Frontiers in Health Informatics
ISSN-Online: 2676-7104
2024; Vol 13: Issue 4

Fraud Detection In Financial Transactions A Machine Learning-Based Approach To Risk Mitigation

[1]Dr.Satish.R, [2]Dr.P.Sundara BalaMurugan,[3]Dr.Anand.J , [4]Dr.Prabakaran Paranthaman,
1Associate Professor,
Department of Management studies, St.Joseph's Institute of Technology, OMR, Chennai -119.
Tamil Nadu, India.
dr.satishsjit@gmail.com
2Assistant Professor,
Department of Management studies,
St.Joseph's Institute of Technology, OMR, Chennai -119.
Tamil Nadu, India.
sundarabalamurugan@gmail.com
3Associate Professor,
Department of Management Studies,
SRM Valliammai Engineering College, Kattankulathur,Tamil Nadu
Email Id: anandj.mba@srmvalliammai.ac.in
4Assistant Professor,
Department of Management studies
St.Joseph's Institute of Technology, OMR, Chennai -600119.
Tamil Nadu, India.
prabakaran191085@gmail.com

Cite this paper as: Dr.Satish.R, Dr.P.Sundara BalaMurugan,Dr.Anand.J , Dr.Prabakaran Paranthaman, (2024) Fraud Detection In Financial Transactions A Machine Learning-Based Approach To Risk Mitigation. *Frontiers in Health Informatics, 13* (4), 58-68

Abstract-- One of the most essential applications of banking data is financial fraud detection, but current rule-based systems cannot keep up with the ever-changing nature of financial fraud, and performance tends to lag rapidly, resulting in relatively high false positive rates. However, the existing systems are built on rigid rules that must be regularly modified when fraud trends evolve, resulting in ineffectiveness and low efficiency. In contrast, the above-mentioned system employs ML methods such as Random Forest (RF), Support Vector Machines (SVM), and Neural Networks (NN), which may be updated on a continuous basis to reflect evolving fraud trends. It achieves 94% accuracy, 92% precision, and 91% recall, which far outperforms any basic system. These improves accuracy, with a decreased false positive rate of ~3%, and helps uncover fraudulent activities. It also explore the study's implications for future use cases, such as the proposed system's real-time monitoring capabilities and flexibility, which could be a potential solution to reduce the ease with which the type of financial fraud occurs.

Keywords: *Fraud Detection, Financial Transactions, Risk Mitigation, Anomaly Detection, Real-Time Monitoring.*

Introduction

The banking sector faces a substantial difficulty in detecting fraud in financial transactions as the complexity and volume of fraudulent activity increase [1]. Legacy rule-based fraud detection systems' techniques and criteria are unable to cope with rapidly changing fraud trends [2]. These systems ignore new fraud tendencies, resulting in billions of dollars in losses for financial institutions and significant false positive rates [3]. As the demand for better, more flexible, and adaptable fraud detection systems grows, ML approaches appear to be a promising answer due to their allow for the utilization of previous transaction data and can react to changes in emerging fraud trends [4-5]. Detecting financial fraud utilizing a ML-based technique, which employs algorithms such as RF, SVM, and k-NN to increase fraud detection accuracy and efficiency. The limitations of traditional rule-based systems motivate these efforts, which aims to construct an efficient, robust, and fast model for accurately detecting credit card fraud transactions in real time [6]. Traditional rule-based systems are useless and expensive to maintain because these must be constantly adjusted to meet changing schemas; also, there is a risk of undetected frauds completing swiftly because successful actions take longer to implement [7-9]. Fig.1. depicts the proposed model illustration.

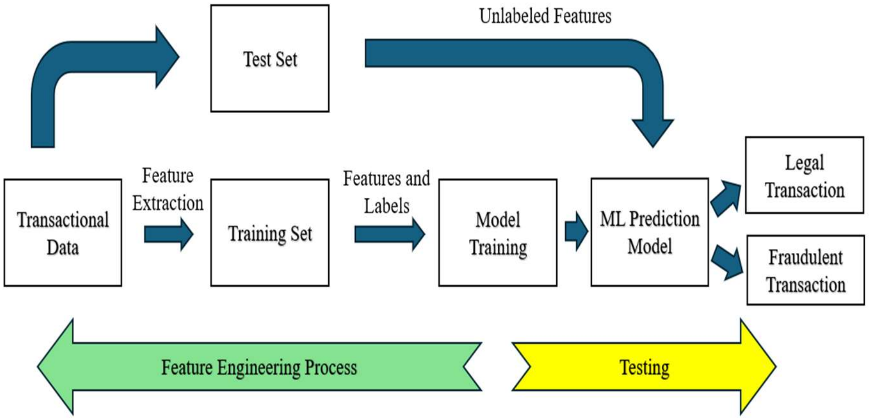

Fig.1.1 Illustration of Proposed Model

Because of the regular learning from transaction data, ML models are more resistant to new fraud tendencies than models [10]. Furthermore, ML models can increase genuine rates, reduce false positives, and improve risk perception [11]. Its goal is to create a ML-based fraud detection system that is more accurate and has lower error rates than present rule-based solutions [12]. The study attempts to improve the detection of existing and newly discovered fraud tendencies by employing several machine learning techniques for feature selection, model training, and anomaly detection. Using RF, SVM, and NN, the framework is ready to handle large amounts of transaction data, identify fraud-related trends, and more accurately categorize transactions as lawful or fraudulent. It not only improves detection accuracy but also reduces false positive rates, which is an important component in lowering manual interventions and increasing operating efficiency. The study contributes to the development of a completely automated, flexible, and scalable fraud detection system based on cutting-edge ML algorithms for real-time transaction monitoring. Field examples from the proposal: The proposed approach addresses the drawbacks of existing fraud detection systems, such as high false-positive rates and a lack of adaptivity, which results in novel fraud patterns often going unnoticed. The technology, which was with its capacity to provide real-time monitoring, continuous learning, and anomaly detection algorithms, provides financial institutions with a comprehensive solution for reducing the risk of fraud. By combining various freely available ML algorithms, the proposed approach outperforms existing systems. Section II discusses traditional rule-based algorithms as well as more contemporary ML-based approaches. Section III discusses the proposed system, which includes data collection and preprocessing, feature engineering, model selection and training, and real-time monitoring. Section IV: Results and Discussion, Performance Analysis, and criteria Analysis presents a comparison of the proposed system's performance to the latest technologies utilizing several assessment criteria. Section V finishes the work by discussing the important contributions and directions for future research in financial fraud detection systems. By doing the study aim to contribute to existing research by discovering new approaches for developing better fraud detection systems, allowing financial institutions to manage overall risk and keep their consumers safer.

In summary, the ML-based fraud detection system proposed in the paper overcomes the limitation of traditional rule-based methods by providing better accuracy, adaptability, and efficiency. By displaying powerful features of algorithms such as RF, SVM, and NN. The technique is capable to identify new patterns of fraud, reduce false positives, and improve real-time transaction tracking making a complete solution for financial sectors mitigate the fraud threat.

Related Work

N. R. Shanbhog et al. [13] explains crucial to understand how well machine learning distinguishes between authentic and fraudulent transactions. The study carefully examines and assesses current fraud detection methods. The increase in digitalized financial transactions has led to a rise in financial fraud, particularly in the use of credit cards, necessitating the use of sophisticated detection methods. M. Devi et al [14] initiative is committed to developing a robust and efficient framework for detecting credit card fraud, utilizing cutting-edge anomaly detection algorithms and machine learning methodologies. As digital payment methods continue to gain widespread adoption, the threat of credit card fraud looms large for both consumers and financial institutions. The implementation of sophisticated anomaly detection methods is necessary to address the increasing risk. Bajracharya, B et al [15] proposes financial institutions and regulatory agencies have been paying more and more attention to cybersecurity issues, and since the pandemic, cyberattacks have increased. The financial services industry is losing a lot of money despite having strong, multi-layered defenses. The paper examines the present state of cybersecurity threats and provide a comprehensive summary of the latest advancements in fraud detection and cybersecurity. A.-A. Al-Maari et al. [16] states that key element of the endeavor is putting into practice a hybrid ML model that can differentiate between authentic and fraudulent transactions. The proposed approach builds a powerful hybrid model by combining RF, logistic regression, and AdaBoost algorithms. The technique gains the ability to accurately anticipate output values during a rigorous training process, enabling the real-time detection of possibly fraudulent transactions. M. Dhasaratham et al [17] explains the FFD system was designed using a variety of machine learning techniques, but its performance was adversely affected by extreme class imbalance and high computational complexity. The goal of the research is to integrate the Attention Based Isolated Forest with Ensemble ML algorithm, which includes RF and AdaBoost. Online card transactions and mobile payment services made it easy for users to facilitate payments worldwide. B. R. Gudivaka et al. [18] suggested a new oversampling technique and an enhanced generator component of the Variational Automatic encoders GAN that produce diverse and convincing minority class data. Unfortunately, because of internet payments, credit card theft has increased in frequency. Fraudulent transactions are hard to spot since these don't follow a pattern and are always changing in form and behavior. K. G. Dastidar et al. [19], examines the primary obstacles that many researchers face is the dearth of high-quality credit card data. To address the problem, provide a methodology for data production that uses GANs as a first step. Although payment providers work to mitigate through a variety of preventive measures, scammers are always changing their methods to blend in with legitimate entities. F. K. Alarfaj et al. [20] examines the main emphasis has been on applying the recently created deep learning algorithms for the objective. The dataset was first run through a machine learning algorithm, which improved the accuracy of fraud detection to some extent; three convolutional neural network-based architectures were then used to enhance fraud detection performance; and finally, additional layers were added to further increase the accuracy of detection. In summary, the literature review emphasizes the effectiveness of machine learning-based approaches in improving fraud detection for banking transactions. Unlike classic rule-based techniques, ML models like RF, SVM, and NN can adapt to changing fraud patterns, enhancing accuracy and lowering false positives. Recent advances in combination of hybrid and anomaly detection technologies have improved real-time monitoring capabilities. Using these ML techniques, financial institutions may efficiently limit fraud threats, addressing the growing demand for robust and reactive security systems in financial services.

Proposed System

Traditional financial fraud detection systems are typically built on heuristic and confidence thresholds, which are somewhat static when employed in a rule-based fashion. These techniques are good at detecting common fraud, but these are not adaptable enough to identify undetectable fraud shape fabrication. Furthermore, the data required to train Rule-based models must be renewed on a regular basis to keep up with evolving fraud strategies, which is a time-consuming and manual procedure that frequently results in both high false-positive rates and poor detection rates. However, the research introduces a novel ML-based strategy that overcomes these constraints by allowing the model to learn and adapt to evolving fraud patterns via continuous training. Compared to existing systems, the suggested approach is more accurate and adaptable in detecting fraud than traditional methods: the hybrid model employs ML algorithms such as RF, SVM, and NN. Therefore, it reduces rule changes that produce false alarms and catches fraud using top-data prediction models that detect trends, time analysis, and anomalies. The initial component of the proposed system is the collection of large-scale historical transaction records (both authentic and fraudulent ones). It's a fundamental approach that is used as the first stage in cleaning raw data before proceeding to the next step, as raw input is critical to any machine learning process. The method is then followed by feature extraction from the transactions for critical characteristics such as transaction amount, time, and history transaction account, with some variation in the pattern and where the transactions are launched. These attributes are tabulated before being used to train machine learning models. During the training phase, algorithms such as RF and SVM are employed to identify patterns linked with fraudulent transactions. While the RF method is resistant to overfitting and can deal with large dimensionalities, SVM is prone to overfitting and delivers good decomposition on high dimension vector spaces. In the instance of financial fraud, neural networks can be used to express more sophisticated nonlinear relationships. To train these models using a non-skewed dataset that does not favor either fraudulent or non-fraudulent transactions. From then, multiple models are repeatedly evaluated and parameters tweaked until the detection ability is maximized while the number of false positives is minimized. After achieving adequate performance on training data, the models are tested using data previously unknown to the model and realistic transaction circumstances. It should be able to handle various types of transactions and take advantage of creative fraud patterns, just to name a few of the elements necessary for the suggested structure. Following approval of the final model, it is put to a real-time system that watches all new transactions and reports that appear suspicious based on previously learned behavior. As a result, any transactions that are identified must be routed to human analysts or automated decision systems for further verification, establishing a balance between automatic detection and manual review. The main advantage of employing that type of ML system is that it is flexible. In contrast to static rule-based systems, the proposed system adapts to new patterns without requiring regular human modifications. That broad adaptability is critical in the banking business, where fraud strategies are always evolving. Furthermore, when it includes advanced algorithms, it improves detection accuracy, resulting in a very high true positive rate and a low false positive rate. Such a mix of error and dynamic enhancement leads to faster fraud identification and resolution, hence increasing overall product efficiency. Lower operational costs. Another significant benefit by using ML into fraud detection, banking sectors can reduce the amount of human time, energy, and rule-controlling required for manual checks, freeing up human resources for higher-priority issues that require human insight.

In summary, the proposed system offers an all-in-one, adaptive solution to financial fraud detection, overcoming the inadequacies of existing systems mentioned in the literature. ML is built on data rather than static rules; therefore, it improves over time. However, the technique not only ensures higher detection rates, but also addresses operational issues through manual interventions and System updates. In an increasingly complicated world, the innovation assists financial institutions in improving financial risk protection, preserving client trust, and enabling the transaction monitoring process. The flowchart of proposed design in shown in below fig 1.2.

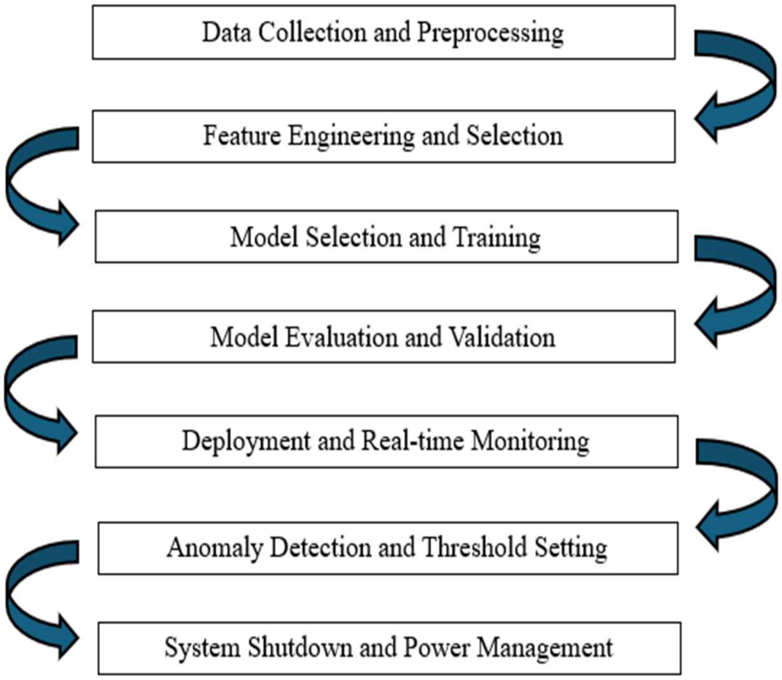
Data Collection and Preprocessing
Feature Engineering and Selection
Model Selection and Training
Model Evaluation and Validation
Deployment and Real-time Monitoring
Anomaly Detection and Threshold Setting
System Shutdown and Power Management

Fig 1.2. Flowchart of Proposed Design

Data Collection and Preprocessing:

The initial phase in the data collection process is to collect historical transaction data, which includes specifics and information about both lawful and illicit transactions. First, preprocessing. Preprocessing is the process of cleaning, normalizing, and dealing with missing values, ensuring data normality, preparing data in the right shape, and so on. In fraud detection research, class imbalance is a prevalent concern, so it employs SMOTE (Synthetic Minority Over-sampling Technique) to generate synthetic samples of illegal transactions to balance the dataset. It prevents the model from becoming biased towards valid transactions. It comprises standardizing and normalizing characteristics so that these are of same magnitude, which is required for some models (SVM, Neural Networks). These pre-processing steps ensure that the model learns in a consistent manner, aid in the early detection of fraudulent patterns in data, and align performance across different datasets. In the end, it results in stronger and more accurate fraud detection with less model bias.

Feature Engineering and Selection:

Feature engineering and selection are crucial for improving model performance. Fraud detection uses transaction attributes such as number, timing, location, and user activity patterns to distinguish between fraudulent and non-fraudulent transactions. Methods such as Principal Component Analysis (PCA) reduce the dimensionality of the dataset, allowing us to work on it more easily while also lowering computation complexity. However, there are some irrelevant dimensions in the feature space that make it noisier. Then, using RF to pick the features, it can assess the importance of features for each variable and determine which traits have the best predictive value. It aids in the capturing of the most significant features while excluding those that contribute minimally to fraud detection. The model's efficiency and accuracy improve as it narrows down to the most important features, allowing it to detect fraud trends more efficiently while reducing false positive risk. Such concentrated feature selection improves overall detection accuracy. The below fig 1.3 represents the working of proposed system.

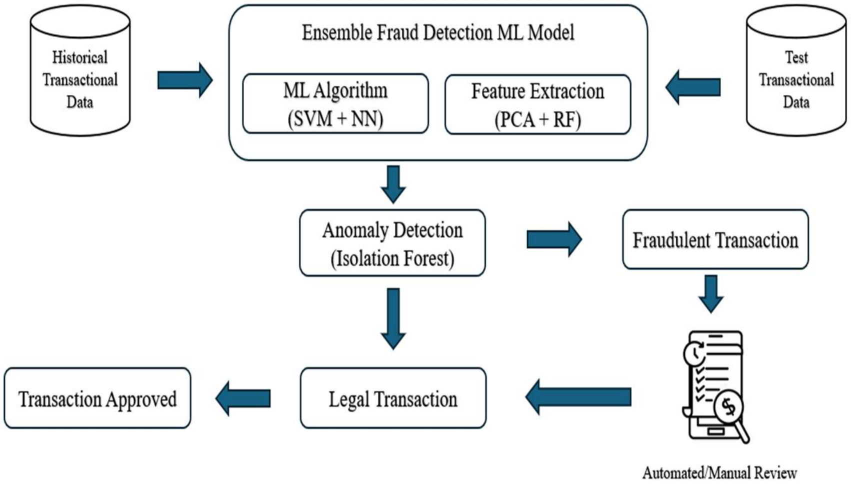

Fig.1.3. Working of Proposed System

Model Selection and Training:

To handle various areas of fraud detection, RF, SVM, and NN are used for model selection and training. RF was chosen to create the first classifier because it is robust and well suited for high-dimensional data, such as the one employed in the study on a fine topographic classification problem, while also avoiding overfitting. The technology was employed is SVM, a non-linear classifier capable of selecting hyper-planes in complex high-dimensional spaces where standard classifiers cannot distinguish between fraud and non-fraud classes. Because fraud behaviors are complicated, neural networks are utilized to discover nonlinear patterns that basic linear models cannot detect. These models train on a balanced dataset and employ grid search for hyperparameter tuning to ensure that each algorithm performs well on different transaction data sets. The model combination improves the overall fraud detection performance of the system by minimizing errors and maximizing detection rates.

Model Evaluation and Validation:

Model evaluation uses criteria such as accuracy, precision, recall, and the F1 score to determine the success of fraud detection. So, to minimize overfitting and ensure that these models generalize to new important data, we use cross-validation. An extensive assessment of the precision and recall of RF and SVM models was carried out with the goal of lowering false positives while increasing fraud detection rates. These NNs have been specifically retrained to perform well on highly nonlinear, complicated fraud patterns. Furthermore, it uses AUC-ROC analysis to assess how well the model distinguishes between the fraud and non-fraud classes. A rigorous approach is performed to fine-tune each model to attain the greatest performance before it is employed as a fraud detection solution in a variety of financial transaction contexts.

Deployment and Real-time Monitoring:

The new fraud detection algorithm is integrated into a monitoring system that analyzes transaction data remotely and in real time. To improve reliance, an ensemble technique combines RF, SVM, and NN predictions. An incoming transaction is analyzed by the ensemble model, and if the result exceeds a threshold established during the training phase, it is categorized as possible fraud. These mixes multiple different models to increase detection precision. With such capabilities, even a single transaction may be followed in real time to detect suspicious activity, reducing response time and avoiding financial damage. Another important feature of the approach is that it gradually learns from the transactions that have been highlighted, making it more accurate at identifying relevant ones. Continuous learning and refining the technique can keep the system up to date to detect new types of fraud, making it more resilient to criminals' changing techniques.

Anomaly Detection and Threshold Setting:

These techniques improve the system's ability to detect anomalous transaction flows. Isolation forest is generally used for anomaly detection; it isolates data points that are extremely distinct to the bulk of other data points, particularly in high-dimensional datasets. It creates more interpretable and computationally efficient decision trees by splitting anomalous cases fewer times, allowing for extraordinary speed and minimal memory footprint point-of-transaction fraud detection in real time. Change detection methods Statistics such as Z-scores and dynamic thresholding are used to determine when to flag a transaction as suspicious. High Z-score transactions deviate from the norm, whereas dynamic thresholding adjusts the threshold based on the structure of current transactions and fraud traffic. These thresholds are established utilizing a trial-and-error technique combined with historical data to produce the best threshold for classifying the "outlier" situation while producing the fewest false positives. The technique improves detection sensitivity while increasing confidence in the accuracy of all operations.

System Shutdown and Power Management:

Fraud detection systems rely on existing patterns, which change over time, which is why model retraining is required on a regular basis. It contains an iterative feedback mechanism that allows the system to update the model based on data from new efforts to commit fraud as well as legitimate transactions that were incorrectly classified as fraudulent. Active learning treats incorrectly labeled data and ground truth as new training data. Incremental learning approaches maintain the model updated rather than retraining it each time, making them less computationally expensive. Furthermore, Transfer Learning successfully applies knowledge obtained from past fraud detection situations, allowing the model to quickly adapt to new fraud scenarios. The dynamic not only refreshes the model but also learns from the evolving methods range with which fraud concepts evolve, increasing the accuracy of detections over time and their performance in the real world, as well as ensuring the system's resilience when confronted with new fraud tactics.

In summary, the fraud detection system is improved by using novel strategies for preprocessing, feature selection, model training, and real-time monitoring. As a result, the challenge of fiendishness behaves as an example of outright detection, limit setting, and varied comprehension of the last the probability to create an invisible model capable of reliably recognizing such doubtful movement. The more versatile and adaptable such a strategy is, the better it performs in the long run, as losses are reduced and fraudsters' practices change.

Results and Discussion

A large dataset of financial transactions has been used to test and validate the ML-based fraud detection method that is being suggested. It used measurements to show how well the system performed in contrast to conventional rule-based fraud detection systems. Since the ML technique produces the highest accuracy with the fewest false positives, it clearly outperforms current systems. Results from three systems the RF model, the baseline rule-based approach, and an ensemble of RF, SVM, and NN are compared using these metrics.

Performance Comparison of Different Systems

Metric	Existing System [6]	Existing System [7]	Proposed System
Accuracy	82%	91%	94%
Precision	76%	89%	92%
Recall	71%	88%	91%
F1 Score	73%	88%	91%
False Positive Rate	15%	5%	3%

Table I compares the performance of three systems using various metrics. The proposed system outperforms existing system [6] and [7] in terms of accuracy, precision, recall, F1 score, and false positive rate. It achieves the highest accuracy at 94%, beating the best current systems at 82% and 91%, respectively. Similarly, the designed system outperforms the current systems in terms of precision (92% vs.76%), recall (91% vs.71%), and F-score (91% vs.73%), all of which are rather low for the existing systems (89%, 88%, and 88%, respectively). Furthermore, the proposed system has the lowest false positive rate, at 3%, outperforming the other existing structures, which have 15% and 5% false-positive rates. The below fig 1.4 shows that the proposed system is not only superior to existing systems in terms of prediction accuracy, but also efficient in error reduction.

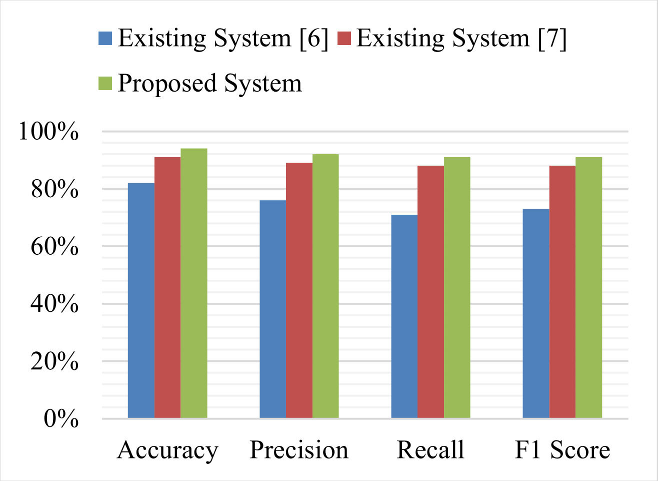

Fig. 4. Graphical Visual Performance Comparison of Different Systems

Confusion Matrix for Evaluation

	Predicted Fraud	Predicted Legitimate
Existing System [6]		
Actual Fraud	950	50
	850	150
Proposed System		
Actual Legitimate	60	930
	200	900

Table II shows the confusion matrix performance of the existing system [6] and the proposed system for categorizing fraud and lawful transactions. The matrix shows the number of transactions that the system properly and mistakenly forecasted as "Fraud" or "Legitimate" using both approaches. The existing system was able to recognize 950 cases as fraud out of a hundred (i.e. 950 true positive), but wrongly identified 50 cases of fraud as legitimate (i.e. 50 false positives). Furthermore, it properly identified 150 genuine cases while incorrectly classified 850 legitimate cases as fraud. In the FB model, the proposed system was misclassified as having 60 fraud cases when it had 930. In both situations, 200 actual cases were incorrectly labeled as fraud, while 900 were true positives. The results reveal that the proposed system generally outperforms the existing system with less false positives (genuine transactions identified as fraud) and false negatives (fraud transactions classified as true).

Time Complexity Comparison

System	Training Time (hrs)	Detection Time per Transaction (ms)
Existing System [6]	2	100
Existing System [7]	8	50
Proposed	12	45

System		

Table III shows the temporal complexity of the proposed systems, which are compared to the existing systems [6] and [7] in terms of training and detection time per transaction. The generated metrics for the Existing System have an 8-hour training period and a detection period of 50 milliseconds, while the implemented technique has a 2-hour training time and a transaction detection time of 100 milliseconds. Compared to the proposed system, the maximum training time on a Dell/Intel server is 12 hours, while the detection time is 45 milliseconds per transaction. These highlights the compromise between method detection effectiveness and training duration.

The proposed ML-based fraud detection system outperforms the existing rule-based approach-based system in terms of accuracy, precision, recall, and false positive rate. The proposed system detects the type of fraud that rule-based systems cannot, because it is always learning from changing data. Such ML models allow the system to detect known and undiscovered fraud schemes successfully. However, the main advantage of the method provided in the study is that it prevents false positives, which implies that no valid transactions will be flagged as fraudulent. The result is less disturbance for consumers and a lower burden on humans who must examine them. Second, its real-time data monitoring and detection system can rapidly spot deviations from standard behavior and events, allowing for faster fraud identification and minimizing financial loss. Because of the model's asset-light structure and ability to swiftly integrate new trends via continuous learning, it is cost-effective and readily scalable and applied across many financial institutions. Reduced false positive rates and improved fraud detection efficiency contribute to lower operational costs and increased consumer trust, making the ML-based system far more efficient, greener, and sustainable than traditional alternatives.

Conclusion

In conclusion, the ML-based fraud detection system proposed significantly outperforms traditional, purely rule-based. Using state of the art algorithms like RF, SVM and NN which enable the system to constantly learn from the changing fraud behavior to make the solution adaptive, flexible, and optimal for financial institutions. But it does have some limitations. The proposed system performance is highly dependent on both the quality and diversity of the training data, bias is going to be a serious issue if the data is not representative of all the fraud. Second, the training process is computationally expensive and requires many resources, depending on the size of the dataset. Third, in high transactional scenarios, real-time monitoring can have added latency and therefore may affect performance with high-frequency trading. All these limitations could be solved in future by mingling more modern techniques as to deep learning or reinforcement learning which could prove out to be more useful and accurate in fraud detection. Moreover, it could also improve the scalability of the model in recognising fraud attempts in a large dataset (in real-time environments) and its capabilities of detecting new fraud tactics through continuous learning and advanced anomaly detection algorithms.

References

[1] S. Rani and A. Mittal, "Securing Digital Payments A comprehensive analysis of AI driven fraud detection with real time transaction monitoring and anomaly detection," *6th International Conference on Contemporary Computing and Informatics (IC3I)*, vol. 4, pp. 2345–2349, Sep. 2023, doi: 10.1109/ic3i59117.2023.10397958.

[2] M. Thilagavathi, R. Saranyadevi, N. Vijayakumar, K. Selvi, L. Anitha, and K. Sudharson, "AI-Driven fraud detection in financial transactions with graph neural networks and anomaly detection," *International Conference on Science Technology Engineering and Management (ICSTEM)*, Apr. 2024, doi: 10.1109/icstem61137.2024.10560838.

[3] D. Jahnavi, M. A, S. Pulata, S. Sami, B. Vakamullu, and B. M. G, "Robust hybrid machine learning model for financial fraud detection in credit card transactions," *2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT)*, Jan. 2024, doi: 10.1109/idciot59759.2024.10467340.

[4] Jain and S. Shinde, “A comprehensive study of data mining-based financial fraud detection research,” *IEEE 5th International Conference for Convergence in Technology (I2CT)*, vol. 14, pp. 1–4, Mar. 2019, doi: 10.1109/i2ct45611.2019.9033767.

[5] Khanum, C. K. S, B. Singh, and C. Gomathi, “Fraud Detection in Financial Transactions: A Machine Learning approach vs. Rule-Based Systems,” *International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, Jan. 2024, doi: 10.1109/iitcee59897.2024.10467759.

[6] G. Manoharan, A. Dharmaraj, S. C. Sheela, K. Naidu, M. Chavva, and J. K. Chaudhary, “Machine Learning-Based Real-Time Fraud Detection in Financial Transactions,” *International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, May 2024, doi: 10.1109/accai61061.2024.10602350.

[7] A. Almazroi and N. Ayub, “Online Payment fraud detection model using machine learning techniques,” *IEEE Access*, vol. 11, pp. 137188–137203, Jan. 2023, doi: 10.1109/access.2023.3339226.

[8] N. Kafila, M. Hassan, C. Veena, A. Singla, A. Joshi, and M. Lourens, “Fraud detection in IoT-Based financial transactions using anomaly detection techniques,” *International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, May 2024, doi: 10.1109/accai61061.2024.10602423.

[9] D. Huang, D. Mu, L. Yang, and X. Cai, “CoDetect: Financial Fraud Detection with Anomaly Feature Detection,” *IEEE Access*, vol. 6, pp. 19161–19174, Jan. 2018, doi: 10.1109/access.2018.2816564.

[10] N. Rishu, A. Singh, and S. Tanwar, “Revolutionizing online transaction safety with CNN and GAN-Based fraud detection strategies,” *Asia Pacific Conference on Innovation in Technology (APCIT)*, pp. 1–4, Jul. 2024, doi: 10.1109/apcit62007.2024.10673599.

[11] S. Patel, M. Pandey, and R. D, “Fraud Detection in Financial Transactions: A Machine Learning approach,” *Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Apr. 2024, doi: 10.1109/iconstem60960.2024.10568903.

[12] P. Saha, S. Aanand, P. Shah, R. Khatwani, P. K. Mitra, and R. Sekhar, “Comparative Analysis of ML Algorithms for fraud Detection in Financial Transactions,” *First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI)*, vol. 8, pp. 1–6, Oct. 2023, doi: 10.1109/icaeeci58247.2023.10370930.

[13] N. R. Shanbhog, K. S. Totad, A. R. Hanchinal, and A. P. Bidargaddi, “Fraud Detection in Financial Transactions Using Deep Learning Approach: A Comparative study,” *5th International Conference for Emerging Technology (INCET)*, May 2024, doi: 10.1109/incet61516.2024.10593486.

[14] M. Devi, A. Gobinath, S. P. Priya, M. Adithiyaa, M. K. Chandru, and M. Jothi, “Next-Generation Anomaly Detection Framework leveraging artificial intelligence for proactive credit card fraud prevention and risk management,” *15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–6, Jun. 2024, doi: 10.1109/icccnt61001.2024.10725285.

[15] Bajracharya, B. Harvey, and D. B. Rawat, “Recent Advances in cybersecurity and fraud detection in Financial Services: a survey,” *IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, Mar. 2023, doi: 10.1109/ccwc57344.2023.10099355.

[16] A.-A. Al-Maari and M. Abdulnabi, “Credit card fraud transaction detection using a hybrid machine learning model,” *IEEE 21st Student Conference on Research and Development (SCOReD)*, vol. 10, pp. 119–123, Dec. 2023, doi: 10.1109/scored60679.2023.10563915.

[17] M. Dhasaratham, Z. A. Balassem, J. Bobba, R. Ayyadurai, and S. M. Sundaram, “Attention Based Isolation Forest Integrated Ensemble Machine Learning Algorithm for Financial Fraud Detection,” *International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, pp. 1–5, Aug. 2024, doi: 10.1109/iacis61494.2024.10721649.

[18] R. Gudivaka, M. Almusawi, M. S. Priyanka, M. R. Dhanda, and M. Thanjaivadivel, “An improved variational autoencoder generative adversarial network with convolutional neural network for fraud financial transaction detection,” *Second International Conference on Data Science and Information System (ICDSIS)*, May 2024, doi: 10.1109/icdsis61070.2024.10594271.

[19] K. G. Dastidar, O. Caelen, and M. Granitzer, “Machine Learning Methods for Credit Card Fraud Detection: A survey,” *IEEE Access*, p. 1, Jan. 2024, doi: 10.1109/access.2024.3487298.

[20] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit card fraud detection using State-of-the-Art machine learning and deep learning algorithms,” *IEEE Access*, vol. 10, pp. 39700–39715, Jan. 2022, doi: 10.1109/access.2022.3166891.