

Scientiarum: A Multidisciplinary Journal
Vol. 2 No. S1 (2026): Supplement Issue
DOI: 10.54646/SAPARS.2026.89

SAPAR SERVICES LLP
Scholarly Articles Publication And Repository Services

SMART BANKING SYSTEM (GREEN BANKING)

A UNIFIED, SECURE AND INTELLIGENT CORE BANKING PLATFORM FOR CUSTOMERS, COMPLIANCE OFFICERS, AND ADMINISTRATORS

Jerbin J S[1], Dr. K. Adisesha[2]

MCA 2nd year[1], Associate Professor[2],

Department of Computer Science and Applications

S.E.A. College of Science, Commerce and Arts, Bangalore

jerbin06js@gmail.com[1] ,adisesha1@rediffmail.com[2]

Abstract

Modern financial operations and digital banking exist in a mission-critical area where security vulnerabilities, unauthorized overdrafts, fraudulent transactions, money laundering risks, and manual credit underwriting delays can profoundly undermine institutional integrity and customer trust. This paper proposes Green Banking (Smart Banking System), a unified, secure, and intelligent core banking platform connecting retail customers, compliance officers and bank administrators through a real-time digital financial ecosystem.

The system is focused around an atomic double-entry General Ledger bookkeeping engine, two-step OTP multi-factor authentication, real-time AI Neural Sentinel fraud and anomaly detection, automated Anti-Money Laundering (AML) compliance monitoring, CIBIL-based loan underwriting with reducing-balance EMI amortization

schedules, ISO/IEC 7812 Luhn Mod-10 card lifecycle management and standardized identifier generation (IFSC, UPI VPA and ISO 13616 IBAN). The platform is built using a four-tier architecture encompassing a presentation tier, an Express REST API gateway tier, a business services tier and an ACID-compliant persistence tier utilizing SQLite in Write-Ahead Logging (WAL) mode. Security is enforced through JWT-based Role-Based Access Control (RBAC), bcrypt password hashing and tamper-evident audit logging and the API is documented with OpenAPI/Swagger.

The primary aim of the system is to transform every banking operation into an atomic, verified and auditable lifecycle in which no transaction is committed without balance verification, AML screening and fraud-risk scoring. The proposed design also serves as the foundation for future technologies including blockchain-based ESG bond tokenization, IoT smart-meter verification, Central Bank Digital Currency (CBDC) settlement and biometric authentication.

Keywords: Core Banking System, Double-Entry General Ledger, AI Fraud Detection, Anti-Money Laundering (AML), CIBIL Loan Underwriting, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), SQLite WAL, FinTech, Financial Cybersecurity.

Introduction

Financial operations are mission-critical, time-critical, and strictly regulated. Conventional banking workflows often suffer from fragmented ledger systems, manual loan underwriting delays, delayed detection of suspicious transactions, and vulnerability to unauthorized account overdrafts. A single error in a ledger entry or a missed fraudulent transfer can directly affect customers and the institution.

Green Banking is proposed as a platform that brings the major parts of a banking process together. Every financial event is verified against anti-money laundering

(AML) rules, scored for fraud risk by an AI Neural Sentinel, and committed to an immutable double-entry ledger within a single transactional lifecycle. The platform is designed around the principle "Zero Discrepancy. Real-Time Intelligence. Absolute Security."

The system mainly involves three users. The Customer requires rapid digital banking services, secure fund transfers, real-time balance tracking, card management, and transparent loan schedules. The Compliance Officer requires immediate AML alerts, high-value transaction monitoring, fraud investigation tools, and audit reporting. The Administrator (Super Admin) requires real-time operational visibility, General Ledger auditing, user management, and regulatory compliance oversight.

The scope of the project includes digital customer onboarding and account management, atomic double-entry General Ledger bookkeeping, real-time AI fraud and anomaly detection, regulatory AML compliance and CTR reporting, automated loan underwriting and EMI schedules, card lifecycle management with Luhn verification, centralized admin monitoring and audit logs, and an accessible, responsive light/dark banking interface.

Literature Review

Recent studies on digital banking explored topics that include financial fraud detection, cybersecurity, automated transaction monitoring, and sustainable banking. The cited works provide a foundation for developing a secure and integrated Smart Banking System.

Hafez et al. [1] investigated the application of artificial intelligence (AI), machine learning (ML), and deep learning techniques for credit card fraud detection. Their work identified multiple approaches to detect fraudulent transactions and associated challenges. Thus, the findings emphasize the importance of applying AI in the

banking sector. Nonetheless, the authors stress the importance of transaction data quality, selected models, and transaction behaviors in fraud detection.

Aros et al. [2] conducted a literature review that explores the use of machine learning approaches for financial fraud detection. Their study analyzed 104 articles to identify detection methods and their common input data, as well as to evaluate performance assessment practices. In particular, the authors focus on the role of data mining and automated detection of financial fraud and risks. The findings indicate that such an approach can be applied in a Smart Banking System, where automated procedures would ensure the highest safety level.

Modern banking faces a significant risk of cybersecurity breaches involving illegal access to databases and financial transactions. For instance, a systematic review of studies published in the Journal of Financial Crime [3] focuses on security issues and strategies for digital banking. The review highlights the need to implement authentication, access control, and risk management practices and emphasizes the importance of auditing and monitoring procedures. These security measures can be implemented in a Smart Banking System to ensure the safety of customers' data and increase the level of trust.

Green banking is another significant area of modern transaction processing that is gaining increasing attention due to growing environmental concerns. Indeed, research on green banking and environmental sustainability [4] offers a conceptual framework that can be integrated into the Smart Banking System. The article explores the connection between commercial banks in India and environmental performance, suggesting that paperless transactions and green financial products, such as green loans and green bonds, help reduce the impact of the banking activities on the environment. Thus, the study provides numerous ideas for developing a prototype of a

paperless and sustainable Smart Banking System.

Based on the reviewed articles, a conceptual framework of a Smart Banking System would integrate customer's bank transactions, including double-entry accounting, AI-powered fraud detection and surveillance of suspicious transactions, loan and EMI processing, card processing, and administrative management. Moreover, the goals of green banking and paperless transactions described in the selected articles will be included in the design of a Smart Banking System. The proposed system would combine the benefits of automated and secure transaction processing, as well as advanced sustainability practices. The framework will be tested to ensure the accuracy of financial transactions, security, and fraud detection capabilities and check the efficiency of processing. In addition, the correctness of ESG scores calculation and the accuracy of green financial products identification will be evaluated.

Problem Statement

In the traditional banking setup, processing of transactions, balances, loan underwriting and compliance typically involves disparate systems, branch interventions and batch settlements. The customers have to go through disconnected portals or even visit the branch, causing multi-day delays in transaction clearing. The manual nature of verification leads to manual data entry and human errors. Loans underwriting is manual and slow, and fraud and AML management is periodic and not automated. Unauthorized overdrafts are possible due to unverified balance checks, and there is no single source of ledger-truth. Further, there is no real-time computation for fraud risk scores, automated AML alerts or centralized administration. The design of Green Banking, therefore, aims to capture every financial transaction as a persistent digital object, with a unique reference and audit history, which requires double-entry ledger-legs, real-time AI fraud checkers, and immutability to

unauthorized overdrafts.

Research Gap

Traditional banking processes treat ledger posting, underwriting, fraud review, and compliance checks as separate functions, frequently processed in batches by different entities. Green Banking tries to bring these financial operations into a single unified platform where a particular payment goes via steps Initiated → Authenticated → AML Screened → AI Scored → Balance Verified → Double-Entry Posted → Settled → Audited. It covers all the necessary stages in a financial transaction and makes it easy to read.

Research gap and contribution

Research objectives

Add a short section defining what the research aims to achieve.

Example objectives:

- Design a unified smart banking architecture.
- Maintain transaction consistency using double-entry accounting.
- Identify suspicious transactions using a fraud-risk scoring method.
- Evaluate transaction correctness, response time, and security controls.
- Explore paperless and sustainability-oriented banking features.

Reference	Research focus	Limitation relevant to your work
[1]	AI-based credit card fraud detection	Identify a limitation supported by the paper
[2]	ML-based financial fraud detection	Identify a limitation supported by the paper

[3]	Digital banking cybersecurity	Identify a limitation supported by the paper
[4]	Green banking and environmental performance	Identify a limitation supported by the paper

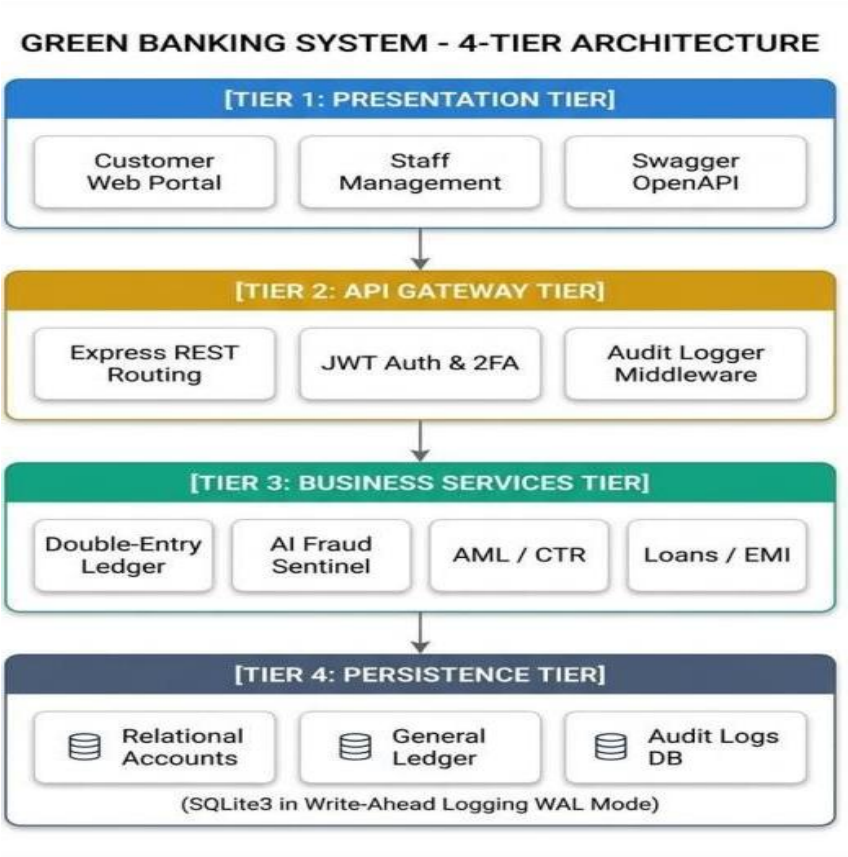


Fig :1 High-Level Architecture

The architecture is partitioned into several tiers.

Presentation Tier

This tier consists of the interfaces through which customers and staff members interact with the system: a Customer Web Portal, a Staff Management interface, and a Swagger/OpenAPI documentation interface.

API Gateway Tier

This tier contains the Express REST routing, JWT authentication with 2FA, and the

audit logger middleware. The middleware is used to verify the bearer token, check the user's role, and log an incoming audit entry, before passing the authenticated context to the next handler.

Business Services Tier

This tier consists of the core engines: the Double-Entry Ledger, the AI Fraud Sentinel, the AML/CTR engine, and the Loans/EMI engine.

Persistence Tier

This tier is concerned with storing relational accounts, the General Ledger, and audit logs in SQLite3 configured in Write-Ahead Logging (WAL) mode, which provides ACID compliance, foreign key constraints, concurrent read-write access, and atomic rollback.

Technology Stack

The frontend uses HTML5, CSS3, and JavaScript (ES6+) with light/dark theme support, and the backend is specified on Node.js, TypeScript, and the Express framework. For security, we utilize JWT, bcrypt, time-based OTP for 2FA, and RBAC middleware. The AI Neural Sentinel offers a heuristic fraud analysis, detecting scam keywords via NLP in transaction memos, while the loan engine performs reducing-balance EMI calculation. The backend code listing in the project report shows similar services using Python FastAPI with WebSocket channels and Redis Pub/Sub (with an in-memory fallback cache).

System Components

Customer Module

The customer is the person who utilizes the banking services. The customer can register and log in securely with 2FA OTP verification, open accounts with automatically generated IFSC, UPI VPA, and ISO 13616 IBAN identifiers, and view

real-time balance, transaction history, and account statements. The customer can also initiate atomic fund transfers (UPI, NEFT, RTGS), manage cards and lock or unlock them, apply for loans and inspect amortization schedules, and download transaction receipts.

Whenever a transfer is created, the system captures information such as the unique transaction reference (TXN ID), transaction type, amount, source account, destination account, timestamp, and settlement status. This provides the system the full context it needs to carry out AML screening and fraud scoring prior to updating the ledger.

1Compliance Officer Module

The compliance officer is responsible for monitoring regulatory risk. The compliance officer can access the compliance monitoring dashboard, review high-value transactions at or above the statutory threshold (≥ ₹10 Lakhs), inspect AI fraud risk scores and NLP scam markers, investigate flagged accounts, and resolve alerts and file statutory regulatory reports. The alert process can take the path of Normal Monitoring → Sentinel Alert Triggered → Temporary Protective Hold → Auditor Resolution / Clearance.

Administrator Module

The administrator provides centralized monitoring and governance. The administrator can monitor real-time system transactions, manage user and staff credentials, verify General Ledger equilibrium (∑ Debits = ∑ Credits), review immutable audit logs, inspect database health, and configure global operational settings. Access is controlled by a five-tier Role-Based Access Control (RBAC) matrix covering Super Admin, Manager, KYC Officer, Loan Officer, and Support Agent, enforced by backend middleware on every protected endpoint.

Core Banking Engines

Double-Entry Ledger. Every transaction causes exactly two balanced ledger entries (one debit and one credit) within a single atomic database transaction (BEGIN TRANSACTION to COMMIT, with immediate ROLLBACK on failure). The sender balance is verified before posting, so overdrafts are rejected with zero ledger change.

AI Fraud Sentinel. The Sentinel scores behavioral risk, monitors Account Takeover (ATO) surges and transaction velocity, and detects scam keywords in transaction memos using NLP.

AML Engine. The AML engine screens transactions against PMLA thresholds (≥ ₹10 Lakhs), performs blacklist verification, and generates Cash Transaction Report (CTR) compliance alerts.

Loans and Underwriting. Loan applications are evaluated using a CIBIL credit score, an interest rate is determined, and a reducing-balance monthly EMI with a zero-balance amortization schedule is generated.

Cards. 16-digit card numbers are issued and validated using the ISO/IEC 7812 Luhn Mod-10 algorithm, with CVV generation, card limits, and instant lock/unlock controls.

Green Banking Features. The prototype also includes green lending for categories such as Solar Rooftop, Electric Vehicle, Organic Agri, and EcoBuilding at a concessional interest rate, and a paperless-banking carbon-savings estimate that credits green rewards points to customers.

Real-Time Notification System

A real-time communication layer is necessary so that customers, compliance officers, and administrators receive updates without manual intervention. The prototype uses channel-based WebSocket endpoints (/ws/customer/{id}, /ws/compliance, and /ws/admin), with Redis Pub/Sub and an in-memory fallback for event broadcasting. The basic process begins when the customer initiates a transfer from the web

dashboard. The API gateway then verifies the JWT, checks the role, and writes an audit entry, after which the Transactions Controller triggers the AML Engine and then the AI Fraud Sentinel. If the transaction is approved, the Ledger Engine verifies balance and posts the balanced debit and credit entries atomically. Finally, the audit record is persisted and a receipt is returned to the customer, while alerts are pushed to the compliance and admin dashboards in real time.

Methodology

Green Banking is developed based on the Software Development Life Cycle (SDLC) following the Waterfall process, in which every phase is concluded with a particular deliverable and approval to proceed to the next stage. The below-mentioned steps are performed one after another while developing this application.

Step 1 – Requirement Analysis

Customer, compliance, and administration requirements, such as user roles, financial processes, accounting procedures, and security measures, are collected.

Step 2 – Feasibility Study

Technical, operational, economic, and legal and privacy aspects are examined; standards like RBI Cyber Security Framework, PMLA, FIU-IND, and data privacy principles are considered.

Step 3 – System Design

The application's system architecture, relational database design, UML class, use case, activity, sequence, data flow, entity-relationship, and API boundary diagrams are conceptualized.

Step 4 – User Authentication

A user is redirected to the login page where they are authenticated using a JSON Web Token and a two-step One-Time Password (OTP) procedure; their access to features

is managed through a multi-tiered Role-Based Access Control (RBAC) matrix.

Step 5 – Transaction Request

A customer submits a fund transfer request that is received and authenticated by the API gateway.

Step 6 – AML and Fraud Screening

Screening for Anti-Money Laundering (AML) thresholds and AI-powered fraud detection called Neural Sentinel take place, and suspicious transactions are moved to the compliance alert queue.

Step 7 – Balance Verification and Ledger Posting

Ledger Engine checks the balance and makes a debit and credit entry of the correct amount in one single transaction.

Step 8 – Notification and Audit

A customer is notified and sent a receipt link; at the same time, alerts are triggered and an append-only audit record is created.

Step 9 – Testing

Unit, integration, system, and acceptance, security, and usability and accessibility tests are conducted.

Step 10 – Deployment and Maintenance

Once launched, the application undergoes maintenance, such as database performance analysis, bug fixing, dependency management, security patching, ledger balance validation, and performance optimization.

Limitations

Like any other software system, Green Banking too comes with its limitations.

Internet Connectivity

Transactions in real-time, WebSocket notifications, and OTP delivery need an active internet connection and network stability; interruption during an atomic fund transfer transaction at commit is a technical risk.

Database Write Contention

While SQLite in WAL mode does allow concurrent reads and writes, there could be write contention issues at the file level when doing high-volume transactions.

False Positives in Fraud Scoring

Heuristic fraud-scoring by the AI engine may have false positives that could waste the compliance officers' time.

External Services

OTP delivery through SMS/email gateways and connections to identity or credit bureau APIs could add latency.

Regulatory Readiness

The software needs to strictly follow the RBI Cyber Security Framework, PMLA, FIU-IND guidelines, and data protection regulations for production-grade deployment.

Prototype Scope

The prototype code listing shown uses a mock in-memory database for brevity; a production-grade system would use the persistent database as mentioned in the architecture section.

Security and Privacy

The system deals with sensitive personal and financial information. Appropriate measures such as authentication, authorization, encryption, and data protection need to be taken.

System Components

The described components will comprise the general structure and process of the

Smart Banking System. The system will facilitate banking, finance monitoring, transactions, and green or sustainable banking features.

3Customer Module

The customer module will allow customers to set up their profile, authenticate, and perform banking operations, including viewing the balance, transaction history, make payments and transfers, manage cards, view and repay loans, and receipts of transactions.

Authentication and Security Module

The authentication and security module will include the customer's password encryption, OTP, JSON web token, and role-based access control to authorize the customers' banking activities. In the system, this component will ensure that customers can only access banking services according to their roles.

Double-Entry Ledger Module

The double-entry ledger module will record the entries of debit and credit with balanced amounts. This component will allow the system to run both entries in a single transaction and rollback one or both if one fails, ensuring atomicity between them. As a result, it will secure banking transactions from errors and fraudulent activities.

AI-Assisted Fraud Detection Module

The AI-assisted fraud detection module will help the system identify and prevent fraud. Notably, the component will conduct its analysis on transaction information and specific risk indicators, after which it will provide risk scores and alerts for specific transactions. In this case, the detection model will rely on the method's accuracy in detecting fraud, the data used, and the testing process.

Anti-Money Laundering and Compliance Module

The anti-money laundering (AML) and compliance module will allow the system to monitor transactions and detect suspicious activities. Moreover, it will provide the compliance team with information and reports on suspicious transactions, including alerts and cases. Here, the system will provide the necessary details to help the compliance team investigate and prepare any regulatory filing for each case.

Loan and EMI Calculator Module

The loan and EMI calculator module will enable the system to receive and assess a customer's application for credit. In this case, the component will ensure that the system follows the specified criteria while evaluating the application. The calculator will use the reducing balance method to determine the monthly instalments and show the repayment schedules. However, the integration of a system that provides the credit score for the loan applications must be set up and tested.

Card Management Module

The card management module will be used to create cards in the prototype. It will also include a Luhn algorithm to verify the card numbers, in addition to features to lock, unlock cards, and limit amounts. The cards could also be issued to customers but require appropriate infrastructure and authorization services.

Administrator and Audit Module

The administrator and audit module will comprise the dashboard where the admin can monitor the users, transactions, and staff, and check the system's overall activity and ledger balances. Moreover, this component will provide an auditing trail for the system, supporting the reconciliation of banking activities and transactions, and identifying problems in the system.

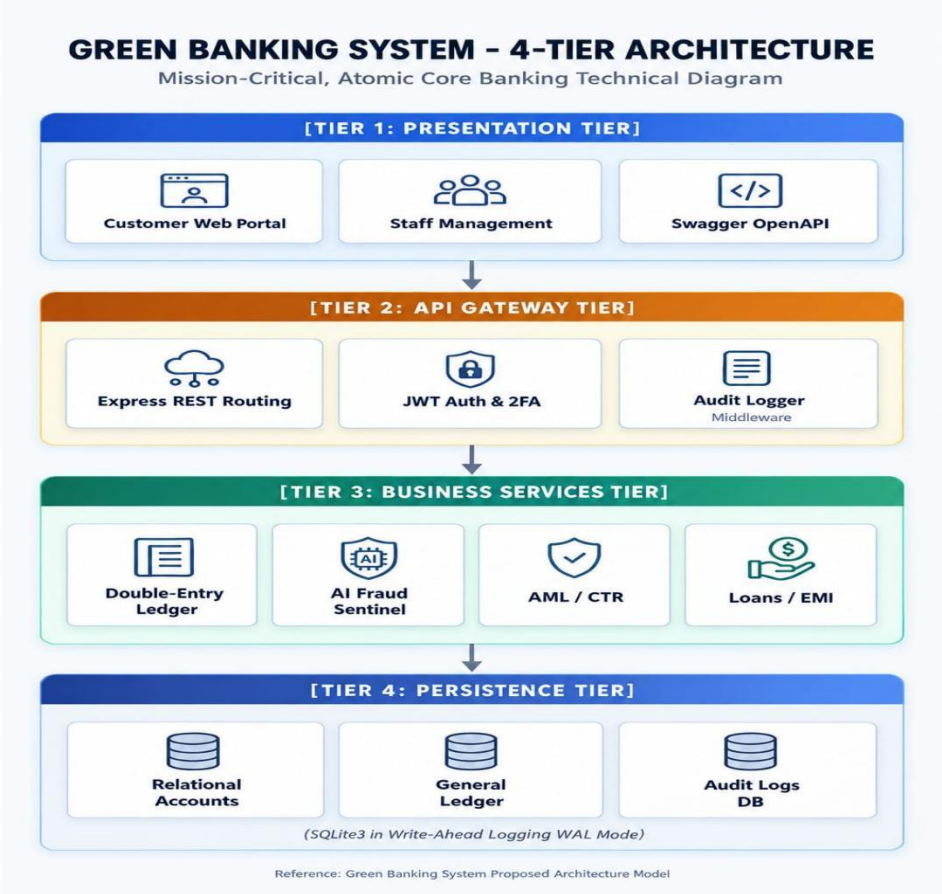
Real-Time Notification Module

The real-time notification module will ensure that notifications, alerts, messages, and

receipts of transactions are delivered to the relevant users in the form of a web socket or through another configured channel.

Green Banking Module

The green banking module will include green features such as paperless banking, green records, green loans, and green balance, which will estimate the amount of CO2 emissions reduced by the system. Here, the carbon footprint of the green balance should be determined using a specific formula and specify the assumptions.



Challenges

Modern enterprise-grade banking platform development comes with a set of challenges:

Transaction Concurrency

The main problem was to avoid race conditions and ledger inconsistencies on a large scale.

Low-Latency AI Risk Scoring

Fraud detection systems should not add significant latency to the transaction processing pipeline.

Real-Time Multi-Tenant Communication

The system should provide channels for customers, compliance officers, and administrators to communicate in isolation.

OTP Security

Time-sensitive 2FA tokens should be protected from replay attacks.

Verifiable Sustainability Accounting

The system should store carbon-savings metrics in a verifiable scientific manner

Results and discussion

This is one of the most essential additions. Describe the results obtained from your prototype testing and experiments, such as

- the number of transactions processed,
- successful and failed transactions,
- verification of the correctness of the ledger balance,
- average response time of the API, and
- fraud-detection precision and recall (if you have labelled test data)
- plus the results of authentication and authorization tests.

System Scalability

The API gateway, AI fraud sentinel, and database workloads shall scale independently with growing transaction volumes.

1.Expected Outcome

It is expected that the main outcome of Green Banking be represented by a structured platform in which customers, compliance officers and administrators share a

controlled secure financial lifecycle. The proposed system is expected to provide centralized immutable General Ledger records as well as real-time transaction processing and instant settlement status. It is expected to maintain double-entry balance equilibrium (∑ Debits = ∑ Credits) and reject overdrafts with atomic pre-transaction validation. It is expected to provide role-based dashboards for customers, compliance officers and administrators as well as maintain an immutable audit history with regulatory reporting (FIU-IND / PMLA) and offer a reusable UI component library as well as interactive charts and tables in responsive, accessibility-conscious light and dark design.

System Testing Scenarios

ID	Scenario	Expected Result
ST-01	Customer initiates fund transfer	Transaction created, balance debited/credited atomically, and receipt displayed.
ST-02	Customer attempts unauthorized overdraft	Request rejected with insufficient funds exception and zero ledger change.
ST-03	User transfers ≥ ₹10 Lakhs	AML rule triggers and high-value compliance alert is logged into queue.
ST-04	Customer applies for loan	CIBIL score evaluated, rate assigned, and zero-balance EMI schedule generated.
ST-05	User enters invalid 2FA OTP	Session access denied and failed security attempt logged in audit trail.
ST-06	Admin opens command dashboard	Live General Ledger status verified balanced with zero discrepancy.

The actual performance of the system must be tested. The following design target indicators can be measured: end-to-end transaction settlement latency (< 150 ms), 2FA OTP delivery and verification latency (< 3 seconds), WebSocket alert propagation (< 35 ms), median API response time (< 80 ms), AI Sentinel scoring latency (< 25 ms), peak throughput (≥ 500 TPS), and transaction error and rollback rate (< 0.01%). Daily General Ledger reconciliation of the invariant ∑ Debits = ∑ Credits should also be verified.

Future Scope

Green Banking can be significantly improved upon in future versions.

AI-Driven Green Budgeting

Personal carbon footprint forecasting and automated green budgeting.

Blockchain ESG Bond Tokenization

Blockchain-based ESG bond tokenization and fractional green asset investing.

IoT Smart-Meter Integration

Automated solar power generation verification and subsidy disbursement.

Voice-Activated Multilingual Banking

Voice-based banking for enhanced rural accessibility and financial inclusion.

CBDC (e-Rupee) Integration

Low-energy instant micro-settlements using the Central Bank Digital Currency.

Biometric and Passwordless Authentication

FIDO2 and Face ID authentication for zero-card digital ATM access.

Green Rewards Marketplace

Gamified green rewards with carbon offset credit trading and verified tree-planting initiatives.

ESG Compliance Modules

Automated ESG compliance scoring and BRSR reporting for corporate enterprise clients.

Offline-First Wallet Payments

Offline-first cryptographic wallet payments for low-connectivity agricultural and rural regions.

Climate Risk Underwriting

Satellite imagery and climate risk analytics for automated underwriting of sustainable agriculture loans.

Wearable Payments

Smartwatch and wearable tap-to-pay integration with real-time CO2 milestone feedback.

Open Banking Green APIs

Integration with EV charging stations and eco-commerce platforms.

Advantages of Using the Proposed System

Green Banking provides numerous benefits over traditional banking procedures. Atomic double-entry General Ledger ensures that all transactions commit precisely one debit and one credit within a single database transaction to keep the ledger always balanced (∑ Debits = ∑Credits) while rejecting any overdrafts with no ledger change. Every transfer undergoes a complete lifecycle of authentication, AML screening, AI fraud scoring, balance verification, ledger posting, and audit logging, thus eliminating the gaps that arise from fragmented systems and periodic offline reviews. The two-step OTP authentication, JWT-based five-tier role-based access control, bcrypt password hashing, and tamper-evident audit logs, along with the AI Neural Sentinel detecting suspicious behavior, account takeover surges, and scam keywords, improve security. The automated AML screening for the

₹10 Lakh PMLA threshold and CTR alerts expedite regulatory compliance for compliance officers while CIBIL-based underwriting with reducing-balance EMI schedules accelerates loan decisions, offering customers an intuitive view of their repayment schedules. Customers receive immediate settlement status, real-time balance, lock and unlock cards, download receipts, and a responsive, accessible light and dark interface, while administrators rely on a single source of truth and live ledger verification. Four-tier modular architecture facilitates easy extension and scaling, while the system's green lending, paperless-banking rewards, and sustainability features promote eco-friendly banking while reserving room for future technologies such as blockchain ESG bonds, CBDC settlement, IoT verification, and biometric authentication.

Conclusion

Green Banking – Smart Banking System is proposed as a unified platform for digitizing financial transactions to enhance processing, security, and monitoring. The system links customers, compliance officers, and administrators to a shared, real-time transactional lifecycle. A customer initiates fund transfers and receives settlement status updates, the compliance officer investigates suspicious transactions, and the administrator confirms that total debits equal total credits.

The system's underlying principle is that no transaction is committed unless it undergoes authentication, balance verification, AML screening, and fraud-risk scoring, and all committed transactions are recorded in an immutable double-entry ledger and audit trail. The architecture is modular and extensible to host future services such as blockchain ESG bond tokenization, IoT smart-meter solar verification, CBDC settlement, and satellite-driven sustainable agriculture underwriting.

Nevertheless, the proposals should be subjected to practical tests to demonstrate the

system’s efficacy instead of conjecturing its likely performance. Future evaluations may focus on settlement latency, OTP delivery time, fraud-scoring accuracy, throughput, reliability, scalability.

References

Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. (2025). *Journal of Financial Crime, 32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data, 12*, Article 6. https://doi.org/10.1186/s40537-024-01048-8

Hernandez Aros, L., et al. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications, 11*, Article 1130. https://doi.org/10.1057/s41599-024-03606-0

Thapliyal, K., Gupta, C., Jindal, P., et al. (2025). Measuring the impact of green banking practices on banks' environmental performance and sources of green financing: A study on Indian banks. *Discover Sustainability, 6*, Article 169. https://doi.org/10.1007/s43621-024-00678-5