*A project report on*

**VAULT - A FULLY SECURE TRANSACTION APPLICATION**

*Submitted in partial fulfillment for the J component Review of*

## **Master of Technology in Software Engineering (Integrated)**

*by*

**Nancy Saxena (21MIS1024)  
Aakarsh Mishra (21MIS1025)**



**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

April, 2024

**Course Title: Information and System Security**

**Course Code: SWE3002**

**Slot: E2**

**Faculty: Dr. Malathi D Sign:**

**Date: 26/04/2024**

**CONTENTS**

**CHAPTER 1**

**INTRODUCTION**

* 1. Abstract………………………………………………………………………………….3
  2. Introduction…………………………………………………………………..………….3
  3. Problem statement……………………………………………………………………….4

**CHAPTER 2**

**TECHNOLOGIES USED**

2.1 Technologies Used………………………………………………………………………………………………..……..5

2.2 Algorithm Used…………………………………………………………………………..………………………………..6

**CHAPTER 3**

**PROPOSED SYSTEM**

3.1 Proposed System………………………………………………………………….………………………………………7

3.2 Novelty…………………………………………………………………………………………………………………………8

3.3 System Architecture………………………………………………………………………………………………….….2

**CHAPTER 4**

**IMPLEMENTATION**

4.1 Application Implementation………………………………………….…………………………………………...10

4.2 Algorithm Implementation………………………………………………………………………………………...10

**CHAPTER 5**

**RESULTS**

5.1 Results………………………………………………………………………………………..………………………………14

**CHAPTER 6**

**CONCLUSION AND FUTURE WORK**

6.1 Conclusion ………………………………………………………………………………………..……………………….16

6.2 Future Work…………………………..………………………………………………….……………………………….17

**Chapter 1**

**Abstract**

* 1. **Abstract**

In an era of ubiquitous digital transactions, ensuring user data security and confidentiality is paramount. "VAULT - A Fully Secure Transaction App" is an innovative payment gateway designed to address the growing concerns surrounding cybersecurity in financial transactions.

At the core of VAULT lies a robust security architecture fortified with multiple layers of authentication and encryption. The login module implements a three-factor authorization mechanism, requiring facial recognition, fingerprint scanning, and traditional username-password credentials. This significantly reduces the risk of unauthorized access by ensuring only authorized individuals can access the app.

Furthermore, VAULT employs advanced encryption techniques to safeguard user data collected during the Know Your Customer (KYC) process. We propose a novel algorithm, TriSecurEncrypt, for encrypting all text data. TriSecurEncrypt leverages a combination of AES (symmetric encryption) for confidentiality, RSA (asymmetric encryption) for secure key exchange, and HMAC (message authentication code) for data integrity. Personal identification information is encrypted with TriSecurEncrypt, protecting it against unauthorized access or data breaches. Additionally, steganography, or image encryption, further enhances data security by concealing sensitive information within images, minimizing the risk of data leakage.

For credit and debit card transactions, as well as bill generation, VAULT utilizes specialized encryption protocols tailored to financial transactions. This ensures that all payment information remains confidential and protected against potential cyber threats.

In the event of a forgotten password, VAULT implements a two-factor authentication process for password recovery. Users receive a one-time password (OTP) via email or mobile number, adding an extra layer of security.

VAULT strives to provide users with a payment app devoid of security vulnerabilities. With its comprehensive security features, including the novel TriSecurEncrypt algorithm, and unwavering commitment to data confidentiality, VAULT sets a new standard for secure and user-friendly digital transactions.

* 1. **Introduction**

In today's digital world, where convenience and speed often come at the cost of security, managing your finances online can feel like a gamble. But what if there was a payment app designed from the ground up to prioritize your safety? Introducing VAULT, the revolutionary app that redefines secure transactions.

VAULT goes beyond standard security measures to create an impenetrable fortress for your financial data. Our ground-breaking TriSecurEncrypt algorithm, a multi-layered encryption system, acts as your digital vault, safeguarding your sensitive information.

Here's a glimpse into the unparalleled security VAULT offers:

* **Fort Knox Login:** No more worrying about weak passwords. VAULT utilizes a robust three-factor authentication system, requiring facial recognition, fingerprint scanning, and your traditional login credentials for ultimate access control.
* **Impregnable KYC Protection:** KYC (Know Your Customer) details are the cornerstone of secure transactions. VAULT encrypts all your KYC information, including your photo ID, using a combination of steganography and TriSecurEncrypt, ensuring it remains invisible and inaccessible to unauthorized eyes.
* **Unbreachable Banking Data:** VAULT employs specialized encryption protocols specifically designed for financial transactions, shielding your credit card details and banking information from cyber threats.
* **Encrypted Transactions & Secure Recovery:** Every transaction you make within VAULT is meticulously encrypted, ensuring complete confidentiality. Even if you forget your password, our secure two-factor authentication process for password recovery ensures only you regain access.

VAULT doesn't just protect your data; it empowers you. With features like instant fund transfers, encrypted transaction history, and a user-friendly interface, VAULT simplifies your financial life while keeping your security paramount.

* 1. **Problem Statement**

While mobile payment applications like Bharat Interface for Money (BHIM) aim to revolutionize digital transactions in India, the recent discovery by vpnMentor's research team highlights a critical vulnerability in the security infrastructure of such platforms. The exposure of a massive amount of highly sensitive financial data linked to BHIM on a misconfigured Amazon Web Services S3 bucket underscores the urgent need for robust security measures to safeguard user information and prevent unauthorized access.

The vpnMentor report reveals that the BHIM website, developed by CSC eGovernance Services LTD. in collaboration with the Indian government, was utilized to enroll a significant number of users and business merchants onto the app. However, the misconfiguration of the S3 bucket led to the inadvertent exposure of confidential data related to this enrollment campaign, including personal and financial details of millions of individuals and businesses.

Despite the data appearing to be limited to records from February 2019, the sheer volume of over 7 million exposed records underscores the magnitude of the security lapse and the potential risks posed to user privacy and financial security. This incident highlights the critical importance of implementing comprehensive multi-factor authentication, encryption techniques, and access controls to safeguard sensitive data and mitigate the risk of unauthorized access and data breaches in mobile payment applications.

As stakeholders in the digital payments ecosystem seek to foster trust and confidence among users and merchants, addressing vulnerabilities and ensuring robust security measures must be prioritized to uphold the integrity and reliability of these platforms in facilitating secure and seamless financial transactions.

**Chapter 2  
Technologies used**

**2.1 Technologies Used**

VAULT prioritizes robust security and a seamless user experience. This section details the key technologies that make VAULT a reliable and user-friendly platform for financial transactions.

**1. Android Development Environment:**

* **Android Studio with Java:** The primary development platform for VAULT leverages Android Studio, the official Integrated Development Environment (IDE) for Android app development. Java, a high-level object-oriented programming language, serves as the foundation for building the app's functionalities.
* **XML:** Android utilizes XML (Extensible Markup Language) for defining the app's user interface (UI) layout and configuring various app components. XML provides a flexible and declarative way to design the visual elements users interact with.

**2. Firebase Integration:**

* **Firebase Realtime Database:** VAULT employs Firebase Realtime Database, a NoSQL cloud database from Google, for storing and synchronizing a limited amount of frequently accessed user data. This real-time data storage enables features like quick balance updates or limited transaction history retrieval.
* **Firebase Realtime Storage:** Firebase Realtime Storage serves as the secure storage solution for user-uploaded KYC documents (photo IDs) within VAULT. This cloud storage offers scalability and built-in security features.
* **Firebase Authentication Methods:** VAULT leverages Firebase Authentication, a comprehensive user authentication system, to implement the robust 3FA login process. This service provides features like username/password authentication, biometric authentication integration (fingerprint, facial recognition), and OTP verification via email or SMS.
* **Firestore Database (Optional):** For future development, VAULT can consider migrating to Firestore, a more scalable and flexible NoSQL database offering from Firebase. Firestore can handle larger datasets and complex queries compared to Realtime Database.

**3. Modern Android Development Tools:**

* **Latest AndroidX Libraries:** VAULT utilizes the latest AndroidX libraries, the official set of Android Jetpack libraries, to benefit from performance improvements, new functionalities, and enhanced security features provided by Google.

**4. Security Libraries:**

* **AndroidX Biometric Library:** This library facilitates the integration of fingerprint or facial recognition authentication for secure user login within the app.
* **Third-Party Security Libraries:** VAULT employs additional security libraries like Scottylab:aescrypt to perform specific encryption tasks beyond the capabilities of standard Android libraries.

**5. Custom Encryption Algorithm: TriSecurEncrypt**

VAULT leverages a novel encryption algorithm, TriSecurEncrypt, designed to offer superior data security. This algorithm combines the strengths of three cryptographic techniques:

* **AES (Advanced Encryption Standard):** Provides data confidentiality with a 256-bit secret key and utilizes GCM mode for data integrity.
* **RSA (Rivest-Shamir-Adleman):** Enables secure key exchange using public and private key pairs. TriSecurEncrypt encrypts the AES key with RSA for enhanced protection.
* **HMAC (Hash-based Message Authentication Code):** Ensures data integrity through a secret key and a hash function, verifying if the encrypted data has been tampered with during transmission.

**Overall, VAULT utilizes a combination of industry-standard development tools, secure cloud storage solutions, robust authentication methods, and cutting-edge encryption techniques to create a secure and user-friendly mobile payment application.**

**2.2 Encryption Algorithm Used**

TriSecurEncrypt is a novel encryption algorithm designed to provide robust protection for data transmission and storage. It achieves this by combining the strengths of three well-established cryptographic techniques:

1. **AES (Advanced Encryption Standard):** This widely used symmetric encryption algorithm ensures data confidentiality using a shared secret key. TriSecurEncrypt leverages AES in **GCM (Galois/Counter Mode)** for efficiency and data integrity.
2. **RSA (Rivest-Shamir-Adleman):** This asymmetric encryption technique employs public and private key pairs for secure key exchange. In TriSecurEncrypt, RSA safeguards the transmission of the AES key.
3. **HMAC (Hash-based Message Authentication Code):** This cryptographic method utilizes a hash function and a secret key to verify data integrity and authenticity. TriSecurEncrypt utilizes HMAC with SHA-256 for tamper detection.

**Uniqueness of TriSecurEncrypt:**

TriSecurEncrypt differentiates itself from traditional encryption algorithms by offering a multi-layered security approach:

* **Comprehensive Security:** It combines the confidentiality of AES with the secure key exchange of RSA and the data integrity verification of HMAC, providing a more holistic security solution.
* **Enhanced Key Exchange Security:** By encrypting the AES key with RSA, TriSecurEncrypt eliminates the need to transmit the secret key openly, significantly reducing the risk of interception.
* **Stronger Encryption Strength:** The algorithm utilizes 256-bit AES keys and potentially 2048-bit RSA keys, offering superior encryption strength compared to many existing algorithms.

In summary, TriSecurEncrypt leverages the strengths of multiple cryptographic techniques to provide a robust and secure solution for data protection. Its multi-layered approach and emphasis on secure key exchange make it a valuable tool for safeguarding sensitive information in various applications.

**Chapter 3**

**PROPOSED SYSTEM**

**3.1 Proposed System**

This section dives into the detailed workings of VAULT, a secure payment gateway application designed to address contemporary cybersecurity concerns in financial transactions.

### **User Authentication and Onboarding**

VAULT prioritizes robust user authentication to safeguard access and user data. The onboarding process incorporates a three-factor authentication (3FA) mechanism:

1. **Biometric Authentication:** Users can utilize fingerprint or facial recognition technology for initial login and subsequent access attempts. This leverages the user's unique physical characteristics for a secure first layer of defense.
2. **Username and Password:** A traditional username and password combination serves as the second layer. VAULT enforces strong password policies to discourage easily guessable credentials and recommends regular password changes for enhanced security.
3. **One-Time Password (OTP):** For added security, VAULT can integrate with SMS or email for OTP verification during login or critical actions like adding a new bank account. This time-sensitive code adds a dynamic layer of authentication, ensuring the user actively initiates the action.

Following successful login, users proceed with the Know Your Customer (KYC) process. This step gathers essential user information for regulatory compliance and identity verification. VAULT prioritizes secure storage of this sensitive data through:

* **TriSecurEncrypt Algorithm:** As described previously, all text-based KYC data (name, address, etc.) undergoes encryption using the novel TriSecurEncrypt algorithm. This multi-layered approach combines AES for confidentiality, RSA for secure key exchange, and HMAC for data integrity, offering superior protection compared to traditional encryption methods.
* **Secure Database Storage:** The encrypted KYC data is then stored within VAULT's secure database. Industry-standard security practices like access controls, encryption at rest, and regular security audits ensure the data remains protected from unauthorized access or breaches.

### **Enhanced KYC with Steganography**

VAULT goes beyond encrypting text data. It incorporates steganography, a technique for concealing information within seemingly innocuous media like images. During KYC, users upload a photo ID (e.g., driver's license). This image undergoes two-factor encryption:

1. **Steganography:** The user's KYC data (encrypted with TriSecurEncrypt) is embedded within the photo ID using steganographic techniques. This makes it virtually undetectable to the naked eye, further obfuscating the sensitive information.
2. **TriSecurEncrypt Encryption:** The steganographically modified image itself is then additionally encrypted using TriSecurEncrypt, providing a double layer of protection.

### **Secure Data Access and Retrieval**

VAULT ensures user control over their information while maintaining security. Here's how users can access their previously uploaded photo ID:

1. **Two-Factor Authentication:** Users must first undergo a two-factor authentication process. This could involve a combination of fingerprint scanning and entering the first four digits of their registered mobile number.
2. **Decryption Process:** Upon successful authentication, VAULT retrieves the encrypted image containing the steganographically hidden data. The TriSecurEncrypt layer is first decrypted, followed by the extraction of the embedded KYC data using steganographic techniques. Only then can the user view their original KYC information.

### **Secure Financial Transactions**

VAULT facilitates secure financial transactions. Here's a breakdown of the process:

* **Secure Banking Details Storage:** All user banking details and card information are stored within the app in an encrypted format. This encryption leverages industry-standard card encryption methods like those specified by PCI DSS (Payment Card Industry Data Security Standard). Additionally, TriSecurEncrypt provides an extra layer of protection for this sensitive data.
* **UPI Integration:** Following KYC completion, VAULT generates a unique encrypted QR code representing the user's UPI (Unified Payments Interface) address. This encrypted QR code can be used for secure offline payments at merchants accepting UPI.
* **Wallet Top-Up:** Users can conveniently add funds to their VAULT wallet directly from their linked bank accounts. A two-factor authentication process ensures only authorized users can initiate top-up transactions.
* **Transaction Encryption:** All financial transactions conducted through VAULT, including money transfers and bill payments, are encrypted using industry-standard protocols. This protects the transaction details from unauthorized interception or tampering.
* **Secure Transaction History:** Users can view their transaction history within the app. However, to ensure data privacy, this history is also stored in an encrypted format. Accessing the history requires two-factor authentication, similar to viewing the KYC photo ID.

### **Secure Password Recovery**

VAULT acknowledges that users might forget their passwords. To facilitate secure password recovery, the app employs a two-factor authentication process:

1. **OTP Verification:** Users can initiate password recovery by entering their registered email address or phone number. VAULT then sends a time-sensitive OTP to the chosen verification method.
2. Password Reset: Upon successful OTP verification, users can create a new, strong password. VAULT enforces password complexity requirements to ensure the new password is resistant to brute-force attacks.

### **Secure Communication**

VAULT prioritizes secure communication between the app and its servers to safeguard user data during transmission. This is achieved through the following mechanisms:

* **HTTPS Protocol:** All communication between VAULT and its servers utilizes the HTTPS protocol. HTTPS encrypts data in transit using Transport Layer Security (TLS), protecting it from eavesdropping or man-in-the-middle attacks.
* **Certificate Validation:** VAULT implements server certificate validation to ensure secure connections. This verifies the authenticity of the server the app is communicating with, preventing man-in-the-middle attacks where a malicious actor impersonates the legitimate server.

### **User Privacy and Data Protection**

VAULT recognizes the importance of user privacy and adheres to strict data protection principles. Here's how VAULT safeguards user data:

* **Minimal Data Collection:** VAULT only collects the user information essential for account creation, KYC compliance, and smooth transaction processing. It avoids collecting unnecessary data that could be a privacy risk.
* **Data Anonymization:** Whenever possible, VAULT anonymizes user data before internal processing or analysis. This reduces the risk of linking anonymized data back to individual users.
* **User Control over Data:** VAULT empowers users with control over their data. Users can access, modify, or request deletion of their personal information within the app, subject to regulatory limitations.
* **Regular Data Backups:** VAULT maintains regular backups of user data using secure storage practices. This ensures data recovery in case of unforeseen events like system failures or cyberattacks.

### **Administrative Access Controls**

VAULT implements robust access control mechanisms to restrict access to user data and critical system functions. This includes:

* **Least Privilege Principle:** The principle of least privilege is enforced, granting users only the minimum level of access required to perform their designated tasks.
* **Role-Based Access Control (RBAC):** A role-based access control system is implemented, where user access permissions are assigned based on predefined roles (e.g., administrator, customer support).
* **Multi-Factor Authentication for Admins:** Administrative access to VAULT's back-end systems requires multi-factor authentication for added security. This ensures only authorized personnel can access sensitive data and system settings.

### **Security Auditing and Monitoring**

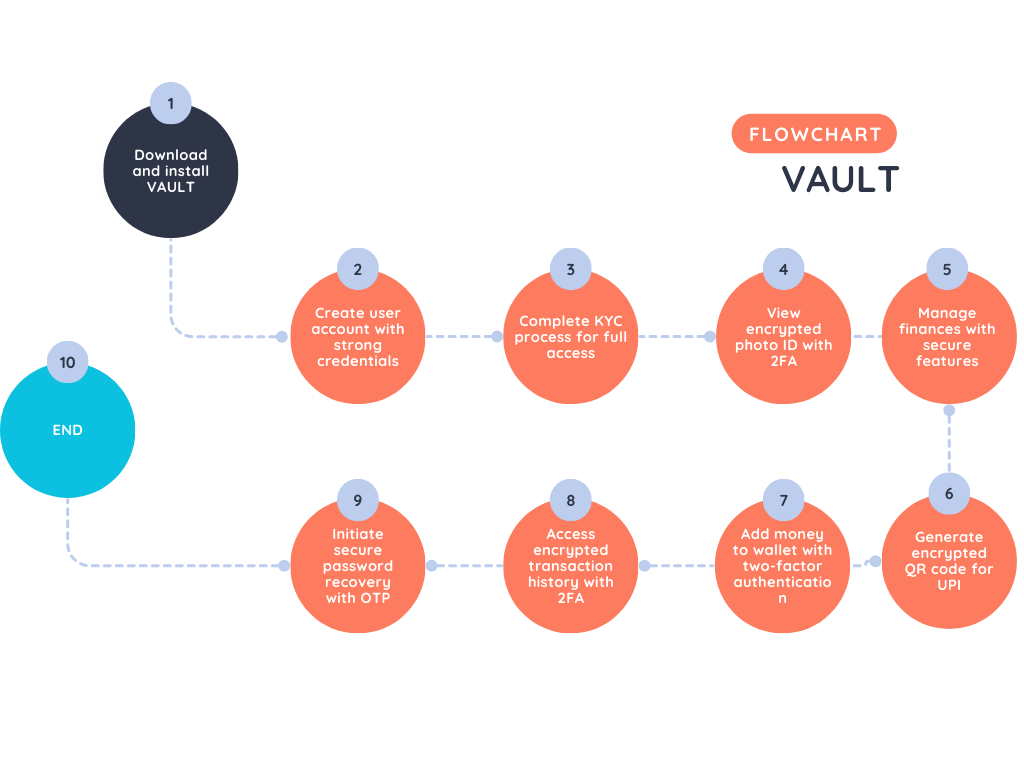
VAULT prioritizes continuous security monitoring to identify and address potential vulnerabilities. This includes:

* **Regular Security Audits:** VAULT undergoes regular penetration testing and vulnerability assessments by qualified security professionals. These assessments identify potential weaknesses in the system's security posture.
* **Security Information and Event Management (SIEM):** A SIEM system is implemented to collect and analyze security logs from various sources within VAULT's infrastructure. This allows for real-time monitoring of security events and prompt response to potential threats.
* **Incident Response Plan:** VAULT has a well-defined incident response plan that outlines the procedures for identifying, containing, and recovering from security incidents.

VAULT offers a comprehensive security framework designed to address contemporary cybersecurity concerns in the financial transactions domain. Through a combination of robust user authentication, multi-layered data encryption (including the novel TriSecurEncrypt algorithm), secure communication protocols, and user privacy-centric practices, VAULT strives to provide a secure and trustworthy platform for users to manage their finances. The secure access controls, security auditing, and monitoring further strengthen VAULT's security posture, making it a reliable choice for users seeking a secure and user-friendly payment gateway application.

This detailed explanation of VAULT's proposed system highlights its commitment to user data security and provides users with a clear understanding of how their information is protected throughout the application's functionalities.

**3.2 System Architecture**

****

The architecture of the VAULT system prioritizes both user experience and security in financial transactions. It begins with the user downloading and installing the VAULT app, followed by creating a user account with strong credentials. VAULT employs robust three-factor authentication (3FA), including biometric authentication and username/password verification, ensuring secure login.

Upon completing the KYC process, users gain full access to VAULT's features, including viewing encrypted photo ID with two-factor authentication (2FA) and managing finances securely. VAULT employs industry-standard encryption protocols and its proprietary TriSecurEncrypt algorithm to safeguard sensitive data, such as banking details and transaction history.

The system facilitates secure payments through encrypted QR codes for UPI transactions and provides secure wallet management with two-factor authentication for money transfers. Additionally, users can access their encrypted transaction history, protected by 2FA, and initiate secure password recovery through one-time passwords (OTPs) sent via registered email or mobile number.

Overall, VAULT's architecture integrates multiple layers of security measures seamlessly into its user experience, ensuring that users can manage their finances with confidence and peace of mind.

**3.3 Novelty**

VAULT distinguishes itself from existing transaction applications by offering a unique combination of innovative security features and user-centric design principles. Here's a breakdown of VAULT's key aspects that contribute to its novelty:

**1. Multi-Layered Encryption with TriSecurEncrypt:**

* **Novel Algorithm:** VAULT introduces TriSecurEncrypt, a novel encryption algorithm that leverages the strengths of both symmetric and asymmetric encryption techniques. This multi-layered approach surpasses the security offered by traditional algorithms like AES, which rely solely on symmetric encryption.
* **Enhanced Security:** TriSecurEncrypt combines AES for data confidentiality, RSA for secure key exchange, and HMAC for data integrity. This comprehensive approach safeguards user data against various cyber threats, including unauthorized access, data breaches, and message tampering.
* **Comparison with Existing Solutions:** Existing secure transaction applications often employ a single encryption method or a combination of less sophisticated techniques. TriSecurEncrypt offers a more robust and secure solution by integrating multiple encryption methods with message authentication.

**2. Secure KYC with Steganography:**

* **Beyond Traditional Encryption:** VAULT goes beyond just encrypting text-based KYC data. It leverages steganography, a technique for concealing information within seemingly harmless media like images. This adds an extra layer of protection for sensitive KYC information.
* **Double Encryption:** During KYC, user's encrypted KYC data (using TriSecurEncrypt) is embedded within the uploaded photo ID using steganographic techniques. This double encryption significantly increases the difficulty of extracting the sensitive information.
* **Enhanced User Confidence:** Steganography provides peace of mind to users by making their KYC information virtually undetectable to the naked eye, further bolstering trust in VAULT's security measures.

**3. Robust User Authentication and Access Control:**

* **Three-Factor Authentication:** VAULT implements a robust 3FA mechanism for user login. This multi-factor approach requires a combination of biometric authentication (fingerprint or facial recognition), username, and password. This significantly reduces the risk of unauthorized access compared to single-factor or two-factor authentication methods commonly used in existing apps.
* **Two-Factor Access Control:** VAULT employs a two-factor authentication process for accessing sensitive data like the uploaded KYC photo ID and transaction history. This additional layer of security ensures that only authorized users can view their information, even if someone gains access to the app.
* **Focus on User Control:** VAULT prioritizes user control over their information. While data is securely stored, users retain the ability to access it using the appropriate authentication methods.

**4. User-Centric Design and Usability:**

* **Balancing Security with Usability:** VAULT recognizes the importance of a user-friendly interface. The app is designed to be intuitive and easy to navigate, allowing users to perform transactions efficiently. This ensures that robust security features do not hinder the user experience.
* **Accessibility Features:** VAULT incorporates accessibility features to cater to users with disabilities. This may include elements like screen reader compatibility and adjustable font sizes, ensuring inclusivity and ease of use for a wider audience.
* **Security Prompts and User Education:** VAULT strives to educate users about cybersecurity best practices. The app provides subtle prompts and notifications that raise awareness about potential risks and encourage secure behavior without being intrusive.

**In conclusion, VAULT's novelty lies in the innovative combination of TriSecurEncrypt, steganography, robust user authentication, two-factor access control, and a user-centric design approach. These features distinguish VAULT from existing transaction applications by elevating security measures to a new level while maintaining a user-friendly and accessible experience.**

**Chapter 4**

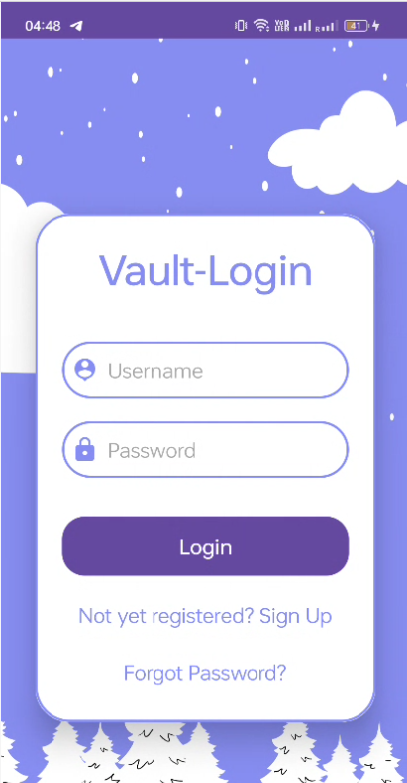
**Implementation**

**4.1 Application Implementation**

VAULT prioritizes user experience while ensuring the highest security standards for financial transactions. Here's a step-by-step guide to using VAULT's features:

**1. Secure Login:**

* Download and install VAULT from your app store.
* Upon first launch, create a user account using strong credentials.
* VAULT safeguards your login with robust **three-factor authentication (3FA)**. This involves:
  + **Facial Recognition or Fingerprint Scan:** Utilizing your phone's biometric authentication for a secure first layer.
  + **Username and Password:** Enter your unique username and a strong password you created.



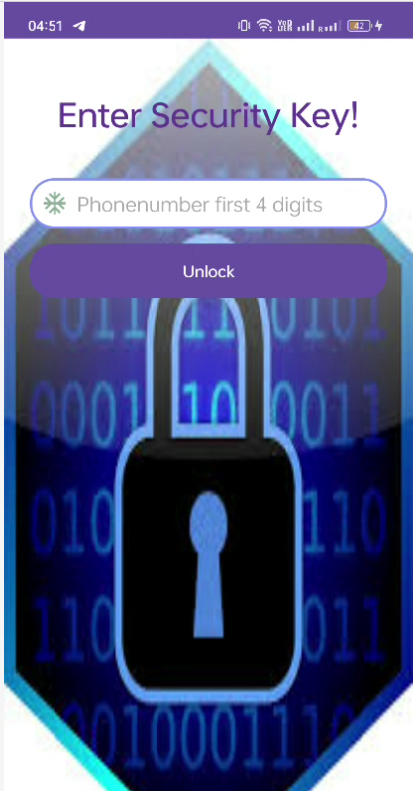
**2. Secure User Onboarding (KYC):**

* Complete your KYC (Know Your Customer) process to unlock VAULT's full potential.
* Provide your details securely, including:
  + **Personal Information:** Enter your name, address, and other required details. VAULT encrypts this data using our innovative **TriSecurEncrypt algorithm**.
  + **Photo ID Upload:** Upload a government-issued photo ID for verification. VAULT utilizes a two-pronged approach for maximum security:
    - **Steganography:** This technique invisibly embeds your ID information within an image file, further protecting your data.
    - **TriSecurEncrypt Encryption:** The embedded data is then encrypted using TriSecurEncrypt for an additional layer of security.



**3. Secure Data Viewing:**

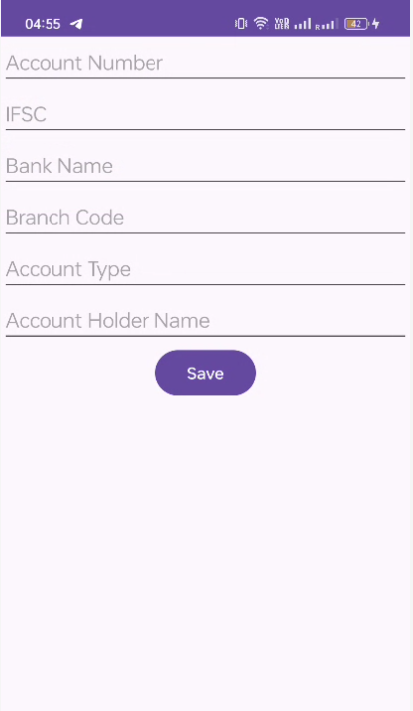
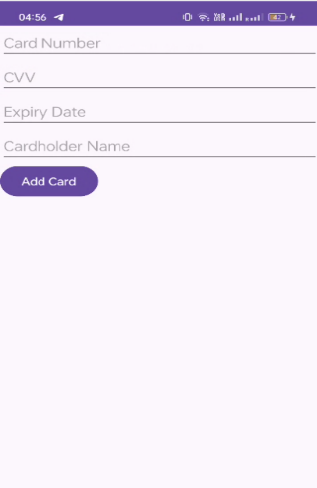
* VAULT ensures complete control over your sensitive information.
* To view your uploaded photo ID, you'll need to pass through **two-factor authentication (2FA)**:
  + **Fingerprint Scan:** Use your fingerprint scanner for verification.
  + **Mobile Number Verification:** Enter the first four digits of your registered mobile number for an extra layer of security.



**4. Secure Banking and Transactions:**

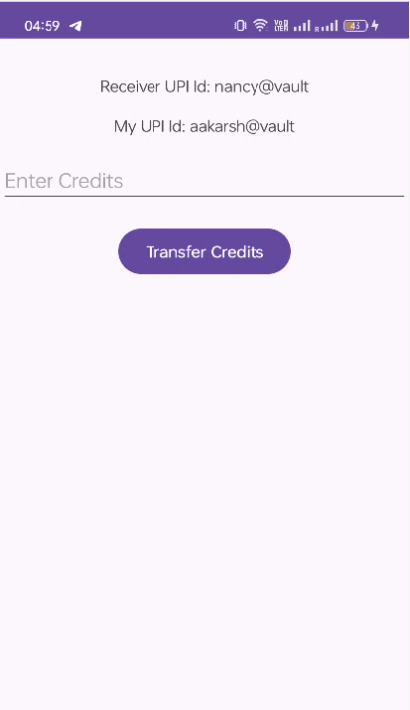
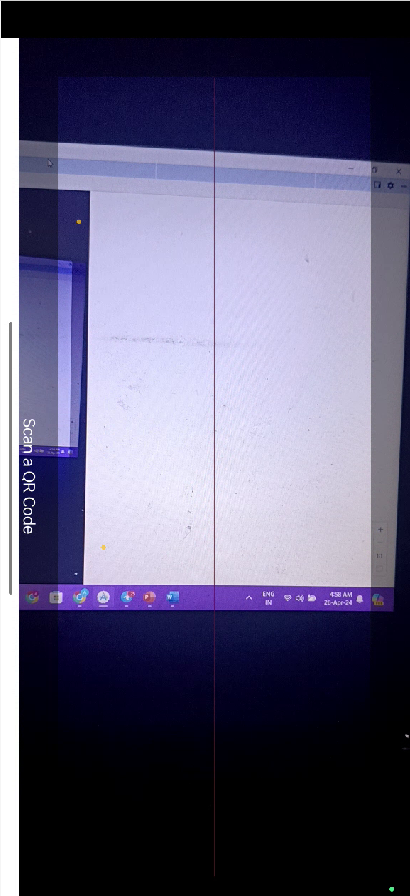
* Manage your finances with confidence using VAULT's secure features.
* All your banking details and card information are encrypted using a combination of:
  + **Card Encryption Methods:** Industry-standard encryption protocols safeguard your credit and debit card details.
  + **TriSecurEncrypt Algorithm:** VAULT's TriSecurEncrypt algorithm provides an additional layer of encryption for enhanced security.

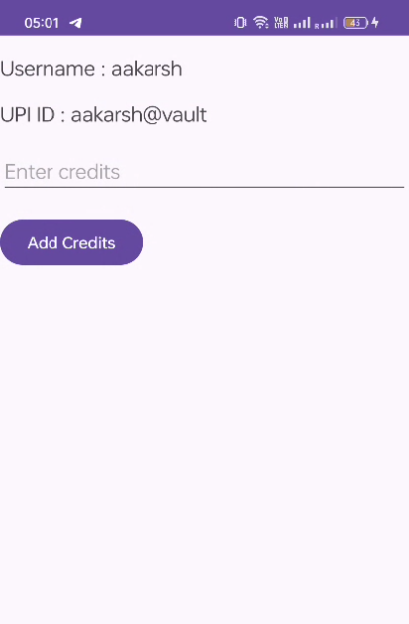
**5. Secure and Convenient Payments:**

* Experience a seamless and secure way to pay with VAULT.
* After completing KYC, a unique encrypted QR code for UPI payments will be generated within the app.
* This QR code can be used for secure UPI transactions, with the underlying data remaining encrypted.

****

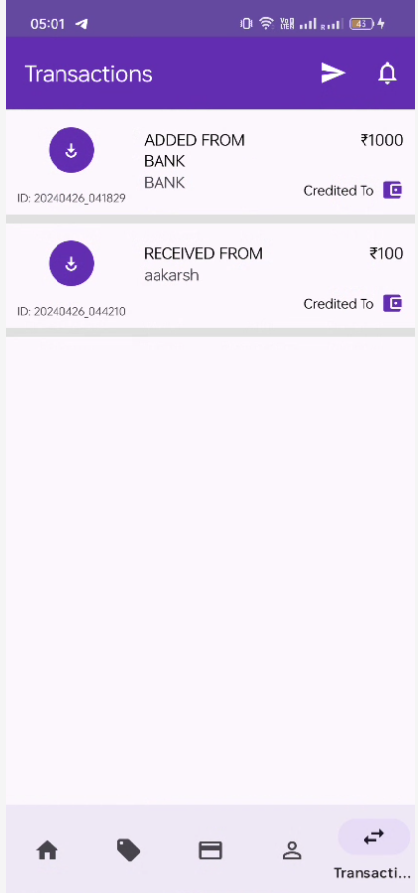
**6. Secure Wallet Management:**

* Add money to your VAULT wallet directly from your bank account.
* Two-factor authentication ensures secure money transfers:
  + **Fingerprint Scan or Other Biometric Verification:** Use your phone's biometric authentication for the first layer of security.
  + **Password Verification:** Enter your VAULT password for an extra layer of protection.



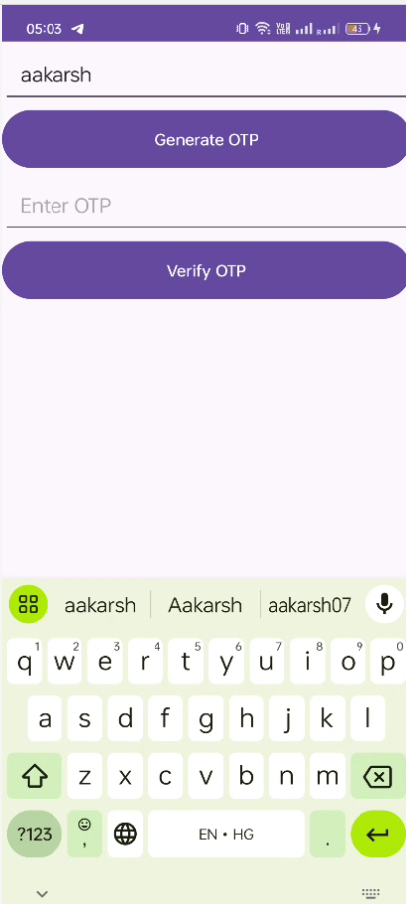
**7. Secure Transaction History:**

* Keep track of your spending habits with confidence.
* VAULT stores your transaction history in an encrypted format.
* To view your transaction history, you'll need to pass through 2FA, ensuring only you can access this sensitive information.



**8. Secure Password Recovery:**

* In case you forget your password, VAULT offers a secure recovery process.
* You'll initiate password recovery by requesting a one-time password (OTP) via your registered email or mobile number.
* This OTP acts as an additional security measure to prevent unauthorized password resets.



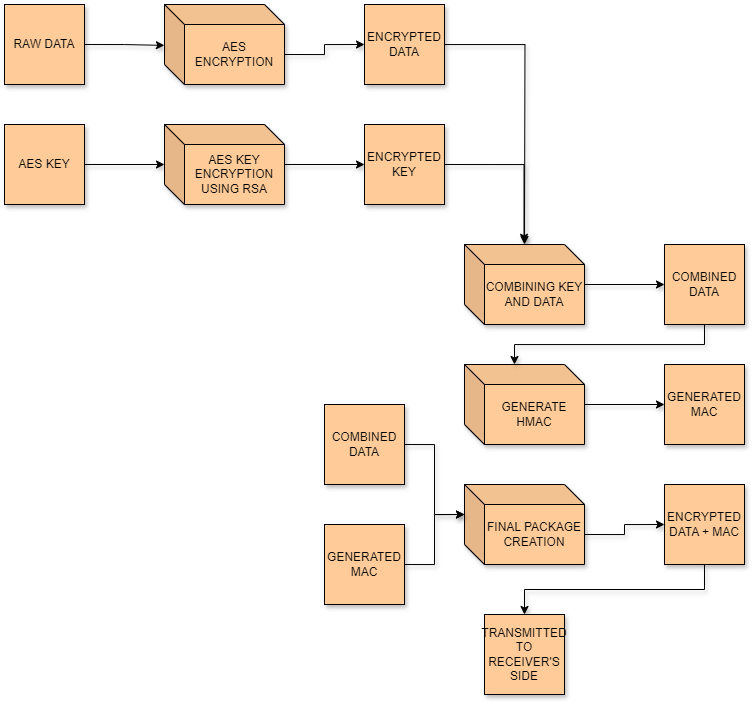
By following these steps, you can leverage VAULT's robust security features to manage your finances with complete peace of mind. VAULT goes beyond standard encryption protocols, offering a multi-layered approach to data security with our innovative TriSecurEncrypt algorithm at its core.

Download VAULT today and experience the future of secure financial transactions!

**4.2 Algorithm Implementation**

Here's a detailed flowchart explaining the TriSecurEncrypt encryption and decryption process using the algorithm described:

**Sender Side:**



1. Encrypt Data with AES

- Original data is encrypted using the AES algorithm with a shared secret key.

2. Encrypt AES Key with RSA

- The AES secret key is encrypted using RSA with the receiver's public key.

3. Combine Encrypted Data and AES Key

- The encrypted data and the encrypted AES key are combined.

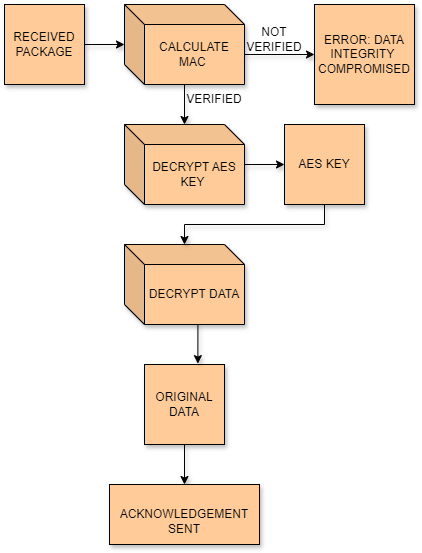
4. Generate HMAC

- HMAC with a secret key is applied to the combined data to generate a Message Authentication Code (MAC).

5. Create Final Encrypted Data Package

- The final encrypted data package consists of the combined encrypted data and the MAC.

**Receiver Side:**



1. Receive Encrypted Data Package

- Receiver obtains the encrypted data package.

2. Verify MAC

- Receiver calculates HMAC using the received data and compares it with the MAC.

3. Decrypt AES Key with RSA

- The RSA private key is used to decrypt the AES key.

4. Decrypt Data with AES

- AES key is used to decrypt the encrypted data.

**Working of the Proposed Algorithm:**

1. **AES Encryption**: The original data is encrypted using the Advanced Encryption Standard (AES) algorithm with a shared secret key. AES is a symmetric key encryption algorithm widely used for securing sensitive data.

2**. RSA Encryption:** The AES secret key is encrypted using the RSA algorithm with the receiver's public key. RSA is an asymmetric encryption algorithm where the public key is used for encryption, and the private key is used for decryption. This step ensures that only the intended recipient, possessing the corresponding private key, can decrypt the AES key.

3. **Combination:** The encrypted data and the encrypted AES key are combined into a single package. This step prepares the data for transmission.

4. **HMAC Generation**: HMAC (Hash-based Message Authentication Code) is generated by applying a cryptographic hash function to the combined data using a secret key. This MAC serves as a fingerprint to verify the integrity of the data during transmission.

5. Final Package Creation: The final encrypted data package consists of the combined encrypted data and the MAC. This package is ready for transmission to the recipient.

On the receiver side, the steps are essentially the reverse of the sender side. The receiver first verifies the integrity of the data by checking the MAC. Then, it decrypts the AES key using its private RSA key and finally decrypts the original data using the AES key. This ensures secure and authenticated communication between the sender and the receiver.

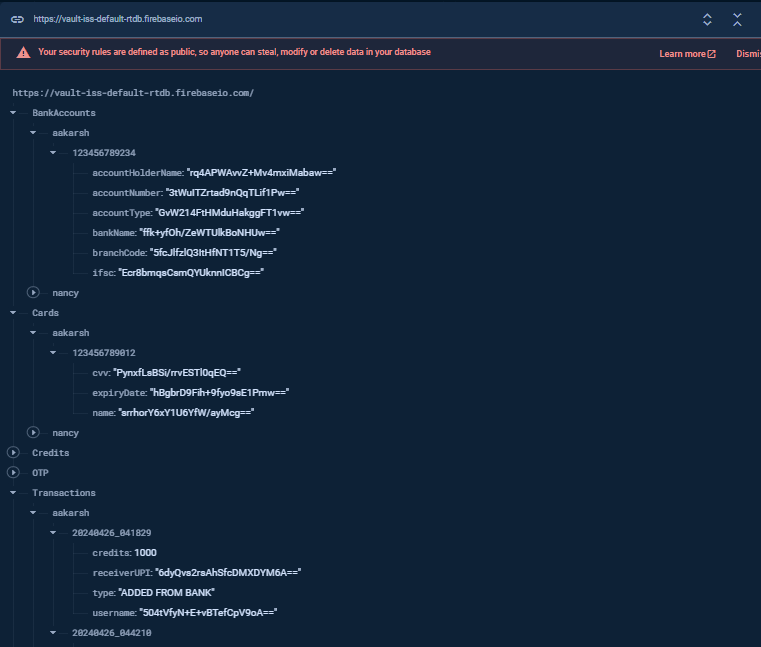
**Chapter 5**

**Results**

**5.1 Results**

The data storage mechanism employed by VAULT incorporates advanced encryption techniques to ensure the utmost security and privacy of user information collected during the Know Your Customer (KYC) process. Our proposed algorithm, TriSecurEncrypt, stands at the forefront of data protection, employing a sophisticated blend of encryption methods to fortify confidentiality, secure key exchange, and ensure data integrity.

TriSecurEncrypt integrates the robustness of AES (Advanced Encryption Standard), a symmetric encryption algorithm renowned for its strength in safeguarding data confidentiality. By leveraging AES, sensitive text data undergoes encryption, rendering it inaccessible to unauthorized entities, thereby thwarting any potential breaches or unauthorized access attempts.





**Chapter 6**

**Conclusion and Future Work**

**6.1 Conclusion**

VAULT carves a unique path in the realm of secure financial transactions. By prioritizing robust user authentication with three-factor methods and innovative encryption techniques, including the novel TriSecurEncrypt algorithm, VAULT aims to establish a new paradigm for data security.

This project leverages a powerful combination of technologies. The secure foundation is built using Android Studio with Java, XML, and Firebase's suite of services like Realtime Database, Realtime Storage, Authentication, and Firestore. Additionally, the project incorporates the latest Android X libraries and industry-standard security practices.

VAULT's commitment to security extends beyond its core functionalities. The app adheres to best practices like regular security audits, secure coding practices, data minimization, and secure communication channels. This comprehensive approach ensures ongoing protection against potential vulnerabilities.

But security doesn't have to come at the expense of usability. VAULT's user interface is designed with simplicity and accessibility in mind, providing a seamless user experience for managing finances. Real-time feedback, clear instructions, and well-labeled functionalities ensure users can navigate the app with ease.

Looking ahead, VAULT's potential for growth is vast. The secure architecture can be adapted to integrate with various financial institutions and services. Continuous improvement through regular updates and security assessments will ensure VAULT remains at the forefront of secure and user-friendly financial transactions in the digital age.

**6.2 Future Work**

VAULT's focus on robust security positions it as a valuable tool for secure financial transactions. However, there's always room for advancement. This section explores potential future endeavors to enhance VAULT's capabilities and contribute positively to society.

**1. Integration with Blockchain Technology:**

* Explore the integration of blockchain technology to create a decentralized and tamper-proof record of transactions. This can further enhance security and transparency for users.
* Develop a secure and user-friendly interface for interacting with blockchain features within the VAULT app.

**2. Expansion of Financial Services:**

* Implement functionalities for features like bill splitting, micro-investments, and peer-to-peer (P2P) money transfers within VAULT. This can create a more comprehensive financial management platform for users.
* Integrate with existing investment platforms or create a secure investment module within VAULT, allowing users to manage their investments alongside their daily transactions.

**3. Social Impact Initiatives:**

* Partner with charitable organizations to enable secure and transparent donations directly through VAULT. This can leverage the app's strong security features to encourage user trust and participation in charitable giving.
* Develop features for micro-lending or microfinancing initiatives within VAULT, empowering users to contribute to financial inclusion and social development efforts.

**4. Artificial Intelligence (AI) and Machine Learning (ML) Integration:**

* Implement AI and ML algorithms to analyze user spending habits and generate personalized financial insights and budgeting recommendations. This can empower users to make informed financial decisions.
* Explore the potential for AI-powered fraud detection within VAULT, further safeguarding user accounts and transactions from malicious activities.

**5. Accessibility Features:**

* Enhance VAULT's accessibility features to cater to users with visual impairments or other disabilities. This can include features like voice commands, screen reader compatibility, and adjustable font sizes.
* Develop functionalities for users in geographically diverse regions by incorporating multi-language support and adapting the app to different cultural contexts.

**Impact on Mankind**

By focusing on these future endeavors, VAULT can contribute significantly to society in several ways:

* **Financial Empowerment:** VAULT's secure and user-friendly platform can empower individuals to manage their finances effectively, fostering financial inclusion and economic well-being.
* **Increased Security and Transparency:** Blockchain integration and robust encryption algorithms can significantly enhance trust and transparency in financial transactions, protecting users from cyber threats and fraud.
* **Social Responsibility:** Enabling secure donations and micro-financing initiatives can encourage users to contribute to social causes and promote financial inclusion for underbanked populations.
* **Financial Literacy:** AI-powered insights and budgeting tools within VAULT can empower users to make informed financial decisions, leading to greater financial stability.
* **Accessibility and Inclusivity:** By prioritizing accessibility features and multi-language support, VAULT can cater to a broader user base, fostering financial inclusion on a global scale.

In conclusion, VAULT's proposed future work focuses on expanding its functionalities beyond secure transactions, aiming to empower users, enhance financial literacy, and contribute positively to society. By leveraging cutting-edge technologies and prioritizing accessibility, VAULT can become a valuable tool for financial security, social good, and overall well-being.