Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com

AI-Powered Financial Fraud Detection System Using Machine Learning and Predictive Analytics for Real-Time Transaction Monitoring & Risk Prevention

[1]S Illiyaz, [2]J Prathyusha, [3]C Venkatesh, [4]S Premsagar, [5]P Vishal Karthik, [6]T Srikanth

[1,2,3,4,5,6]Department of Computer Science Engineering (Data Science), GATES Institute of Technology, Gooty, Andhra Pradesh, India
E-mails: [1]illiyaz@gmail.com, [2]jangamreddyprathu@gmail.com, [3]venkeyvasu32@gmail.com, [4]premsagar@gmail.com, [5]vishalkarthik@gmail.com, [6]srikanth@gmail.com

Abstract: Fraudulent activities in financial transactions pose significant challenges to businesses and consumers alike, leading to substantial financial losses and eroding trust in digital payment systems. This project presents a comprehensive machine learning framework aimed at real-time fraud detection and prevention in transactions. The framework leverages advanced algorithms and large datasets to identify fraudulent behaviours with high accuracy and minimal false positives. The methodology begins with the collection and preprocessing of transaction data, which includes user profiles, transaction histories, and contextual features such as time. A range of classification algorithms including logistic regression, decision trees, random forests, are employed to build predictive models. The performance of these models is evaluated using key metrics such as accuracy, precision, recall and F1 score, ensuring a robust assessment of their effectiveness.

Keywords: Financial Fraud Detection, Machine Learning, Predictive Analytics, Risk Monitoring, Artificial Intelligence.

I. INTRODUCTION

The rapid growth of digital payment systems has revolutionized the way businesses and consumers interact, enabling seamless transactions across various platforms such as e-commerce sites, mobile wallets, and online banking. With digital payment adoption skyrocketing, traditional methods of handling cash and checks are being replaced by more efficient, convenient, and faster alternatives. As a result, online transactions have become an integral part of the global economy, offering a range of benefits, including speed, convenience, and broader access to financial services. However, alongside these advantages, the rise of digital payments has also introduced new challenges. Fraudulent activities targeting digital payment systems have become increasingly sophisticated, with cybercriminals finding novel ways to exploit vulnerabilities in online platforms. The financial losses attributed to fraud are staggering, affecting consumers, businesses, and financial institutions alike. From card- not-present fraud to identity theft and account takeover, the variety of fraudulent activities presents a significant threat to both the integrity of digital payment systems and consumer trust. To combat this ever-evolving threat, businesses are turning to artificial intelligence (AI) and machine learning (ML) technologies. AI- driven fraud detection systems leverage advanced algorithms that can analyze vast amounts of transactional data in real-time, enabling the identification of potentially fraudulent behavior before it results in significant financial loss. Unlike traditional rule-based systems, which rely on predefined patterns, AI-powered solutions have the ability to adapt and learn from new data, improving their accuracy and effectiveness over time. In this context, machine learning has emerged as a game-changer in the fight against digital payment fraud. By leveraging data- driven insights and predictive analytics, machine learning models can continuously assess transaction risk, detect anomalous patterns, and provide immediate alerts when suspicious activity is detected. This enables businesses to take timely actions to prevent fraud, minimize damage, and protect their customers' financial security. This paper will explore how AI and machine learning are transforming fraud detection in digital payment systems, highlighting the potential of real-time risk assessment and the benefits of automated fraud prevention.

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com

II. RELATED WORK

Several researchers have proposed different techniques to detect financial fraud using machine learning and artificial intelligence.

Several studies have used Logistic Regression and Decision Tree algorithms to detect credit card fraud by analyzing transaction patterns. These models provide basic classification of fraudulent and non-fraudulent transactions.

Researchers have also applied Random Forest and Support Vector Machine (SVM) algorithms to improve fraud detection accuracy. These models can handle large datasets and identify complex patterns.

Deep learning techniques such as Artificial Neural Networks (ANN) and Convolutional Neural Networks (CNN) have been used to detect fraud in real-time transaction systems.

Some researchers proposed behavior-based fraud detection systems, which analyze user behavior such as transaction location, spending patterns, and device information.

Although these approaches have improved fraud detection, challenges still remain such as high false positive rates and slow detection speed. Therefore, an advanced system using predictive analytics and real- time monitoring is required.

Despite these advancements, many systems lack real- time monitoring and easy-to-use interfaces. The proposed system aims to address these limitations by combining machine learning algorithms with an interactive web-based platform.

III. PROPOSED SYSTEM

The proposed system introduces an intelligent financial fraud detection mechanism that uses machine learning and predictive analytics to monitor financial transactions and identify suspicious activities. Unlike traditional rule-based systems, the proposed system analyzes large amounts of financial data and automatically detects unusual patterns that may indicate fraud. This approach improves the efficiency and accuracy of fraud detection in financial institutions.

The system is designed as a web-based application that allows users to upload financial datasets and analyze them using machine learning algorithms. The system first collects financial data such as revenue, net income, earnings per share (EPS), credit risk score, and operational risk score. These financial parameters are important indicators of a company's financial condition and help the system understand potential risk levels.

After receiving the dataset, the system performs data preprocessing to clean and organize the data. This process includes removing missing values, correcting inconsistent entries, and converting the data into a structured format suitable for machine learning analysis. Data preprocessing ensures that the model receives accurate and high-quality information, which improves prediction performance.

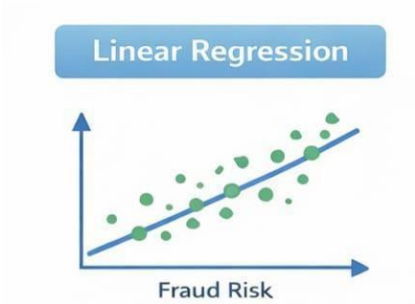
The next stage involves feature extraction, where significant attributes are selected from the dataset. These features represent important financial indicators that influence fraud detection. By focusing on the most relevant features, the machine learning model can learn patterns more effectively and detect abnormal financial behavior.

Linear Regression Model

Linear Regression is a supervised machine learning algorithm used to predict numerical values by identifying the relationship between input variables and an output variable. In the financial fraud detection system, linear regression analyzes financial parameters such as

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com

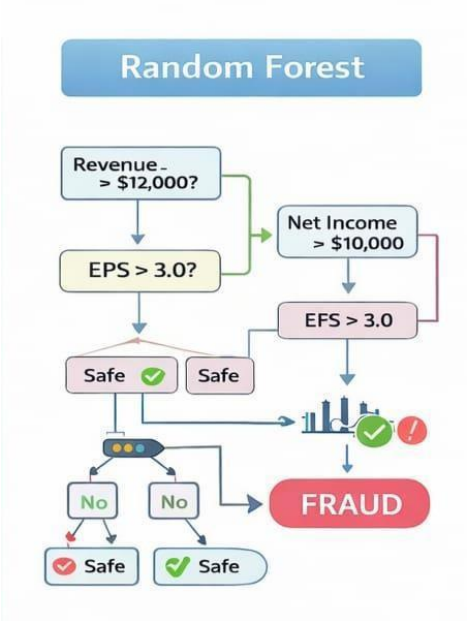
revenue, net income, and earnings per share (EPS) to estimate the potential risk level of a transaction or financial record. The algorithm fits a straight line to the dataset and calculates coefficients for each feature to predict the output value. By analyzing the relationship between financial indicators and risk scores, the model can identify abnormal financial patterns that may indicate fraudulent behavior.



Features	Revenue	Net Income
$10,000	$15,000	$8,000
$10,000	$15,000	$4,000
$15,000	$11,000	$4,000

Random Forest Model

Random Forest is an ensemble machine learning algorithm that improves prediction accuracy by combining multiple decision trees. Each tree is trained on a random subset of the dataset and makes its own prediction about whether a transaction is safe or fraudulent. The final result is determined by combining the predictions of all trees using a majority voting method.

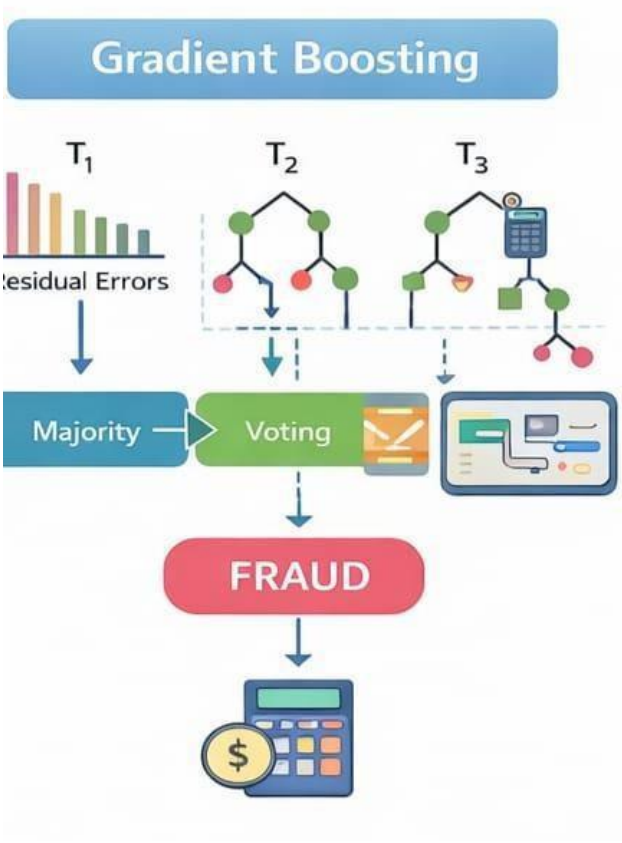


Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com

In the proposed financial fraud detection system, Random Forest analyzes various financial features such as revenue changes, income patterns, and risk scores to detect suspicious financial activities.This algorithm is effective because it can handle large datasets and capture complex relationships between financial variables.

Gradient Boosting Model

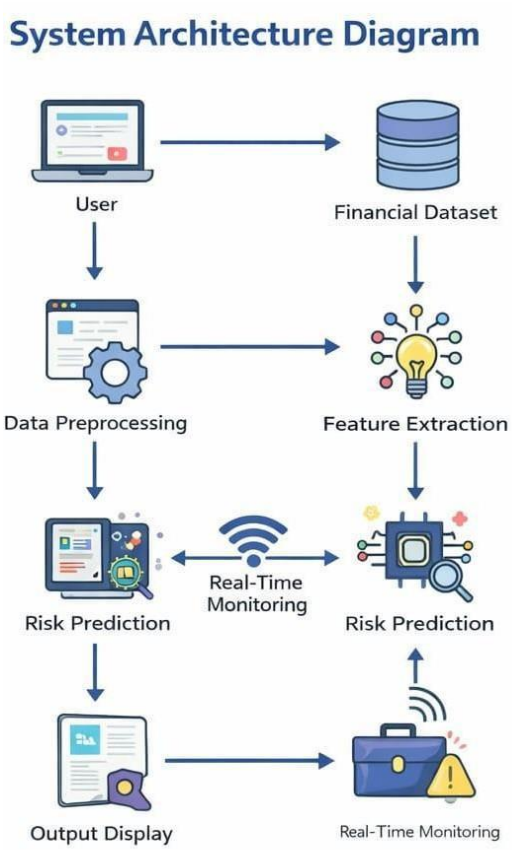
Gradient Boosting is an advanced ensemble machine learning technique that builds prediction models sequentially. Unlike Random Forest, where trees work independently, Gradient Boosting creates each new decision tree to correct the errors made by previous trees. The algorithm gradually improves prediction accuracy by minimizing the difference between actual and predicted values. In the financial fraud detection system, Gradient Boosting analyzes financial datasets and continuously refines its predictions to detect subtle fraud patterns. This approach helps identify complex and hidden relationships in financial data, making it highly effective for detecting fraudulent activities.



SoftMax classifier

The System Architecture Diagram represents the overall structure and working process of the AI- powered financial fraud detection system. It illustrates how financial data flows through different components of the system to identify potential fraud risks. The architecture begins with the user interface, where the user uploads financial datasets or manually enters financial information such as revenue, net income, earnings per share (EPS), credit risk score, and operational risk score. These inputs act as the primary data source for the system.

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com



IV. RESULTS

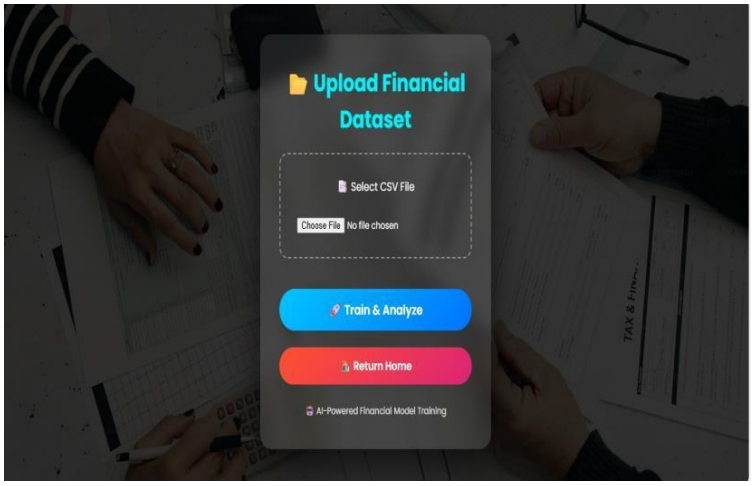
The proposed AI-Powered Financial Fraud Detection System was successfully implemented using machine learning algorithms such as Linear Regression, Random Forest, and Gradient Boosting to analyze financial datasets and predict fraud risk levels. The system was tested using financial data containing parameters like revenue, net income, earnings per share (EPS), credit risk score, and operational risk score. The dataset was uploaded through the web-based interface, and the machine learning models were trained to identify patterns associated with normal and suspicious financial behavior. The developed system also provides a user-

friendly interface where users can upload datasets, train the model, and enter financial parameters for risk prediction. The prediction results are displayed as Low Risk (Safe) or High Risk (Fraud Alert), which helps organizations quickly identify suspicious financial activities.

1. Upload financial datasets in CSV format

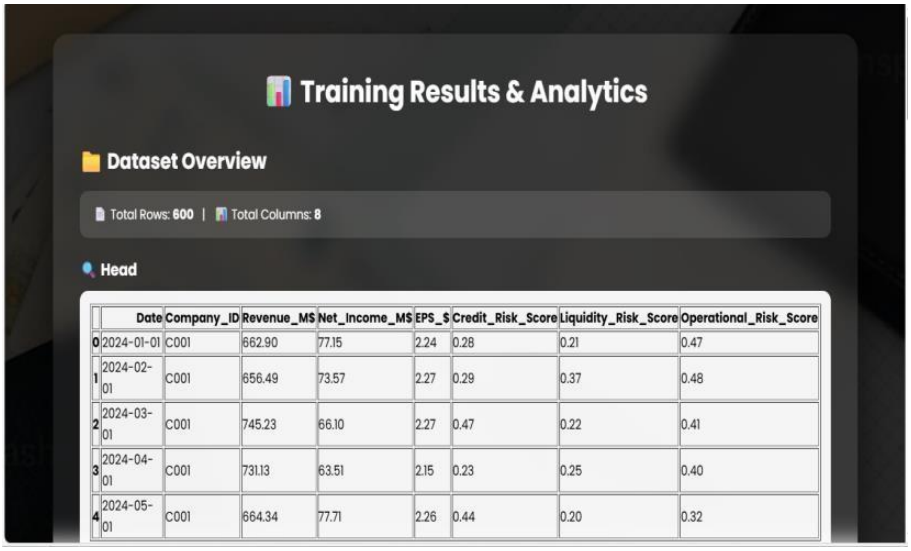
In the first step of the system, users upload financial datasets in CSV (Comma-Separated Values) format through the web interface. The CSV file contains financial information such as company ID, revenue, net income, earnings per share (EPS), credit risk score, and operational risk score. This dataset acts as the input for the machine learning model. Once the dataset is uploaded, the system reads the data and prepares it for further analysis. Using CSV format makes it easy to store, manage, and process large financial datasets efficiently.

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com



2. Train Machine Learning Models

After the dataset is uploaded, the system performs training of machine learning models. During this stage, algorithms such as Linear Regression, Random Forest, and Gradient Boosting analyze the dataset to learn patterns and relationships between financial parameters and fraud risk. The training process helps the model understand which financial behaviors are normal and which may indicate suspicious or fraudulent activities. By learning from historical financial data, the model becomes capable of predicting fraud risk for new financial records.



	Date	Company_ID	Revenue_M$	Net_Income_M$	EPS_$	Credit_Risk_Score	Liquidity_Risk_Score	Operational_Risk_Score
0	2024-01-01	C001	662.90	77.15	2.24	0.28	0.21	0.47
1	2024-02-01	C001	656.49	73.57	2.27	0.29	0.37	0.48
2	2024-03-01	C001	745.23	66.10	2.27	0.47	0.22	0.41
3	2024-04-01	C001	731.13	63.51	2.15	0.23	0.25	0.40
4	2024-05-01	C001	664.34	77.71	2.26	0.44	0.20	0.32

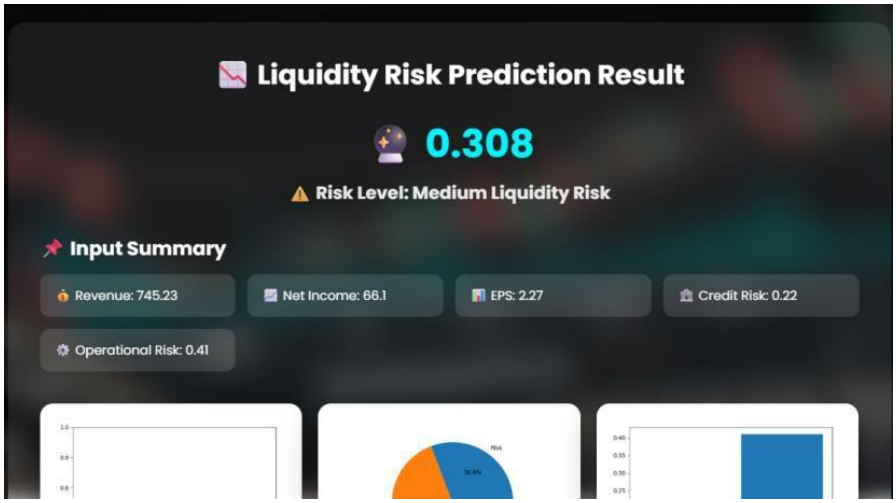
3. Enter Financial Parameters

Once the model is trained, the user can manually enter financial parameters through the system interface. These parameters include values such as revenue, net income, EPS, credit risk score, and operational risk score. This step allows users to test or analyze new financial data without uploading a complete dataset. The entered parameters represent the current financial condition or transaction that needs to be evaluated for potential risk.

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com

4. Predict Financial Risk Levels

In the final step, the trained machine learning model analyzes the entered financial parameters and predicts the financial risk level. The model processes the input values and compares them with patterns learned during the training phase. Based on this analysis, the system determines whether the financial condition is low risk (safe) or high risk (possible fraud). The prediction result is then displayed to the user, helping organizations quickly identify suspicious financial activities and take preventive actions.



V. CONCLUSION

AI-powered fraud detection has become an indispensable tool in securing digital payment systems. As financial transactions increasingly shift online, fraudsters continue to develop more sophisticated attack methods, making traditional rule based fraud detection insufficient. AI and machine learning offer real-time, adaptive, and intelligent solutions to counter these threats effectively.

Key Takeaways:

AI Enhances Fraud Detection Efficiency: Machine learning models analyze vast amounts of transactional data, identifying fraud patterns faster and more accurately than traditional systems.

Current Journal of Engineering and Science Research
Volume 3, Issue 4, pp 39-46, April 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.304005
Available Online at https://www.cjesr.com

Real-Time Risk Assessment: AI enables instant fraud detection, reducing financial losses and improving customer trust.

Behavioral Analytics & Biometrics Improve Security: AI-powered behavioral biometrics enhance fraud prevention by detecting anomalies in user actions, reducing false positives.

Challenges Exist but Can Be Overcome: Issues like model bias, false positives, regulatory constraints, and evolving fraud tactics must be addressed through continuous AI updates, transparency, and human oversight.

Final Thoughts: AI-driven fraud detection will continue to evolve and adapt to emerging threats, making digital payment systems safer, more reliable, and resilient against fraud. Financial institutions, fintech companies, and businesses must embrace AI-powered security measures while ensuring compliance with regulations and maintaining ethical AI practices.

REFERENCES

[1] Singh, J. (2021). The Rise of Synthetic Data: Enhancing AI and Machine Learning Model Training to Address Data Scarcity and Mitigate Privacy Risks. Journal of Artificial Intelligence Research and Applications, 1(2), 292-332.

[2] Narne, S., Adedoja, T., Mohan, M., & Ayyalasomayajula, T. (2024). AI-Driven Decision Support Systems in Management: Enhancing Strategic Planning and Execution. International Journal on Recent and Innovation Trends in Computing and Communication, 12(1), 268-276.

[3] Boddapati, V. N., Galla, E. P., Sunkara, J. R., Bauskar, S., Patra, G. K., Kuraku, C., & Madhavaram, C. R. (2021). Harnessing the Power of Big Data: The Evolution of AI and Machine Learning in Modern Times. ESP Journal of Engineering & Technology Advancements, 1(2), 134-146.

[4] Galla, E. P., Boddapati, V. N., Patra, G. K., Madhavaram, C. R., & Sunkara, J. (2023). AI Powered Insights: Leveraging Machine Learning And Big Data For Advanced Genomic Research In Healthcare. Educational Administration: Theory and Practice.

[5] Anjum, K. N., & Luz, A. Investigating the Role of Internet of Things (IoT) Sensors in Enhancing Construction Site Safety and Efficiency.

[6] Patra, G. K., Rajaram, S. K., & Boddapati, V. N. (2019). Ai And Big Data In Digital Payments: A Comprehensive Model For Secure Biometric Authentication. Educational Administration: Theory and Practice.

[7] Chintala, S. (2019). IoT and Cloud Computing: Enhancing Connectivity. International Journal of New Media Studies (IJNMS), 6(1), 18-25.

[8] Chintala, S. (2020). The Role of AI in Predicting and Managing Chronic Diseases. International Journal of New Media Studies: International Peer Reviewed Scholarly Indexed Journal, 7, 16-22.

****