Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1 (2025)

AI-Powered Fraud Prevention: Strategic Machine Learning in E-Commerce Transactions

Dr Kamalakkannan Adhisekar
Department of Corporate Secretaryship and Accounting & Finance,
SRM Institute of Science and Technology, Chengalpattu, India.
kamalaka@srmist.edu.in
Dr Sanjay Kumar
Assistant Professor, Department of Management,
Central University of Rajasthan, Kishangarh, Rajasthan, India,
sanjaygarg@curaj.ac.in
Pavithra A
Assistant Professor, Department of Information Technology,
K. Ramakrishnan College of Engineering (Autonomous) Trichy,
Tamilnadu, India.
paviaru0906@gmail.com
Mohammad Shahanwaz Nasir
Lecturer, Department of Computer Science,
College of Engineering and Computer Science, Jazan University,
Saudi Arabia.
mnasir@jazanu.edu.sa
Dr Prashant Gupta
Department of E-Business,
Welingkar Institute of Management Development and Research,
Mumbai, India.
prashantgupta197@gmail.com
P K Sudhakar
Assistant Professor, Rajalakshmi Institute of Technology,
Tamilnadu, India.
sudhakarpk_susila@yahoo.com

ABSTRACT:
Combining AI with predictive analytics is changing the way fraud detection and risk assessment are done in the ever-changing world of financial services. Identifying complex fraudulent activities and evaluating financial risks can be challenging using traditional methods since they are reactive and based on past data. On the other hand, AI-powered predictive analytics provides a preventative measure by analysing massive volumes of data in real-time using sophisticated algorithms and ML approaches. Financial institutions can quickly and accurately identify patterns of suspicious activity that could be caused by fraud using this method. Artificial intelligence models can anticipate dangers before they happen by analysing past transactions, user habits, and external variables. Adaptive learning allows machine learning algorithms to continuously improve their predictions, making them better able to spot new forms of fraud and evaluate risk indicators on the go. In addition, financial services may now personalize their risk assessment tactics for each client and transaction with the use of AI's predictive analytics. Operational efficiency and customer happiness are both enhanced by this personalization, which enables more accurate risk management and decreases the probability of false positives. Insights generated by AI also help with decision-making because they give useful information for things like strategic planning and allocating resources. A more robust and secure financial ecosystem is the end result of incorporating AI and predictive analytics into the financial services industry, which also improves the capacity to detect fraud and evaluate risk.

Keywords: Random Forest Regression, Fraud Detection, E-commerce.

1. Introduction

The e-commerce business has reached unprecedented heights in recent years, thanks to the ubiquitous availability of mobile devices and the ever-expanding internet. The digital revolution has changed consumer behavior in a profound way, ushering in a new culture that values accessibility and ease of use. Traditional, brick-and-mortar retailers no longer dictate how customers shop. These days, consumers may choose from an almost endless variety of things while shopping online, all from the comfort of their own homes. Using trusted online payment gateways, making a purchase is as simple as clicking a button. Companies and customers alike have undoubtedly benefited from the arrival of this era of unprecedented development in e-commerce. Companies benefit from a global marketplace with few territorial limits, and customers enjoy unparalleled convenience, affordable costs, and a significantly larger variety of items. The growing online marketplace is a fertile ground for bad actors who are adept at exploiting its vulnerabilities[1]. Electronic commerce fraud, which encompasses a broad range of unethical practices aimed at obtaining goods or funds without appropriate payment, poses a significant threat to the financial security and reputation of online businesses. The financial and insurance sectors are feeling the full force of the technological revolution brought about by artificial intelligence and predictive analytics. The way institutions handle fraud detection and risk assessment is being transformed by new technologies, which overcome the flaws of conventional approaches. Conventional systems often rely on static rules and prior data. As the intricacy and complexity of financial processes increase, so does the need for state-of-the-art methods to reduce risk and combat fraud. The foundation of fraud detection systems in the financial sector has always been predefined criteria and historical trends[2]. Although these technologies are useful to a certain extent, they may struggle to keep up with the constantly evolving tactics used by fraudsters. The fast development of new types of fraud means that conventional methods often fall behind. Similarly, if risk assessment methodologies rely on static data and don't properly predict potential financial hazards, organizations could be exposed to unanticipated dangers. In order to detect potential instances of fraud, these algorithms search for unusual or suspicious patterns. Because of their ability to learn and adapt in real-time, AI models outperform more traditional methods when it comes to detecting sophisticated fraud schemes. Because fraudulent conduct in e-commerce platforms poses major challenges to transaction security systems, strong detection and prevention strategies are necessary. Experts in the field and those in academia have been working together to fortify online payment systems against fraudulent transactions[3]. The intrinsic complexity and ever-changing nature of e-commerce operations make successful fraud prevention a considerable issue. The obfuscation tactics employed by malicious actors make it difficult to identify and prevent fraudulent operations based solely on past order data. In the past, rule-based systems and analysis of previous transactions have been the mainstays of online retail fraud prevention and detection efforts[4]. Although these methods have shown some promise, they often fall short when it comes to capturing the dynamic behaviors exhibited by online buyers. Due to the diverse user behaviors and rapid evolution of online commerce, a more advanced and adaptable technique is needed to detect fraud. This study presents a novel technique to fraud detection that makes use of several viewpoints, which aims to circumvent the shortcomings of traditional methods. By integrating process mining and machine learning to analyze user actions in real-time from different angles, the proposed method aims to enhance the effectiveness of fraud detection.

2. Literature Survey

The use of Machine Learning (ML) models has revolutionized fraud detection by making it more accurate and scalable [5]. Banking, financial services, and online shopping rely heavily on these models due to the enormous transaction volumes that necessitate ongoing monitoring for fraud. ML techniques include Supervised Learning frameworks, unsupervised learning methodologies, and

hybrid models have helped solve many fraud detection challenges. E-commerce algorithms' novel ML-based financial transactions and application are examined [6] with accuracy of 99.89%. The winning Back Propagation Neural Network (BPNN) model detected financial fraud. This work [7] suggests real-time online fraud detection with Support Vector Machine (SVM). Supervised learning models are the backbone of many anti-fraud solutions. Using tagged training data, these models can differentiate between real and suspected fraudulent transactions [8]. To distinguish between legitimate and fraudulently labeled transaction histories, the model requires a dataset including both types of data. Many popular supervised learning methods include Logistic Regression (LR), Gradient Boosting Machines (GBM), Decision Trees (DT), and Random Forests (RF) [9]. LR is commonly used when a detailed description of the model is required because it is easy to understand and use. Using the amount, type of merchant, and time of transaction as input features[10], this model can estimate the likelihood of a fraudulent transaction. This study [11] demonstrated ML and Deep Learning (DL) algorithms can detect internet fraud. Sequential Convolutional Neural Network (CNN), Naïve Bayes (NB), LR, K-nearest Neighbor (KNN), and Random Forest (RF) learning algorithms use regular and exceptional transaction characteristics. We test the model with public data. Many algorithms had visual accuracy: NB 96.2%, LR 94.7%, KNN 95.88%, RF 97.55%, and Series CNN 92.4%. Kaggle's Fraud Detection dataset can detect fraudulent transactions [12][13]. Due to its linear decision boundary, LR could miss intricate fraud patterns involving features with non-linear relationships. DT have long been a part of it; they make greater use of decision rules learnt from the dataset to repeatedly partition the feature space into distinct areas [14]. ML algorithms are becoming crucial for the detection of fraudulent activities in e-commerce supply chains. The majority of models are either DT, Neural Networks (NNs), or SVMs[15]. Each of these models has its own set of pros and cons, particularly when used for transaction-level analysis [16]. When DT are too huge, they become less interpretable and more complicated, which can reduce their efficiency in large-scale applications. Kaggle detected and prevented financial transaction fraud. Big data is used to evaluate online banking dangers and user behavior. Internet banking and large data concerns start this risk management article. These algorithms were evaluated for accuracy (96.38%), recall (70.97%), precision (88.15%), and F-Score (16.37). The lowest error detection method was 7.18%. One type of powerful classifier that works well with high-dimensional data is the SVM, which can distinguish between classes with a considerable margin of separation [17]. Because they may use kernel functions to handle both linear and non-linear decision boundaries, they are adaptable to complex fraud detection scenarios. DL models, which are a subset of NNs, have shown remarkable performance in challenging fraud detection tests. Data architectures with connected nodes might help them make sense of complicated patterns and correlations [18]. They stand out from simpler models due to their extraordinary ability to identify complex and subtle patterns of deception. Because of their adaptability, neural networks can handle large datasets and keep up with changing fraud trends. Many authors have proposed [19]. We are expanding our marketing efforts beyond first-time buyers by leveraging the Fraud detection framework to raise the profile and credibility of emerging online services and goods. The proposed SVM model beats state-of-the-art simulation methods with 97.7% recall, 96.8% accuracy, 96.7% f1-score ratio, and 20.9 percent error rate. We employ BiGRUs and BiLSTMs in our BiLSTM-MaxPooling model. Also employed were six ML classifiers: NB, Ada boosting, Voting, RF, LR, and DT. Compared to ML classifiers, our model was 91.38% efficient. LR is a leading tool for detecting fraudulent transactions when outcomes are categorized. Fitting the data to a logical function can anticipate many events, including fraud, by correcting for known variables and historical data. DT, adaptable algorithms, were examined because they may produce intelligible rules depending on transaction features [20]. For fraud detection, decision trees sort or partition data by transaction factors like amount, location, and frequency. Fraud probability can be predicted. Rule-based systems' intelligence lets them detect questionable transactions and alert authorities. RF used ensemble learning to reduce overfitting and improve fraud detection [21][22]. By integrating several decision trees, random forests improve fraud detection. Its better capacity to analyze massive data

sets and complicated patterns makes it adept in detecting fraudulent conduct across a variety of trading scenarios, benefiting the financial industry's risk mitigation efforts. Engineered to mimic the brain's architecture, NNs can understand complicated data patterns and relationships. NNs excel in detecting fraudulent tendencies, abnormalities, and misclassified transactions in huge transaction data.

3. Methodology

The essay delves into the changing function of AI in classrooms, highlighting the revolutionary changes it has brought about in the ways students learn and teachers present information. It explores the ways in which AI technologies, including ChatGPT and other machine learning algorithms, remodel classroom instruction. It focusses mainly with two areas: first, how students use new tools to their advantage in the classroom, and second, how educators might incorporate them into their own educational practices.

A. Preprocessing

The process of extracting useful features from raw data, is an essential part of data preparation. The AI model's capacity to learn and detect fraudulent behaviours is heavily influenced by these qualities, which serve as its foundation. A thorough familiarity with the data and the particulars of the fraud detection job at hand is necessary for feature engineering[23]. For example, characteristics like the amount of time that elapses between an order's placement and the delivery attempt, or the frequency with which a user's account is linked to changes in location, can be particularly helpful in detecting fraudulent behavior. Online retailers may take their fraud detection to the next level by making good use of artificial intelligence technology and carefully maintaining their data. Through data pre-processing, raw data can be transformed into a clean dataset. In other words, when data is gathered from multiple sources, it is unfair to use unprocessed data for evaluation. Preprocessing refers to the steps taken with a dataset before feeding it into an algorithm. Here are the main steps of the preprocessing:

1) Missing and Null Values

Essential to data preparation is the management of null values. To deal with missing data correctly, imputation and removal methods are employed. As a result, investigators can be assured that their dataset is accurate and of high quality before diving into analysis and modeling.

2) Encoding Categorical Variables:

The possible values of a variable are usually described by a set of predefined categories.

3) Data Scaling:

The Data noise can be effectively reduced through scaling. Here, a regular scalar is used to perform data scaling. By applying z-score normalization, standard scalar ensures that all values fall inside a predetermined range. A popular technique for

$$\mathrm{R(T)} = 1 + \mathrm{e}^{-(\mathrm{c+lt})} \quad (1)$$

Z-score normalization (Equ.1), where is the input variable and is the base of the natural logarithm, can be defined as:

$$\mathrm{Z} = \frac{(\mathrm{T} - \rho)}{\tau} \quad (2)$$

where z represents the value that has been standardized, T represents the value that was originally set,

ρ represents the mean of the feature, and τ represents its standard deviation.

B. **Feature Selection:**

Data mining and knowledge-based authentication rely on feature selection. Machine learning, pattern recognition, and statistics are just a few of the fields that have done extensive research on the feature selection problem. It created a new feature selection method based on Hausdorff distance for evaluating online traffic data, and he noted that most data mining programs spend 80% of their efforts on cleaning and prepping the data. Any learning algorithm relies on feature selection, which, if done incorrectly, can cause issues including inadequate information, irrelevant or noisy features, not using the best set of features, and many more[24]. It used the simplest statistical technique in the characteristic's selection phase of this investigation. One of the effective methods for selecting features is the t-statistic. The features are ranked using the formula shown below. In fact, it pioneered the use of the t-statistic in bioinformatics for feature selection.

$$\mathrm{t-statistic} = \frac{|\rho_1 - \rho_2|}{\sqrt{\frac{\tau_1^2}{z_1} + \frac{\tau_2^2}{z_2}}} \qquad (3)$$

The standard deviation of the samples of non-fraudulent companies for a given feature is denoted by υ2, whereas the means of the samples of fraudulent companies are represented by μ1 and μ2, respectively. In this case, n1 and n2 are the sample sizes of fraudulent and non-fraudulent companies, respectively, for the specified feature. Consideration is given to the top 18 features in the first case and the top 10 features in the second case based on the t-statistic values that were computed for each feature. If the feature's t-statistic is large, it means it can distinguish between samples of fraudulent and non-fraudulent organizations with surprising accuracy.

C. **Model Training**

1) LR:

When the results are categorical, like in deciding if a transaction is fraudulent or not, logistic regression—a baseline approach in fraud detection—is especially helpful. Through the process of fitting the data to a logical function, it is possible to predict the probabilities of various events. This tool can shed light on the possibility of fraud depending on certain parameters and past data. Analyzing transaction data and identifying possibly fraudulent activity is made easier with its straightforward and understandable design. Because of its ability to forecast binary outcomes using numerous predictor variables, logistic regression is generally acknowledged as a crucial method in the domain of binary classification[25]. To estimate the likelihood that an input is connected with a specific category, logistic regression uses the logistic function, also called the sigmoid function, $\tau(n) = \frac{1}{1+q-n}$ A linear combination of features denoted as $n = \alpha_0 + \alpha_1 t_1 + \alpha_2 t_2 + \cdots + \alpha_z t_z$ is typically used as an input to the function, which is designed to provide a value between 0 and 1. The given value indicates the likelihood that the dependent variable will equal 1. Methods like maximum likelihood estimation are used to estimate the model coefficients $\alpha_0, \alpha_1, \ldots, \alpha_z$, with the goal of maximizing the probability of observing the provided sample data. Logistic regression's simplification and ease of interpretation have made it a popular choice as a methodology in many different industries, including healthcare, business, and finance. The fact that this occurrence can shed light on the likelihood of different events makes its probabilistic component very esteemed[26]. When it comes to making decisions and evaluating risks, this quality is crucial. The ability to adjust the classification threshold, which is often set at 0.6, provides flexibility in different scenarios, allowing for the optimization of the false positive/false negative trade-off based on the specific context. Despite its apparent simplicity, logistic regression demonstrates an impressive degree of

accuracy, especially when the relationship between the variables and the result is linear. Overfitting is less likely to occur with this model compared to more complex ones. A further advantage is that it is easy to understand and use because the coefficients are directly related to the odds ratios, which provides clear information about how each predictor variable is influencing the outcome.

2) RF:

Because of its ease of use, little computing requirements, and straightforward design, random forest is frequently considered a technologically integrated solution. When applied to a variety of real-world scenarios, the Random Forest algorithm has proven to be very effective. Training decision trees using bagging integration, the random forest method employs a random selection of attributes. Learners who rely on decision trees often use this tactic. In a perfect world, we could divide the current sample evenly in half and use the resulting decision tree model to accurately forecast what's to come. There are never any situations that are this simple in reality[27]. An overflow of data and overfitting occur when the division level is too exact, and a substantial difference between the expected and actual values makes it difficult to accurately complete the prediction task. Researchers have come up with new ways to measure the necessity of more segregation, like the Gini index and knowledge gain.

The information entropy of A is defined as the fraction of class k samples in the current sample set A, where $r_i (i = 1,2, \dots, |\delta|)$.

$$\mathrm{Ent(a)} = -\sum_{i=1}^{|M|} r_i \log_2 r_i \quad (4)$$

The discrete attribute an is assumed to have H potential values. The information gained from partitioning sample set A with attribute an is, where a^H denotes the samples in set A whose value is a^H when divided according to discrete attribute c.

$$\mathrm{Gain(a,c)} = \mathrm{Ent(c)} \sum_{H=1}^{H} \frac{|a^H|}{|a|} \mathrm{Ent}(a^H) \quad (5)$$

Partitioning using attribute a usually results in a purity boost that increases in direct proportion to the information obtained. Therefore, the data collected can be used to determine if this attribute is divided up in the subsequent step of decision tree creation.

3) NN:

Neural networks are strong algorithms that can understand intricate data patterns and correlations by modelling themselves after the architecture of the human brain. Neural networks stand out in the field of fraud detection for their exceptional ability to efficiently handle massive volumes of transaction data in order to spot irregularities, categorize transactions, and uncover patterns of fraud. In the never-ending battle against financial fraud, their adaptability and detection of complex fraud schemes make them an essential instrument. This allows organizations to safeguard their assets by staying ahead of developing risks. When it comes to protecting online transactions and boosting confidence in online interactions, the use of AI for fraud detection is a huge leap forward. Artificial intelligence systems are able to anticipate and prevent fraud because they use data analytics and machine learning to adapt to new fraud strategies. More effective and efficient fraud detection is on the horizon as AI technology develops further, which will bolster security measures in all kinds of businesses[22]. However, in order to keep trust and accountability in AI-driven fraud detection systems, it is

necessary to address ethical issues and ensure transparency. Enhancing security and encouraging trust in the digital environment will remain a top priority for AI researchers and industry stakeholders.

4) DT:

As a multi-purpose algorithm, decision trees are great at using transactional details to generate rules that are easy to understand and apply. For the purpose of fraud detection, decision trees are employed to categorize or divide data in order to forecast the probability of fraud according to attributes of transactions including number, place, and frequency. Their natural intelligence paves the way for rule-based systems to discreetly detect questionable transactions and alert authorities.

II. RESULTS AND DISCUSSION

To make use of and analyse the vast quantities of data produced by online transactions, advanced cyber-infrastructure and information technology approaches are required. This research presents an e-commerce industry-specific big data platform for online merchants to use in responding to a range of challenges. As a global issue, fraud affects both individuals and companies. Machine learning (ML) and artificial intelligence (AI) have been tremendous allies in the fight against fraud in today's tech-driven world. This essay examines the common knowledge of fraud prevention and demonstrates how it is out of date in comparison to contemporary fraud tactics. Learn more about how ML and AI are facilitating rapid digitization and how it is changing the game when it comes to preventing fraud. Businesses can now sift through mountains of data in search of irregularities that may indicate fraudulent behaviour thanks to AI and machine learning technologies.

TABLE I. PERFORMANCE PREDICTION(%)

Model	Accuracy	Precision	Recall
DT	93.44	90.15	91.05
NN	91.60	89.54	90.34
LR	95.86	93.44	94.80
RF	89.21	87.60	88.43

Table 1 shows a comparison of four ML models for e-commerce fraud prevention: DT, NN, LR, and RF. The models are evaluated according to recall, precision, and accuracy. Accuracy (95.66%), precision (93.44%), and recall (94.8%) are all best achieved by LR. This demonstrates how well LR works for accurate and trustworthy predictions in the field of e-commerce fraud prevention.

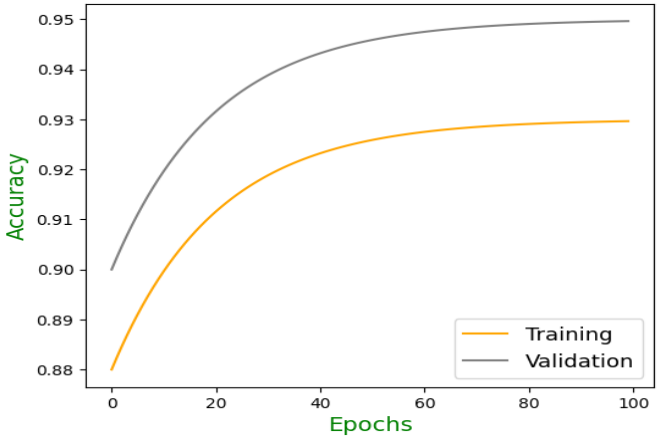

Fig. 1. Training and Validation Accuracy of ML Models

Figure 1 shows the growth in accuracy for both the training and validation datasets over the course of an epoch, demonstrating the effectiveness of AI-powered fraud prevention models in online purchases. The model's capacity to generalize and successfully detect fraud is demonstrated by the continual rise in validation accuracy. These systems are able to adapt to new fraud patterns because they use strategic machine learning techniques like neural networks. This improves confidence in online transactions, protects e-commerce platforms, and guarantees strong fraud detection.

TABLE II. AUC PERFORMANCE PREDICTION (%)

Model	**ROC**
DT	95.62
NN	97.04
LR	97.48
RF	96.29

The AUC-ROC performance of various models for e-commerce transaction fraud detection is evaluated in table 2. The greatest area under the curve is achieved by LR, suggesting that it is better at differentiating between fraudulent transactions.

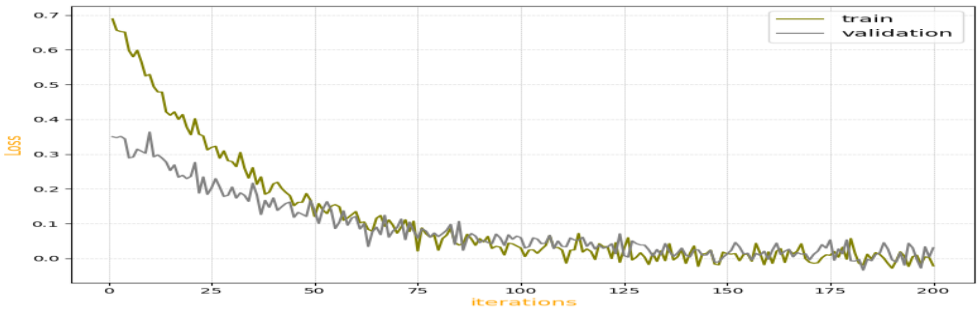

Fig. 2. Training and Validation Loss of the Models

Fig. 3.

In a system that uses artificial intelligence to detect online shopping fraud, the training and testing loss converges, as shown in figure 2. Both curves are trending downward, which means the machine learning algorithm is picking up trends to identify fraud. The model appears to avoid overfitting, as evidenced by the near alignment of the train and test losses, which indicates strong generalization. For accurate fraud detection across different types of transactions.

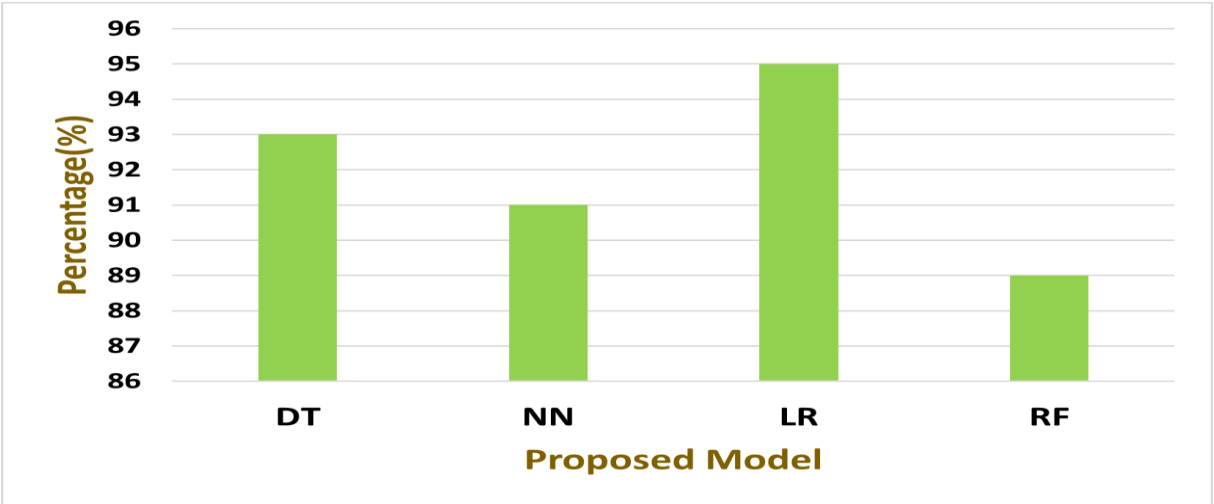

Fig. 4. Accuracy Comparison of Various Models

Figure 3 is a bar chart comparing the accuracy rates of four different models used for e-commerce fraud detection: DT, LR, NN, and RF. When compared to other models, the suggested one (LR) achieves the best accuracy, showing how well it can detect fraudulent actions. With the help of AI models, e-commerce platforms can conduct transactions reliably and securely.

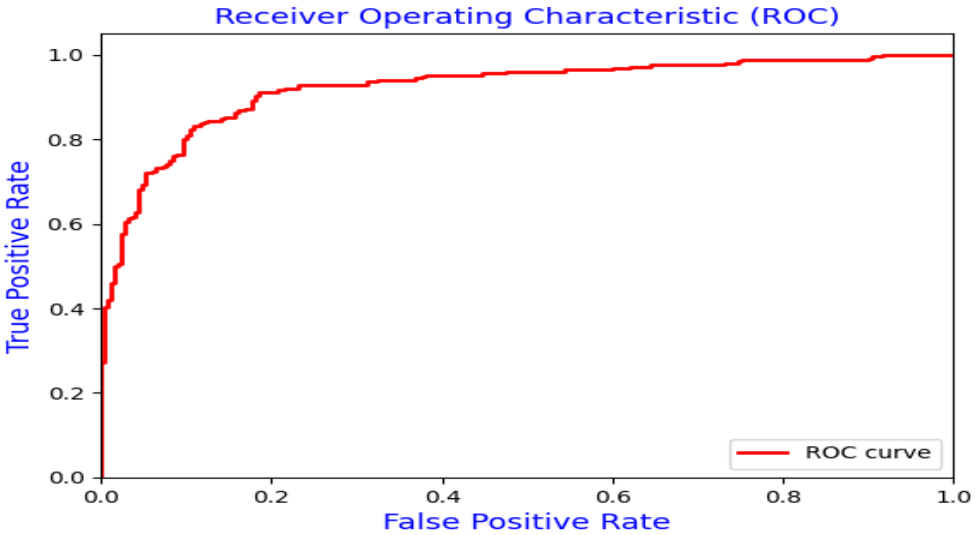

Fig. 5. ROC Curve for Fraud Prevention Strategic Machine Learning in E-Commerce Transactions

The ROC curve in Figure 4 shows how well an e-commerce fraud detection model driven by AI performs. The curve shows the compromise between the two rates, one representing the detection of fraud and the other the flagging of legitimate transactions as fraudulent. High fraud detection accuracy with minimum false alarms is shown by the curve nearing the top-left corner, indicating the model's effectiveness.

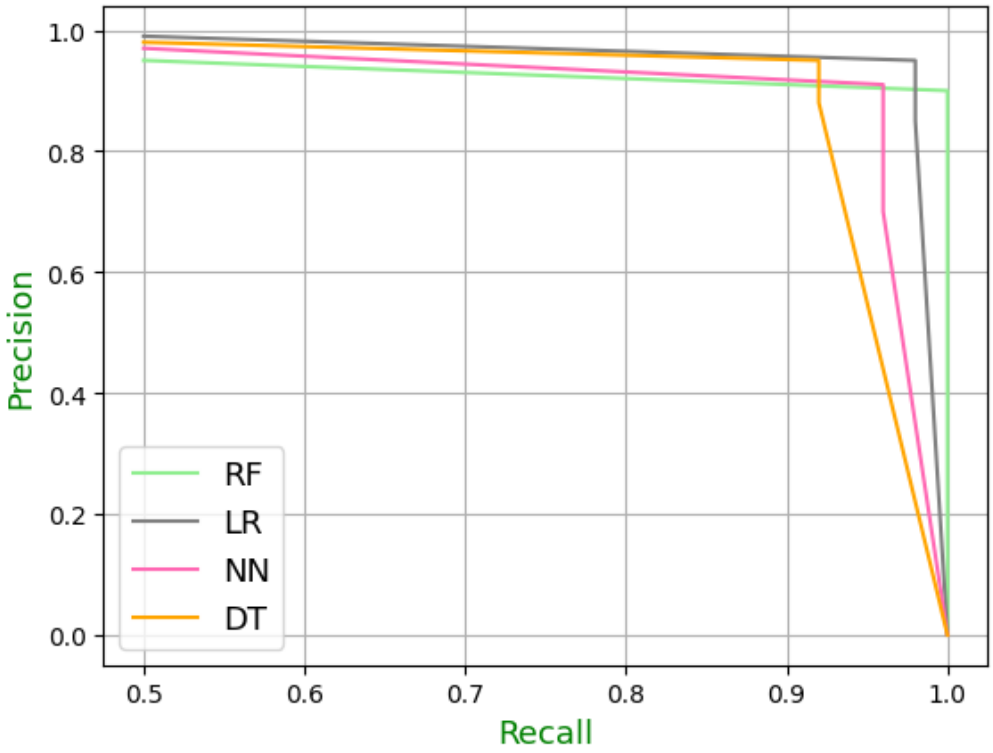

Fig. 6. Precision-Recall Curve for Fraud Prevention in E-Commerce Transactions

Figure 5 shows a comparison of four machine learning models used for e-commerce fraud detection: RF, LR, NN, and DT. It reveals how well any model finds a happy medium between recall (the number of actual fraud cases found) and accuracy (the number of fraud cases correctly identified). Model performance is better indicated by curves close to the top-right corner. By comparing different models, we can choose the one that best detects fraudulent actions with the fewest false positives.

III. CONCLUSION AND FUTURE DIRECTIONS

With its unrivaled accessibility and ease, e-commerce has completely transformed the retail industry, thanks to its meteoric rise. On the flip side, fraud has flourished in this digitally transformed world. Online firms are particularly vulnerable to e-commerce fraud, which includes misleading transactions with the intent to steal money or items without proper payment. It causes huge financial losses, customer trust, and messes with operational efficiency. Enhancing e-commerce fraud detection skills through the deployment of AI techniques is the focus of this proposed. A formidable weapon against fraudulent operations is AI, thanks to its capacity to sift through enormous datasets, spot intricate patterns, and adjust to new dangers. Anomaly detection, transaction monitoring, and risk reduction are the three essential components of AI-driven fraud detection that are examined in this study. An LR model was used for training. At its peak, the suggested model achieves an accuracy of 95.86 percent.

REFERENCES

[1] S. R. Gayam, "AI-Driven Fraud Detection in E-Commerce : Advanced Techniques for Anomaly Detection , Transaction Monitoring , and Risk Mitigation," Distrib. Learn. Broad Appl. Sci. Res., vol. 6, pp. 124–151, 2020.

[2] W. Yu, Y. Wang, L. Liu, Y. An, B. Yuan, and J. Panneerselvam, "A Multiperspective Fraud Detection Method for Multiparticipant E-Commerce Transactions," IEEE Trans. Comput. Soc. Syst., vol. 11, no. 2, pp. 1564–1576, 2024, doi: 10.1109/TCSS.2022.3232619.

[3] A. Yuille, "AI-Powered Financial Services : Enhancing Fraud Detection and Risk Assessment with Predictive Analytics," ResearchGate, no. August, 2024, doi: 10.13140/RG.2.2.23580.09603.

[4] E.-A. MINASTIREANU and G. MESNITA, "An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection," Inform. Econ., vol. 23, no. 1/2019, pp. 5–16, 2019, doi: 10.12948/issn14531305/23.1.2019.01.

[5] K. Yamini, V. Anitha, S. Polepaka, R. Chauhan, Y. Varshney, and M. Singh, "An Intelligent Method for Credit Card Fraud Detection using Improved CNN and Extreme Learning Machine," in 2023 8th International Conference on Communication and Electronics Systems (ICCES), IEEE, Jun. 2023, pp. 810–815. doi: 10.1109/ICCES57224.2023.10192774.

[6] N. M. Reddy, K. A. Sharada, D. Pilli, R. N. Paranthaman, K. S. Reddy, and A. Chauhan, "CNN-Bidirectional LSTM based Approach for Financial Fraud Detection and Prevention System," in 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), IEEE, Jun. 2023, pp. 541–546. doi: 10.1109/ICSCSS57650.2023.10169800.

[7] R. Rajkumar, N. Kogila, S. Rajesh, and A. R. Begum, "Intelligent System for Fraud Detection in Online Banking using Improved Particle Swarm Optimization and Support Vector Machine," in 2023 8th International Conference on Communication and Electronics Systems (ICCES), IEEE, Jun. 2023, pp. 644–649. doi: 10.1109/ICCES57224.2023.10192690.

[8] I. A. K. Shaikh, R. P. Pujar, S. P. Kishore, S. Ragamayi, P. V. Krishna, and A. B. Nadaf, "A Novel Approach for E-Commerce System for Sale Prediction with Denoised Auto Encoder and SVM based Approach," in 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), IEEE, Jun. 2023, pp. 1684–1689. doi:

10.1109/ICSCSS57650.2023.10169595.

[9] K. Rathor, S. Vidya, M. Jeeva, M. Karthivel, S. N. Ghate, and V. Malathy, "Intelligent System for ATM Fraud Detection System using C-LSTM Approach," in 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE, Jul. 2023, pp. 1439–1444. doi: 10.1109/ICESC57686.2023.10193398.

[10] S. Kakkar, "Analysis of Discovering Fraud in Master Card based on Bidirectional GRU and CNN based Model," 2023 Int. Conf. Self Sustain. Artif. Intell. Syst., no. Icssas, pp. 50–55, 2023, doi: 10.1109/ICSSAS57918.2023.10331770.

[11] K. Prabhakar, M. S. Giridhar, A. Tatia, T. M. Joshi, S. Pal, and U. S. Aswal, "Comparative Evaluation of Fraud Detection in Online Payments Using CNN-BiGRU-A Approach," Int. Conf. Self Sustain. Artif. Intell. Syst. ICSSAS 2023 - Proc., no. Icssas, pp. 105–110, 2023, doi: 10.1109/ICSSAS57918.2023.10331745.

[12] S. Yadav, R. Singh, E. Manigandan, M. V. Unni, S. Bhuvaneswari, and N. Girdharwal, "Research on Factors Affecting Consumer Purchasing Behavior on E-commerce Website During COVID-19 Pandemic based on RBF-SVM Network," 2nd Int. Conf. Autom. Comput. Renew. Syst. ICACRS 2023 - Proc., pp. 371–376, 2023, doi: 10.1109/ICACRS58579.2023.10404765.

[13] R. Udayakumar, A. Joshi, S. S. Boomiga, and R. Sugumar, "Deep Fraud Net: A Deep Learning Approach for Cyber Security and Financial Fraud Detection and Classification," J. Internet Serv. Inf. Secur., vol. 13, no. 4, pp. 138–157, 2023, doi: 10.58346/JISIS.2023.I4.010.

[14] K. Kumar et al., "Forecasting E-Commerce Sales Adoption Based on DE-ELM-RGSO Approach," 2nd Int. Conf. Intell. Data Commun. Technol. Internet Things, IDCIoT 2024, pp. 954–959, 2024, doi: 10.1109/IDCIoT59759.2024.10467941.

[15] D. Prusti and S. K. Rath, "Fraudulent Transaction Detection in Credit Card by Applying Ensemble Machine Learning techniques," 2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019, 2019, doi: 10.1109/ICCCNT45670.2019.8944867.

[16] T. Porkodi, "An Automatic ATM Card Fraud Detection Using Advanced Security Model Based on AOA-CNN- XGBoost Approach," 2024 Int. Conf. Electron. Comput. Commun. Control Technol., pp. 1–7, 2024, doi: 10.1109/ICECCC61767.2024.10593851.

[17] N. Kogila, R. Rajkumar, S. Rajesh, and S. Vennila, "A Novel Approach of Ecommerce for Sales Prediction Using Hybrid ABC and AdaBoost Approach," in 1st International Conference on Electronics, Computing, Communication and Control Technology, ICECCC 2024, IEEE, 2024, pp. 1–6. doi: 10.1109/ICECCC61767.2024.10593970.

[18] N. Pol and S. Agarwal, "Online Transaction Fraud Detection : Exploring the Hybrid SSA-TCN-BiGRU Approach," 2024 2nd World Conf. Commun. & Comput., pp. 1–6, 2024, doi: 10.1109/WCONF61366.2024.10692254.

[19] S. Vii, G. D. Rede, P. Ramesh, R. Kumar A, A. Bharathi, and M. C. J. Anand, "Optimizing E-Commerce Fraud Detection with BiGRU and Capsule Network Architectures," in 2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024, 2024, pp. 1–6. doi: 10.1109/ICDSNS62112.2024.10691229.

[20] B. Vyas, "Java in Action : AI for Fraud Detection and Prevention," Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., pp. 58–69, 2023, doi: 10.32628/cseit239063.

[21] C. Ghayor, I. Bhattacharya, and F. E. Weber, "Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics," Mater. Des., p. 109650, 2021, [Online]. Available: https://doi.org/10.1016/j.matdes.2021.109650

[22] J. Xu, T. Yang, S. Zhuang, H. Li, and W. Lu, "AI-based financial transaction monitoring and fraud prevention with behaviour prediction," Appl. Comput. Eng., vol. 67, no. 1, pp. 76–82, 2024, doi: 10.54254/2755-2721/67/2024ma0068.

[23] P. Khare and S. Srivastava, "AI-Powered Fraud Prevention: A Comprehensive Analysis of Machine Learning Applications in Online Transactions," J. Emerg. Technol. Innov. Res., vol.

10, no. July, pp. f518–f525, 2023.

[24] P. Ravisankar, V. Ravi, G. Raghava Rao, and I. Bose, "Detection of financial statement fraud and feature selection using data mining techniques," Decis. Support Syst., vol. 50, no. 2, pp. 491–500, 2011, doi: 10.1016/j.dss.2010.11.006.

[25] A. J. Balyemah, S. J. Y. Weamie, J. Bin, K. V. Jarnda, and F. J. Joshua, "Predicting Purchasing Behavior on E-Commerce Platforms: A Regression Model Approach for Understanding User Features that Lead to Purchasing," Int. J. Commun. Netw. Syst. Sci., vol. 17, no. 06, pp. 81–103, 2024, doi: 10.4236/ijcns.2024.176006.

[26] T. Xiong, Z. Ma, Z. Li, and J. Dai, "The analysis of influence mechanism for internet financial fraud identification and user behavior based on machine learning approaches," Int. J. Syst. Assur. Eng. Manag., vol. 13, pp. 996–1007, 2022, doi: 10.1007/s13198-021-01181-0.

[27] H. Zhou, G. Sun, S. Fu, W. Jiang, and J. Xue, "A scalable approach for fraud detection in online e-commerce transactions with big data analytics," Comput. Mater. Contin., vol. 60, no. 1, pp. 179–192, 2019, doi: 10.32604/cmc.2019.05214.