International Research Journal of Education and Technology

Peer Reviewed Journal, **ISSN: 2581-7795**

ANTI-FRAUD MEASURES IN BANKING SYSTEM

DR.S.SUBASHREE[1],ROSHINI A[2],SANDHIYA N[3], SIVASANKARI M[4]

[1]Project Supervisor, Assistant Professor,

[2,3,4] Final Year Student

[1,2,3,4] Department of Computer Science and Engineering,

[1,2,3,4] E.G.S. PILLAY ENGINEERING COLLEGE, Nagapattinam, India

Abstract -Digital transactions and online banking are widely used, but fraud activities have increased. This project focuses on using Artificial Intelligence (AI) and Machine Learning (ML) techniques to detect and prevent fraud in financial transactions. By analyzing transaction data and identifying unusual patterns, the system provides real-time alerts and reduces fraudulent activities. The report covers techniques such as supervised learning, unsupervised learning, deep learning, and natural language processing (NLP), along with their applications, benefits, and challenges.. Python is employed for analysis, emphasizing the ability of deep learning to manage and prevent fraud in real-time on dynamic datasets. In the end, this study concludes that by using deep learning algorithms, we can control online credit card fraud detection in banks, in this project efficency to improve the efficiency of the banking system. We can manage fraudulent activity in real-time and on dynamic datasets by utilizing deep learning algorithms, which allows for ongoing improvement of the fraud detection and prevention system.

I. INTRODUCTION

Fraud is a major threat to financial institutions, businesses, and customers. Traditional methods struggle to detect complex fraud patterns. AI-based systems provide solutions by analyzing large datasets and identifying suspicious behavior in real time. This project aims to build a machine learning model that helps detect fraud in credit card transactions, banking systems, and e-commerce platforms. The system will assist organizations to protect customer information and ensure trust in digital transactions.Detecting banking fraud presents a set of complex challenges for financial institutions . One of the primary challenges is the evolving nature of fraudulent methods. Fraudsters develop new methods to exploit vulnerabilities in the system, making it difficult for traditional rule-based systems to keep up. The sheer volume of transactions and data processed by banks further complicates the task. Manual analysis is time-consuming and often ineffective in identifying subtle patterns and anomalies indicative of fraud. Additionally, the need to balance fraud detection with customer convenience is a delicate task; overly strict securitymeasures can lead to false positives and inconvenience legitimate customers, potentially driving them away.

II. PROPOSED SYSTEM

2.1 Support Vector Machine

SVM works by mapping data to a high-dimensional feature space so that data points can be categorized, even when the data are not otherwise linearly separable. A separator between the categories is found, then the data are transformed in such a way that the separator could be drawn as a hyperplane Training regression model and finding out the best one.

Random Forest Classifier

Features are cheekbone to jaw width, width to upper facial height ratio, perimeter to area ratio, eye size, lower face to face height ratio, face width to lower face heightratio and mean of eyebrow height. The extracted features are normalized and finally subjected to support regression.

Decision Tree

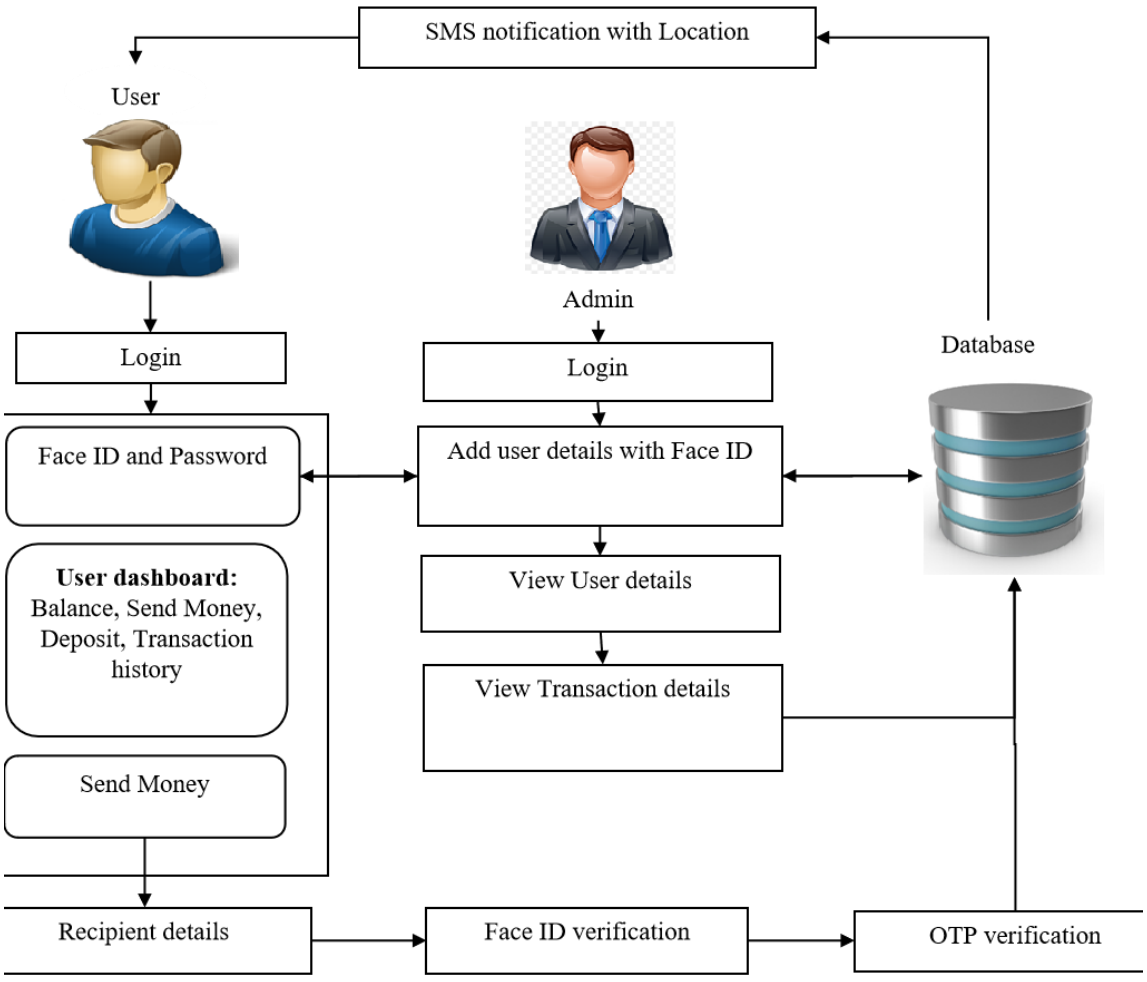
A decision tree is a type of supervised machine learning used to categorize or make predictions based on how a previous set of questions were answered. The model is a formofsupervised learning, meaning that the model is trained and tested on a set of data that contains the desired categorization.

2.2 Working of proposed system

A modern banking system is designed as a secure, integrated platform that manages customer accounts, transactions, and financial services while ensuring trust and compliance. At its core, the system provides facilities for deposits, withdrawals, transfers, and loan processing, supported by digital channels such as mobile applications, web portals, and ATMs. To safeguard operations, anti-fraud measures are embedded throughout the architecture. Multi-factor authentication and biometric verification protect customer access, while real-time transaction monitoring powered by machine learning detects unusual pattern s such as rapid transfers, abnormal geolocation activity, or suspicious spending behavior. Data security is reinforced through encryption and tokenization of sensitive information, ensuring that account numbers and personal details remain protected. Compliance with

regulatory frameworks like KYC and AML further strengthens defenses by verifying customer identities and monitoring for money-laundering risks. In addition, customers receive instant alerts for transactions, enabling them to quickly identify unauthorized activity, and banks employ strict employee access controls to prevent insider threats. Together, these layered mechanisms create a resilient banking environment that balances convenience with robust fraud prevention.

III. SYSTEM ARCHITECTURE



3.1Components Used in the Proposed System

1. **User Interface Layer**

- Mobile app, web portal, and ATM interface.

- Provides customers with secure access to accounts and services.
- Includes intuitive dashboards, transaction history, and notifications.
-

2. **Application Layer**

- **Core Banking Module**: Handles deposits, withdrawals, transfers, loans, and account management.
- **Transaction Processing Engine**: Executes and validates transactions in real time.
- **Customer Service Module**: Chatbots, helpdesk, and support ticketing.

3. **Security & Anti-Fraud Layer**

- **Authentication System**: Multi-factor authentication, biometrics, device binding.
- **Fraud Detection Engine**: AI/ML models for anomaly detection, rule-based checks, velocity monitoring.
- **Alert & Response System**: Instant SMS/email/push notifications for suspicious activity.
- **Access Control**: Role-based permissions for employees, insider threat monitoring.

4. **Compliance & Risk Management Layer**

- **KYC (Know Your Customer)**: Customer identity verification.
- **AML (Anti-Money Laundering)**: Monitoring transactions for suspicious activity.
- **Audit & Reporting**: Generates compliance reports and logs for regulators.

5. **Data Management Layer**

- **Database System**: Secure storage of customer and transaction data.
- **Encryption & Tokenization**: Protects sensitive information like account numbers.
- **Analytics Module**: Provides insights into customer behavior and fraud trends.

6. **Integration Layer**

- **API Gateway**: Secure APIs for third-party services (payment gateways, credit bureaus).
- **External Systems**: Integration with UPI, SWIFT, and other financial networks.

7. **Infrastructure Layer**

- **Cloud/On-Premise Servers**: Scalable hosting environment.
- **Backup & Recovery**: Disaster recovery and business continuity planning.
- **Monitoring Tools**: System health checks, performance monitoring.

IV. EXISTING SYSTEM

Current digital payment apps (UPI, wallets, banking apps) mainly depend on PIN / Password based loginOTP (One-Time Password) authentication Passwords are vulnerable to hacking, guessing, or malware attacks.Fraudsters can perform unauthorized transactions once OTP/PIN is compromised.No location tracking users cannot know where the transaction actually occurred.Limited fraud detection features system reacts only after fraud happens, not before Since the credit card fraud detection system is a highly researched field, thereare many different algorithms and techniques for performing the credit card fraud detection system. One of the earliest systems is CCFD system using Markov model. Some other various existing algorithms used in the credit cards fraud detection system includes Cost sensitivedecision Treecard fraud detection system using neural network follows the whale swarmoptimizationalgorithm to obtain an incentive value. It the uses BP network to rectify the values which are found error.

V. METHODOLOGY

First the Dataset is read. Exploratory Data Analysis is performed on the dataset to clearly understand the statistics of the data, Feature selection is used, A machine learning model is developed. Train and test the model and analysis the performance of the model using certainevaluation techniques such as accuracy, confusion matrix, precision etc.

VI. CONCLUSION

The AI-based fraud detection system successfully identifies fraudulent transactions with high accuracy. The use of machine learning algorithms enhances security in online transactions. Real-time alerts and predictive analytics provide users and organizations with tools to prevent fraud before significant damage occurs. While data privacy and interpretability challenges exist, proper security protocols and explainable AI techniques can address these concerns.To improve overall performance, autoencoders can be used in conjunction with other fraud detection strategies. For instance, to develop a complete fraud detection solution, rule-based systems, machine learning classifiers, or network analysis algorithms can be combined with anomaly detection utilizing autoencoders. It is feasible to create a fraud detection system using a deep learning strategy, and it is possible to minimize the work required to manually label a dataset using both supervised and unsupervised learning approaches. During the model update, there is a possibility to integrate the identification of novel fraud types. The method for updating the model relies on the amount of labelled data. In our research work we use Python for the analysis purpose to boost the efficiency of the business organization. Hence, in the end, we conclude that deep learning with business intelligence offers feasible explanations for the various business domains, and by using artificial intelligence with deep learning in business intelligence, we can achieve our targets more efficiently

REFERENCES

1. F.K.Alarfaj ,S.Shahzadi "Enhancing Fraud Detection in Banking With Deep Learning: Graph Neural Networks and Autoencoders for Real- Time Credit Card Fraud Prevention by 23 Sep 2024 .

2. Dimpal U. Chavan, Brijendra Gupta in AI-Based Banking Security System using Face and Liveness Detection using ML & Image Processing by 2024.

3. S. Sruthi, S. Emadaboina, and C. Jyotsna, "Enhancing credit card fraud detection with light gradient-boosting machine: An advanced machine learning approach," in *Proc. Int. Conf.* Knowledge Eng. Commun. Syst. (ICKECS), IEEE, 2024.

4. X. Yu, M. Zhou, G. Liu, L. Wei, H. Zhu, and P. De Meo, "A transactional-behavior-based hierarchical

gated network for credit card fraud detection,"IEEE/CAA J. Automatica Sinica, vol. 12, no. 7, pp. 1–15, 2025.

5. S. Islam, G. R. Gupta, A. Chakraborty, et al., "Detecting fraudulent transactions for different patterns in financial networks using layer weighted GCN," SN Computer Science, vol. 6, no. 2, pp. 1–10, 2025.

ONLINE RESOURCES:

1. Reserve Bank of India (RBI), "Fraud risk management and monitoring framework," 2024. https://www.rbi.org.in

2. Organisation for Economic Co-operation and Development (OECD), "Financial crime and fraud prevention in banking," 2021.https://www.oecd.org/finance

3. World Bank, "Financial sector integrity and anti-fraud measures," 2023. [Online]. Available: https://www.worldbank.org/en/topic/financialsector

4. PwC, "Global economic crime and fraud survey," 2022. https://www.pwc.com/fraudsurvey