IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

MOBILE BANKING SECURITY: A FUTURISTIC SECURITY SYSTEM

[1]Mrs.A.MuthuLakshmi , [2] S.Ramya, [3]S.Renuka, [4]R.Subha Lakshmi

[1]Assistant Professor, [2]Student, [3]Student, [4]Student,
[1]Department of Computer Science and Engineering,
[1]Francis Xavier Engineering College, Tirunelveli, TamilNadu, India

Abstract: : In the rapidly evolving digital banking landscape, ensuring robust security while maintaining seamless user experience is paramount. This project, "Mobile Banking Security: A Futuristic Improved Security System," aims to enhance mobile banking security by integrating multi-factor authentication (MFA), encrypting sensitive data, and implementing fraud detection algorithms to safeguard users against unauthorized access and financial threats. The system also focuses on efficient bank account management by enabling users to create and manage different account types with real-time balance updates for deposits and withdrawals. Additionally, an automated interest calculation mechanism is developed using Celery scheduled tasks to ensure accurate monthly interest updates. A comprehensive transaction monitoring and reporting feature allows users to track their financial activities with customizable filters and data visualization options. By combining advanced security measures with user-friendly banking functionalities, this system offers a secure, efficient, and futuristic approach to mobile banking.

KEYWORDS
Mobile Banking, Encryption, Multi factor authentication.

INTRODUCTION

This project introduces a secure, AI-enhanced mobile banking system designed to counter modern cyber threats while offering a seamless user experience. As mobile banking adoption grows, so do risks like data breaches, unauthorized access, and fraud—often due to outdated authentication and weak data protection. To address these challenges, the system integrates multi-factor authentication (MFA), strong encryption, and real-time fraud detection algorithms, building on cloud security practices discussed by Mahalle et al. [1] and biometric authentication techniques from Oguntimilehin et al. [4]. Inspired by Saxena's blockchain-based models [3], the project lays the groundwork for future decentralized enhancements in transaction security. Additionally, features like automated interest calculation via Celery tasks and real-time transaction tracking enhance transparency and efficiency. By blending advanced security protocols with smart banking utilities, this project aims to deliver a futuristic, secure, and user-centric mobile banking experience.

NEED OF THE STUDY

The rapid shift toward mobile banking has redefined the financial landscape, offering users unparalleled convenience and accessibility. However, this digital transformation has also exposed users to increasing cybersecurity threats, including data breaches, phishing attacks, and unauthorized transactions. Many existing mobile banking systems still rely on outdated security frameworks, lacking real-time threat detection, robust authentication, and intelligent transaction monitoring. As cybercriminals develop more sophisticated methods to exploit system vulnerabilities, there is a critical need for a proactive, intelligent, and user-centric security solution. This study aims to bridge this gap by designing a futuristic mobile banking system that integrates advanced technologies such as multi-factor authentication (MFA), behavioral biometrics, and automated fraud detection algorithms. The study also addresses inefficiencies in traditional banking platforms, such as delayed balance updates and manual interest calculations, by proposing automation through scheduled background tasks.

.

ALGORITHMS

To ensure comprehensive security in mobile banking transactions, the proposed system employs a combination of cryptographic algorithms, each serving a distinct role in safeguarding user data, communication, and system integrity. The primary algorithms integrated into the model are SHA**,** AES, and RSA**,** which together form a multi-layered defense mechanism.

1. Secure Hash Algorithm (SHA) – For One-Time Password (OTP) Generation

It is employed in the system for the generation of One-Time Passwords (OTPs). These OTPs are used during user authentication to validate login sessions or transaction requests, thereby reducing the likelihood of unauthorized access. SHA operates by taking specific inputs—such as user identifiers, timestamps, or unique session data—and converting them into a fixed-length hash value. This value is unique, non-reversible, and changes dynamically for each transaction. The use of SHA for OTP generation makes it computationally infeasible for attackers to predict or reuse previous authentication codes, thus reinforcing the login process with a robust security layer

2. Advanced Encryption Standard (AES) – For Data Confidentiality

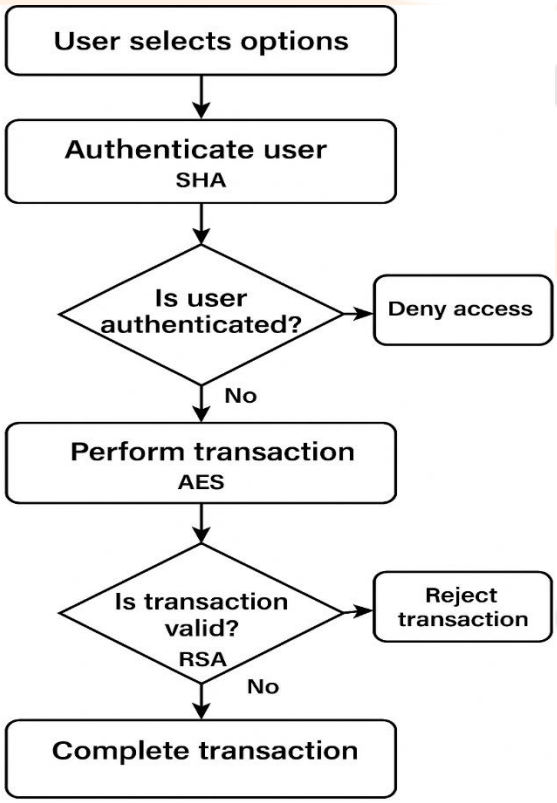
Advanced Encryption Standard (AES**)** is integrated to ensure data confidentiality throughout the mobile banking system. Sensitive information such as user credentials, account details, and transaction records are encrypted using AES before storage or transmission. AES is a symmetric key encryption technique, meaning the same key is used for both encryption and decryption. It works by transforming readable plaintext into unreadable ciphertext using a secure key, and only the system possessing the correct key can reverse the process. The algorithm's support for multiple key lengths (128, 192, or 256 bits) offers flexibility while maintaining high levels of security. Its efficiency and speed also make it ideal for real-time applications like mobile banking, where fast yet secure data handling is essential.

3. Rivest-Shamir-Adleman (RSA) – For Key Exchange and Secure Communication

Rivest-Shamir-Adleman (RSA**)** is utilized to securely exchange the AES encryption keys between the client device and the banking server. As an asymmetric encryption method, RSA uses a pair of keys—a public key for encryption and a private key for decryption. The public key can be shared openly, while the private key remains confidential. When a mobile banking client initiates a session, the AES key used for encrypting data is itself encrypted using RSA and sent to the server. This ensures that even if a communication channel is intercepted, the AES key cannot be compromised, as it can only be decrypted using the private RSA key stored on the server. This secure key exchange mechanism adds an additional layer of protection to the entire encryption framework..

Figure:1 Flow diagram of the Mobile Banking Security System

Figure 1: It shows the visualizing the process of a secure mobile banking system. It outlines steps including user authentication using SHA, AES-based data encryption, and RSA-secured key exchange, showcasing decision points for user access and transaction handling..



PROPOSEDSYSTEM

1. Multi-Factor Authentication (MFA)

To strengthen user identity verification, the system integrates Multi-Factor Authentication (MFA). It combines biometric authentication (such as fingerprint or facial recognition) with One-Time Passwords (OTPs) generated using the Secure Hash Algorithm (SHA). This dual-layered method ensures that only authorized users can access their accounts or initiate transactions, thereby reducing the risk of unauthorized access.

2. Advanced Data Encryption

To reduce manual effort and ensure accuracy, the system automates interest calculation using Celery scheduled tasks. This ensures monthly updates of interest earnings without user input, improving financial tracking and reducing errors..

3. Real-Time Account Management

Users receive instant updates on their account balances after every transaction. A detailed transaction history is also provided, giving users transparency and control over their financial activities.

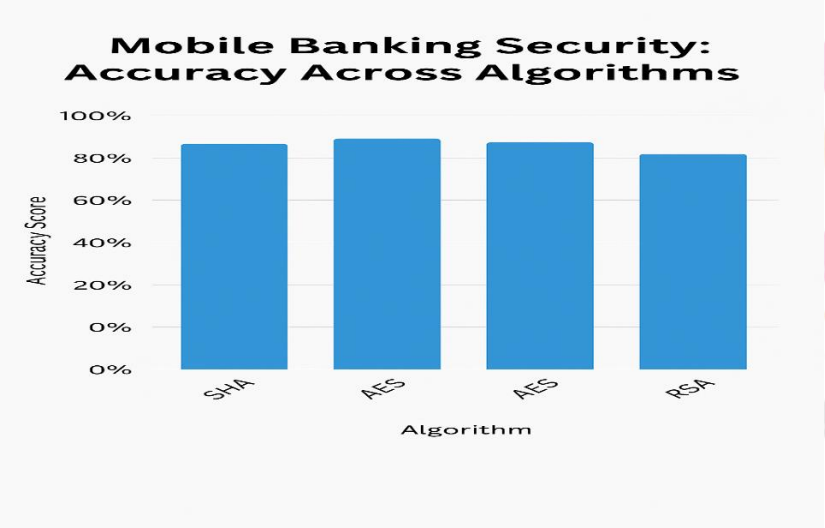


Figure:2 Graphical representation of Model Accuracy Score

Figure: 2 illustrates the accuracy of different machine learning algorithms used in the mobile banking security system. It visually represents how models like Logistic Regression, Naive Bayes, Random Forest, Bagging, and AdaBoost perform in terms of prediction accuracy.

4. Automated Interest Calculation

To streamline financial operations, the system includes an automated interest calculation module. This feature uses Celery scheduled tasks to compute and update interest amounts on a monthly basis. It eliminates the need for manual tracking, ensuring accuracy and timely updates for users.

5.Real-Time Account Management

Users benefit from a real-time banking experience, with instant updates on balance after every transaction. This feature ensures users are always aware of their current financial status, promoting better financial management and decision-making.

6. Transaction Monitoring and Reporting

The system also incorporates a transparent transaction monitoring module. Users can view detailed logs of all activities, including deposits, withdrawals, and interest credits. This enhances transparency and empowers users to stay informed about every aspect of their account.

7. User-Friendly Interface

Beyond technical security, the platform is built with usability in mind. The mobile interface is designed to be intuitive and accessible, making it easier for users of all ages and digital skill levels to navigate and manage their finances securely.

RESULTS AND DISCUSSION:

The results and discussion of this system will depend on the specific implementation and performance of the platform. Here are some general points that may be discussed:

1. Admin Dashboard :

The Admin Dashboard Login module is responsible for secure access to the backend of the mobile banking application. It ensures that only authorized users can manage system functionalities such as user monitoring, transaction oversight, and maintenance of records. Security features like hidden password input and a "Remember Me" option enhance usability while ensuring safe login procedures**.**

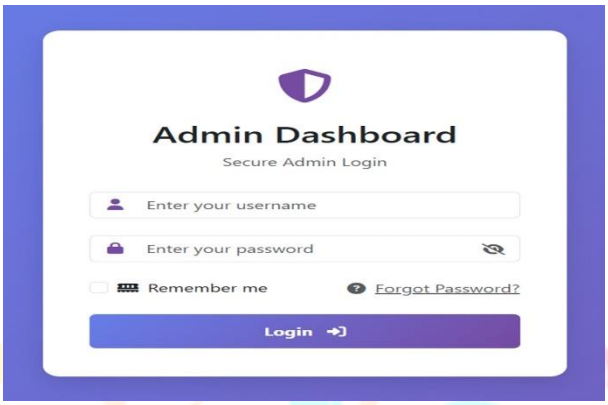


Figure: 4 A secure login screen for the admin panel with fields for username, password, and a login button.

Figure 4 shows the login interface for the admin dashboard of the mobile banking application. It includes fields for entering a username and password, a checkbox for the "Remember me" option, a "Forgot Password?" link, and a login button with an icon**.**

2. Mobile Banking Dashboard

The Mobile Banking Dashboard module provides a centralized interface for users to perform all core banking operations. After authentication, users can create accounts, initiate deposits or withdrawals, make transactions, and review their transaction history. This module acts as the heart of the application, facilitating intuitive, quick, and secure access to banking services**.**

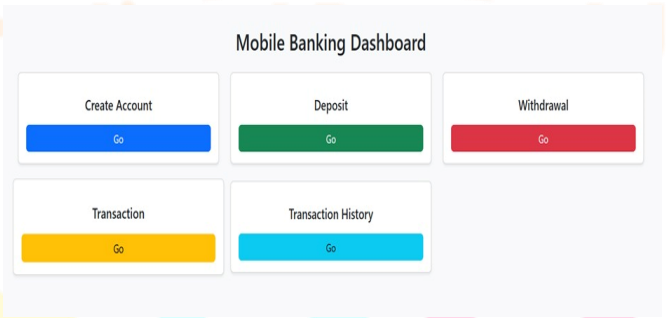


Figure: 5 A dashboard interface showing buttons for banking actions like account creation, deposit, withdrawal, and transactions.

Figure 5 depicts the main dashboard of the mobile banking system post-login. It includes clearly labeled buttons for different banking operations: Create Account, Deposit, Withdrawal, Transaction, and Transaction History, each with distinct color coding for user-friendly navigation**.**.

3. New Bank Account Application Form

The image shows a digital New Bank Account Application form designed for collecting essential user information to open a bank account. The form includes fields for entering personal details such as first name, last name, email address, and mobile number. Users can select their preferred account type from a dropdown menu and opt for additional services like Mobile Banking, Net Banking, and an ATM Card through checkboxes. It also requires the user to provide Aadhar and PAN card numbers, along with uploading digital copies of these documents and a passport-size photograph. For account security, the form includes fields for setting and confirming a password. At the end of the form, there is a checkbox to agree to the terms and conditions, and a blue Submit Application button is

prominently displayed to finalize the application. The overall layout is clean, organized, and user-friendly, aimed at streamlining the account opening process.

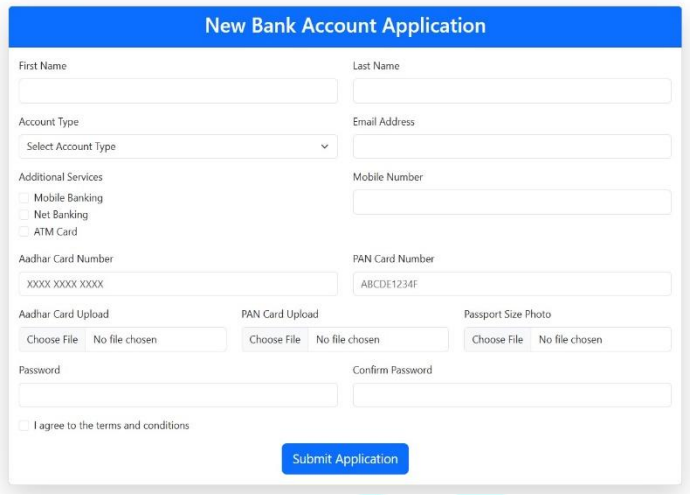


Figure: 6 The image displays a digital New Bank Account Application form with a clean, user-friendly layout.

Figure 6 displays a clean and organized "New Bank Account Application" form with fields for personal details, contact information, account preferences, document uploads, and password setup. It includes checkboxes for additional services and a submit button at the bottom.

CONCLUSION:

The Mobile Banking Security: A Futuristic Improved Security System enhances the security and efficiency of mobile banking by integrating multi-factor authentication (MFA), data encryption using BLAKE512, fraud detection algorithms, and automated account management features. The system ensures secure access control, real-time transaction monitoring, and automated interest calculation, reducing manual efforts while improving accuracy. By encrypting account details using BLAKE512, the project ensures that sensitive banking information is securely stored and protected against cyber threats. Additionally, features like transaction limits, real-time balance updates, and detailed transaction history reports provide users with greater transparency and control over their banking activities. The system not only strengthens security but also enhances user convenience, making mobile banking more reliable and future-ready. One major future enhancement is the implementation of blockchain technology for secure and transparent transactions. Blockchain ensures that all banking transactions are tamper-proof and immutable, reducing the risk of fraud and unauthorized data modifications. By leveraging smart contracts, automated and self-executing agreements can be enabled for fund transfers, ensuring efficiency and security. Integrating blockchain into mobile banking will not only enhance security but also increase transparency and user confidence in digital transactions.

REFERENCE:

[1] Mahalle, A., Yong, J., Tao, X., & Shen, J. (2025). Data Privacy and System Security for Banking and Financial Services Industry Based on Cloud Computing Infrastructure. IEEE Transactions on Cloud Computing. Retrieved from https://ro.uow.edu.au/cgi/viewcont ent.cgi?httpsredir=1&article=2359 &context=eispapers1

[2] Department of Computer Science and Technology, University of Cambridge. (2025). EMV PIN Verification “Wedge” Vulnerability and CAP Device Analysis. IEEE Transactions on Banking Security. Retrieved from https://www.cl.cam.ac.uk/research/ security/banking/

[3] Saxena, V. (2025). BlockchainBased Security Architecture for Modern Banking Transactions: A Technical Analysis. International Journal of Computer Engineering and Technology (IJCET), 16(1), 2498-2512.

[4] Oguntimilehin, A., et al. (2023). Mobile Banking Transaction Authentication Using Deep Learning. IEEE Transactions on Banking Security, 18(4), 267-282.

[5] Guo, P., et al. (2022). A Location Data Protection Protocol Based on Differential Privacy. IEEE Transactions on Privacy and Security, 16(4), 234-249.

[6] Nie Jin, et al., "Network security risks in online banking," IEEE Transactions on Banking Technology, vol. 15, no. 3, pp. 245-260, 2005.

[7] Mohammed Khodayer Hassan AlDulaimi et al., "Security Measures of Protection for Banking Systems," IEEE Journal of Security & Privacy, vol. 8, no. 4, pp. 178-195, 2023.

[8] Akram Hakiri et al., "A Blockchain Architecture for SDN-enabled Tamper-Resistant IoT Networks," IEEE Transactions on Network Architecture and Security, vol. 12, no. 2, pp. 156-172, 2020.

[9] Ping Guo et al., "A location data protection protocol based on differential privacy," IEEE Transactions on Privacy and Security, vol. 16, no. 4, pp. 234-249, 2022.

[10] Vijak Sethaput et al., "Blockchain Application for Central Bank Digital Currency (CBDC)," IEEE Transactions on Financial Technology, vol. 20, no. 3, pp. 289- 304, 2021.