Group 7

Aaryan Darad	21110001
Bhavik Patel	22110047
Chiragkumar Patel	22110183
Gaurav Budhwani	22110085
Hitesh Kumar	22110098
Pranav Patil	22110199
Ruchit Jagodara	22110102

CS431 - Design Document

4th September

OVERVIEW

This project involves creating a secure communication system between an ATM client and a bank server, allowing users to perform basic banking transactions like deposits, withdrawals, balance checks, deleting an account, and some extra features like money transfers between two different accounts. The system ensures only authorized users can access and modify their account information.

LANGUAGES/FRAMEWORKS

1. Programming languages C++: Implementing the core functionality of the ATM and Bank programs due to its low-level access to system resources and efficient handling of TCP sockets.
2. POSIX Sockets: These are used to implement the TCP communication between the ATM and Bank programs.
3. JSON Library: To handle JSON encoding/decoding in ATM and Bank programs.

COMPONENTS

ATM Client (ATM):

- **Transaction Module:** Handles user interactions and performs account creation, deposits, withdrawals, and balance inquiries.
- **Communication Module:** Manages secure communication with the Bank server, ensuring that all data exchanged is encrypted and authenticated.
- **Error Handling Module:** Manages the exit codes and ensures that the ATM exits gracefully on errors.

Bank Server (Bank):

- **Account Management Module:** Keeps track of customer accounts, including balances and transaction history.
- **Communication Module:** Handles incoming requests from ATM clients, validates them, and processes the transactions.
- **Security Module:** Authenticates incoming requests using the shared auth file and ensures only legitimate clients can interact with the server.
- **Inter-Bank Communication Module:** Handles bank communication to ensure secure transactions using inter-bank authentication files.

FUNCTIONALITIES & MODULES

1. **Account Creation/Deletion:**
    - The ATM client sends an account creation/deletion request to the Bank server, specifying the account name and initial balance in case of creation.
    - The Bank server validates the request, creates/deletes the account, and returns a confirmation to the ATM.
    - The ATM creates a card file associated with the new account in case of creating an account and invalidates the existing card file in case of deletion.
2. **Deposit/Withdrawal:**
    - The ATM client sends a request to deposit or withdraw a specific amount.
    - The Bank server verifies the account and card file, updates the balance, and returns a confirmation.
3. **Balance Inquiry:**
    - The ATM client requests the current balance for a specific account.
    - The Bank server verifies the request and responds with the account balance.
4. **Account Management:**
    - The Bank server manages the customer accounts, including balance tracking and transaction logging.
5. **Communication Handling:**
    - The Bank Server manages incoming requests from the ATM Client and ensures secure communication via a secure channel unavailable to others.
6. **Inter-Bank Fund Transfer:**
    - The Bank Server communicates securely with the target bank's server over a designated port to transfer funds and update account balances.
    - This functionality enables the transfer of funds between accounts at different banks.

SECURITY PROPERTIES

Authentication:

- ATM and bank must validate each other using the auth file to ensure mutual trust before processing transactions.
- Two banks must validate each other when money transfers from the account in one bank to the account of another.
- The card file must be securely generated and stored, acting as a customer’s "PIN code."

Data Integrity:

- All communications between the ATM and the bank and between two banks must be transmitted over a secure channel to prevent tampering by a "man-in-the-middle" attacker.
- Transaction requests and responses must be checked for integrity, ensuring they haven’t been altered in transit.

Atomicity of Transactions:

- The bank server must ensure that each transaction is atomic, meaning the account balance must remain consistent despite multiple concurrent transactions.

Error Handling:

- The system must detect and adequately handle protocol errors, timeouts, and unauthorized access attempts with appropriate exit codes and rollback mechanisms.

WORKING

When a user initiates a transaction (e.g., deposit, withdrawal) through the ATM client, the client first reads the user's card file and uses it to authenticate with the bank server. The ATM and the bank use a shared authentication file to establish a secure communication channel. The ATM then sends the transaction request (such as deposit or withdrawal) to the bank server, which processes the request. The bank checks the user's account details, updates the balance as needed (otherwise, it will give an appropriate error message), and sends a JSON-encoded response back to the ATM, confirming the transaction. The ATM client displays the result to the user, and the communication ends. Throughout the process, the system ensures that all data is securely transmitted and only the authorized user can modify their account.

WORK DIVISION

Hitesh Kumar: Responsible for Secure Communication between ATM Client and Bank Server. Hitesh will help with the different functionalities of the Bank and ATM. He will also assist in testing the system under various attacks.

Ruchit Jagodara: Create a structured flow for the multi-bank system and assist in implementing the bank module and Security Module.

Chirag Patel: Responsible for implementing the Error Handling Module in the ATM and Bank programs, ensuring that errors are managed gracefully and that appropriate exit codes are returned. Chirag will also assist with testing the system for various edge cases.

Aaryan Darad: Focus on the Transaction Module of the ATM client, handling user interactions for account creation, deposits, withdrawals, and balance inquiries. Aaryan will ensure that all transactions are correctly processed and logged.

Bhavik Patel: Tasked with developing the Security Module within the Bank server. This includes authenticating incoming requests and ensuring secure communication between the ATM and Bank using the auth file.

Gaurav Budhwani: Responsible for the Account Management Module in the Bank server, including balance tracking and transaction logging. Gaurav will also assist with implementing the inter-bank fund transfer functionality.

Pranav Patil: Work on the Communication Module for the ATM and Bank programs. Pranav will ensure that secure communication channels are established and maintained and will handle the TCP socket programming using POSIX standards.

ADDITIONAL FEATURES

***Disclaimer:** These features will be implemented if time permits, and they are not guaranteed to be present at the end of the project. But an honest effort will be made to implement them.

1. **Inter Account Money Transfer:** The user can transfer money from his account to another. For this, the user will require the account name of the receiving account.
2. **Account Deletion:** The user can remove his account from the bank, and all his data will be removed from the bank database.
3. **Multiple Banks:** There will be multiple banks. A user can create different accounts in different banks. Interbank fund transfers will also be possible.