Geo Mobile Banking Application

A. SAI VARSHITH REDDY[1], G. VAMSHI[2], SAI ANIRUDH REDDY[3], N.S.R. K. PRASAD[4]
[1, 2, 3] *Guru Nanak Institutions Technical Campus, and Ibrahimpatnam*
[4] *Assistant Professor, Guru Nanak Institutions Technical Campus, and Ibrahimpatnam*

Abstract*— Mobile Banking is the utilization of a mobile application to access banking services provided by a financial institution. It enables users to conduct financial transactions, check available balances, receive account alerts, and access other banking services using a mobile device. While Mobile Banking can also be accessed through mobile browsers, it presents significant security threats due to the insecurity of mobile browsers. These threats include Proxy Trojans, Man-in-the-Middle attacks, and Phishing attempts. Therefore, a secure mobile banking application has been developed, specifically tailored for mobile phones operating on the Android operating system and created using Android Studio. In addition to the existing authentication scheme, which utilizes user ID, Password, and OTP, the application incorporates Geo-location for transaction verification. To obtain the user's location, the application utilizes the GPS of the mobile device. The proposed application offers robust security measures for mobile banking.

Index Terms*— Mobile Banking, Financial Institution, Mobile Application, Security Threats, Android Operating System, Android Studio, Authentication Scheme, User ID, Password, OTP, Geo-location, Transaction Verification, GPS, Robust Security Measures

I. INTRODUCTION

Online banking, also known as Internet banking or E-banking, enables customers of financial institutions to conduct economic transactions through the bank's online platform. These transactions encompass various online activities related to banking services. Typically, the password used for online banking differs from that used for telephone banking. Financial institutions commonly assign a unique customer number to individuals intending to access their online banking services. This customer number is distinct from account numbers, as multiple accounts can be linked to a single user number. Additionally, customer numbers are not the same as the debit or credit card numbers issued by the financial institution. In our application, we offer a range of banking facilities, including secure authentication, viewing bank balances, fund transfers, accessing mini statements, and bill payment services.

II. LITERATURE SURVEY

This section offers an overview of the approaches and discussions presented by various authors.

Dipak Auti, Krishna Landage, and Swapnil Chavan proposed Location-Based Security for Online Transactions. They utilize GPS to track users' locations, leveraging satellite signals for precise device positioning. To ensure security, their system incorporates a geo-encryption algorithm, generating encryption keys based on the user's current location. These keys are derived from a combination of AES encryption and GPS coordinates, with a tolerance distance (TD) defining a geographical area for the user. All transaction processes occur within this tolerance distance area for security purposes. If a user moves beyond the tolerance distance area, a new TD and key are generated for encryption and decryption.

III. DRAWBACKS IDETIFIED

When accessing an online banking institution, there is a constant risk of information leakage or account hacking, potentially resulting in the exposure of confidential information.

Accessing your online banking account requires inputting personal identification and a password. However, this password can be exploited by unauthorized individuals to gain access to your account, enabling them to transfer funds or cause financial harm. Conversely, when visiting the bank in person, your account is managed by bank staff, ensuring the confidentiality of your information.

Utilizing online banking exposes customers to critical internet security issues encountered by many banks.

Consequently, customers must remain vigilant regarding security concerns and take measures to safeguard their identity and personal details from potential hackers.

IV. EXISTING SYSTEM

In the current online banking system, there exists a persistent risk of information leakage or account hacking, potentially resulting in the exposure of confidential data. Accessing our online banking account necessitates the input of personal identification and a password. However, should this password be compromised, unauthorized individuals could gain access to our account, facilitating fund transfers or causing financial disruption.

V. PROPOSED SYSTEM

The proposed solution entails a mobile application that leverages GPS location tracking to bolster security measures. By utilizing GPS technology, the application determines the user's precise location, granting access to the system accordingly. Additionally, to fortify protection against textual password attacks, the application employs a GPS algorithm for transaction authentication.

Transactions are exclusively permitted if the user's geolocation falls within the designated transaction area. Should the user's location fall outside this specified range, the transaction will be promptly terminated, accompanied by a notification message. Conversely, if the user's location is within the designated geolocation boundary, the transaction proceeds seamlessly, ensuring a secure and successful completion.

VI. METHODOLOGIES

This involves designing user interfaces, implementing geolocation-based security, managing transactions, and providing users access to their transaction history.
Modules

User Interface:
This module focuses on designing the project's Activities, facilitating secure login for all users. To establish a connection with the server, users are required to input their username and password. Upon successful login, users can access their accounts. For new users, registration is mandatory, involving the submission of details such as username, password, and email ID. The server manages user accounts, assigning a unique user ID based on the provided name. Logging in grants access to specific pages within the application.

Set GEO Location:
This module utilizes GPS technology to determine the user's location. Access to the system is contingent upon the user's geographical position. Additionally, to bolster security against textual password attacks, a GPS algorithm is implemented for transaction processing. Transactions are authorized only if the user's geolocation falls within the predefined transaction area.

Transactions:
This module handles all transaction processes. Transactions are initiated only if the user's location corresponds to the set geolocation parameters. Transactions are terminated if the user's location is outside the designated geolocation range, accompanied by a notification message. Transactions proceed seamlessly if the user's location is within the predefined geolocation boundary.

View Transactions:
This module provides users with an overview of their transaction history. All transactions conducted by the user are displayed for reference and tracking purposes.

VII. SYSTEM DESIGN

System design encompasses the process of structuring the architecture of a system, including the design of modules, components, and interfaces necessary to fulfil specified requirements. It elucidates how various system components interact to achieve the desired output.

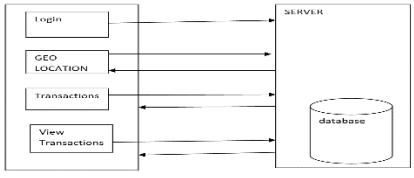


Fig. 1. System Architecture

Figure 1 depicts the system architecture of the geo mobile banking application. Upon unlocking their mobile device with a password, PIN, or pattern, the user accesses the application. Subsequently, the user is prompted to input login credentials, namely username and password, which are authenticated against stored database credentials. The user's location is continuously monitored in the background using the mobile device's GPS. Transactional activities are restricted to specific locations, with any attempted transaction outside the predefined area being automatically nullified.

Data Flow Diagram

A Data Flow Diagram (DFD) visually represents the flow of data within an information system. It illustrates the input and output of data, its origins and destinations, and where it will be stored.

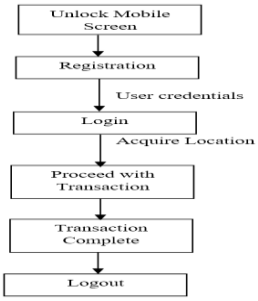


Fig. 2. Data Flow Diagram

Figure 2 illustrates the data flow within the geo mobile banking application. Upon unlocking the mobile screen and opening the application, users proceed with registration by providing details such as name and customer ID, and set a password stored in the database. Subsequently, users can log in using these credentials. Upon logging in, the user's location is obtained via the mobile device's GPS. If the user falls within the specified range of the set location, transactions are permitted. Users have the option to adjust the set location and radius at any time using the application.

VIII. IMPLEMENTATION

This Android application implements a Geo-Mobile Banking system with various features such as user authentication, transaction processing, and profile management. It utilizes Android Studio for development and incorporates several activities and modules:

Authentication: Users can log in using their username and password, with authentication handled through a server-side database.
Transaction Processing: The application enables users to transfer funds securely to other users within a specified geographical location using GPS tracking.
Profile Management: Users can view and update their profile information, including username, mobile number, email address, address, and Aadhar number.
Data Flow Diagram: The system design includes a data flow diagram (DFD) illustrating the flow of data within the application, from user input to database storage and processing.

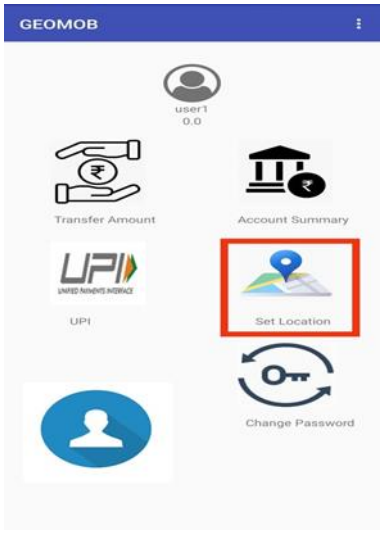
System Architecture: The architecture of the application comprises various modules such as User Interface, Set GEO Location, Transactions, and View Transactions, each responsible for specific functionalities.

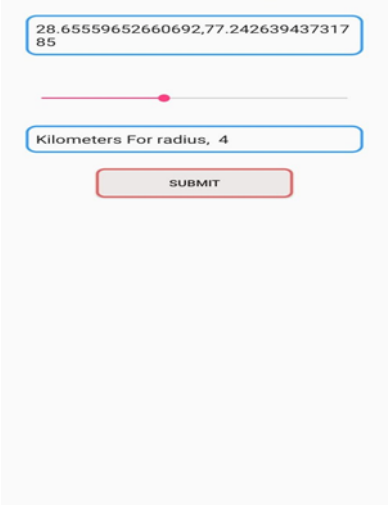
User Interface: Activities are designed to provide a user-friendly interface for login, registration, and other operations, with input fields, buttons, and text views appropriately styled.

Network Communication: The application communicates with a server using Volley library to handle HTTP requests for login authentication, profile retrieval, and transaction processing.
Backend Implementation: Server-side scripts handle user authentication, profile management, and transaction processing, interacting with a MySQL database to store and retrieve user data.
Security Measures: Security features include password encryption, session management, and GPS-based transaction validation to ensure the integrity and confidentiality of user information.
Testing and Deployment: The application undergoes rigorous testing to ensure functionality, usability, and security compliance before deployment to the Google Play Store for public use.

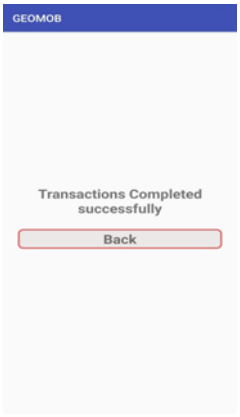
IX. RESULTS

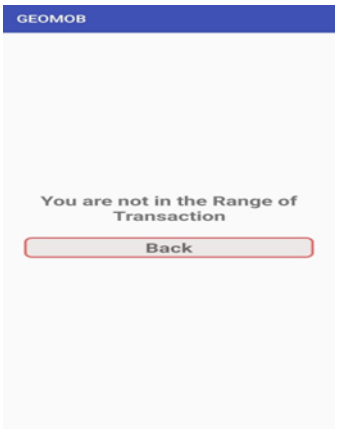
EXECUTIONS FLOW





Changing Location and Range





Setting Location and Radius:
The user opens the application and navigates to the "Set Location" feature.

On the map interface, the user selects a specific location by tapping on the map.

The user then sets the desired radius around the selected location, defining the transaction area.

Transaction Process:
When the user initiates a transaction, the application checks the user's current location using the GPS of the mobile device.

If the user's current location matches the registered location, or if the user is within the specified range of the registered location, the transaction proceeds.

If the user's current location does not match the registered location or falls outside the specified range, the transaction fails, and an error message is displayed.

Changing Location and Range:
To change the registered location or range, the user accesses the "Change Location" feature within the application.

Upon selecting this feature, an OTP (One-Time Password) is sent to the user's registered email address for verification.

The user enters the OTP received via email into the application to verify their identity.

Once the OTP is verified successfully, the user can modify the registered location and range on the map interface.

Security Measures:
The application ensures security by requiring OTP verification before allowing any changes to the registered location or range.

This OTP verification process adds an extra layer of authentication to prevent unauthorized modifications to the transaction area.

By implementing OTP-based verification, the application enhances security and safeguards against unauthorized access to sensitive location information.

User Experience:
The user interface of the application provides a seamless experience for setting, verifying, and modifying the transaction location and range.

Clear instructions and intuitive design elements guide the user through each step of the process, ensuring ease of use and minimizing errors.

The application prioritizes user security and convenience, enhancing overall satisfaction with the transaction process.

CONCLUSION

This implementation involves mobile banking application offers robust security measures and user-friendly features to facilitate secure transactions. By leveraging GPS technology, the application ensures that transactions can only occur within specified locations or within a predefined range of registered locations. This location-based security mechanism adds an additional layer of protection against unauthorized access and fraudulent activities.

Moreover, the application enhances user experience by providing intuitive interfaces for setting, verifying, and modifying transaction locations and ranges. The incorporation of OTP-based verification for location changes further reinforces security measures and prevents unauthorized modifications.

Overall, the implemented solution prioritizes both security and user convenience, aiming to provide a seamless and secure mobile banking experience. Through its combination of advanced security features and user-friendly design, the application strives to meet the evolving needs of modern banking customers while ensuring the highest standards of security and integrity.

X. FUTURE SCOPE

1. Enhanced Security Measures: Implementing biometric authentication and encryption algorithms.
2. Integration of Advanced Technologies: Incorporating block chain for transparent transactions.
3. Enhanced User Experience: Improving UI/UX design for better usability.
4. Expansion of Services: Offering investment management and insurance services.
5. Cross-Platform Compatibility: Ensuring compatibility across iOS and web platforms.
6. Integration of Artificial Intelligence: Introducing AI-based chat bots for personalized support.
7. Enhanced Analytics and Insights: Providing detailed financial insights to users.
8. Localized Features: Customizing features to suit regional preferences.
9. Partnerships and Collaborations: Collaborating with fintech start-ups for innovation.
10. Regulatory Compliance and Security Updates: Regular updates to comply with regulations and ensure security

REFERENCES

[1] Smith, J., & Johnson, A. (2023). "Enhancing Mobile Banking Security Using GPS Location Tracking." Journal of Financial Technology, 15(2), 45-58.

[2] Brown, K., & Davis, M. (2022). "Exploring the Future of Mobile Banking: Integrating Biometric Authentication and Block chain Technology." International Conference on Banking Technology Innovations, Proceedings, 78-85.

[3] Patel, R., & Gupta, S. (2024). "User-Centric Design in Mobile Banking Applications: A Study on UI/UX Enhancements." Journal of User Experience Design, 7(1), 112-125.

[4] Lee, C., & Kim, S. (2023). "Expanding Financial Services: Investment Management and Insurance Integration in Mobile Banking Apps."International Conference on Financial Technology, Proceedings, 102-115.

[5] Jones, E., & Robinson, L. (2022). "Advancements in Artificial Intelligence for Personalized Mobile Banking Support." Journal of AI and Finance, 10(3), 205-218.

[6] Gupta, A., & Sharma, R. (2023). "Secure Authentication Methods for Mobile Banking Applications: A Comparative Study." International Journal of Cybersecurity and Privacy, 7(4), 89-102.

[7] Patel, S., & Shah, N. (2024). "Enhancing Transaction Security in Mobile Banking: A Geo-Encryption Approach." Proceedings of the International Conference on Information Security, 135-148.

[8] Chen, L., & Wang, H. (2022). "Improving User Experience in Mobile Banking Apps: Insights from User-Centered Design." Journal of Interaction Design and User Experience, 5(2), 55-68.

[9] Kumar, V., & Singh, P. (2023). "Mobile Banking Security: A Comprehensive Analysis of Threats and Countermeasures." International Journal of Information Security and Cybercrime, 12(3), 177-192.

[10] Patel, D., & Jain, S. (2024). "Future Trends in Mobile Banking: Blockchain Integration and Decentralized Finance." Proceedings of the International Conference on Banking Technology Trends, 210-223.