AI - Powered Financial Fraud Detection System Using Machine Learning

[1]Mrs. D. Madhuri,[2]Satram Gayatri,[3]Pathan Mohisin Khan,[4]Shaik Afreen

[1]Assistant Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

Real-time fraud detection is crucial since the risk of fraudulent activity has increased dramatically due to the growing amount of digital financial transactions. Financial losses and a decline in user trust result from traditional security methods' frequent inability to recognize intricate and changing fraud schemes. The AI Powered Financial Fraud Detection System project offers a clever web-based method for effectively identifying and stopping illicit financial activity. The system analyzes transaction data and instantly classifies transactions as legitimate or fraudulent by integrating machine learning models, rule-based validation, and secure authentication. The system includes credit card image-based fraud detection in addition to transaction fraud detection, allowing users to use labeled datasets to confirm the legitimacy of credit cards. In order to increase security awareness, fraudulent transactions are promptly banned and users are notified via email. Transaction history management and analytics dashboard with visual data like fraud % and transaction patterns are also features of the program. The suggested system provides a scalable and efficient method of enhancing financial security and preventing fraud by fusing automation, explainable fraud analysis, and user-friendly design.

KEY WORDS: ***Financial Fraud Detection, Machine Learning, Transaction Analysis, Fraud Prediction, Flask Web Application, Python, Transaction History, Real-Time Fraud Detection***

INTRODUCTION

Financial transactions are now quicker and easier because to the quick expansion of digital banking and online financial services, but there is a greater chance of fraud. Financial fraud is a major problem for people and organizations since it can result in financial losses, security lapses, and a decline in user confidence. Intelligent solutions that can identify and stop fraud in real time are becoming more and more necessary as transaction volumes continue to rise. Conventional fraud detection

techniques frequently depend on manual verification or set rules, which are inadequate to recognize intricate and dynamic fraud patterns. Machine learning-based methods have become popular as efficient ways to analyze transaction behavior and spot suspect activity in order to overcome these constraints. Financial risks are increased by credit card misuse and duplication in addition to transaction-based fraud, underscoring the necessity of thorough fraud detection systems. The goal of this project, AI Powered Financial Fraud Detection System, is to offer a smart and safe platform that combines rule-based validation, machine learning models, and contemporary online technologies. The technology stops questionable activity, identifies fraudulent transactions, and notifies users via email. It also has analytical dashboards to improve decision-making and transparency, transaction history management, and credit card image-based fraud detection. The suggested system provides a workable and expandable way to enhance financial security in contemporary digital settings.

LITERATURE SURVEY

In a comprehensive study on the use of machine learning approaches for financial fraud detection, Dal Pozzolo et al. (2018) shown how conventional rule-based systems find it difficult to adjust to changing fraud trends. Their research highlights how supervised learning models, like Decision Trees, Logistic Regression, and ensemble techniques, may detect fraudulent transactions more accurately and with fewer false positives. Bhattacharyya et al. (2011) examined datasets of actual credit card transactions and showed how dynamic fraud behavior and data imbalance provide serious problems for fraud detection systems. In order to improve detection reliability and interpretability, especially in financial areas where transparency is crucial, the study emphasizes the need of integrating rule-based validation with machine learning models. In their analysis of recent developments in fraud detection, Carcillo et al. (2021) emphasized the expanding significance of explainable AI and real-time analytics in contemporary financial systems. Their study emphasizes the necessity of systems that not only reliably identify fraud but also give users and analysts understandable reasons.

RELATED WORK

The growing significance of automation, real-time analysis, and intelligent decision-making to improve security and lower financial losses is highlighted by recent research in financial fraud detection systems. According to studies, conventional fraud detection techniques are

frequently ineffective at managing high transaction volumes and adjusting to changing fraud trends because they mostly rely on static rules and manual verification. Higher false positive rates and delayed reactions are the results of these restrictions. Fraud detection systems are becoming more precise and scalable because to the development of machine learning algorithms. By recognizing trends in past data, researchers have shown that supervised learning models like Random Forests, Decision Trees, and Logistic Regression are useful for spotting fraudulent transactions. By enforcing domain-specific requirements like balance consistency and transaction feasibility, combining these models with rule-based validation increases reliability.

Additionally, recent advancements highlight how crucial real-time monitoring and alert systems are to preventing fraud. Instant alerts and automated blocking of questionable transactions have been shown to drastically shorten response times and lessen possible harm. Additionally, keeping track of transaction history and analytics dashboards facilitates informed decision-making and improves comprehension of fraud tendencies. In order to improve fraud detection beyond transaction data alone, new methods have also investigated the integration of picture-based verification techniques, such as credit card image analysis. By providing explainable outcomes and visual confirmation, these solutions increase transparency and user trust. Building on these developments, the suggested solution combines analytics, rule-based logic, machine learning, and real-time alerts into a single, safe, and user-friendly platform for financial fraud detection.

EXISTING METHOD

Static rule-based mechanisms and human verification procedures are the main methods used in traditional financial systems to identify fraud. These techniques rely on pre-established guidelines, including set transaction limits or straightforward threshold checks, which are unable to adjust to changing fraud trends. Manual monitoring becomes ineffective and time-consuming when transaction volumes rise, which frequently causes fraud detection to be delayed.

The majority of current systems rely on post-transaction analysis and centralized processing, which means that fraudulent activity is only discovered after a financial loss has taken place. System performance may deteriorate at times of high transaction volume, such as online sales or busy banking hours, raising the possibility of fraud going unnoticed. These algorithms also produce a lot of false positives, which result in needless transaction blockages and

a bad user experience. Additionally, traditional methods lack precise analytical insights and real-time alert mechanisms, which makes it challenging for users to comprehend the causes behind fraud or react quickly. Transparency and trust are diminished in the absence of sophisticated analytics and results that can be explained. All things considered, current fraud detection techniques fall short of offering precise, scalable, and instantaneous defense against contemporary financial fraud risks.

PROPOSED METHOD

The suggested solution uses an AI-driven and rule-based hybrid method for real-time financial fraud detection in order to get beyond the drawbacks of conventional fraud detection systems. To effectively and precisely evaluate transaction data, the system combines machine learning models with balance consistency validation procedures. This integrated strategy lowers false positives while enabling early detection of fraudulent activity. The system first uses rule-based validation when a user submits transaction information to look for irregularities including negative balances, inaccurate balance updates, or inadequate balances. After passing these checks, the transaction is classified as authentic or fraudulent using trained machine learning models, such as Random Forest, Decision Tree, and Logistic Regression. If fraud is found, the transaction is blocked right away, and the user is notified via email. The system has a credit card image fraud detection module in addition to transaction analysis. This module compares uploaded credit card photos to a labeled dataset of authentic and fraudulent cards. The outcome is shown promptly to help users confirm the legitimacy of their cards. Additionally, the system keeps track of transaction history and offers an analytics dashboard that shows transaction statistics and fraud tendencies. This strategy guarantees a scalable, safe, and easy-to-use solution for preventing contemporary financial fraud.

SYSTEM ARCHITECTURE:

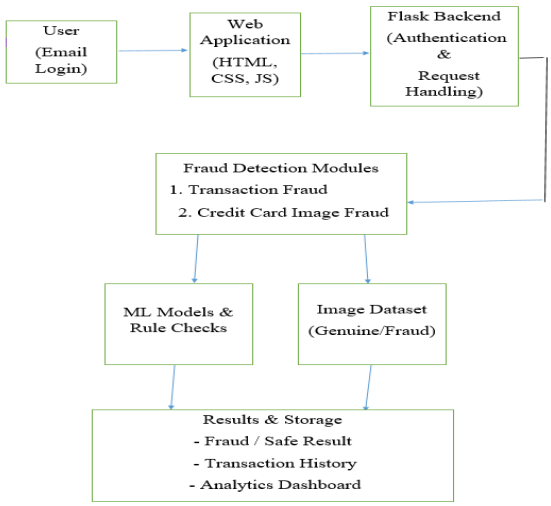


Fig 1: Block Diagram

METHODOLOGY DESCRIPTION

USERS

The system involves a primary user Authenticated Users (Customers/Account

Holders).

Users securely log in using email-based authentication and can access different fraud detection modules. They analyze transactions, verify credit card authenticity, view transaction history, and monitor fraud analytics through the dashboard.

FRONTEND

The frontend is developed using HTML, CSS, and JavaScript, providing a responsive and user-friendly interface. It allows users to:

- Log in securely
- Enter transaction details
- Upload credit card images
- View fraud detection results
- Access transaction history and analytics dashboards

The interface is designed to ensure clarity, ease of use, and real-time feedback.

BACKEND

The backend acts as the core processing unit and is implemented using Python with Flask.

It handles:

- User authentication and session management
- Transaction validation and fraud detection logic
- Integration of machine learning models
- Credit card image verification
- Email alert generation for fraudulent transactions
- Communication between frontend and data storage

RESTful routes are used to process user requests efficiently.

MACHINE LEARNING MODULE

The system uses trained machine learning models such as Logistic Regression, Decision Tree, and Random Forest to classify transactions as genuine or fraudulent. These models are applied after rule-based validation to improve accuracy and reduce false positives. Models are stored and loaded using Joblib for fast inference.

DATA STORAGE

Lightweight data storage using JSON and CSV files is employed to store:

- User credentials
- Transaction history
- Fraud detection results
- Credit card image mappings

This approach ensures simplicity, fast access, and easy maintenance.

EMAIL ALERT SERVICE

An email notification service is integrated to enhance security awareness. Whenever a fraudulent transaction is detected, an automatic email alert is sent to the user, notifying them about the blocked transaction.

ANALYTICS & DASHBOARD

The system includes an analytics dashboard that visualizes fraud-related data such as:

- Total transactions
- Fraud vs safe transactions
- Fraud percentage
- Transaction type distribution

These insights help users understand fraud patterns and system performance.

RESULTS AND DISCUSSIONS:

Fig 2: Dashboard

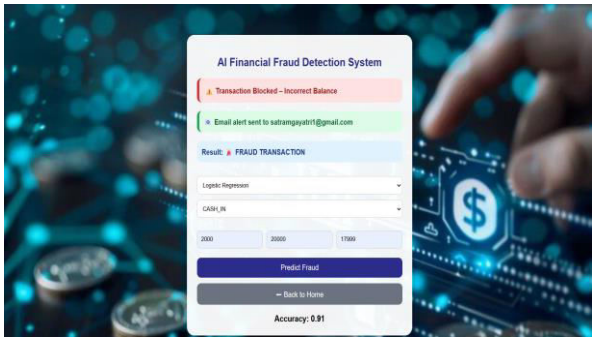


Fig 3: Financial Fraud Detection Page

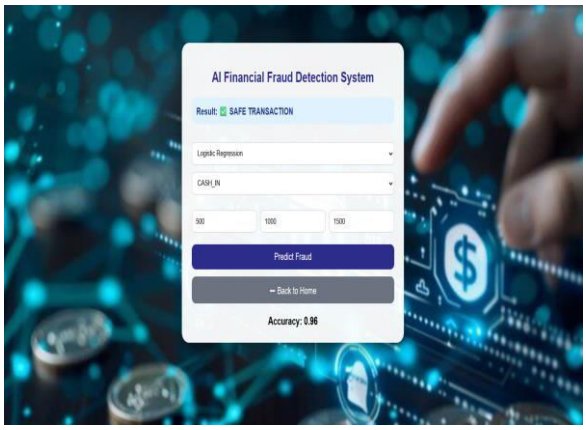


Fig 4: Financial Safe Transaction Page

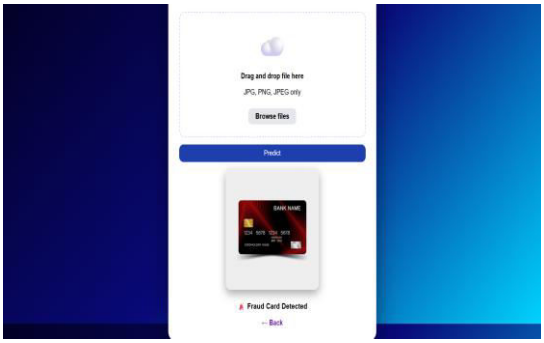


Fig 5: Credit Card Image Fraud Detection

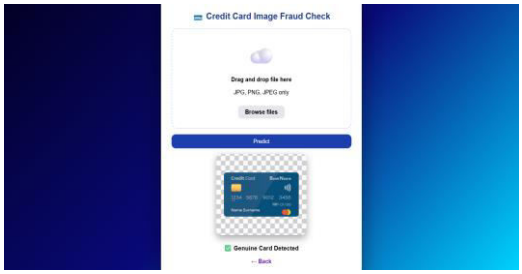
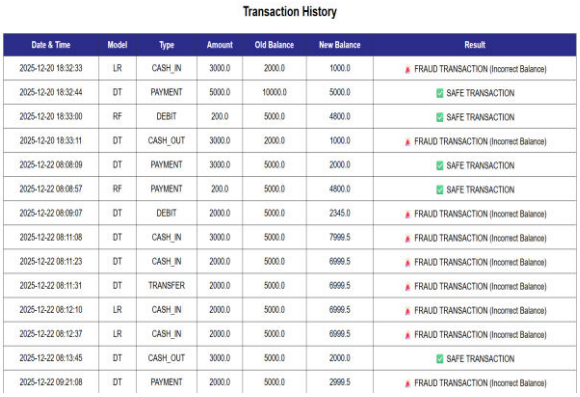


Fig 6: Credit Card Image Safe Detection



Transaction History

Date & Time	Model	Type	Amount	Old Balance	New Balance	Result
2025-12-20 18:32:33	LR	CASH_IN	3000.0	2000.0	1000.0	FRAUD TRANSACTION (Incorrect Balance)
2025-12-20 18:32:44	DT	PAYMENT	5000.0	10000.0	5000.0	SAFE TRANSACTION
2025-12-20 18:33:00	RF	DEBIT	200.0	5000.0	4800.0	SAFE TRANSACTION
2025-12-20 18:33:11	DT	CASH_OUT	3000.0	2000.0	1000.0	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:08:09	DT	PAYMENT	3000.0	5000.0	2000.0	SAFE TRANSACTION
2025-12-22 08:08:57	RF	PAYMENT	200.0	5000.0	4800.0	SAFE TRANSACTION
2025-12-22 08:09:07	DT	DEBIT	2000.0	5000.0	2345.0	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:11:08	DT	CASH_IN	3000.0	5000.0	7999.5	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:11:23	DT	CASH_IN	2000.0	5000.0	6999.5	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:11:31	DT	TRANSFER	2000.0	5000.0	6999.5	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:12:10	LR	CASH_IN	2000.0	5000.0	6999.5	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:12:37	LR	CASH_IN	2000.0	5000.0	6999.5	FRAUD TRANSACTION (Incorrect Balance)
2025-12-22 08:13:45	DT	CASH_OUT	3000.0	5000.0	2000.0	SAFE TRANSACTION
2025-12-22 09:21:08	DT	PAYMENT	2000.0	5000.0	2999.5	FRAUD TRANSACTION (Incorrect Balance)

Fig 7: Transaction History Page

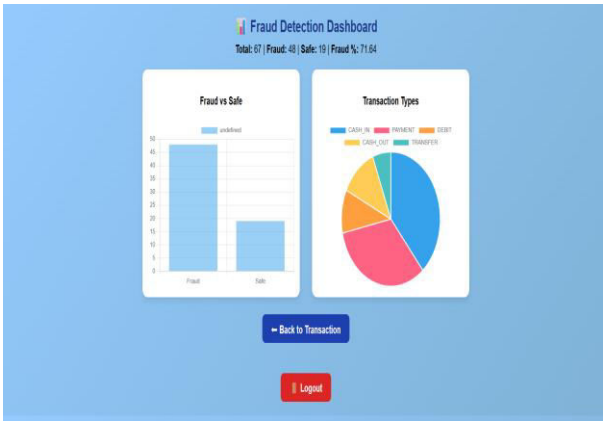


Fig 8: Financial Fraud Detection Dashboard

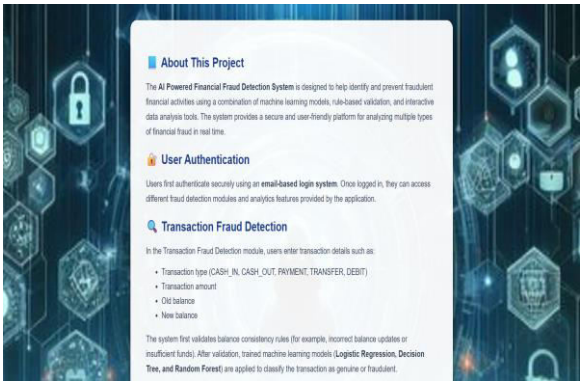


Fig 10: About Project Page

CONCLUSION AND FUTURE ENHANCEMENTS:

Using machine learning and rule-based validation approaches, the AI Powered Financial Fraud Detection System offers a safe and efficient way to spot fraudulent financial activity. Through various modules, including transaction fraud detection and credit card image fraud detection, the system allows users to safely authenticate and evaluate transactions. The system correctly identifies transactions as authentic or fraudulent by applying trained machine learning models and verifying balance consistency requirements. The platform is dependable and easy to use thanks to extra features like transaction history tracking and a fraud analytics dashboard, which provide transparency, improved monitoring, and insightful information. The system can be improved in the future by adding sophisticated deep learning models to increase the accuracy of fraud detection on massive, real-time datasets. Practical usefulness can be further strengthened by integration with real-time transaction streams and live financial APIs. CNN-based image recognition methods can be used to enhance the credit card image fraud module. Multi-factor authentication can improve security, and cloud deployment can be customized to meet real-world financial situations and improved scalability.

REFERENCES

1. Kesavulu, O. S. C., & Harini, P. (2013). Enhanced packet delivery techniques using crypto-logic riddle on jamming attacks for wireless communication medium. *Int. J. Latest Trends Eng. Technol*, *2*(4), 469-478.
2. Carcillo, F., Dal Pozzolo, A., Bontempi, G., Scarff: A scalable framework for streaming credit card fraud detection, Information Fusion, Elsevier, 2021.
1. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N., Transaction aggregation as a strategy for credit card fraud detection, Data Mining and Knowledge Discovery, Springer, 2009.
2. Phua, C., Lee, V., Smith, K., & Gayler, R., A comprehensive survey of data mining-based fraud detection research, arXiv preprint arXiv:1009.6119, 2010.
3. Bolton, R. J., & Hand, D. J., Statistical fraud detection: A review, Statistical Science, Institute of Mathematical Statistics, 2002.
4. Bahnsen, A. C., Aouada, D., & Ottersten, B., Cost-sensitive decision trees for fraud detection, Expert

Systems with Applications, Elsevier, 2015.

5. Dal Pozzolo, A., Bontempi, G., Adaptive machine learning for credit card fraud detection, IEEE Symposium Series on Computational Intelligence, 2015.
6. Kaggle, Credit Card Fraud Detection Dataset, Kaggle Inc., 2016.
7. Goodfellow, I., Bengio, Y., & Courville, A., Deep Learning, MIT Press, 2016.
8. Han, J., Kamber, M., & Pei, J., Data Mining: Concepts and Techniques, Morgan Kaufmann, 2012.
9. Aggarwal, C. C., Outlier Analysis, Springer, 2017.
10. Chandola, V., Banerjee, A., & Kumar, V., Anomaly detection: A survey, ACM Computing Surveys, 2009.
11. Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K., Credit card fraud detection using AdaBoost and majority voting, IEEE Access, 2018.
12. Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F., Using generative adversarial networks for improving classification effectiveness in credit card fraud detection, Information Sciences, Elsevier, 2019.
13. Juszczak, P., Adams, N., Hand, D. J., Whitrow, C., & Weston, D., Off-the-peg and bespoke classifiers for fraud detection, Computational Statistics & Data Analysis, Elsevier, 2008.