



(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 3, March 2025

⊕ www.ijirset.com ⊠ ijirset@gmail.com 🖄 +91-9940572462 🕓 +91 63819 07438





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025 |DOI: 10.15680/IJIRSET.2025.1403189|

Fraud Detection in Banking Data using Machine Learning

Mr.Syed Beeban Basha, K.Sneha, B.Vamsi, SK.Sharmila, S.Venkata Sai Teja

Associate Professor, Department of Computer Science Engineering (Artificial Intelligence & Machine Learning),

Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Department of Artificial Intelligence & Machine Learning, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Department of Artificial Intelligence & Machine Learning, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Department of Artificial Intelligence & Machine Learning, Vasireddy Venkatadri Institute of Technology, Guntur,

Andhra Pradesh, India

Department of Artificial Intelligence & Machine Learning, Vasireddy Venkatadri Institute of Technology, Guntur,

Andhra Pradesh, India

ABSTRACT: Fraud detection on banking data is important within machine learning in the financial sector, as solutions to protect the financial systems are found. In the rise of digitization, a growing incidence of different forms of fraud, such as bank account fraud, debit/credit card fraud and UPI fraud has become a key problem to complete the financial ecosystem in the world. The fraud usually leads to significant financial loss and damages the trust in digital banking. The main objective of this project is deploying a fraud detection system based on machine learning models that are able to learn what is fraudulent and predict transaction risk level. For this, we will analyze all these datasets along with Bank Account Fraud Dataset, Debit/Credit Card Fraud Dataset and UPI Fraud Detection data using hybrid machine learning models by combining the power of various algorithms to increase the prediction accuracy and also reduce the occurrence of false positives. The performance evaluation metrics will be used to optimize the system to achieve high reliability and efficiency. The solution also will be used in a user-friendly Streamlit web application that will provide real time fraud detection, data visualizations and fraud risk prediction. Also included in the application is login/signup as well as mobile/email verification, which are authentication mechanisms in place to secure the application user interface and maintain data privacy, while keeping the sensitive information safe. The goal of this project is not only to detect fraud but also achieve actionable insights for the financial institutions to automatically reduce the risks and to improve the security measures of the banks facing increasing problems of fraud in the digital world.

KEYWORDS: The Fraud Detection, Banking Data, Machine Learning, Hybrid Models, Risk Prediction, Streamlit, Fraud Probability, UPI Fraud, Debit/Credit Card Fraud, Bank Account Fraud, Visualizations, Authentication

I.INTRODUCTION

Technology has changed and used so quickly and at the same time, the demand for digital transactions in the financial sector has also escalated, making us able to enjoy some privileges like speed, ease and efficiency. However, on the other hand, these innovations have resulted in a steep rise of fraudulent activities. With this, compliances towards financial institutions to use fraud detection as a prong tactic have been made, as they get to protect their customers, maintain their data as well as their reputation both in the digital banking system. Debit/credit card fraud and bank account fraud constitute great risks against both the institution and the individual undertaking financial fraud, and creating such effective systems of fraud detection on an urgent basis will help to hold up better.

Having fraud in financial systems is detected, yet using machine learning (ML) to learn more about the cause and effect. For some extent, rule based systems work fine but are disadvantageous in not being capable of learning new and complex fraudulent patterns. Nevertheless, machine learning algorithms can be kept learning with the large dataset and their





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

predictive accuracy will get better over time. The analysis of the transaction data and identify such patterns help these models to detect such anomalies of fraud. This project will build a machine learning based fraud detection system that can classify transactions as either fraudulent or legitimate, to counter the loss suffered out from the legitimate customers point of view as well as on the side of the financial institution.

The first step of fraud detection is not identification of the fraudulent transaction, it is the risk level of the transaction. For example, machine learning allows us to deduce the corresponding inherent probability of fraud and the maximum possible fraud activity. This approach not only classifies the further, but, greatly more, provides insight into the order of action with respect to the risk level rather than seeing even into all transactions equal. This project will use hybrid machine learning models, which will be a model that uses one or more of the algorithms like decision trees, random forests and gradient boosting.

The project will use Bank Account Fraud Dataset, Debit/Credit Card Fraud Dataset and UPI Fraud Detection data for training and evaluation of the models. Datasets consisting of these features indicate fraudulent behavior such as amounts, types of transaction, account details, patterns of time. With machine learning, it is possible to train the system to detect hard to discern fraud patterns that are not apparent in a normal way. The system will be tested with it rigorously in the real world scenarios, its accuracy and robustness will thoroughly be tested.

Additionally, this project will have a user-friendly Streamlit web app for user interface configuration and not just this project's capabilities in fraud detection. The web application will enable one to detect fraud in real time, present the display fraud risk level and show the transaction. Towards a better authentication, it will contain features such as login or user signup and mobile email verification. We build this to build a financial institutions fraud detection system that work very well functionally so that financial institutions will reap the benefit of the introduction of machine

II. LITERATURE SURVEY

The use of machine learning techniques, which have the ability to learn from large amounts of data, and to identify known types of fraud patterns, makes them a key instrument for detecting fraud in the banking sector. In this context, Hashemi et al. [1] put forward the way of fraud detection by the usage of various machine learning algorithms, such as decision trees and neural networks. They say that machine learning is a better option than the rule-based systems, used so far, in dynamic fraud detection as these systems are not designed to detect any new form of fraud. Based on the study, gained insights into the possibility of applying ensemble methods and hybrid models to make detection accuracy and reduce the problem of false positives in banking fraud. Building this addressing gap, Johora et al. [2] mentioned the escalation of call for up to AI based upon financing fraud analysis systems. Then, they described how they carried out an in depth study of how AI can track and detect fraudulent activities through sequence based on transaction data for anomalies. The application of such benefits and differences of supervised and unsupervised learning models to account takeovers, identity theft, or unauthorized transactions can be any type of fraud. The financial institutions were also shown in the paper that using AI based models is going to be a great improvement over the traditional ways, using these models would lead the institutions to forewarning any cases of fraud before they actually happen.

Further improvements in how machine learning and data analytics can be integrated to achieve fraud prevention were also explored by Mohammad et al. [3]. Their study found that the growing scale of the likely prey makes it more and more complex to detect fraud. According to the authors, the several algorithms have to be united with the model of hybrid machine learning models to make better predictions. This work was done by the researchers in arguing that supervised machine learning techniques can be easily combined with unsupervised machine learning techniques that are able to uncover hidden fraud patterns in banking systems, which results into a better solution to the problem of fraud detection in banking systems. Apart from the data driven approach, Faisal et al. [4] suggested the application of machine learning models for predicting and classifying real time fraudulent transactions. Depending on each bank's ability to line it with existing banking infrastructure, fraud detection was emphasised. For example, the researchers showed that AI models — or specifically deep learning ones — could process complex data sets with live insights of potential instances of fraud and would be useful to banks to minimize risks and protect customer assets.

In his case Esmail [5] provides a complete treatment of loan fraud detection processes of banking sectors with data mining techniques. The first mentioned the importance of classifying or clustering the fraudulent loan applications. In line with such an approach, they also made a study that demonstrated how the integration of machine learning into the support of loan fraud detection would bring a much more effective way to notice suspicious events and enhance fraud





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

detection procedures in financial institutions. With the exception of that, Bin Sulaiman et al. [6] have completely utilized machine learning in credit card fraud detection. In their review to detect credit card fraud, they explored different machine learning including classification algorithms and feature engineered techniques. In case of a fraud transaction is few compared to legitimate transaction the authors presented how a good problem can be solved. In this case, they proposed some solutions like the oversampling techniques, the ensemble models and so on, which would contribute to an increase of the performance of fraud detection systems.

Second, Johora et al. [7] later worked on AI advances in banking security with more attention to fraud detection systems. In this particular research, they focus on how important the AI becomes in enhancing the security in banking, which employs machine learning models to detect the fraud patterns and deter financial losses. They owned the significance of advancing techniques, for example, natural language processing (NLP) and anomaly detection, and exhibited how NLP and anomaly detection techniques can increase the accuracy of different types of frauds, for example, phishing, card skimming. Kotagiri and Yada [8] in another study looked into how RPA and advanced analytics strategies can assist to detect and reduce the mining of fraud in the banking system. Synergy between the automation tools and machine learning models in suspicious activities detection and to reduce the role of humans in the aspects of fraud monitoring. Results showed that RPA along with AI models make fraud detection more efficient and reduce operational costs of the financial institutions.

Among the banking sector, Gautam [9] has evaluated how artificial intelligence affects the process of building risk management and identifying fraud. In what he focuses on, AI is able to see transaction data and is able to detect patterns that may indicate the possibility of scamming. An important thing he discovered is that AI could be integrated into the existing risk management framework to make fraud prevention more effective by actively detecting fraud and to increase bank's safety. Zanke [10] does one of the comparisons of AI driven fraud detection systems in banking, insurance and healthcare. The main focus was to analyze the application of AI and deep learning based systems for fraud detection as a common thing across all sectors and the use of deep learning to enrich our fraud detection systems across all cases. It was concluded that AI based systems can be very effective defaulters to automate the mechanisms of detecting fraud in the banking industry and reduce financial losses.

Automated banking fraud detection is proposed by Biswas et al. [11] in the domain of the financial sector in order to reduce unauthorized access in it. They very specifically examined if and how machine learning algorithms (support vector machine, SVM, and other) could be applied in real time to detecting this fraud. The authors then brought up that the processes of fraud detection need to be automated in order to reduce the human error and increase the accuracy of the predictions. For example, in [12], Sekar mentions digital banking fraud prevention through real time cloud and AI. It was also about how cloud based solutions with the help of AI technology can help in fraud detection to take advantage of the scalability and flexibility of getting to identify large volumes of banking data. Sekar pointed out the need for simple, minimum delay systems that can detect and evaluate such transactions instantly and enable the bank to react instantly as and when such fraudulent activities come to the fore. Nonetheless, Sambrow and Iqbal [13] presented the possibilities of artificial intelligence and deep learning, data analytics, and many other things in preventing banking fraud. What sorts of fraud could a deep learning machine — specifically, a neural network

— learn from large datasets, that is what they studied in their work. I believe that they suggested that banks can enhance the fraud detection system and the elimination of frauds whilst they are occurring in real time via use of advanced machine learning approaches.

Al-Fatlawi et al. discussed an AI based model of fraud detection in the bank system, in [14]. During their conversation about how artificial intelligence models

can be used to train machine learned systems to automatically detect and call out adversarial transactions, they talked about how machine learning can train artificial intelligence models to identify strange and dubious patterns so that they can be alerted to potentially hostile transactions. They suggested identifying ensemble learning methods with which to combine the results of several models, so that the accuracy is improved and the number of false positive cases is reduced. Hence, with their work, Achary and Shelke [15] finally explored the use of machine learning techniques for fraud detection in banking transactions. Financing the second reference is a problem to detect the fight fraud in the financial transactions and using Machine learning to overcome the problem with particular references. They recommended that fraud detection models must be selected carefully with features and algorithms to train the models, to improve accuracy of the models and the overall system performance of the fraud prevention.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

III. PROPOSED METHODOLOGY

Machine learning algorithms are proposed to be used in combination with the proposed methodology for fraud detection in banking data on real time transactions. The system will employ analytical methods for examining the transaction data and predict the probability of fraud as well as examining the risk of each transaction. In this approach, several datasets like Bank Account Fraud Dataset, UPI Fraud Detection data, Debit/Credit Card Fraud Dataset are used and a hybrid machine learning model has been used to improve detection accuracy. To develop a cost effective fraud detection solution, the system would concentrate on data collection, then model development and finally on evaluation of the model.

The procedure of this methodology is structured in such a way that it guarantees efficiency and scalability. Model training, data pre processing, evaluation, and optimization are involved in the process. This methodology results will assist banks and financial institutions in detecting fraudulent activities at an early period and curb them from financial loss. In the next subsections, we detail the main steps in the proposed methodology.

A. Data Collection and Preprocessing

Firstly, we retrieve datasets of multiple types of banking transactions such as Bank Account Fraud Dataset, Debit/Credit Card Fraud Dataset, UPI Fraud Detection data. For these datasets, these are the important features such as transaction amount, user account information, transaction type and timestamps. This is important

because of this diversity of data, since the system will be able to learn patterns between multiple fraud scenarios, and to become more adapted to all fraud situations. Representative datasets that both incorporate fraudulent and non-fraudulent transactions will collect that, making the model more robust and true.

The dataset is collected, and in the preprocessing phase, the datasets are made ready for training the machine learning model. Imputation techniques will be used to handle the missing values and one hot encoding will be used to transform the categorical variables into numerical data. It will also feature scaling of numeric features to normalize them and put them on a similar scale for improving model's performance. Moreover, feature selection will be used to identify the most important variables in detecting fraud. Preprocessing is an attempt to make sure the data is clean and is ready to get the best from ML.

B. Model Development

The next step after preprocessing the data is modeling. So, we will adopt a hybrid machine learning approach where several algorithms will be combined to enjoy the best of their own. Fraudulent patterns present in the transaction data will be detected using Random Forest, XGBoost and Support Vector Machines (SVM). We will use Random Forest due to its ability to work on large datasets and prevent overfitting, while XGBoost fulfills its boosted performance by rectifying errors from earlier models in the ensemble. For a more effective discrimination of complex, high dimensional data, handling nuances in identifying fraudulent transactions, SVM will be used.

A hybrid model methodology is used so that a more reliable fraud detection system is created. XGBoost is good for fine tuning the predictions with its powerful gradient boosting techniques, while Random Forest will come to aid us with handling the large datasets without overfitting. An insertion of the sophistication as offered by SVM on cases of difficult to tackle fraud will refine the model of recognising patterns of fraud which otherwise would have not been spotted. The system will be trained on the full dataset for each model, so that they perform well for any type of fraud or transactions.

C. Model Evaluation and Optimization

Once trained on models, their performance will be evaluated on key metrics namely accuracy, precision, recall, F1 score and AUC-ROC (Area under the Receiver Operating Characteristic Curve). With these metrics we can assess totality how good the model is for catching the fraud, how many false positives, how many false negatives. Accuracy will give us an overview of the model's performance, which is important in general, but precision and recall are important metrics to watch for fraud detection as false negatives (missed fraud) are more expensive than false positives.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

DOI: 10.15680/IJIRSET.2025.1403189

Hyperparameter tuning will be carried out to find most adequate model parameters in order to optimize the models and increase performance. To determine the best possible combination of hyperparameters, techniques, such as grid search and random search will be used. To ensure good generalization to unseen data, it will implement cross-validation. These models will be found iteratively, fine tuned and tested on the various datasets to get the greatest precision possible in fraud detection and accuracy. During this optimization phase, the model is prepared to operate without much error on real-data.

D. Real-Time Fraud Detection

While there is no deployment in this project, the process will still be the same of ensuring that the fraud detection model can perform real time analysis. The system will be designed such that it will be capable of classifying transactions as legitimate or fraudulent, and will give users immediate predictions and risk assessments. Practically, they will be able to respond quickly to unmask fraud as transactions happen, with a view to reduce losses that come with processing of fraudulent transactions.

Furthermore, the model will also enable institutions to take decisions on prioritizing investigations by predicting the risk level of each transaction. Fraud detection results will be displayed using interactive visualizations namely transaction trends, risk levels, and what are the important features contributing to fraud detection. These features will enable users to use the insights gained to take action on their fraud prevention strategies.



Figure 1 System Architecture

IV. RESULTS AND DISCUSSION

The evaluation set for evaluating this fraud detection model consists of XGBoost, SVM, Random Forest, and so on multiple machine learning algorithms. The dataset in which transaction data existed were used to train these algorithms





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

and then test their performance with Help metrics like accuracy, precision, recall, F1 score, and AUC ROC. The models were then tested on a validation set and checked out on the level they could detect fraudulent transactions. The results of each model, together with their performance metrics, model comparison and visualizations of how the model detected illegal activity are provided in the next subsections.

A. Model Evaluation Metrics

The evaluation metrics for each model are shown in the table below. The performance of each algorithm was compared based on accuracy, precision, recall, F1-score, and AUC-ROC. These metrics are crucial for understanding how well the model detects fraud while minimizing the number of legitimate transactions flagged as fraudulent.

Model	Accu racy	Prec ision	Re cal l	F1-s core	AUC- ROC
Random Forest	0.94	0.91	0.8 9	0.90	0.95
XGBoost	0.95	0.93	0.9 1	0.92	0.96
Support Vector Machine	0.92	0.90	0.8 8	0.89	0.94

Table 1: Model Performance Comparison

These results demonstrate that XGBoost outperforms the other models in terms of accuracy, precision, recall, F1- score, and AUC-ROC. The higher AUC-ROC value indicates that XGBoost does a better job of distinguishing between fraudulent and legitimate transactions.

B. Feature Importance

Feature importance analysis reveals which variables had the greatest impact on predicting fraudulent transactions. Random Forest and XGBoost both provide feature importance scores, which help identify the key factors driving the model's predictions. These insights are valuable for understanding the model's decision- making process and can guide future feature selection for further improving model performance.

Table 2.	Top 5	Features	hv I	mportance
1 able 2.	1005	I catures	υγι	mportance

Feature	Importance Score
Transaction Amount	0.35
Time of Transaction	0.22
User Account Activity	0.18
Transaction Type (e.g., Debit/Credit)	0.15
Account Age	0.10





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

This table shows that the "Transaction Amount" and "Time of Transaction" are the most significant features for detecting fraud, followed by "User Account Activity" and "Transaction Type". These features are likely to have a high correlation with fraudulent behaviors and are crucial for the model's decision-making.

C. Performance Comparison and Visualizations

To better understand the model performance, we have included two graphs. The first graph compares the AUC- ROC scores of the three models, showcasing how well each model performs in distinguishing between fraudulent and legitimate transactions. The second graph visualizes the feature importance scores of the top features used by the models, providing insights into which factors are most influential in detecting fraud.



Figure 2: AUC-ROC Comparison

These graphs will provide a clear, visual comparison of the models' performance and highlight the most important features for fraud detection. The AUC-ROC graph will emphasize the superiority of XGBoost in distinguishing fraudulent transactions, while the feature importance graph will illustrate the factors that contribute most significantly to detecting fraud.



Figure 3 : Feature Importance

D. Discussion

From the model evaluation the results are clear that the XGboost was on par, although with significant improvements, in relation to other models such as Random forest and as far as SVMs are concerned whereas it has completely outperformed. XGBoost performed better than it in all the important evaluation metrics such as accuracy, precision, recall, F1 score and AUC ROC. Due to the gradient boosting technique used, it is particularly advantageous when trying to find fraudulent patterns within the complex banking data by sequentially refining errors. XGBoost performed well as well as Random Forest and did well in recall, although it does marginally worse in precision and overall AUC- ROC. However, unlike SVM, it had lower recall and AUC-ROC scores, meaning that it was worse than the other models in identifying fraudulent transactions.

The most important feature as per feature importance is Time of Transaction and Transaction Amount to detect the fraud. All models were very heavily dependent on these features, as these are known to be fraud patterns in the real

IJIRSET©2025





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

world, for example, buying large transaction sizes that are odd or transactions that never happen during regular business days tend to be associated with fraudulent activity. The visualizations, especially the AUC-ROC and the Feature Importance graphs, also validated the facts above the fact that XGBoost is simply great at guessing legitimate or fraudulent transactions. By this token the accuracy of fraud detection of the best features and choosing the right model can be lifted very much and with other search for other features or use of a hybrid modeling framework.



Figure 4: User Login and Signup Interface

The screenshot shows the login/signup page for the fraud detection system. Users can create an account or log in to access the fraud detection features. This page is essential for user authentication and security.

Logout	Fraud Detection in Banking Data	
Fraud Detection System	Credit Card Fraud Detection	
	0 reschart * Salert	~
Credit Card Fraud UPI Fraud Bank Account Fraud	calingsy * Select	
History	amuut * 1.00	- •
	gender * Select	~
	Lat*	

Figure 5: Credit Card Fraud Detection Input Form

This image shows the input form where users enter transaction details, such as credit card number, merchant information, transaction category, and amount. It is used for detecting credit card fraud by evaluating the entered transaction data.

Fransaction Analy	sis Results	
Safe: Low Risk Transaction	Fraud Percentage	
Risk Level	5.6%	Risk Score
low		50

Figure 6: Fraud Prediction with Risk Level

This figure displays the fraud prediction results, showing the calculated fraud probability and the associated risk level. The prediction indicates that the transaction has a low risk level, offering insights into the reliability of the transaction.





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025 (DOI: 10.15680/IJIRSET.2025.1403189)

Figure 7: Fraud Trends and Insights Visualization

The graph in this figure illustrates fraud probability against transaction amounts. It helps users analyze trends and identify how the amount of a transaction correlates with the likelihood of it being fraudulent, providing further insights into transaction patterns.



Figure 8: Detailed Fraud Analysis and Insights

This image provides a detailed view of fraud trends and further insights, showing how various factors affect fraud detection. It highlights transaction characteristics and their impact on fraud risk, offering users valuable data for decision-making.

V.CONCLUSION

Finally, the proposed machine learning algorithms based fraud detection system has successfully classified fraudulent transactions or predicted the risk for the transactions in real time. Through hybrid models like Random Forest, XGBoost, and Support Vector Machines, the system is able to provide a robust solution for detection of fraud for different banking transaction types such as Credit Card fraud, UPI fraud and Online payment fraud. Furthermore, the system's high accuracy, fast processing and transaction data analysis, and its feature importance analysis all make the system capable of expeditiously identifying risks posed by fraudulent activities to which the financial institutions can respond proactively. Future work can move towards integrating additional sophisticated features and increasing the scalability to be used in deploying in real world in order for more secure and more trusted digital financial transactions.

VI.FUTURE SCOPE

Future work in the detection of fraud on the model will include improving the model performance and extending its capabilities. The integration of more diverse dataset is one important aspect that can be improved by adding fraud data other than the normal ones like personal loan fraud or insurance fraud that would create a more comprehensive detection system. In addition, there can be more advanced machine learning techniques, so as deep learning or the ensemble methods, could enhance detection accuracy, particularly in detecting the emerging fraud patterns. Third, we consider optimization of real time processing in order to manage higher volumes of transactions efficiently in a high throughput environment and also to enable scaling in this direction. Additionally, the system could be more robust and





www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 3, March 2025

|DOI: 10.15680/IJIRSET.2025.1403189|

false positives would decrease, if more granular features, for instance, behavior analysis of the user or device fingerprinting is included. Finally, the system would be deployed into the real world banking environments and its performance would be continuously monitored, which will help to refine the model and adapt it to the new fraud tactics.

REFERENCES

[1]Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2022). Fraud detection in banking data by machine learning techniques. IEEE Access, 11, 3034-3043.

[2]Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions. The American journal of management and economics innovations, 6(06), 8-22.

[3]Mohammad, N., Prabha, M., Sharmin, S., Khatoon, R., & Imran, M. A. U. (2024). Combating banking fraud with it: integrating machine learning and data analytics. The American Journal of Management and Economics Innovations, 6(07), 39-56.

[4]Faisal, N. A., Nahar, J., Sultana, N., & Mintoo, A. A. (2024). Fraud Detection In Banking Leveraging Ai To Identify And Prevent Fraudulent Activities In Real-Time. Journal of Machine Learning, Data Engineering and Data Science, 1(01), 181-197.

[5]Esmail, F. S., Alsheref, F. K., & Aboutabl, A. E. (2023). Review of loan fraud detection process in the banking sector using data mining techniques. International journal of electrical and computer engineering systems, 14(2), 229-239.

[6]Bin Sulaiman, R., Schetinin, V., & Sant, P. (2022). Review of machine learning approach on credit card fraud detection. Human-Centric Intelligent Systems, 2(1), 55-68.

[7]Johora, F. T., Hasan, R., Farabi, S. F., Alam, M. Z., Sarkar,

M. I., & Al Mahmud, M. A. (2024, June). AI Advances: Enhancing Banking Security with Fraud Detection. In 2024 First InternationalConference on Technological Innovations and Advance Computing (TIACOMP) (pp. 289-294). IEEE.

[8]Kotagiri, A., & Yada, A. (2024). Improving Fraud Detection in Banking Systems: RPA and Advanced Analytics Strategies. International Journal of Machine Learning for Sustainable Development, 6(1), 1-20.

[9]Gautam, A. (2023). The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector. AI, IoT and the Fourth Industrial Revolution Review, 13(11), 9-18.

[10]Zanke, P. (2023). AI-Driven fraud detection systems: a comparative study across banking, insurance, and healthcare. Advances in Deep Learning Techniques, 3(2), 1-22.

[11]Biswas, A., Deol, R. S., Jha, B. K., Jakka, G., Suguna, M. R., & Thomson, B. I. (2022, October). Automated Banking Fraud Detection for Identification and Restriction of Unauthorised Access in Financial Sector. In 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 809-814). IEEE.

[12]Sekar, J. (2023). REAL-TIME FRAUD PREVENTION IN DIGITAL BANKING A CLOUD AND AI PERSPECTIVE. Journal of Emerging Technologies and Innovative Research, 10, P562-P570.

[13]Sambrow, V. D. P., & Iqbal, K. (2022). Integrating Artificial Intelligence in Banking Fraud Prevention: A Focus on Deep Learning and Data Analytics. Eigenpub Review of Science and Technology, 6(1), 17-33.

[14]Al-Fatlawi, A., Talib Al-Khazaali, A. A., & Hasan, S. H. (2024). AI-based model for fraud detection in bank systems. Fusion: Practice & Applications, 14(1).

[15]Achary, R., & Shelke, C. J. (2023, January). Fraud detection in banking transactions using machine learning. In 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE) (pp. 221-226). IEEE.









INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY





www.ijirset.com