iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** XI **Month of publication:** November 2025

DOI: https://doi.org/10.22214/ijraset.2025.75761

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

FinSecure: Financial Assistance and Transaction Fraud Detection System

Divya Patil[1], Afreen G D[2], Anusha G S[3], Gousiya Asma I[4], Vidyashree V[5]
[1]*Assistant Professor, Department of CSBS, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India*
[2,3,4,5]*U.G. Students, Department of CSBS, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India*

Abstract: ***The Financial Assistance and Transaction Fraud Detection System is designed to address one of the most critical challenges in today's digital economy ensuring security and transparency in financial transactions. The rapid digitization of financial services has revolutionized the way individuals and organizations manage money, offering ease of access and speed. However, it has also given rise to a surge in sophisticated fraudulent activities, such as fake claims, identity theft, and unauthorized transactions. These issues threaten the reliability of financial systems and lead to significant monetary losses for both institutions and users.***
Keywords: ***Financial Security, Fraud Detection, Secure Authentication, Transaction Monitoring, Fintech System.***

I. INTRODUCTION

In today's digital economy, financial transactions have become faster, easier, and more widespread due to the rapid growth of online banking, e-commerce, and digital payment platforms. However, this convenience also brings increased risks of fraudulent activities such as unauthorized transactions, identity theft, and money laundering. To address these challenges, the Financial Assistance and Transaction Fraud Detection System aims to ensure secure, efficient, and trustworthy financial operations. With the rapid growth of digital banking, ecommerce, and online transactions, financial systems have become more accessible but also more vulnerable to fraud. With the rise of online banking and digital payments, financial frauds such as phishing, fake transactions, and identity theft have increased. The system aims to provide financial assistance by tracking user transactions and offering insights, alerts, or recommendations.

The financial sector plays a vital role in the modern digital economy, where billions of transactions occur daily through online banking, credit cards, and digital payment platforms. As digital transactions continue to grow, so do the risks of fraudulent activities such as phishing, identity theft, and unauthorized access. Hence, the domain of financial assistance and fraud detection has become critically important. This project domain focuses on ensuring the security, reliability, and transparency of financial systems while also helping users manage their finances effectively. Implementing technologies like machine learning, data analytics, and artificial intelligence allows for real time detection of abnormal patterns and prevention of fraud before it causes harm.

II. OBJECTIVES

The primary goals of this project are:

1) To provide real-time financial assistance.
2) To detect and prevent transaction fraud.
3) To ensure data security and privacy.
4) To improve user trust and engagement.
5) To automatically send financial suggestions via email.

III. EXISTING SYSTEM

Most traditional financial systems used by banks and financial institutions rely heavily on rule-based mechanisms and manual oversight to detect fraudulent activities and provide financial assistance. These systems typically operate using predefined rules such as identifying unusually large or frequent transactions that do not adapt to emerging fraud tactics, making them ineffective against evolving threats. Manual verification is often required for suspicious activities or financial assistance approvals, resulting in slower processing, increased operational costs, and the possibility of human error or inconsistencies. Traditional systems also suffer from high false positives and false negatives, where legitimate transactions are flagged as fraud or actual fraud goes undetected, thereby affecting customer trust and system reliability. Another major drawback is the absence of behavioral analysis, as these systems do

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XI Nov 2025- Available at www.ijraset.com

not consider user-specific patterns, transaction context, device information, or spending habits, preventing them from identifying subtle or personalized fraudulent behavior.

The lack of real-time monitoring further causes delays in detecting and responding to fraud, giving fraudsters enough time to complete unauthorized activities before intervention occurs. Additionally, financial assistance models in existing systems rely on generic parameters like income or credit history, ignoring real financial behaviors and individual circumstances, which results in inaccurate eligibility decisions.

These systems also struggle with imbalanced data, since fraudulent transactions form only a small portion of overall activity, making it difficult for models to learn from rare events and leading to missed detections. As the volume of financial transactions increases, legacy systems face scalability issues, resulting in delays, slow processing, and system overload. Moreover, traditional platforms are inflexible and lack the ability to learn from new patterns or update themselves over time, making them ineffective against adaptive fraud strategies. semantic meaning, contextual relevance, or the authenticity of claimed skills. As a result, these systems often overlook essential aspects of candidate capability, such as clarity of communication, relevance of experience, and alignment between job requirements and actual competencies.

IV. PROPOSED SOLUTION

The proposed system is an advanced, intelligent framework designed to enhance the detection of fraudulent financial transactions while also providing tailored financial assistance based on user behavior and risk assessment. Unlike traditional rule based systems, this approach leverages machine learning algorithms such as Decision Trees, Random Forest, XGBoost, and Neural Networks to identify complex fraud patterns within large volumes of transaction data. The system is capable of learning from historical and real time data, allowing it to adapt to evolving fraud techniques and improve its accuracy over time. To address the common issue of class imbalance in fraud datasets where genuine transactions significantly outnumber fraudulent ones techniques like SMOTE (Synthetic Minority Over sampling Technique) and cost sensitive learning are employed. These methods ensure that the model can effectively recognize rare fraud cases without overfitting. Furthermore, the system includes real time processing capabilities using modern stream processing tools, enabling immediate detection and response to suspicious transactions.

V. METHODOLOGY

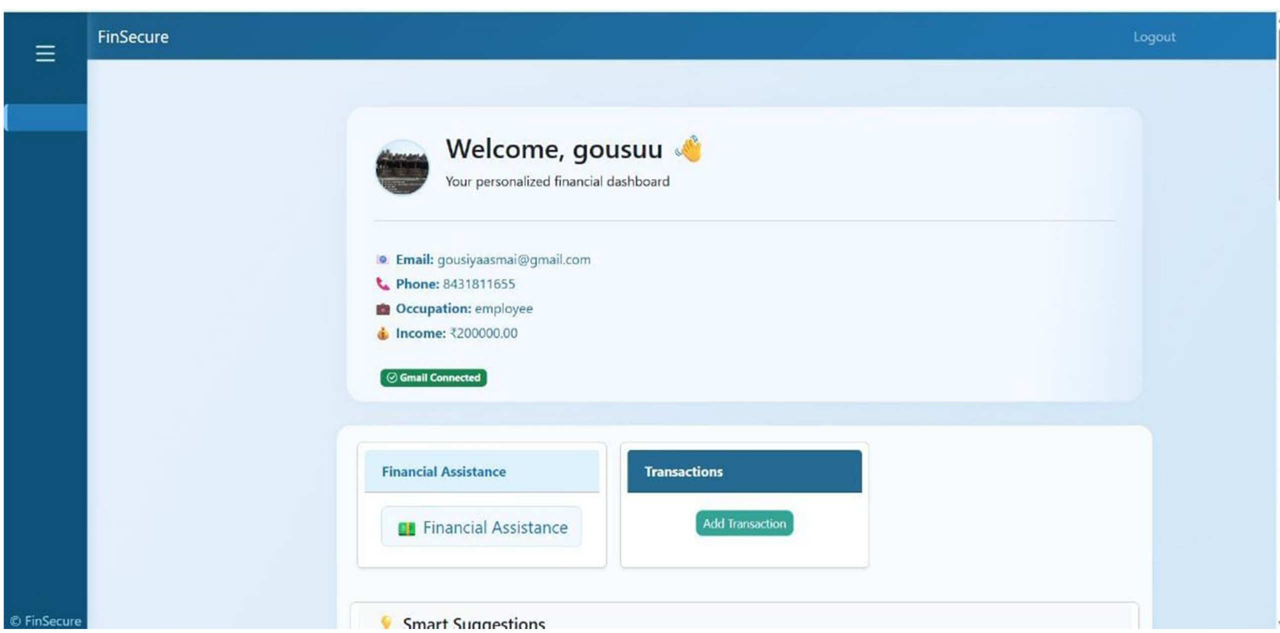
This project integrates machine learning**,** data engineering**,** and financial analytics to build a smart system capable of detecting fraudulent transactions and providing users with personalized financial recommendations. The methodologyconsists of clearly defined phases that ensure the solution is robust, scalable, and adaptable to real world use.

1) Problem Understanding and Requirement Analysis: The project begins by identifying two critical financial challenges: (1) real time fraud detection in financial transactions, and (2) offering intelligent financial assistance through investment or budgeting advice. Stakeholder inputs are gathered to understandexpected features, such as transaction monitoring, investment guidance, alerts, and user profiles.
2) Data Collection: Historical transactional data, user financial profiles, and API-based financial data (mock or real-time) are collected from platforms like Kaggle and simulated user inputs to support both fraud detection and financial assistance prediction.
3) Data Ingestion and Preprocessing: Collected data is passed through an ingestion module where it undergoes cleaning, feature engineering, encoding, normalization, and outlier handling. The processed data is then stored in structured relational or NoSQL databases for model training and real-time use.
4) Model Building: Machine learning models are developed for predicting financial assistance eligibility and identifying fraudulent transactions. The data used for training is cleaned, standardized, encoded, normalized, and enhanced through feature engineering to ensure accurate and reliable predictions.
5) Backend and API Development: APIs are created using frameworks like Flask or FastAPI to connect the machine learning models with the application. These APIs accept input, preprocess data, generate predictions, manage authentication, and maintain logs for monitoring.
6) Frontend / Dashboard Development: A responsive dashboard is built using frameworks such as Streamlit, React, or Angular, enabling secure user login, transaction input, financial detail submission, fraud detection visualization, and investment suggestion display.

7) Model Deployment and Integration: The machine learning models are containerized using Docker and deployed on cloud platforms like AWS, Google Cloud, or Azure. Kubernetes is used to manage scaling and ensure smooth integration of all services including frontend, backend, database, and ML models.

VI. IMPLEMENTATION

1) User Authentication Module: This module handles user registration and login to ensure only authorized individuals can access the system. Users register by providing personal details such as name, email, phone number, and password. During login, the entered credentials are validated with the database, and passwords are stored in encrypted form for security. Once authenticated, users are directed to their personalized dashboard, where they can perform transactions and apply for financial assistance.
2) Transaction Management Module: This module manages the recording, validation, and processing of all financial transactions. Users can carry out activities such as fund transfers, bill payments, and deposits. Every transaction is stored with details like transaction ID, amount, type, and timestamp. The module ensures that transactions are within the user's permitted limits and free from inconsistencies before securely storing them for further analysis.
3) Financial Assistance and Advisory Module: This module evaluates user spending patterns, transaction history, and financial behavior to provide personalized budgeting and saving suggestions.
4) Admin Control Module: This module allows administrators to oversee system operations, manage user accounts, and handle flagged transactions. Admins can track alerts, review suspicious activity, monitor system performance, and maintain overall platform security and efficiency.
5) Email Notification and Alert Module: This module automatically sends alerts and notifications to users using the Gmail API. It informs users immediately when suspicious transactions are detected and delivers financial advice or guidance when required. It also provides real-time updates on transaction status and generates reports related to fraud alerts, user activity, and financial assistance approvals.
6) Reporting and Analytics Module: This module generates detailed reports, visual analytics, and data summaries related to transactions, fraud patterns, and financial behavior. It provides charts, dashboards, and graphs that help both users and administrators interpret complex data easily. Customized reports such as fraud trend analysis, transaction summaries, and financial assistance statistics are created to support decision-making, enhance fraud detection accuracy, and improve financial policies.



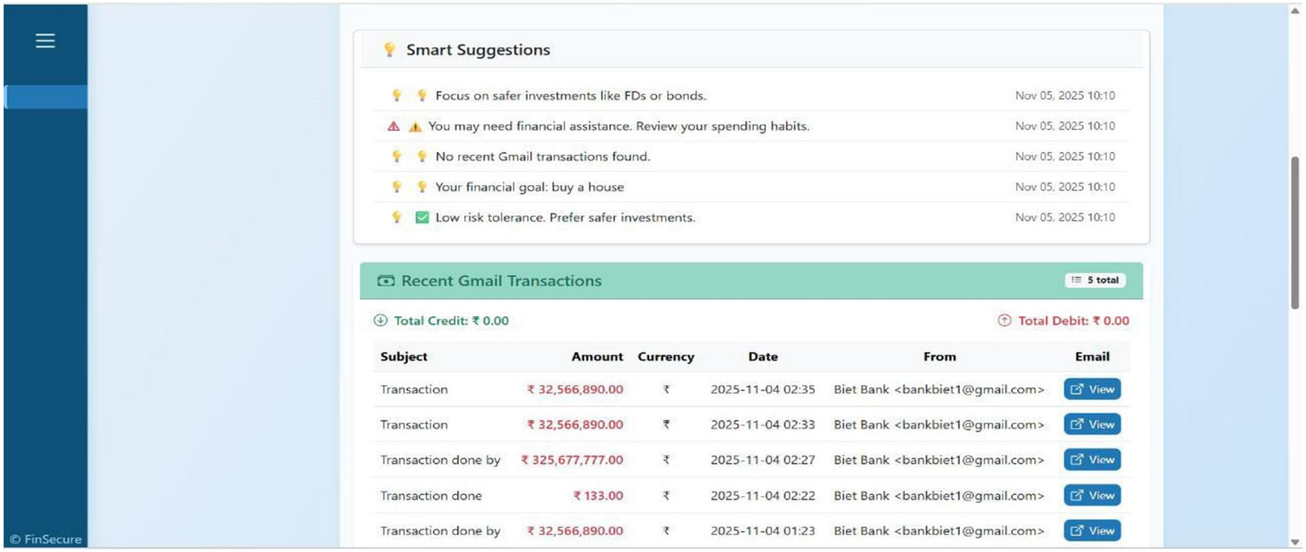


Fig: FinSecure Dashboard

VII. RESULTS

The implementation of FinSecure yielded effective results across authentication, fraud detection, and financial assistance functionalities. The system successfully processed user inputs through the Django web interface and stored data securely in the backend database. The fraud detection module accurately identified suspicious activities based on the machine-learning model, generating timely email alerts whenever anomalies were detected. Transactions classified as safe were processed smoothly, and the financial assistance module provided meaningful spending insights and recommendations by analyzing user transaction history. The dashboard displayed real-time results, including fraud alerts, financial summaries, and user activity history, ensuring clear interactive visualization. Additionally, system testing confirmed stable API communication, fast response times, and consistent model performance, demonstrating that FinSecure effectively enhances both financial security and user awareness.

VIII. CONCLUSION

FinSecure successfully integrates secure authentication, real-time fraud detection, and personalized financial assistance into a single, user-friendly platform. The system addresses major challenges in digital finance by combining machine-learning models, encrypted data handling, and automated alerts to ensure that users receive immediate protection against suspicious activities. At the same time, the financial assistance module enhances user awareness by offering meaningful insights and recommendations based on transaction history. Through systematic design, rigorous testing, and effective module integration, FinSecure demonstrates that financial safety and user guidance can coexist within one intelligent framework. The project ultimately proves that combining security technologies with financial analytics can significantly improve user confidence, reduce fraud risks, and support better financial decision-making

REFERENCES

[1] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637.

[2] Al-dahasi, E. M., Alsheikh, R. K., Khan, F. A., & Jeon, G. (2025). Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation. Expert Systems, 42(2), e13682.

[3] Immadisetty, A. (2025). Real-time fraud detection using streaming data in financial transactions. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), 13(1), 66-76.

[4] Iseal, S., Joseph, O., & Joseph, S. (2025). AI in Financial Services: Using Big Data for Risk Assessment and Fraud Detection.

[5] Kokogho, E., Odio, P. E., Ogunsola, O. Y., & Nwaozomudoh, M. O. (2025). A Cybersecurity framework for fraud detection in financial systems using AI and Microservices. Gulf Journal of Advance Business Research, 3(2), 410-424.

[6] Dayalan, P., & Sundaramurthy, B. (2025). Exploring the Implementation and Challenges of AI-Based Fraud Detection Systems in Financial Institutions: A Review. Creating AI Synergy Through Business Technology Transformation, 25-38.

[7] Islam, M. S., & Rahman, N. (2025). AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study. Journal of Computer Science and Technology Studies, 7(1), 100-112.Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024).

[8] Machine learning approach for fraud detection system in financial institution: A web base application. Machine Learning, 20(4), 01-12

[9] Akash, T. R., Islam, M. S., & Sourav, M. S. A. (2024). Enhancing business security through fraud detection in financial transactions. Global Journal of Engineering and Technology Advances, 21(02), 079-087.
[10] Wu, B., Chao, K. M., & Li, Y. (2024). Heterogeneous graph neural networks for fraud detection and explanation in supply chain finance. Information Systems, 121, 102335.
[11] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences,