reminder notification.

4.5.3 Functional Requirements

- **REQ-1**: The system shall send payment reminders before due dates.

- **REQ-2**: The system shall notify users of reward points and important updates.

4.6 Account and Profile Management

4.6.1 Description and Priority

Allows users to update their profile, manage linked cards, and set preferences. This is a **Medium Priority** feature for maintaining account settings.

4.6.2 Stimulus/Response Sequences

- **User Action**: User accesses profile settings to update personal information.

- **System Response**: System displays editable fields and saves updates.

4.6.3 Functional Requirements

- **REQ-1**: The system shall allow users to update personal information.

- **REQ-2**: The system shall allow users to manage notification preferences and linked credit cards.

5 Other Non-Functional Requirements

5.1 Performance Requirements

The CRED Mobile Application must meet the following performance requirements to ensure a smooth and responsive user experience:

- **Response Time**:

  - The application shall display the main dashboard within 2 seconds of user login.

- Payment processing should complete within 5 seconds after initiation, barring network delays.
- Notifications should be delivered within 1 minute of the triggering event (e.g., payment due reminder).

- **Concurrent Users**:
  - The system should support up to 1 million concurrent users without performance degradation.

- **Data Synchronization**:
  - Real-time data updates between client and server should synchronize within 2 seconds of any change.

- **Availability**:
  - The system shall maintain 99.9% uptime, allowing continuous access for users.

5.2 Safety Requirements

This section outlines the safety requirements for the CRED application, focusing on potential risks, necessary safeguards, and compliance with regulations.

5.2.1 Safety Risks

Identified risks include:

- **Data Breach:** Unauthorized access leading to identity theft.
- **Malfunction:** Software bugs causing unexpected behavior.
- **User Error:** Improper usage due to inadequate instructions.

5.2.2 Safeguards

To mitigate risks, the following measures are required:

1. **Data Protection:**
   - Use strong encryption (e.g., AES-256) for data.
   - Conduct regular security audits.

2. **Error Handling:**
   - Implement robust error logging and feedback.
   - Ensure comprehensive testing (unit, integration, user acceptance).

3. **User Education:**
   - Provide clear documentation and onboarding tutorials.

5.2.3 Preventative Actions

Mandatory actions include:

- **Access Control:** Enforce multi-factor authentication (MFA).
- **Data Retention:** Implement policies to minimize data exposure.

5.2.4 Compliance and Certifications

CRED will comply with:

- **GDPR:** Data protection and privacy regulations.

- **PCI DSS:** Standards for payment information security.

Certifications required:

- **ISO/IEC 27001:** Information security management.

- **SOC 2 Type II:** Data security controls attestation.

5.3 Security Requirements

This section specifies requirements regarding security and privacy issues surrounding the use of the CRED application, as well as the protection of data used or created by the product.

5.3.1 Security and Privacy Issues

The following security requirements must be addressed:

- User Authentication: Implement multi-factor authentication (MFA) to ensure secure user identity verification.

- Data Protection: Utilize strong encryption methods (e.g., AES-256) for both data at rest and in transit.

- Access Control: Define role-based access controls to limit user permissions based on their roles.

5.3.2 External Policies and Regulations

CRED will comply with the following regulations concerning security:

- General Data Protection Regulation (GDPR): Ensure user data privacy and protection rights are upheld.

- Payment Card Industry Data Security Standard (PCI DSS): Adhere to standards for secure handling of payment data.

5.3.3 Security Certifications

The following security certifications are required for CRED:

- ISO/IEC 27001: Certification for information security management systems.

- SOC 2 Type II: Attestation of the effectiveness of controls related to data security and privacy.

5.4 Software Quality Attributes

This section specifies additional quality characteristics for the CRED application that are important to both customers and developers.

5.4.1 Quality Characteristics

The following software quality attributes are critical:

- Adaptability: The system should allow for feature updates within 30 days of a major release.

- Availability: Target 99.9% uptime, ensuring minimal disruption to users.

- Correctness: Aim for 95% test coverage in all core modules to ensure functional accuracy.

- Usability: Achieve a user satisfaction score of at least 85% in usability testing.

- Maintainability: The system should allow for code changes with a maximum of 30 minutes of downtime per update.

5.4.2 Relative Preferences

When prioritizing quality attributes, ease of use is favored over ease of learning. The system should provide intuitive interfaces and clear instructions to minimize the learning curve for users.

5.5 Business Rules

This section outlines the operating principles governing the CRED application, specifying which individuals or roles can perform specific functions under certain circumstances.

5.5.1 Role-Based Access Control

The following business rules apply to user roles within the application:

- Admin Role:
    - Can create, read, update, and delete user accounts.
    - Can manage system settings and configurations.
    - Can view all transaction data and user activity logs.

- User Role:
    - Can create and manage their own profiles.
    - Can view their own transaction history and account details.
    - Cannot access administrative functions or other users' data.

- Guest Role:
    - Can view general application information and features.
    - Cannot perform any transactions or access personal data.
    - Must register or log in to access additional features.

5.5.2 Function-Specific Rules

The following rules dictate specific functions based on user actions:

- Transaction Limits: Users can only initiate transactions up to a specified amount unless they have verified their identity through additional authentication measures.

- Data Retention: User data will be retained for a maximum of five years after account closure, after which it will be permanently deleted.

- Approval Process: Certain actions, such as fund transfers above 5,000, must be approved by an administrator before completion.

6 Other Requirements

This section defines any requirements not covered elsewhere in the SRS, including database requirements, internationalization needs, legal obligations, and other pertinent project objectives.

6.1 Database Requirements

The CRED application must meet the following database requirements:

- Database Management System: Use a relational database management system (RDBMS) such as PostgreSQL for data storage.

- Data Integrity: Ensure referential integrity through foreign key constraints and implement checks for data validation.

- Backup and Recovery: Establish a daily backup schedule with a recovery plan to restore data within 24 hours in the event of a failure.

6.2 Internationalization Requirements

The application will support internationalization with the following features:

- Language Support: Provide user interface translations for at least three languages (e.g., English, Spanish, and Mandarin).

- Date and Currency Formats: Adapt date and currency formats based on user locale settings.

- Cultural Sensitivity: Ensure that content is culturally appropriate for target markets.

6.3 Legal Requirements

CRED will adhere to the following legal obligations:

- Data Protection Laws: Comply with applicable data protection regulations, such as the GDPR and CCPA, ensuring user privacy and data rights.

- Consumer Protection Laws: Ensure compliance with consumer protection regulations relevant to financial transactions and services.

6.4 Reuse Objectives

To promote efficiency and maintainability, the following reuse objectives will be implemented:

- Code Reusability: Implement modular design principles to allow for code reuse across different components of the application.

- Documentation Standards: Maintain comprehensive documentation for all reusable components, enabling easier integration and updates.

6.5 Other Considerations

Additional requirements that may be relevant include:

- Performance Requirements: The application should handle at least 10,000 concurrent users without degradation in performance.

- Accessibility Requirements: Ensure compliance with WCAG 2.1 standards to make the application accessible to users with disabilities.

A   Appendix A: Glossary

This appendix defines the terms necessary to properly interpret the SRS, including acronyms and abbreviations specific to the CRED project.

- API: Application Programming Interface – a set of rules for building and interacting with software applications.

- DBMS: Database Management System – software that interacts with end users, applications, and the database itself to capture and analyze data.

- GDPR: General Data Protection Regulation – European Union regulation on data protection and privacy.

- MFA: Multi-Factor Authentication – a security system that requires more than one method of authentication.

- PCI DSS: Payment Card Industry Data Security Standard – a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

- TBD: To Be Determined – items that are not yet finalized or need further clarification.

B   Appendix B: Analysis Models

This appendix optionally includes pertinent analysis models that provide additional insights into the design and functionality of the CRED application. Diagrams may include:

B.1   Data Flow Diagram

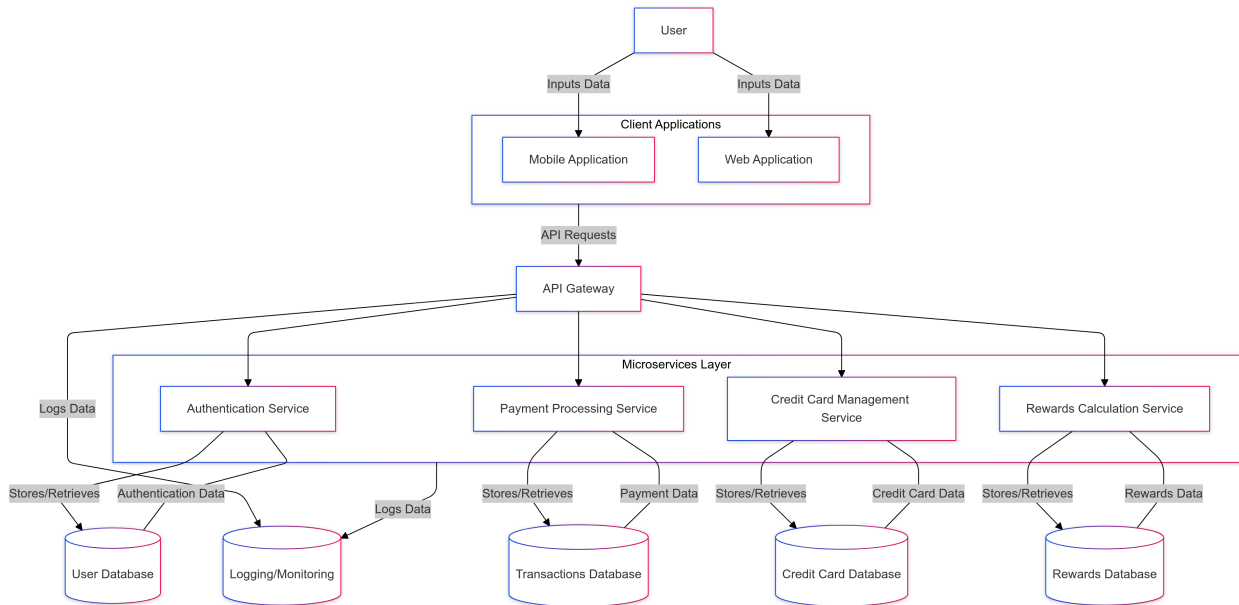A data flow diagram illustrating how data moves through the system.

Figure 1: DataFLow Diagram of CRED
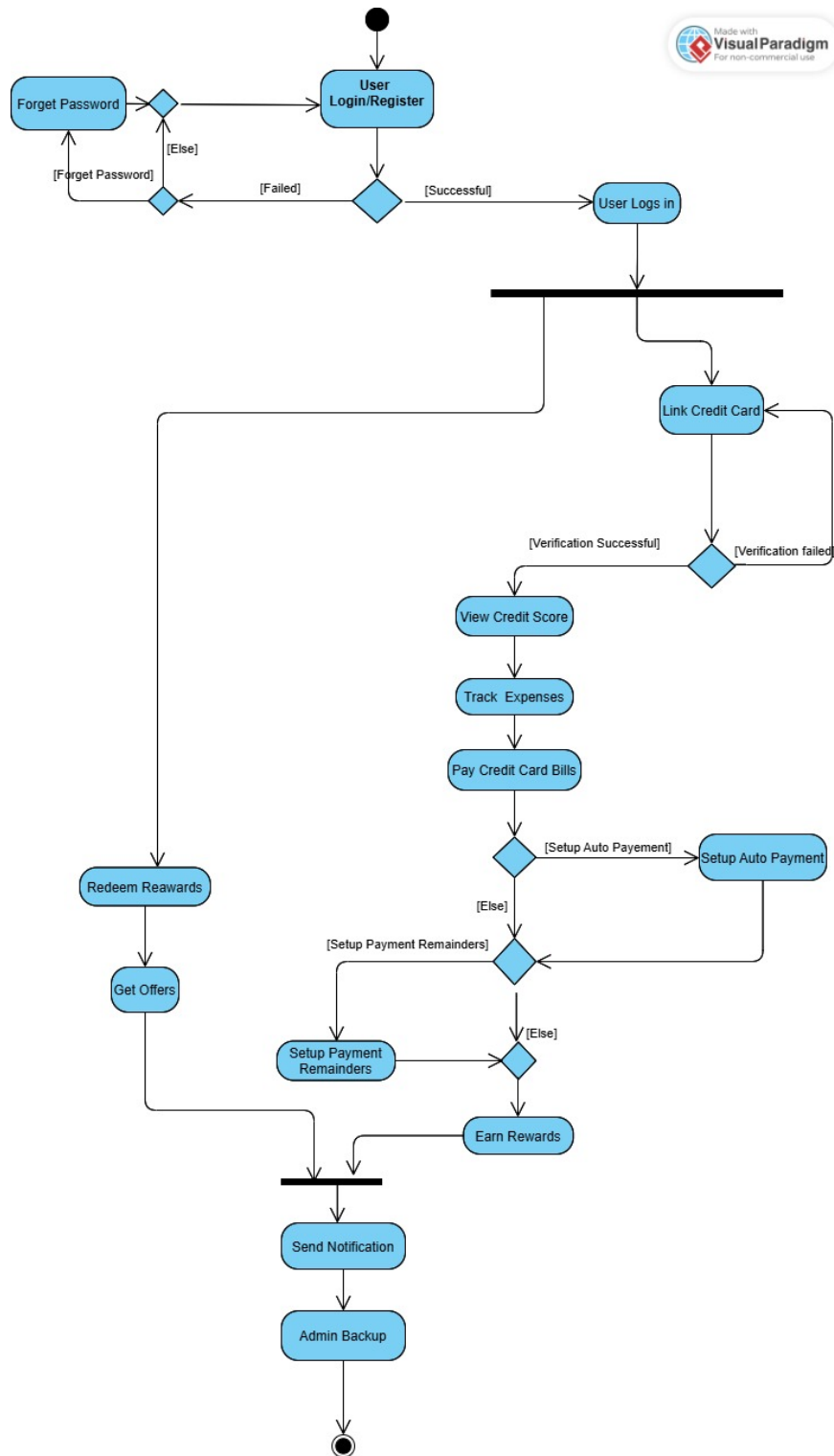
B.2 Activity Diagram

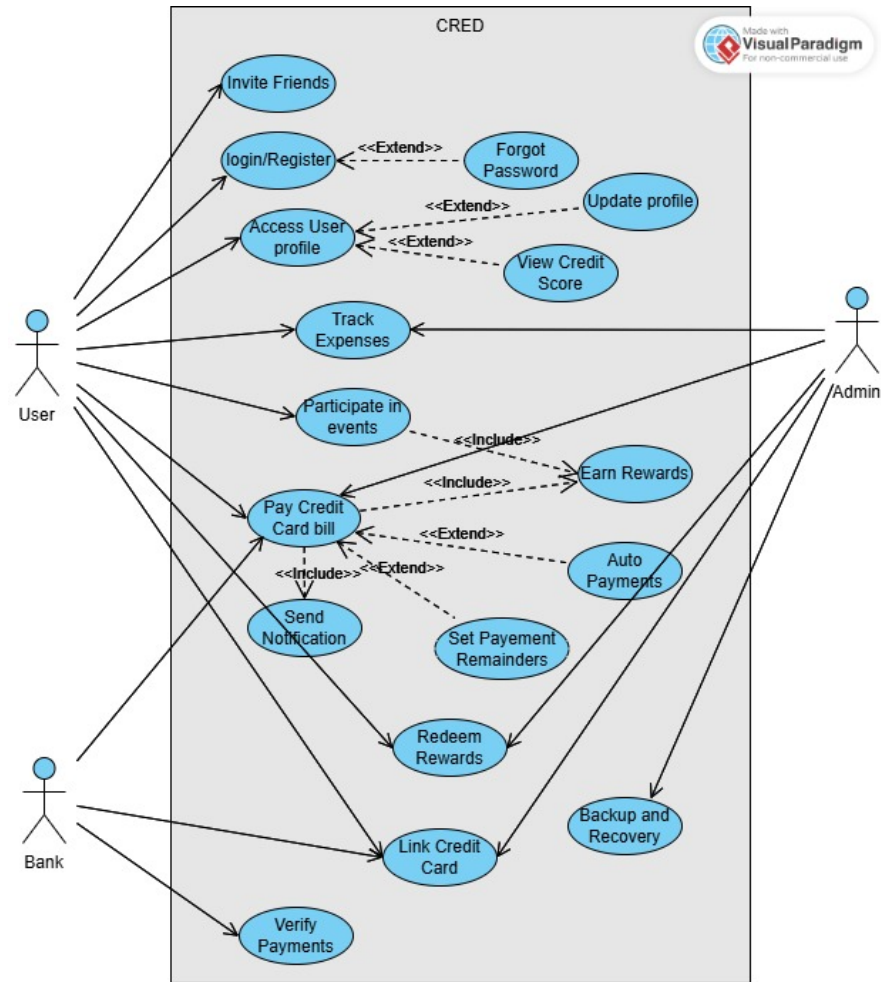Figure 2: Activity Diagram of CRED

B.3 Use-Case Diagram

Figure 3: Activity Diagram of CRED

.

C Appendix C: To Be Determined List

This appendix collects a numbered list of TBD references that remain in the SRS to track them to closure:

1. TBD on third-party integrations and APIs.

2. TBD on specific compliance requirements from local regulations.

3. TBD for performance benchmarks and load testing results.

4. TBD for user acceptance testing criteria.

Architectural Design Analysis of CRED

1 Architectural Design

1.1 Architectural Style

Description: CRED employs a *microservices-based architecture* hosted on cloud infrastructure, designed to support high concurrency, scalability, and security. Each microservice is dedicated to specific business functions, such as user authentication, credit card management, rewards, and payment processing. These services communicate via RESTful APIs and leverage containerization (e.g., Docker and Kubernetes) for deployment, enabling easy scaling and resilience across different instances.

This architecture allows CRED to scale each microservice independently based on user demands. The system is optimized for real-time operations and large data processing, given its focus on managing credit card payments, offers, and real-time rewards across millions of users.
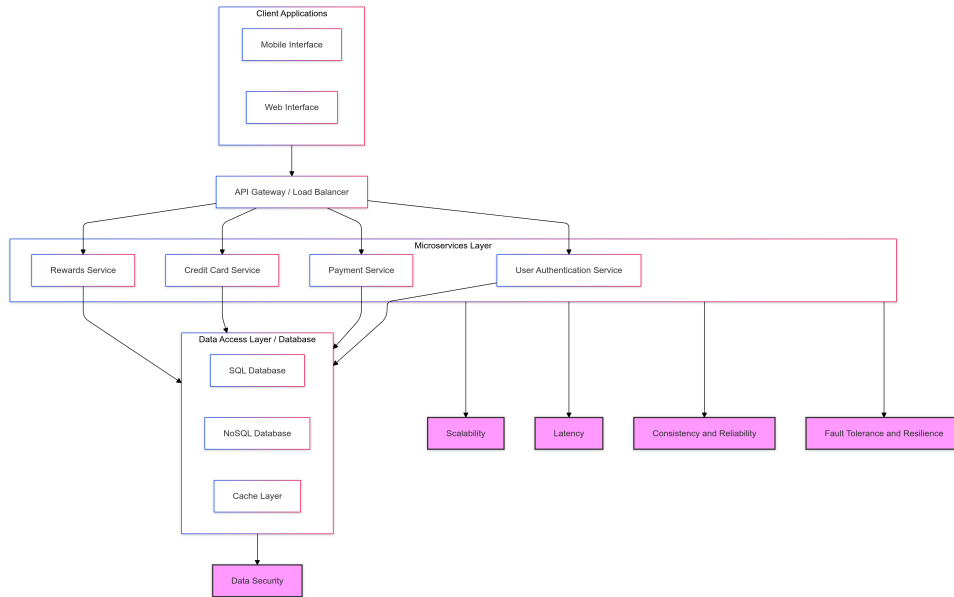
Diagram

Figure 1: High-Level Diagram of CRED's Microservices-Based Architecture

Challenges and Issues:

- **Scalability:** CRED must handle high volumes of user activity, especially during peak times such as monthly payment cycles or during promotional offers. Scaling microservices independently can become complex without optimized orchestration.

- **Latency:** Low-latency performance is critical for seamless payment processing and rewards calculation. Network latency between services and database queries can impact the real-time experience.

- **Data Security:** Given the handling of sensitive financial data, maintaining data security and compliance with industry standards (such as PCI-DSS) is paramount.

- **Consistency and Reliability:** Microservices must maintain data consistency across distributed services (e.g., ensuring payment completion reflects accurately in rewards). Reliability is enhanced through mechanisms like circuit breakers and retries.

- **Fault Tolerance and Resilience:** In a microservices architecture, individual services can fail independently. CRED must ensure services fail gracefully and that dependency on external APIs (e.g., payment gateways) does not impact overall functionality.

- **Monitoring and Logging:** Observability is critical. Logging across microservices and real-time monitoring help in debugging, compliance, and proactive detection of potential issues.

2 Design Models

2.1 Layered Architecture Model

The system design follows a multi-layered approach:

- **Presentation Layer:** Manages user interfaces on mobile (Android and iOS) and web platforms, focusing on intuitive design and responsive interactions. This layer integrates with backend services via secure REST APIs and prioritizes user experience.

- **Business Logic Layer:** Contains the core functionality of CRED, including user authentication, credit card management, rewards calculation, and payment processing. This layer incorporates rate-limiting and throttling to manage load effectively.

- **Data Access Layer:** Manages interactions with databases (e.g., SQL for structured data and NoSQL for large-scale, unstructured data). It includes caching mechanisms for frequently accessed data to enhance performance.

- **Cloud Infrastructure Layer:** Hosted on cloud services (e.g., AWS, GCP), this layer supports scaling, data redundancy, and load balancing. It uses containerization for deployment flexibility and supports CI/CD for efficient updates.

2.2 Client-Server Model

CRED's mobile and web applications act as clients, making requests to backend servers that handle sensitive operations such as payments, user data, and reward calculations. This model separates client-side processing from backend servers, increasing data security and performance. User authentication (e.g., via OAuth) secures these interactions.

2.3 Event-Driven Model

CRED leverages event-driven architecture for handling specific actions like payment completion and rewards issuance. For instance:

- **Events**: Each action (e.g., payment processed, new reward earned) generates an event.

- **Message Queue**: Events are placed in a queue (e.g., Kafka, RabbitMQ) to be processed asynchronously.

- **Event Processors**: Event-driven services process these events, ensuring real-time updates to user accounts and notifying users via the interface.

This model optimizes real-time response and system decoupling.

3 Design Principles and Risk Considerations

3.1 Design Principles

- **Modularity and Decoupling:** Microservices architecture enables modularity, allowing each service to evolve independently, enhancing flexibility in development and deployment.

- **Scalability:** The architecture supports both horizontal (adding more instances) and vertical scaling (enhancing resource capabilities) to meet peak demands without performance degradation.

- **Reliability and Fault Tolerance:** Redundancy and automatic failover mechanisms are used to handle partial service failures, ensuring continuous availability.

- **Security and Compliance:** Secure APIs, encrypted communication, and strict access controls (e.g., OAuth, role-based access) ensure user data protection, meeting compliance requirements like PCI-DSS for payment handling.

- **User-Centered Design and Responsiveness:** The application prioritizes fast and responsive user experience, with feedback mechanisms and minimal load times.

3.2   Risk Considerations

- **Data Breach:** The risk of unauthorized access to sensitive financial information poses a major concern. To mitigate this, the platform uses encryption, secure communication protocols, and multifactor authentication.

- **Payment Failures and Downtime:** Payment processing interruptions can lead to customer dissatisfaction and revenue loss. Payment failures are mitigated by retry policies and backups, while server health monitoring ensures quick detection and resolution of potential issues.

- **Service Downtime and Reliability:** Service interruptions during peak usage or due to high demand may impact user experience. By implementing load balancing and autoscaling, CRED manages server load dynamically to meet user demands.

- **Compliance Risk:** Ensuring adherence to industry standards (e.g., PCI-DSS) for data handling and storage is vital. CRED actively audits data processes and applies compliance-focused controls.

- **Consistency Across Services:** Data synchronization across microservices is crucial for accurate information display. Techniques like event sourcing and distributed transactions ensure consistency while maintaining service independence.

Conclusion

In conclusion, the CRED Mobile Application is intended to offer users a seamless and secure platform to manage credit card payments, rewards, and financial insights. By addressing key challenges in payment management, security, and user experience, CRED aims to empower users to make informed financial decisions with ease. The application's design emphasizes scalability, reliability, and compliance with industry standards, ensuring that users can rely on it for everyday financial management. Future enhancements and features will continue to evolve based on user feedback and technological advancements, making CRED a robust and adaptive solution in the mobile financial landscape.

References

[1] CRED https://cred.club/

[2] Nielsen, J., Budiu, R. (2012).*Mobile Usability*. New Riders Press. This book discusses best practices in mobile application design, focusing on usability and user-centered design principles critical to applications like CRED.

[3] Wikipedia https://en.wikipedia.org/wiki/Cred_(company)

GROUP MEMEBERS CONTRIBUTION:

1. Sai Charan -220911638

SRS & Diagrams

2. Arnav -220911476

Architectural design

3. Ayush -220911632

SRS & Diagrams