Machine Learning Based Fraud Risk Scoring for Financial TransactionsUsing a Comparative Study of Random Forest and Support VectorRegression Models

Article · December 2024

DOI: 10.61096/ijiarec.v12.iss4.2024.1-9

Nagababu Kandula
Cvs Health Corporation

International Journal of Intellectual Advancements and Research in Engineering Computations (IJIAREC)

ISSN: 2348-2079

IJIAREC |Vol.12 | Issue 4 | Oct - Dec -2024
www.ijiarec.com
DOI :https://doi.org/10.61096/ijiarec.v12.iss4.2024.1-9

Review

Machine Learning Based Fraud Risk Scoring for Financial Transactions Using a Comparative Study of Random Forest and Support Vector Regression Models

Nagababu Kandula

Senior Software Development Engineer, CVS Health, Ohio, USA

*Author for Correspondence: Nagababu Kandula
Email: nagababu.kandula@gmail.com

Published on:27 Dec 2024

Published by:
Futuristic Publications

Abstract

Financial fraud poses a significant threat to global economic stability, with losses reaching trillions of dollars annually. Traditional rule-based fraud detection systems, constrained by reactive approaches and limited real-time processing capabilities, are increasingly inadequate against sophisticated modern fraud techniques. This research explores the implementation Using machine learning and artificial intelligence technology to detect financial transaction fraud in real time. The research examines key transaction parameters, including transaction size, transaction time, and fraud risk scoring algorithms, to develop robust detection algorithms. Two primary machine learning approaches are evaluated: random forest regression, which uses ensemble methods to reduce prediction variance through multiple decision trees, and support vector regression, which balances accuracy and model complexity by minimizing prediction errors. Cloud computing integration enhances AI-driven fraud detection by providing the computational scalability and real-time processing capabilities required for comprehensive financial analysis. While AI offers significant potential to improve detection accuracy and operational efficiency, challenges remain in algorithm transparency, interpretability, and data privacy compliance. The research addresses the ethical and regulatory considerations necessary for secure implementation. The results demonstrate that fraud detection systems with AI capabilities can drastically speed up response times and lower false positives, and strengthen financial security frameworks, ultimately protecting both financial institutions and consumers from fraud threats.

Keywords: Financial transactions, fraud detection, machine learning, artificial intelligence (AI), and real-time Processing, Cloud Computing, Fraud Risk Scoring and Financial Security

1. INTRODUCTION

The US banking sector is very concerned about financial transaction fraud, which makes sophisticated detection techniques more important algorithms. Traditional methods are hampered by their reactive nature and inability to handle vast volumes of data instantly, are gradually being AI-based solutions have taken its place. This study examines the application of artificial intelligence to real-time fraud detection, describing its advantages, disadvantages, and potential applications developments. Furthermore, maintaining a balance between Model performance, legal specifications, and moral principles continue to be crucial concerns. Notwithstanding these challenges, ongoing developments in AI offer significant potential. Improved data analytics, partnerships between financial institutions and AI developers, along with supportive regulatory frameworks, will foster innovation and strengthen fraud detection systems [1].ConventionalRule-based systems and historical data analysis-based fraud detection techniques are unable to combat the changing strategies of fraudsters. As a result, the financial industry is under increasing pressure to implement advanced technologies that can identify fraud immediately and effectively.

Artificial intelligence (AI) has become a key tool in this ongoing battle against financial fraud [2]. While AI has significant prospects for enhancing fraud detection, while addressing concerns like data privacy, interpretability, and algorithm openness need to be carefully addressed. Nevertheless, continued Research and development on AI-powered fraud detection has great promise for improving banking's accuracy and efficiency, if the ethical and practical challenges are effectively managed to ensure safe implementation [3]. Legacy Fraud detection systems, which mostly use rule-based techniques, are becoming more and more sophisticated in comparison to the sophisticated techniques employed by modern scammers. These antiquated systems can fall behind the rapidly changing digital fraud landscape, leading to frequent false positives and delayed responses. With the growing volume given the intricacy of financial transactions, quick, precise, and real-time fraud detection is essential solutions [4]. AI has improved operational efficiency across the financial sector and has transformed how organizations address key challenges such as fraud detection and transaction processing. As the volume and complexity of financial transactions continue to increase, conventional methods are proving inadequate, prompting a shift toward AI-powered solutions. Fraud poses a serious risk to financial institutions, leading to significant financial losses and eroding customer trust. Recent estimates suggest that global financial fraud could reach trillions of dollars annually, underscoring the urgent need for more advanced and proactive detection mechanisms [5]. It is crucial to maintain the integrity of financial transactions in the digital banking industry. While digital platforms offer unparalleled convenience, they also increase customer vulnerability to cyber threats, particularly bank account breaches. Fraud poses a serious threat to global economic stability, financial security, and trust in financial institutions. Electronic banking and credit card fraud cause significant annual losses, necessitating robust detection strategies. In response, financial institutions are actively investigating emerging fraud techniques [6].

The study also explores the moral and legal implications of financial fraud involving AI and machine learning detection, addressing key concerns such as privacy, accountability, and transparency in decision-making. By deepening our understanding of how these technologies can be used to combat financial fraud, the research seeks to provide meaningful insights that will influence the evolution of fraud prevention and financial security strategies. Ultimately, incorporating AI and ML into fraud detection systems will transform the financial security landscape, empowering organizations to respond more quickly and accurately in protecting their assets and customers [7]. By analysing case studies of machine learning-based this study emphasizes the efficiency of intelligent systems in safeguarding private information and financial assets through fraud detection in the domains of banking, e-commerce, and cyber security. Future studies ought to look into how emerging technologies such as Fraud detection capabilities can be significantly improved by explainable AI (XAI) and quantum computing. Machine learning enables businesses to improve data protection, increase detection precision, lessen monetary losses, and help create a more secure digital landscape [8]. This in-depth overview of AI-powered fraud detection and prevention explores the key principles of artificial intelligence. It explores a variety of machine learning methods, such as advanced deep learning, that are frequently employed in fraud detection approaches. Fundamental concepts are clarified, with particular emphasis on the role of generative adversarial networks (GANs) in developing innovative strategies for fraud prevention [9]. Cloud computing enhances AI-driven fraud detection by providing the computational scalability, flexible storage, and real-time processing required for comprehensive financial fraud analysis. Cloud-based platforms use distributed computing to handle high-speed transaction data, allowing for near-instantaneous fraud detection with minimal latency. Additionally, cloud infrastructure supports the exchange of fraud intelligence among organizations, enabling financial institutions to work together to detect and combat fraud across global payment systems. Beyond increasing detection accuracy, the combination of AI and cloud computing strengthens fraud prevention through adaptive recognition algorithms [10].

2. MATERIALS AND METHODS

Materials

Transaction Amount

Transaction amount refers to the absolute monetary value exchanged between parties during a financial transaction. It refers to the amount of money sent from one party to another, which typically occurs in purchases, payments, or financial transfers. Depending on the situation, it may also account for taxes, fees, or discounts. Accurate tracking of transaction amounts is essential for accounting, fraud detection, financial valuations, and ensuring clarity in personal and organizational financial activities.

Transaction Time

Transaction time refers to the exact date and time a financial transaction is made or finalized. It acts as a time stamp indicating when the exchange of money or services takes place, which is essential for documentation, audits, and the detection of fraudulent activities. Accurate transaction time helps detect unusual behaviour, verify account transactions, and comply with legal and regulatory standards. It is critical for ensuring transparency and accountability in both personal and corporate finances.

Is Fraud

Fraud is the intentional act of deception intended to achieve illegal or unethical financial gain. It typically involves the manipulation of information, systems, or transactions to deceive others for personal or organizational gain. Examples include credit card fraud, identity theft, and fraudulent financial reporting. Fraud poses significant threats to individuals, organizations, and the broader economy, resulting in financial losses, damage to trust, and the need for robust detection and prevention strategies to protect financial systems and data integrity.

Fraud Risk Score

A fraud risk score is a numerical indicator that reflects the probability of fraudulent behaviour associated with a transaction, user, or account. It is generated using algorithms or machine learning techniques that evaluate elements such as behavioural trends, transaction records, and irregularities. A higher score indicates an increased level of risk. This scoring algorithm helps financial institutions streamline investigations, improve automated fraud detection, implement preventive measures, reduce financial losses, and strengthen overall security.

Instructions for machine learning

Random Forest Regression

In machine learning, random forest regression is an ensemble technique and supervised learning algorithm. It builds multiple decision trees independently and in parallel to make predictions. This approach, often called packing, reduces prediction variance by building a large number of estimates for the same input. Compared to single decision trees, random forests are less likely to be over fitted, producing more accurate results with fewer training cycles. This method averages the outputs from different subsets of the training data used to build deep decision trees, which is intended to reduce variance. Although this can slightly increase bias and reduce model accuracy, it usually leads to a significant improvement in overall model performance.

Support Vector Regression

One kind of support vector machine (SVM) intended for regression applications is support vector regression (SVR). The objective is to identify a function that closely resembles a continuoustarget variable while balancing accuracy and model complexity by minimizing prediction errors. A widely used supervised learning method in machine learning, SVM is used in both classification and regression, with its primary strength in binary classification being its ability to partition data into two groups. The purpose of an SVM is to determine the optimal decision boundary that best separates the classes. The data points that are most important for defining this boundary are called support vectors. The margin shows how far these support vectors are from the decision boundary, which reflects the performance of the class separation.

3. RESULTS AND DISCUSSIONS

It provides data on fraud detection in AI-protected financial transactions. It consists of four main variables: transaction amount, transaction time, fraud indicator, and fraud risk score. The transaction amount shows the monetary value involved, while the transaction time indicates the hour of the transaction. The fraud indicator shows whether or whether the transaction is fraudulent (1). The fraud risk score measures the likelihood of fraud based on AI analysis. Higher scores generally correspond to higher fraud risk. The dataset illustrates how AI models assess transactions in real-time, using these features to effectively identify and predict fraudulent activities.

Table 1: Descriptive Statistics

	Transaction Amount	Transaction Time	Is Fraud	Fraud Risk Score
count	70.00000	70.00000	70.00000	70.00000
mean	468.01429	9.90000	0.15714	30.82857
std	303.64906	7.01169	0.36656	24.24750
min	21.56000	0.00000	0.00000	1.00000
25%	188.45000	4.00000	0.00000	16.25000
50%	436.61000	9.00000	0.00000	26.50000
75%	726.28500	14.00000	0.00000	34.00000
max	986.90000	23.00000	1.00000	99.00000

Table 1 presents descriptive statistics for the 70 transactions, including transaction amount, transaction time, fraud occurrence, and fraud risk score. The average transaction amount was approximately 468, with a wide range from about 22 to almost 987, indicating a high degree of variability. Transactions occurred multiple times, ranging from 0 to 23 units, with an average of 10. Fraud was relatively rare, with only about 16% of transactions being flagged as fraudulent. Fraud risk scores varied widely, with an average of 31 but ranging from 1 to 99. The standard deviations indicate a considerable spread in the sizes, times, and risk scores, highlighting the different transaction patterns and risk levels.

Effect of Process Parameters

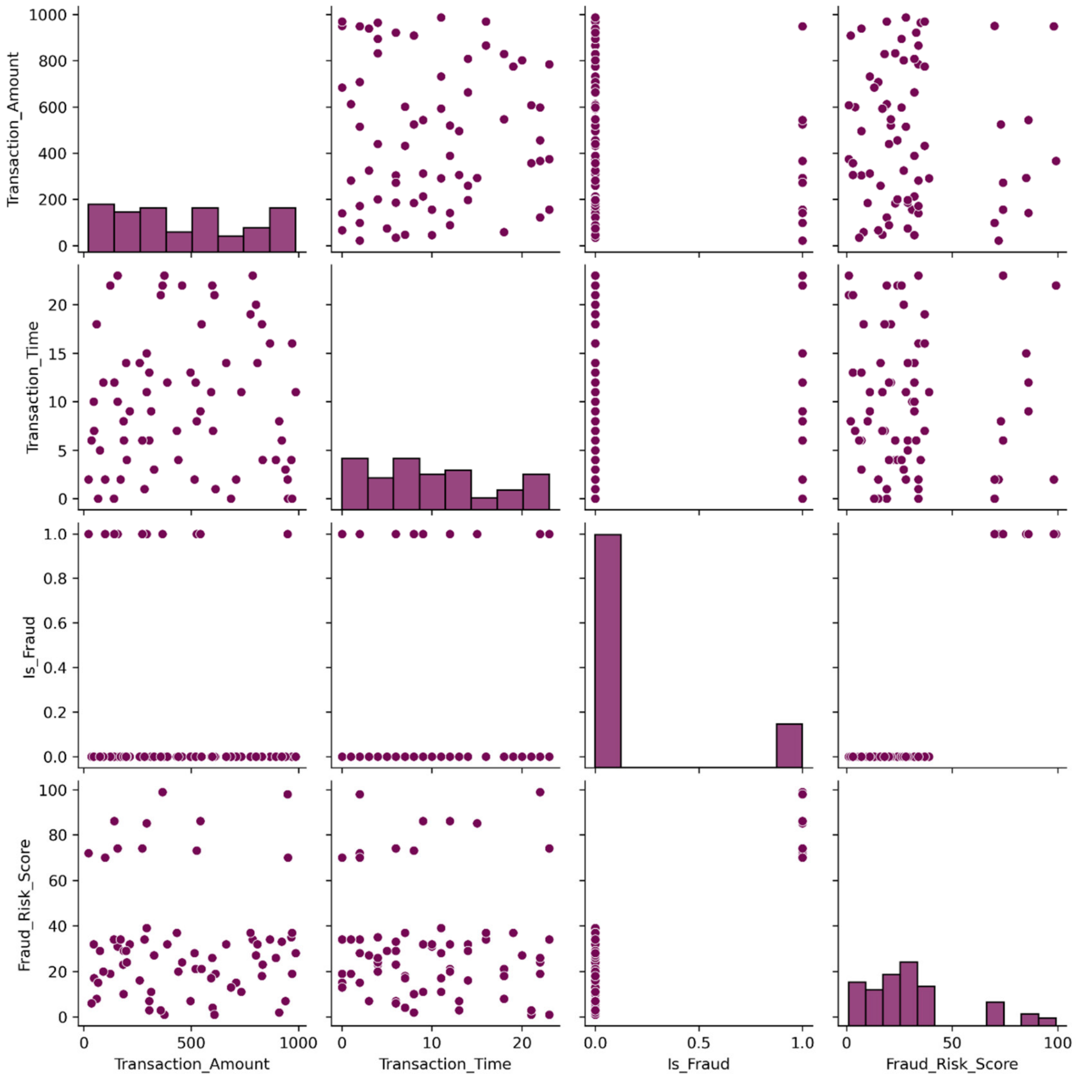

Fig 1: Scatter plot of the variousFraud Detection 20 with AI Securing Financial Transactions

Figure 1 presents a detailed scatter plot matrix that analyses key variables in fraud detection for financial transactions. The visualization reveals several important patterns: transaction amounts show a broad distribution with some high value outliers, transaction time clustering over specific time periods indicates temporal fraud patterns, and the fraud indicator (Is Fraud) shows the binary nature of fraudulent and legitimate transactions. Fraud risk scores show a right-skewed distribution, with most transactions receiving low risk scores, while a small subset shows a high fraud probability, indicating the efficiency of the model in determining suspicious activity.

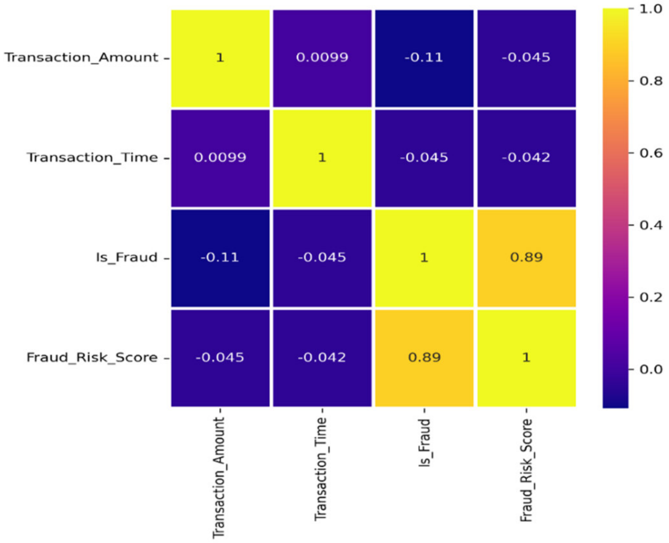

Fig 2: Heat map of the connection between results and process parameters

This Figure 2 correlation heat map reveals the relationships between key fraud detection variables in financial transactions. The most notable finding is the strong positive correlation between Is Fraud and Fraud Risk Score (0.89), indicating The AI model's remarkable prediction accuracy fraudulent activities. Transaction Amount shows weak negative correlations with both fraud indicators (-0.11 and -0.045), indicating that fraudulent transactions are not necessarily characterized by high volumes. Transaction Time shows the least correlation among all variables, indicating that temporal patterns alone are not sufficient predictors of fraud, emphasizing the importance of multidimensional risk assessment approaches.

Random Forest Regression

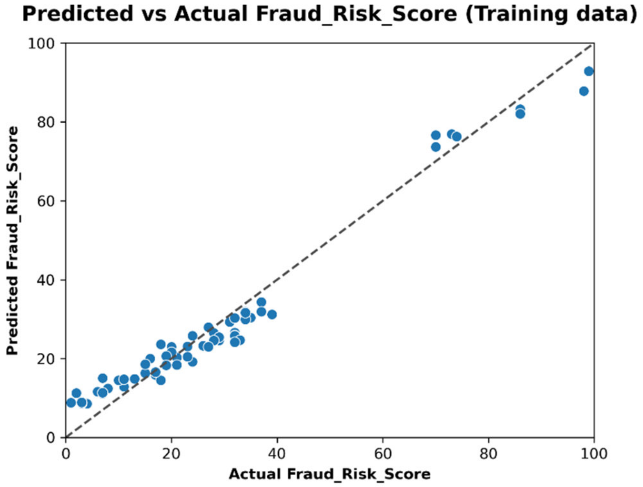

Fig 3: Random Forest Regression (Training data)

This Figure 3 scatterplot demonstrates the performance of the random forest regression model on the training data for fraud risk score prediction. The points that are in tight alignment with the diagonal reference line show that the expected and actual fraud risk scores. The model shows excellent prediction accuracy throughout the whole risk score range, from low risk (0–20) to high risk (80-100) transactions. The tight clustering around the correct prediction line indicates minimal prediction error and confirms the effectiveness of the random forest algorithm in learning complex patterns within the fraud detection dataset during training.

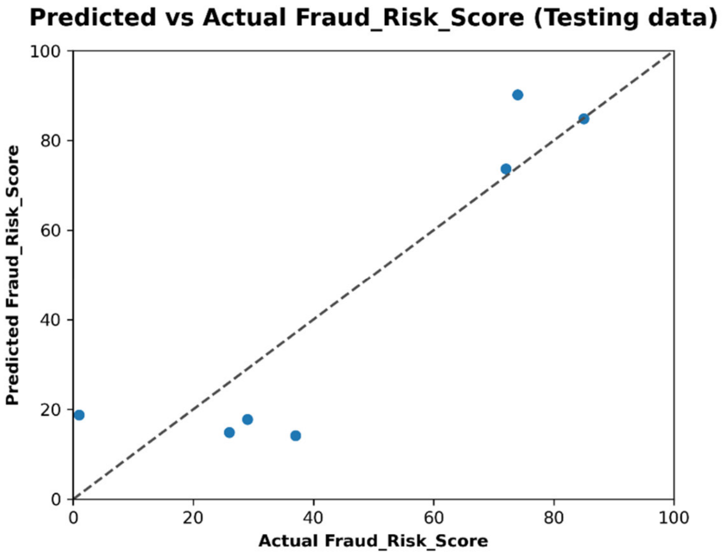

Fig 4: Random Forest Regression (Testing data)

This Figure 4 scatterplot evaluates the performance of the random forest regression model on unobserved test data for fraud risk score prediction. Unlike the training data results, the test performance shows a high variance from the diagonal reference line, indicating some over fitting in the model. While high-risk transactions (range 60-90) maintain reasonable prediction accuracy, there is significant dispersion in the low to moderate risk ranges. The reduced clustering around the correct prediction line compared to the training data indicates that the generalization ability of the model is acceptable, but could benefit from regularization techniques to improve robustness on new data.

Table 2:Performance Metrics of Random Forest Regression (Training Data and Testing Data)

Data	Symbol	Model	R2	EVS	MSE	RMSE	MAE	Max Error	MSLE	MedAE
Train	RFR	Random Forest Regression	0.96171	0.96183	20.01560	4.47388	3.82492	10.17000	0.14262	3.72000
Test	RFR	Random Forest Regression	0.76533	0.76761	193.61660	13.91462	11.57857	22.87000	0.94850	11.24000

Table 2 shows the performance metrics of the random forest regression (RFR) model on both the training and test datasets. On the training data, the model exhibits remarkable performance, with a high R² of 0.96, indicating strong predictive accuracy, and low error values such as an RMSE of 4.47 and an MAE of 3.82. However, the test data exhibits reduced performance, with an R² of 0.77 and considerably more mistakes, with an RMSE of 13.91 and an MAE of 11.58 – indicating some over fitting. Metrics such as Max Error and MSLE also increase significantly in the test, highlighting the challenges in generalizing the model to unseen data.

Support Vector Regression

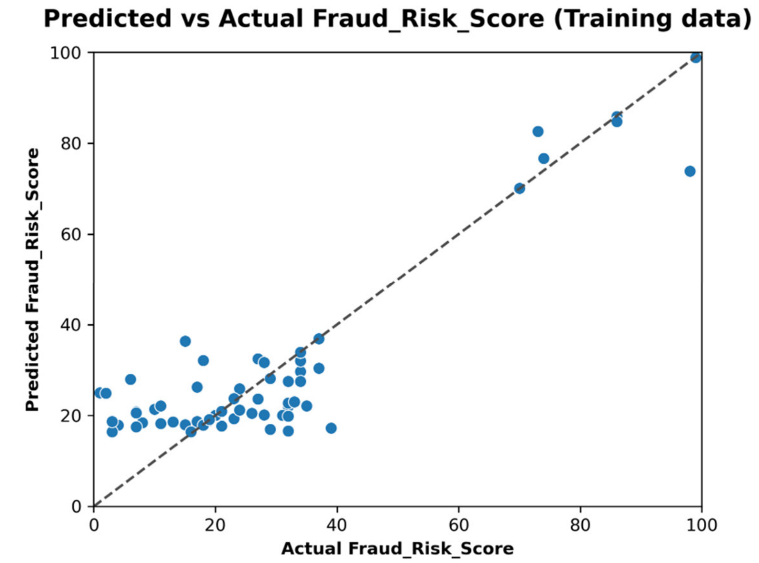

Fig 5:Support Vector Regression (Training data)

Figure 5 illustrates the performance of using the training data and the support vector regression model for fraud risk score prediction. The results show moderate prediction accuracy, especially in the low to moderate risk ranges (0-40), with significant deviation from the best diagonal line. Although high-risk transactions (60-100) show better alignment with the actual scores, there is considerable dispersion across the prediction range. The SVR model appears to struggle with accurate predictions compared to the Random Forest approach, indicating that the nonlinear relationships in the fraud detection data may be better captured by ensemble methods than kernel-based regression techniques.

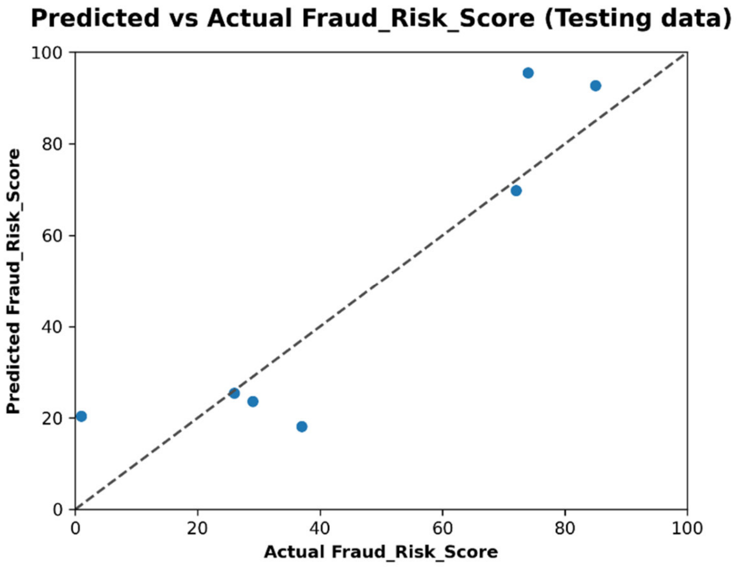

Fig 6: Support Vector Regression (Testing data)

Figure 6 shows a scatterplot of the performance of the support vector regression model in testing the data for fraud risk score prediction. The results reveal significant challenges in the generalization ability of the model, with significant deviation from the best-fit diagonal prediction line. The scattered data points show inconsistent prediction accuracy across different risk score ranges, with some high-risk transactions correctly identified while others show poor alignment. The limited clustering around the reference line indicates that SVR struggles with over fitting and may not effectively capture complex fraud detection methods when applied to unseen data.

Table 3:Performance Metrics of Support Vector Regression (Training Data and Testing Data)

Data	Symbol	Model	R2	EVS	MSE	RMSE	MAE	MaxError	MSLE	MedAE
Train	SV	Support Vector Regression	0.80404	0.80697	102.44040	10.12129	7.32380	24.15677	0.44805	5.52821
Test	SVR	Support Vector Regression	0.77719	0.78892	183.83550	13.55859	10.78213	21.50108	0.88584	7.70995

Table 3 summarizes the performance of the Support Vector Regression (SVR) model on the training and testing datasets. On the training data, SVR shows moderate accuracy with 0.80 R² and 10.12 RMSE, indicating a reasonable fit but high error compared to random forest regression. The testing data exhibits slightly lower performance with 0.78 R² and increased errors, including RMSE 13.56 and MAE 10.78. The Max Error and MSLE values are also higher during testing, reflecting some decrease in prediction accuracy on the unseen data, although overall SVR maintains stable performance between the phases of testing and training.

4. CONCLUSION

This research demonstrates the significant potential Using machine learning and artificial intelligence technology in transforming fraud detection for financial transactions. A comparative analysis between random forest regression and support vector regression reveals unique performance characteristics that inform practical implementation results. Random forest regression emerged as the best approach, achieving exceptional training performance with an R² of 0.96 and minimal error metrics (RMSE: 4.47, MAE: 3.82). However, the model showed some over fitting tendencies, as evidenced by reduced testing performance (R² of 0.77, RMSE: 13.91). Support vector regression showed more consistent but moderate performance in both training (R² of 0.80) and testing phases (R² of 0.78), indicating better generalization capabilities despite lower overall accuracy. The strong correlation between actual fraud indicators and AI-generated fraud risk scores (0.89) confirms the effectiveness of machine learning approaches in identifying fraudulent activities. The analysis revealed that transaction sizes show minimal correlation with fraud occurrences, emphasizing that sophisticated AI models can detect fraud patterns beyond traditional rule-based systems that rely heavily on transaction size limitations. Key findings show that although AI-powered solutions perform noticeably better than traditional fraud detection techniques, challenges remain in model generalization and over fitting prevention. The integration of cloud computing infrastructure enhances real-time processing capabilities, enabling immediate fraud detection with minimal latency. Future studies should concentrate on creating hybrid models that include the precision of ensemble methods with advanced generalization capabilities. Additionally, the addition of explainable AI (XAI) techniques will address transparency concerns while maintaining detection performance. Implementing regularization techniques and cross-validation strategies can mitigate over fitting issues found in high-performance models. The study confirms that fraud detection solutions driven by AI can greatly improve financial security frameworks and lower false positives, and improve response times, ultimately protecting both consumers and financial institutions from new fraud risks in the world of online banking.

REFERENCES

1. Bello, OluwabusayoAdijat, AbidemiOgundipe, Damilola Mohammed, FolorunsoAdebola, and OlalekanAyodejiAlonge. "AI-Driven Approaches for real-time fraud detection in US financial transactions: challenges and opportunities." European Journal of Computer Science and Information Technology 11, no. 6 (2023): 84-102.
2. Johora, FatemaTuz, RakibulHasan, SyedaFarjanaFarabi, Mohammad ZahidulAlam, Md Imran Sarkar, and Md Abdullah Al Mahmud. "AI Advances: Enhancing Banking Security with Fraud Detection." In 2024 First International Conference on Technological Innovations and Advance Computing (TIACOMP), pp. 289-294. IEEE, 2024.
3. Islam, MdZahidul, Sanjib Kumar Shil, and MdRashedBuiya. "AI-driven fraud detection in the US financial sector: Enhancing security and trust." International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence 14, no. 1 (2023): 775-797.

4. Ballamudi, S. "Interleaved Feature Extraction Model Bridging Multiple Techniques for Enhanced Object Identification" Journal of Artificial Intelligence and Machine Learning., 2023, vol. 1, no. 2, pp. 1-7. doi: https://doi.org/10.55124/jbid.v1i2.253
5. Johora, FatemaTuz, RakibulHasan, SayedaFarjanaFarabi, JahanaraAkter, and Md Abdullah Al Mahmud. "AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions." The American journal of management and economics innovations 6, no. 06 (2024): 8-22.
6. Potla, Ravi Teja. "AI in fraud detection: Leveraging real-time machine learning for financial security." Journal of Artificial Intelligence Research and Applications 3, no. 2 (2023): 534-549.
7. Dachepalli. V, "Data Analysis For Students Based On Geolocation Approach" International Journal of Interpreting Enigma Engineers (IJIEE)., 2024, vol. 1, no. 3, pp. 33–41. doi: https://doi.org/10.62674/ijiee.2024.v1i03.005
8. Narsina, Deekshith, Jaya Chandra SrikanthGummadi, S. S. M. G. N. Venkata, A. Manikyala, S. Kothapalli, K. Devarapu, M. Rodriguez, and R. R. Talla. "AI-Driven Database Systems in FinTech: Enhancing Fraud Detection and Transaction Efficiency." Asian Accounting and Auditing Advancement 10, no. 1 (2019): 81-92.
9. Scientific, Little Lion. "AI-Driven Fraud Detection And Security Solutions: Enhancing Accuracy In Financial Systems." Journal Of Theoretical And Applied Information Technology 103, No. 8 (2025).
10. Sridhar Kakulavaram. (2022). Life Insurance Customer Prediction and Sustainbility Analysis Using Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 10(3s), 390 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7649
11. Onabowale, Oreoluwa. "AI and Machine Learning in Fraud Detection: Transforming Financial Security." (2024).
12. Alonge, Enoch Oluwabusayo, Nsisong Louis Eyo-Udo, Bright ChibunnaUbanadu, Andrew IfesinachiDaraojimba, Emmanuel DamilareBalogun, and KoladeOlusolaOgunsola. "Enhancing data security with machine learning: A study on fraud detection algorithms." Journal of Data Security and Fraud Prevention 7, no. 2 (2021): 105-118.
13. Rani, Sonam, and Ajit Mittal. "Securing Digital Payments a Comprehensive Analysis of AI Driven Fraud Detection with Real Time Transaction Monitoring and Anomaly Detection." In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), vol. 6, pp. 2345-2349. IEEE, 2023.
14. Narender, M., and A. Jose Anand. "Artificial Intelligence in Financial Fraud Detection." In Handbook of AI-Driven Threat Detection and Prevention, pp. 193-207. CRC Press, 2025.
15. Sriram, Harish Kumar. "Leveraging AI and Machine Learning for Enhancing Secure Payment Processing: A Study on Generative AI Applications in Real-Time Fraud Detection and Prevention." Available at SSRN 5203586 (2024).
16. Ramancha, N. K., &Ballamudi, S. (2023). Leveraging Machine Learning for Predictive Modeling in 3D Printing of Composite Materials: A Comparative Study. International Journal of Intellectual Advancements and Research in Engineering Computations, 11(4), 39–58. https://doi.org/10.61096/ijiarec.v11.iss4.2023.39-58
17. Elumilade, Oluwafunmike O., IbidapoAbiodunOgundeji, Godwin OzoemenamAchumie, Hope EhiagheOmokhoa, and Bamidele Michael Omowole. "Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security." Journal of Advanced Education and Sciences 1, no. 2 (2021): 55-63.
18. Rehan, Hassan. "Leveraging AI and cloud computing for Real-Time fraud detection in financial systems." Journal of Science & Technology 2, no. 5 (2021): 127.
19. Dhieb, Najmeddine, Hakim Ghazzai, HichemBesbes, and YehiaMassoud. "A secure ai-driven architecture for automated insurance systems: Fraud detection and risk measurement." IEEE Access 8 (2020): 58546-58558.
20. Iseal, Sheed, Oluwaseyi Joseph, and Shalom Joseph. AI in Financial Services: Using Big Data for Risk Assessment and Fraud Detection. 2025.
21. Choi, Dahee, and Kyungho Lee. "An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation." Security and Communication Networks 2018, no. 1 (2018): 5483472.
22. Kalisetty, Srinivas, Chandrashekar Pandugula, Lakshminarayana Reddy Kothapalli Sondinti, Goli Mallesham, and PR Sudha Rani. "AI-Driven Fraud Detection Systems: Enhancing Security in Card-Based Transactions Using Real-Time Analytics." Journal of Electrical Systems 20 (2024): 1452-1464.
23. Islam, MdShakil, and Nayem Rahman. "AI-Driven Fraud Detections in Financial Institutions: A Comprehensive Study." Journal of Computer Science and Technology Studies 7, no. 1 (2025): 100-112.
24. Pramudito, Dendy, JufriadifNa'am, and Ferda Ernawan. "Exploring Blockchain and AI in Digital Banking: A Literature Review on Transactions Enhancement, Fraud Detection, and Financial Inclusion." Sistemasi: JurnalSistemInformasi 14, no. 3 (2025): 1448-1459.
25. Pramudito, Dendy, JufriadifNa'am, and Ferda Ernawan. "Exploring Blockchain and AI in Digital Banking: A Literature Review on Transactions Enhancement, Fraud Detection, and Financial Inclusion." Sistemasi: JurnalSistemInformasi 14, no. 3 (2025): 1448-1459.
26. Bello, OluwabusayoAdijat, AdebolaFolorunso, Oluomachi Eunice Ejiofor, FolakeZainabBudale, Kayode Adebayo, and Olayemi Alex Babatunde. "Machine learning approaches for enhancing fraud prevention in financial transactions." International Journal of Management Technology 10, no. 1 (2023): 85-108.
27. Banu, Akhter. "AI-Powered Digital Identity Protection: Preventing Fraud in Online Transactions." (2024).
28. Al-Mansouri, Ahmed. "Graph Databases for Fraud Detection: A Fresh Look at Financial Security." International Journal of Digital Innovation 2, no. 1 (2021).
29. Fallah, Mohammed Hussein, DharmapuriSiri, G. Ravi Kumar, G. Sheeba, Himanshu Sharma, and A. Devendran. "AI-Powered Blockchain Systems for Real-Time Fraud Detection in Financial Services." In 2024 International Conference on IoT, Communication and Automation Technology (ICICAT), pp. 1287-1291. IEEE, 2024.