International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

NeoFin: A Secure Full-Stack Core Banking System for Digital Banking Applications

Sakshi Pandey[1], Faizan Khan[2], Jayesh Kande[3], Durva Karande[4], Ankita P. Shinde[5], Pravin R. Pachorkar[6]
[1.2.3.4]UG Student, Department of IT, MVPS's KBTCOE, Nashik, India.
[5,6]Assistant Professor, Department of IT, MVPS's KBTCOE, Nashik, India
EmailID: *pandeysakshi1705@gmail.com[1], faizanahmadfk004@gmail.com[2], jayeshkande4@gmail.com[3], durvakarande16@gmail.com[4], shinde.ankita@kbtcoe.org[5], pachorkar.pravin@kbtcoe.org[6]*

Abstract
Developing and implementing a fully functional core banking system for digital banking activities with an Internet-based secure architecture is the goal of this project. The system is designed to address various issues in traditional banking infrastructures, such as manual processes, slow transaction speeds, and inefficiency. The project adopts a client-server architecture using React.js, Node.js, and MongoDB, along with secure user authentication using JSON Web Tokens (JWT). The implementation is divided into frontend development, backend development, and database integration. The system was tested using functional testing to evaluate performance, accuracy, and security. The results show that the system operates efficiently, provides fast transaction processing, and ensures enhanced data security. Additionally, the system integrates AI-based cheque processing and analytics features, improving automation and reporting capabilities. Overall, the proposed solution enhances efficiency, reliability, and user satisfaction in digital banking.

Keywords: *Core Banking System, Full-Stack Development, Web Application, Secure Authentication, MongoDB, REST API, Digital Banking, Transaction Management.*

1. Introduction
In recent years, the rapid advancement of information technology has significantly transformed the banking sector, leading to the rise of digital banking systems. Traditional banking methods, which rely heavily on manual processes and outdated technologies, are no longer sufficient to meet the growing demands of modern users. These conventional systems often result in slow transaction processing, limited accessibility, lack of scalability, and increased vulnerability to security threats. With the increasing use of internet-based services, customers now expect banking systems to be fast, secure, and accessible anytime and from anywhere. Digital banking platforms have therefore become essential for delivering seamless financial services, improving operational efficiency, and enhancing customer satisfaction. However, many existing banking systems still struggle to adopt modern technologies effectively, leading to inefficiencies and potential security risks. Core banking systems play a vital role in managing key banking operations such as customer information, account management, transaction processing, and loan handling. An efficient core banking system must ensure real-time data processing, high reliability, and strong security mechanisms to protect sensitive financial data. The demand for such systems has increased significantly due to the growth of online transactions and digital financial services supporting features. This project, titled NeoFin: A Secure Full-Stack Core Banking System for Digital Banking Applications, aims to overcome the limitations of traditional systems by developing a modern, scalable, and intelligent web-based solution. The system is built using a full-stack architecture with technologies such as React.js, Node.js, and MongoDB. One of the key features of the proposed system is the integration of an AI-Based Cheque Processing and Information Extraction module, which uses Optical Character Recognition (OCR) techniques to automatically extract important

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

details such as cheque number, bank name, IFSC code, date, and amount from scanned cheque images. This significantly re-duces manual data entry and improves accuracy and efficiency. Additionally, the system includes analytics and reporting features, such as real-time transaction monitoring and end-of-day transaction reports, which help in better financial tracking and decision-making. These features enhance transparency and provide valuable insights into banking operations. The system also incorporates secure authentication mechanisms using JSON Web Tokens (JWT), role-based access control, and real-time transaction processing. It is designed to provide a user-friendly interface while ensuring data security, integrity, and reliability

2. Problem Statement and Objectives

This project addresses the limitations and inefficiency of traditional banking systems. These banking systems commonly use outdated software and manual processes to manage customer, transactional, and financial service data. These inefficiencies and limitations affect banks and their customers alike due to the need to process transactions manually, leading to delays, increased workload, and a higher probability of errors, have a higher chance of making errors, not have accurate or timely access to records and have difficulty securing and growing customer data in modern, paperless, internet-based banking environments.

The objectives of this project are as follows.

- To design a secure and user-friendly core banking system for managing digital banking operations efficiently.
- To implement the proposed design using modern technologies such as React.js, Node.js, Express.js, and MongoDB.
- To test and evaluate the performance of the system based on parameters like accuracy, speed, security, and reliability.
- To improve the overall efficiency, data security, and user experience of banking operations through a scalable web-based solution.

3. Related Work

A number of studies have been completed in respect to the fields of Digital Banking and core banking systems. Previous studies conducted in this area have explored multiple different topics from web-based banking applications [1] to cloud-based banking systems [2] to current technology secured transaction processing [3]. Several recent researchers have also looked into using distributed systems and database management techniques to increase the performance and scalability of banks using distributed databases [4]. Nonetheless, existing financial systems have a multitude of limitations that include high development costs, complicated architectures, limited scalability and potential for security breaches [5]. Some of these systems may also have real-time processing capabilities and friendly UIs, which reduce their ability to be effective and efficient in real-world applications [6]. Furthermore, significant issues still exist for the protection of data and the secure authentication of customers using many traditional forms of banking solutions [7]. Recent studies demonstrate the ability for blockchain technology, in addition to using decentralized platforms in financial transactions to enhance transparency and security [8]. Other applications include the use of artificial intelligence and machine learning techniques for fraud detection and risk assessment within banking systems [9]. Cloud computing technology continues to provide banks with a scalable and economical means of managing large amounts of data [10]. However, the above-mentioned existing technologies have several limitations in that development costs are high, architectures are very complicated, scalability is limited, and security vulnerabilities exist [11]. In addition, many existing systems do not allow for real-time processing and provide limited options for a user-friendly interface, therefore limiting their effectiveness as well as their efficiency within actual application environments [12]. A significant number of existing traditional banking technologies have encountered enormous difficulties concerning data privacy and ability to integrate systems, as well as maintenance of systems; these were all major impediments to the success of many traditional banking technologies [13]. In recent research, the authors sought to increase system performance via microservice architectures and API-based integration, however, they continue to experience issues regarding the complexity of implementing

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

various systems and resources [14]. Additionally, there are significant concerns around the security of information and transactions in dis-tributed environments [15]. This specific project differs from existing projects in that it will provide a modern full-stack web-based core banking system that is both simple and scalable, as well as secure. It will include features such as advanced authentication mechanisms for users, efficient database management, and clean, user-friendly interfaces that will allow the system to perform at a higher level than comparable systems. The project will develop a banking system that will provide users with real-time transaction processing capabilities, increased data security, and enhanced user experiences, which should allow the overall functioning of the banking system to be more practical and more efficient than existing banking systems.

4. System Design And Methodology

The proposed system is designed as a three-tier architecture consisting of the front-end (client-side interface), back-end (server-side application), and database. The front-end provides an interactive user interface through which users can access various banking services. The back-end handles business logic, authentication, and API processing, while the database stores all banking-related data such as users, accounts, transactions, loans, and branch information.

4.1. System Overview

The system begins with user authentication, where creden-tials are verified using secure mechanisms such as encrypted password comparison and JSON Web Token (JWT) authenti-cation. Upon successful login, users are granted access based on their roles (Admin, Manager, Clerk). The system supports operations such as customer management, account handling, transaction processing (deposit, withdrawal, transfer), and loan processing, all of which are executed in real time. The figure illustrates the architecture of the proposed Secure Core Banking System. The system is designed using a microservices-based architecture to ensure scalability, security, and efficient processing of banking operations.

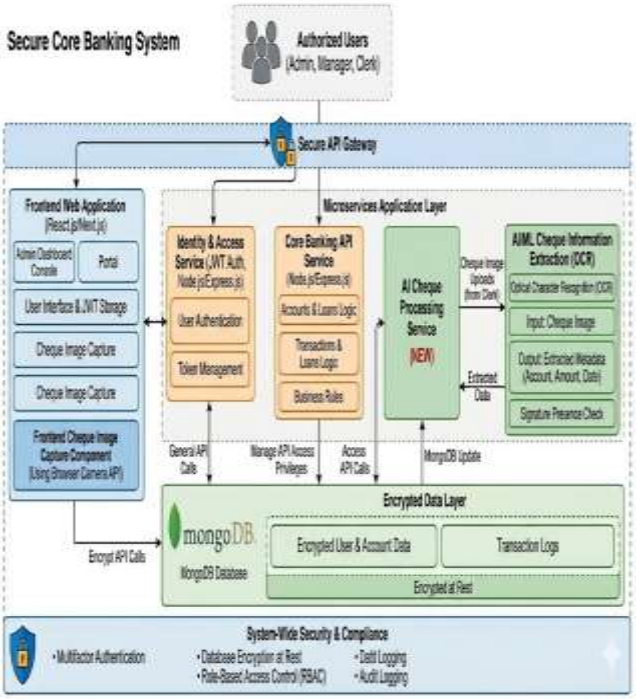

Figure 1 System Architecture

The system is accessed by authorized users such as Ad-min, Manager, and Clerk through a frontend web application developed using React.js and Next.js. The frontend provides an interactive user interface for performing various banking operations and capturing cheque images using the browser camera API. All user requests are securely transmitted to the backend through a Secure API Gateway, which acts as a central entry point for request validation, authentication, and routing. The backend consists of multiple microservices that handle specific functionalities. The Identity and Access Service manages user authentication and session handling using JSON Web Tokens (JWT). The Core Banking API Service implements business logic for account management, transaction processing, and loan operations. Additionally, an AI-based Cheque Processing Service is integrated to handle cheque image processing efficiently. The AI/ML-based Cheque Information Extraction module uses Optical Character Recognition (OCR) techniques to ex-tract key details such as account number, amount, and date from cheque images. It also performs signature presence verification, thereby reducing manual effort and improving accuracy. The system uses MongoDB

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

as the database, forming the encrypted data layer where user data, account details, transaction logs, and extracted cheque information are securely stored. All data is encrypted at rest to ensure confidentiality and integrity. The overall communication flow involves the user inter-acting with the frontend, sending requests through the API Gateway to appropriate microservices, processing the data, and storing or retrieving it from the database before sending the response back to the user. The system also incorporates strong security mechanisms such as role-based access control, encrypted API communication, and multi-factor authentication to ensure secure and reliable banking operations.

4.2. System Modules

The platform is organized into five functional modules, each responsible for a distinct area of the student experience.

4.2.1. Communication Flow

The system follows a structured communication process:

- The user interacts with the front-end interface.
- The front-end sends HTTP requests to the back-end using APIs.
- The back-end validates the request and processes business logic.
- The database is accessed to retrieve or store relevant data.

The processed response is sent back to the front-end and displayed to the user.

4.2.2. Security Features

The system incorporates multiple security mechanisms:

- JWT-based authentication for secure session management.
- Password encryption using hashing techniques.
- Role-Based Access Control (RBAC) to restrict unauthorized access.
- Secure API communication between front-end and back-end.

4.2.3. Components and Materials Used

The system is composed of the following components:

- Frontend Interface Provides responsive web pages for user interaction.
- Backend Server Handles request processing, business logic, and authentication.
- Database (MongoDB) Stores and manages banking data securely.
- API Services Enables communication between frontend and backend.

4.2.4. Software and Tools used

The Technologies were used in system development are React.js and Next.js for frontend development as well as Node.js and Express.js for backend development.

4.3. Development Methodology

The development of the system follows a structured approach:

- **Planning and Requirement Analysis:** Identification of system requirements and defining project scope.
- **System Design:** Designing architecture, modules, and data flow.
- **Technology Selection:** Choosing appropriate tools and technologies.
- Implementation: Developing frontend, backend, and integrating with database.
- **Testing and Evaluation:** Evaluating system performance, accuracy, and security through testing.

5. Implementation

- The implementation phase of the proposed core banking system involved setting up a complete development environment and integrating the frontend, backend, and database components into a unified architecture. The system was developed using modern web technologies to ensure scalability, performance, and security.
- Initially, the database schema was designed and implemented using MongoDB. Multiple collections were created to manage different entities, including Users, Customers, Accounts, Transactions, and Loans. These collections were structured to support efficient data storage and retrieval while maintaining data consistency.
- The frontend of the application was developed using React.js and Next.js, providing a responsive and user-friendly interface. It includes various modules such as user authentication, customer management, account management, transaction processing, and loan

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

handling. The interface was designed to ensure ease of use and real-time interaction.

- The backend was developed using Node.js and Express.js, which handle all business logic and API processing. RESTful APIs were created to enable communication be-tween the frontend and backend. The backend is responsible for validating user requests, processing transactions, managing accounts, and handling loan-related operations.
- Secure authentication was implemented using JSON Web Tokens (JWT), ensuring that only authorized users can access system functionalities. Passwords were encrypted using hashing techniques to enhance data security.
- The application follows a client-server architecture where the frontend communicates with the backend through API calls. The backend interacts with the MongoDB database for storing and retrieving data. All modules, including login, customer management, account processing, trans-action processing, and loan management, were integrated and tested collectively to ensure smooth functionality.
- During the implementation phase, several challenges were encountered, particularly in ensuring data security, managing user roles and permissions, and maintaining real-time updates. These challenges were addressed by implementing Role-Based Access Control (RBAC), optimizing API performance, and improving database query efficiency. The system also integrates AI-based cheque processing and analytics modules, enhancing automation and reporting capabilities. Overall, the system was successfully implemented and demonstrated stable performance across all modules, ensuring efficient and secure banking operations.

6. Results

The functional and performance testing on the deployed project showed proper operation of the system prior to going live. System accuracy, response time and secure data handling were the main parameters measured and The results of the testing are illustrated in Fig. 2.

Figure 2 AI-Based Cheque Processing and Information Extraction System

The figure shows an enhanced cheque scanner interface that uses OCR technology to automatically extract key details from a scanned cheque image. The system identifies and displays information such as cheque number, bank name, branch, IFSC code, date, amount, and payee name, reducing manual data entry and improving accuracy.

- All banking operations such as customer management, transactions and loan processing were processed correctly.
- The time taken to respond to user requests and complete transactions was minimal, providing real-time updates on the dashboard.
- Data was handled securely by the system, with appropriate authentication and encryption in place.

The system was able to handle normal operational loads with many simultaneous users efficiently, providing faster processing times, increased data security, an improved user experience and better adaptability than the methods currently in use.

A few limitations to the system were noted as: it relies on internet connectivity; has limited scaling ability to process large amounts of data without using cloud deployments; and does not have some of the more advanced features available today, such as AI-based fraud detection.

Conclusion

The implementation of the Secure Full-Stack Core Banking System demonstrates an efficient solution for modern digital banking operations. The system successfully completes all phases of design,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

development, and testing using advanced web technologies. The results indicate improvements in accuracy, processing speed, and data security, leading to enhanced overall banking performance. The integration of AI-based cheque processing and analytics further improves automation, accuracy, and decision-making capabilities. This project demonstrates the practical feasibility of deploying scalable and secure digital banking solutions in real-world environments.

Future Work

Examples of potential future enhancements could include greater utilization of AI for fraud detection or risk assessment models; implementation of cloud-based technology to provide greater scalability and effective data management; and additions such as multi-factor authentication to improve security. Improving these interfaces with technology would help create an overall more accurate, automated, scalable, and secure solution for enterprise applications that support considerable volume transactions or volume banks.

Acknowledgements

The authors would like to thank the Department of Information Technology and the institute for providing the necessary support and resources during the development of this project. We also express our sincere gratitude to our project guide and faculty members for their valuable guidance and encouragement throughout the course of this work.

References

[1] E. Indriasari et al., "Intelligent Digital Banking Technology and Architecture: A Systematic Literature Review," International Journal of Interactive Mobile Technologies, 2022.
[2] S. Chen et al., "An Empirical Assessment of Security Risks of Global Android Banking Apps," IEEE Security Privacy, 2018.
[3] P. B. Fernandes, "SecureBank: A Zero Trust Architecture for Banking Systems," arXiv preprint, 2025.
[4] D. Fett et al., "An Extensive Formal Security Analysis of the OpenID Financial-grade API," IEEE European Symposium on Security and Privacy, 2019.
[5] W. Haruna et al., "Defending Against Cybersecurity Threats to the Banking System," Journal of Cybersecurity, 2022.
[6] I. Rahim, "SEPA Clients in a Secure Cloud Banking Environment," International Banking Systems Journal, 2013.
[7] J. Bamini, "Enhanced Authentication Methods for Online Banking Systems," International Research Journal, 2024.
[8] R. Sastri et al., "Development of a Bank Management Application Using Java," Zenodo Research Archive, 2026.
[9] "Design of Bank Application System Using Service-Oriented Architecture," IEEE Conference Paper, 2010.
[10] "Enterprise Banking System Using SOA and Web Services," International Journal of Computer Applications, 2011.
[11] "Cybersecurity Threats and Vulnerabilities in Online Banking," International Journal of Scientific Research and Management, 2023
[12] "Bank Management System," Journal of Engineering Research, 2025.
[13] "Bank Account Management System," Journal of Network and Applications, 2025.
[14] T. Woo et al., "Secure Network Programming," USENIX Conference Proceedings, 1994.
[15] IEEE, "Banking in Cyberspace: An Investment in Itself," IEEE Spectrum, 1995.
[16] "Core Banking Systems and Architecture," Gartner Research Report, 2020.
[17] "Banking Software Systems and Digital Platforms," Financial Technology Review, 2023.
[18] Infosys, "Finacle Digital Banking Solution," Technical White Paper, 2019.
[19] Tata Consultancy Services, "TCS BaNCS Core Banking System," Technical Documentation, 2019.
[20] J. Braeuer et al., "Risk Assessment of ATM Platform Security," Inter-national Journal on Advances in Security, 2016.
[21] A. Gai, Q. Qiu, and X. Sun, "A Survey on FinTech," Journal of Network and Computer Applications, vol. 103, pp. 262–273, 2018.
[22] M. Iansiti and K. R. Lakhani, "The Truth About Blockchain," Harvard Business Review, vol. 95, no. 1, pp. 118–127, 2017.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3614-1832
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0471

[23] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[24] N. Provos and D. Mazieres, "A Future-Adaptable Password Scheme," in Proceedings of the USENIX Annual Technical Conference, 1999, pp. 81–92.
[25] OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021.