Received: 22 November 2024 | Revised: 13 January 2025 | Accepted: 14 March 2025 | Published online: 13 May 2025

RESEARCH ARTICLE

FinTech and Sustainable Innovation
2025, Vol. 1, A7, 9 Pages
DOI: 10.47852/bonviewFSI52024882

BON VIEW PUBLISHING

Enhancing E-commerce Security: A Hybrid Machine Learning Approach to Fraud Detection

Mohit Vasant[1,*], Swathi Ganesan[1,*] and Ganapathy Kumar[2]

[1]*Department of Computer Science, York St John University, United Kingdom*

[2]*Independent Researcher, United Kingdom*

Abstract: In the rapidly expanding e-commerce landscape, ensuring the security of transactions is essential to maintain consumer trust. However, the challenge of accurately distinguishing between genuine and fraudulent transactions persists, largely due to issues such as dataset imbalance, suboptimal feature selection, and varying algorithm performance. As such, this study aims to enhance fraud detection accuracy by developing a hybrid model that combines an artificial neural network (ANN) with a deep neural network (DNN), employing the Synthetic Minority Oversampling Technique (SMOTE) to address class imbalance and linear discriminant analysis (LDA) for effective feature extraction. By integrating SMOTE with LDA, the model is trained to better handle imbalanced datasets and extract relevant features, thereby improving its predictive capabilities. Our results demonstrate that the hybrid model outperforms individual models, achieving a precision rate of 95.46% and an area under the curve (AUC) score of 97.04%. In comparison, the stand-alone ANN model recorded an accuracy of 95.46% and an AUC of 96.92%, while the DNN achieved a success rate of 95.01% and an AUC of 97.17%. These outcomes highlight the significant advantages of combining advanced feature extraction and class imbalance techniques, resulting in superior detection performance. The study concludes that the hybrid model provides a robust solution for improving fraud detection in e-commerce, offering a reliable approach to differentiate between genuine and fraudulent transactions effectively. This approach not only addresses existing challenges but also sets a foundation for future research in enhancing transaction security through innovative deep learning methodologies.

Keywords: e-commerce financial transactions, deep learning algorithms, feed forward neural network, deep artificial neural network, linear discriminant analysis

1. Introduction

The global economy, daily life, and company operations are all affected by financial crimes, as significant amounts of money are lost daily to fraudsters on e-commerce platforms like Alibaba, AliExpress, Jumia, and Amazon [1, 2]. As a result, the e-commerce sector places a strong preference on identifying fraudulent conduct and preventing it [3]. E-commerce frauds are mostly conducted using credit cards [4]. According to Kumar et al. [5], detecting illicit financial dealings is a challenging task. As such, a very important area for the development of AI is in the detection of fraud [6]. Because consumer behavior shifts over time and fraudsters modify their methods, many interconnected issues fall under this category of problems, including concept drift, feature extraction methods, and class imbalance (since several financial transactions undergo periodic audits conducted by authorities) [1]. Be that as it may, when put to the test in real-world scenarios, many of the proposed machine learning (ML) algorithms for e-commerce fraud detection systems end up falling flat [7].

Consequently, Sailusha et al. [8] found that data mining findings for this kind of fraud detection are inaccurate. According to Bagga et al. [9], one potential approach to enhance the accuracy of e-commerce fraud detection is by using advanced algorithms such as deep learning (DL) and ML. The dataset, algorithm performance, class imbalance management, and feature choices are some of the significant challenges that remain after the implementation of several DL and ML tactics to prevent financial fraud. A larger ratio of genuine to fraudulent transactions is seen in certain datasets used to train these algorithms [1].

This inequality in class may cause ML and DL models to underperform, as they tend to favor the majority [10]. Xie et al. [11] noted that training trustworthy models using datasets for online fraud detection might be tough because of things like high-dimensional and class imbalance data. The process of feature selection includes either creating new features from the ground up or narrowing the existing set of features to just those that are relevant to the task at hand [12]. These details are often indicators of fraudulent behavior [13]. Contrarily, fraud detection makes use of class imbalance methodologies. As stated by Boutaher et al. [7], synthetic sampling, undersampling, and oversampling are often used methodologies.

***Corresponding authors:** Mohit Vasant and Swathi Ganesan, Department of Computer Science, York St John University, United Kingdom. Emails: mohit.vasant@yorksj.ac.uk and s.ganesan@yorksj.ac.uk

In order to ensure that the dataset is balanced, synthetic sampling uses methods like the Synthetic Minority Oversampling Technique (SMOTE) to produce fresh instances of the minority class [14]. On the other hand, oversampling makes instances of the minority class redundant, while undersampling randomly picks a fraction of the most populated class [11]. These methods lessen the dominance bias in DL models and increase their accuracy [15]. Concept drift occurs when the pattern in data changes over time, making it difficult for the model to detect or handle new inputs. This study introduces a hybrid model that compares the standalone artificial neural network (ANN) and deep neural network (DNN) techniques to improve the accuracy of e-commerce fraud detection.

2. Literature Review

Using the Ethereum network as a case study, Taher et al. [16] conducted extensive research on detecting fraudulent transactions within cryptocurrency exchanges. The study relied on a massive, pre-processed dataset of Ethereum transactions. It outperformed the individual classifiers and the soft voting method in detecting fraudulent transactions with a 99% accuracy rate by using a few ML methods and ensemble approaches, such as the hard voting ensemble model. However, the study did not utilize two other feature extraction methods: linear discriminant analysis (LDA) and data resampling.

A comparison of logistic regression and random forest methods for fraud detection was conducted in the work by Valli et al. [17]. The researchers used a transaction dataset and employed the R programming language. The best accuracy score, 87.11%, was attained by random forest. While the study's use of individual machines yielded commendable results, the incorporation of hybrid DL techniques could potentially enhance the outcomes by stacking the strengths of multiple models.

In Ali et al. [18], a study focuses on developing a DL model for online transaction fraud prediction using the SMOTE. The findings indicate that a convolutional neural network (CNN) outperformed both ANN and long short-term memory recurrent neural network. However, these algorithms were trained independently, without exploring the potential benefits of combining their strengths. Additionally, class balancing relied solely on SMOTE, and feature selection methods were not considered.

Using ML techniques, Mytnyk et al. [19] aimed to detect bank fraud. Feature engineering and feature transformation were among the various strategies used to fix the datasets that had severe imbalances. The best results were achieved using the logistic regression approach, which had an output area under the curve (AUC) value of around 0.946. The AUC is 0.954, which is better for the stacking generalization. Although the study's usage of the stacked generalization methodology has shown commendable results, it might have been even more effective if the authors had investigated LDA and SMOTE as feature selection techniques.

Research by Abdaljawad et al. [20] looks at how well multiple ML systems detect the validity of financial transactions. When learning from an uneven collection of data following the SMOTE to level the dataset before training the models, the authors found that the Random Forest Classifier had the greatest success rate (99.97%). Conversely, trained on a balanced dataset, the Bagging Classifier attained an amazing accuracy rate of 99.96%. Though the authors applied SMOTE class imbalance methods, the approaches were applied to certain learning algorithms.

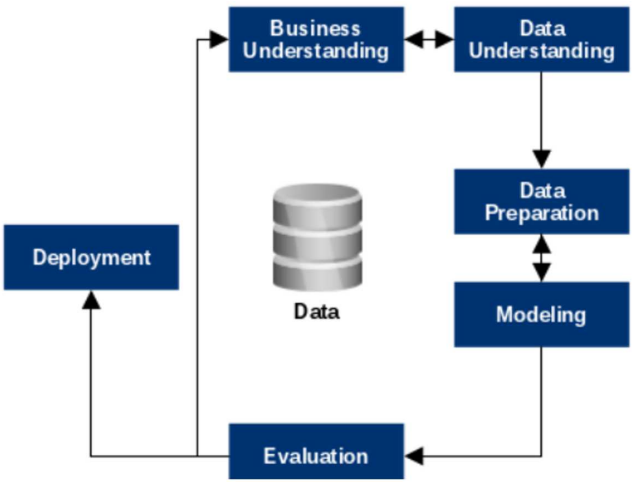
Using decision trees, random forests, linear regression, and gradient boosting, among other ML approaches, Valavan and Rita [21] analyzed and contrasted cases of loan fraud. The study included developing and comparing the proposed models as part of its methodology. The results show that the gradient boosting method is the most effective with a total accuracy of 94.47%. Though the paper used the Gini score to split the decision tree and gradient descent to minimize the error function, other techniques such as LDA and SMOTE weren't explored.

3. Research Methodology

3.1. Research design

This research follows CRISP-DM, which stands for Cross-Industry Standard Process for Data Mining [22]. Data science efforts may be better coordinated with the help of CRISP-DM, facilitating adaptability in real-world applications [23]. The organized and iterative framework of CRISP-DM provides a systematic method for issue characterization, full data exploration, and rigorous model assessment [24]; this gives the reason for adopting this approach. Since fraud detection systems are both dynamic and intricate, this form of fraud prediction is both effective and systematic [17] as depicted in Figure 1.

Figure 1
Methodology for the proposed study



3.2. Dataset and data source

There is an organized attempt to carefully examine the information, as described in CRISP-DM. As such, a detailed search of the relevant dataset for the task was carried out on different ML dataset databases like ICU, Kaggle, Google Dataset, Data.gov, OpenML, and IEEE DataPort. However, the Kaggle e-commerce fraud dataset created by Kerneler [25] was used. The dataset was selected since its attributes are congruent with the objectives of the study. There are 16 columns and 100,000 rows in the dataset. The counts of the target variable 'Fraud' among the 100,000 rows are significantly different; out of these, 7,192 rows are identified as fraud (1), and 92,785 rows are rated as non-fraud (0). Table 1 demonstrates the dataset attributes and description.

Table 1
Description of dataset attributes

Attribute	Description
user_id	Unique identifier for each user
signup_time	The date and time when the user signed up
purchase_time	The date and time when the user made a purchase
purchase_value	The monetary value of the purchase
device_id	Unique identifier for the device used by the user
Source	The marketing channel that led the user to the website (e.g., SEO, Ads, Direct)
Browser	The web browser used by the user
Sex	The gender of the user (M or F)
Age	The age of the user
ip_address	The IP address of the user
Class	An indicator of whether the transaction was genuine or not, expressed as a binary classification variable

3.3. Techniques used

3.3.1. Algorithm

This study employed three DL algorithms: ANN, DNN, and a hybrid model combining both ANN and DNN.

1) ANN: The ANN model was used to process input data through multiple layers of neurons. Each layer applied transformations to the inputs, enhancing classification accuracy through iterative learning, making it suitable for identifying key patterns in phishing detection.
2) DNN: The DNN, a deeper and more complex model than ANN, employed multiple hidden layers to capture nonlinear relationships within the data. This model's depth enabled it to uncover intricate data patterns, improving detection accuracy for subtle variations in input features.
3) Hybrid Model (ANN and DNN): The hybrid model combined ANN and DNN to leverage the strengths of both. By integrating the simplified architecture of ANN with the complex, pattern-detection capabilities of DNN, this model achieved a balance between computational efficiency and high classification performance.

The complementary strengths of ANN and DNN drove the choice of a hybrid model combining them. For less complicated patterns in the data, ANN's rather simpler structure helps to enable effective computation, which qualifies it [18]. On the other hand, DNN's depth and sophisticated design help it find more complex, nonlinear relationships in the data. Combining these methods helps the hybrid model to maximize DNN's depth and ANN's speed, guaranteeing both efficiency and resilience in fraud detection [26]. This twin benefit made the hybrid model an interesting choice over oversampling options or other combinations, such as stacking or ensembling models with like designs.

3.3.2. Feature selection

The dataset has 16 features, which were all not relevant to prediction. As such, feature selection was performed to refine the dataset and enhance model performance by focusing on the most relevant features. LDA by Zhao et al. [27] was utilized as a dimensionality reduction technique to select features that maximize class separability, enhancing model interpretability and reducing computational demands. LDA's capacity to underline class separability, which is essential in fraud detection activities, made it a good fit for this work. This ensures that the chosen features are optimal to differentiate between real and fraudulent transactions, unlike other dimensionality reduction techniques such as principal component analysis, which emphasizes on maximizing variance without considering class labels [27]. LDA improves classification accuracy. Using LDA cut the original 16 features into a subset of the most discriminative ones, including IP location, device type, and transaction amount. These characteristics, which capture trends usually linked with fraudulent activity including unusual transaction sizes, suspicious device changes, or anomalies in geographic location, were absolutely vital for fraud detection. The model's ability to identify minor anomalies is greatly enhanced by giving these aspects top priority.

3.3.3. Handling class imbalance

Given the imbalance in the dataset, the SMOTE [28] was applied to address this issue. SMOTE synthetically generated samples in the minority class, ensuring a more balanced dataset. This adjustment minimized bias in the training process, allowing the models (ANN, DNN, and hybrid) to perform more reliably across classes [29]. The SMOTE approach improved the reliability of model training across all the classes.

3.3.4. Hyperparameter tuning

Hyperparameter tuning was carried out using a grid search technique [30]. This systematic approach improves the model's performance. Key parameters tuned included:

1) ANN: Learning rate, number of hidden layers, and activation function.
2) DNN: Number of layers, dropout rate, and batch size.
3) Hybrid Model: Combination ratios between ANN and DNN components, as well as activation functions for each layer.

4. Data Analysis

4.1. Exploratory data analysis

Graph displaying the proportion of fake and real items in a dataset. This visualization examines the quantity of fraudulent and legitimate transactions to see whether the dataset is balanced as seen in Figure 2.

4.2. Visualization of fraud count based on purchase and age

Figure 3 displays the overall fraud count for the dataset. This visualization, however, looks at the fraud count according to the distribution of ages and purchases in the dataset. Discover how the distributions of 'purchase value' and 'age' vary between fraudulent and non-fraudulent transactions. Figure 4 shows the visualization of fraud count based on purchase value and age.

In the first subplot, we can see that comparing the histograms and kernel density estimation curves reveals that fraudulent transactions often have a higher purchase value than honest ones. Since this data suggests that large purchases may be an indication of fraud, it is useful for building a fraud detection model. In a similar vein, the second subplot reveals a disparity in the ages of the parties involved in fraudulent and legitimate transactions. The fraud detection model may also benefit from this data, as the customer's age is an important variable to consider.

Figure 2
Data visualization of the ratio of valid to fake entries

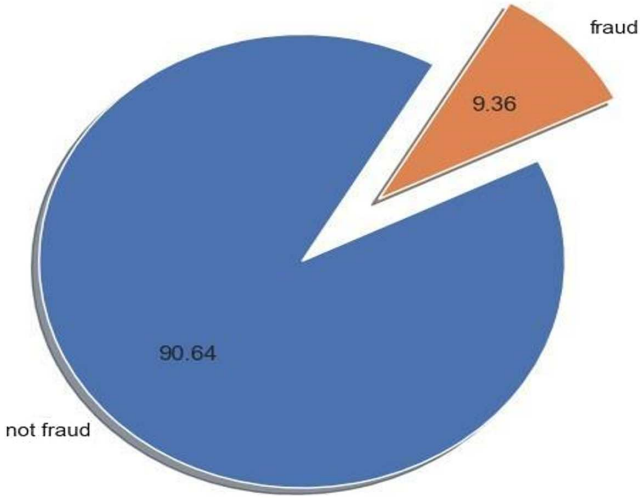


Figure 3
Overall fraud count for the dataset

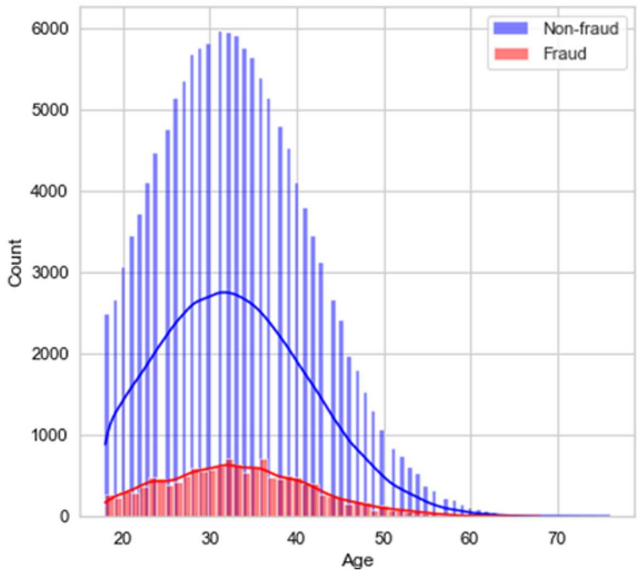


Figure 4
Visualization of fraud count based on purchase value and age

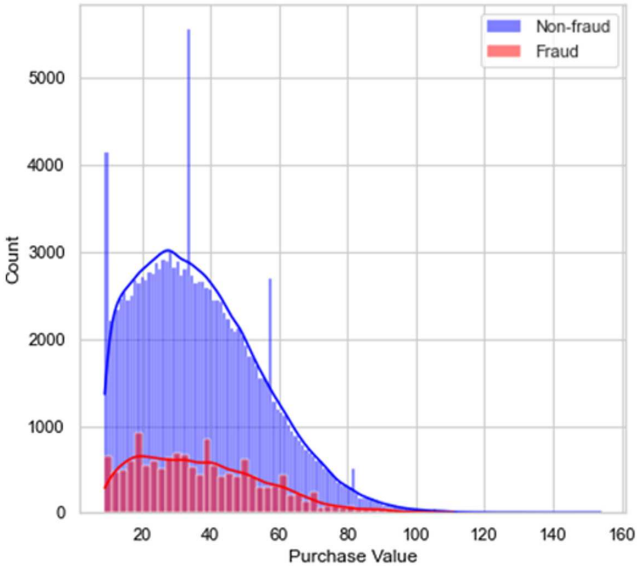


Table 2
Performance of ANN model

Precision	Recall	*F*1-score	AUC	Accuracy
53.37%	98.54%	68.39%	96.92%	95.42%

4.3. Performance analysis

Metrics for recall, accuracy, area under the receiver operating characteristic curve, and *F*1-score were used to evaluate the effectiveness of the trained model. We compared the results of each model, including the hybrid, to those of each other and previous research in the field.

4.3.1. Analyzing the ANN model

It does this by first making a prediction about the target variable using the given test data and then using a 0.5 threshold to convert the predictions into binary classifications. Table 2 shows the performance of the ANN model with the classification metrics.

Figures 5 and 6 determine the performance of the ANN model, which demonstrates its ability to detect fraud effectively. An excellent accuracy rate of 53.37% indicates that the model does a good job of identifying instances of fraud amid positive outcomes. A recall of 98.54% indicates that the model is also adept at detecting a large number of false positives, which is a measure of its ability to identify actual positive situations. The model's 68.39% *F*1-score demonstrates its high general performance on both recall and accuracy. With an AUC of 96.92%, the model is now even better at distinguishing between instances of fraud and those that are not. These results, together with the model's total accuracy of 95.42%, show that the model does a better job than average at identifying fraudulent transactions. A strong recall rate of 98.54% would lower possible financial loss or damage to reputation resulting from undetectable fraud. In high-risk environments like banking or e-

Figure 5
Confusion matrix of ANN model

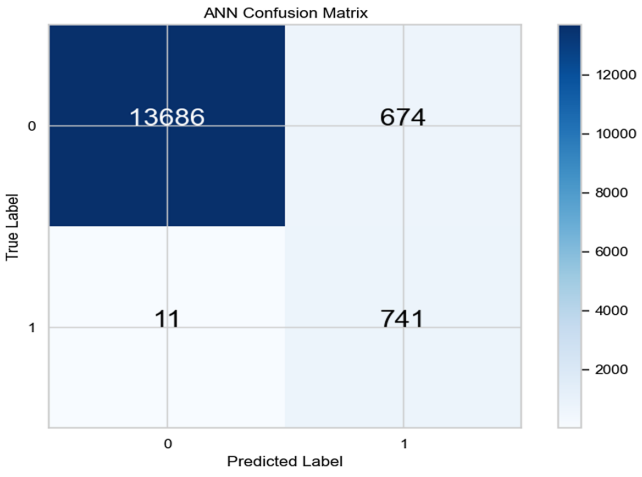
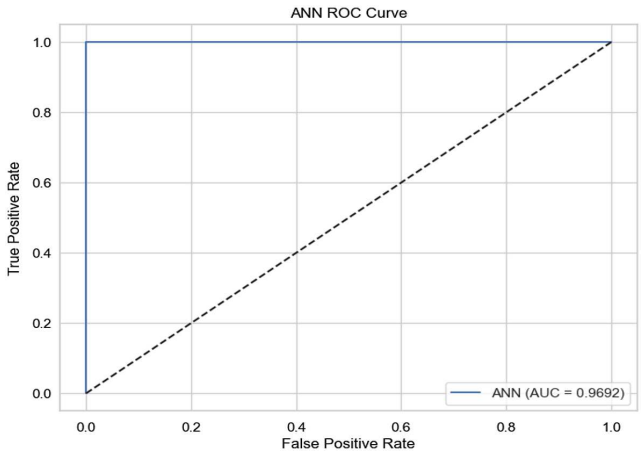


Figure 6
Area under curve from ANN model



commerce, where accuracy and coverage are vital, this accuracy of 95.42% and AUC of 96.92% show consistent and dependable detection capability.

4.3.2. Evaluation of DNN model

The results of the hybrid model as assessed and the outcome are shown in Table 3.

Table 3
Performance of DNN model

Precision	Recall	*F*1-score	AUC score	Accuracy
46.93%	99.55%	63.78%	97.01%	95.01%

Figures 7 and 8 demonstrate that the fraud detection system is performing well, particularly when examining the metrics for the DNN model. Accurately classifying cases of fraud in positive forecasts is shown by a precision of 46.93%. With a recall of 99.55%, the model clearly does a great job at detecting fraudulent transactions. The *F*1-score of 63.78%, which represents the harmonic mean of precision-recall, demonstrates that the model performs balanced. An AUC performance index score of 97.01% indicates

Figure 7
Confusion matrix of DNN model

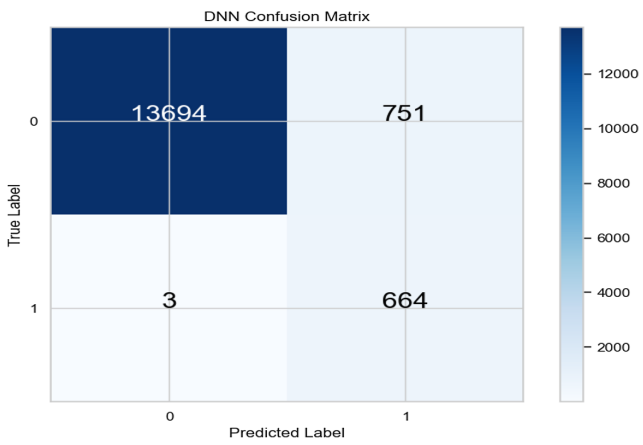


Figure 8
Area under curve from DNN model

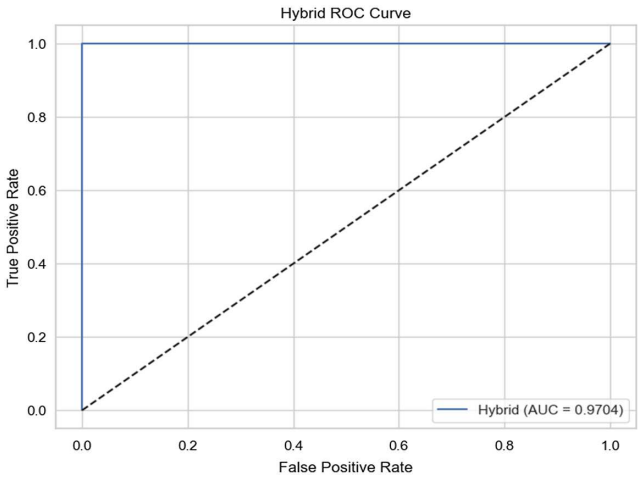


Table 4
Performance of hybrid model

Hybrid model performance				
Precision	Recall	*F*1-score	AUC score	Accuracy
52.16%	98.80%	68.27%	97.04%	95.46%

that the model can distinguish between legitimate and fraudulent instances. Due to its overall accuracy of 95.01%, the DNN model accurately anticipated the outcomes of all affected cases. This degree of dependability and precision makes the DNN model a great tool for helping fraud management systems in making decisions and lowering false activity.

4.3.3. Assessing the hybrid approach

The accuracy of the trained hybrid model is assessed using precision, recall, *F*1-score, AUC score, and accuracy. Table 4 displays the results of the performances.

Figures 9 and 10 determine the performance of the hybrid model and its accuracy in fraud detection through confusion metrics and the AUC curve. The metrics value in Table 4 shows that the hybrid model has a robust and balanced approach to detecting fraud. Accuracy in

Figure 9
Area under curve of hybrid model

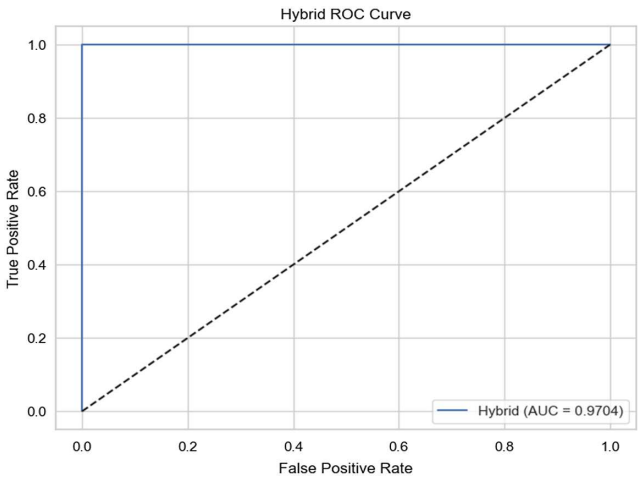
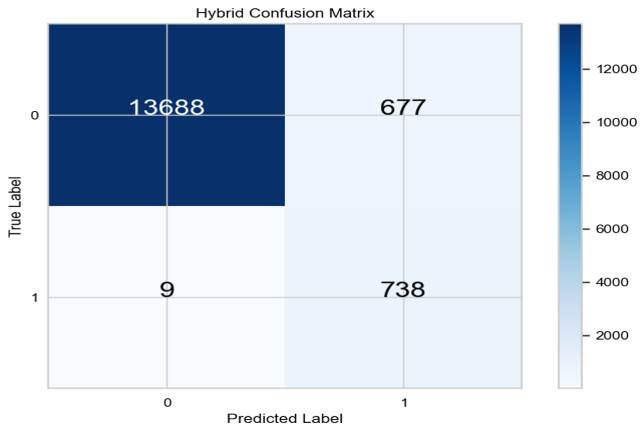


Figure 10
Confusion matrix of hybrid model



identifying fraudulent behavior within positive predictions is rather good at 52.16%. With a recall of 98.80%, the hybrid model is able to identify a high proportion of fraudulent transactions, a measure of the model's ability to discover positive cases. The *F*1-score, which is 68.27%, shows a balanced performance since it is the harmonic mean of recall and accuracy. Its ability to distinguish between real and fake instances is shown by its 97.04% AUC. With a general accuracy of 95.46%, the hybrid model does a great job of making accurate classifications in all instances.

Its 52.16% balanced precision and 98.80% recall guarantee efficient fraud detection without sacrificing reasonable operational requirements. Excellent dependability and robustness shown by the hybrid model's 97.04% AUC and 95.46% accuracy make it a perfect fit for practical uses when both accuracy and efficiency are vital. This model gives companies a consistent and scalable way to fight fraud.

Hybrid models demonstrate superior performance compared to their stand-alone ANN and DNN counterparts, as highlighted in Table 5. While the ANN model achieves the highest precision at 52.37%, it lags behind in recall with 98.54%. The hybrid model, with a recall of 98.80%, surpasses the ANN and closely trails the DNN, which records the highest recall at 99.55%. For the *F*1-score, the hybrid model scores 68.27%, slightly outperforming the ANN (68.39%) and significantly surpassing the DNN (63.78%). In terms of accuracy, the hybrid model leads with 95.46%, marginally ahead of the ANN (95.42%) and the DNN (95.01%). The AUC score, a crucial indicator of model performance, shows the Hybrid model at the top with 97.04%, narrowly exceeding the DNN (97.01%) and the ANN (96.92%).

Table 5
Comparison of the results – ANN, DNN, and hybrid model

Metric	ANN model	DNN model	Hybrid model
Precision	52.37%	46.93%	52.16%
Recall	98.54%	99.55%	98.80%
*F*1-score	68.39%	63.78%	68.27%
Accuracy	95.42%	95.01%	95.46%
AUC score	96.92%	97.01%	97.04%

Overall, the hybrid model provides a well-rounded performance with competitive precision (52.16%), high recall (98.80%), robust *F*1-score (68.27%), excellent accuracy (95.46%), and the highest AUC score (97.04%). These metrics position the hybrid model as the most effective and balanced approach among the three. Figure 11 visually compares the performance of the three

Figure 11
Comparison of the three models – ANN, DNN, and hybrid

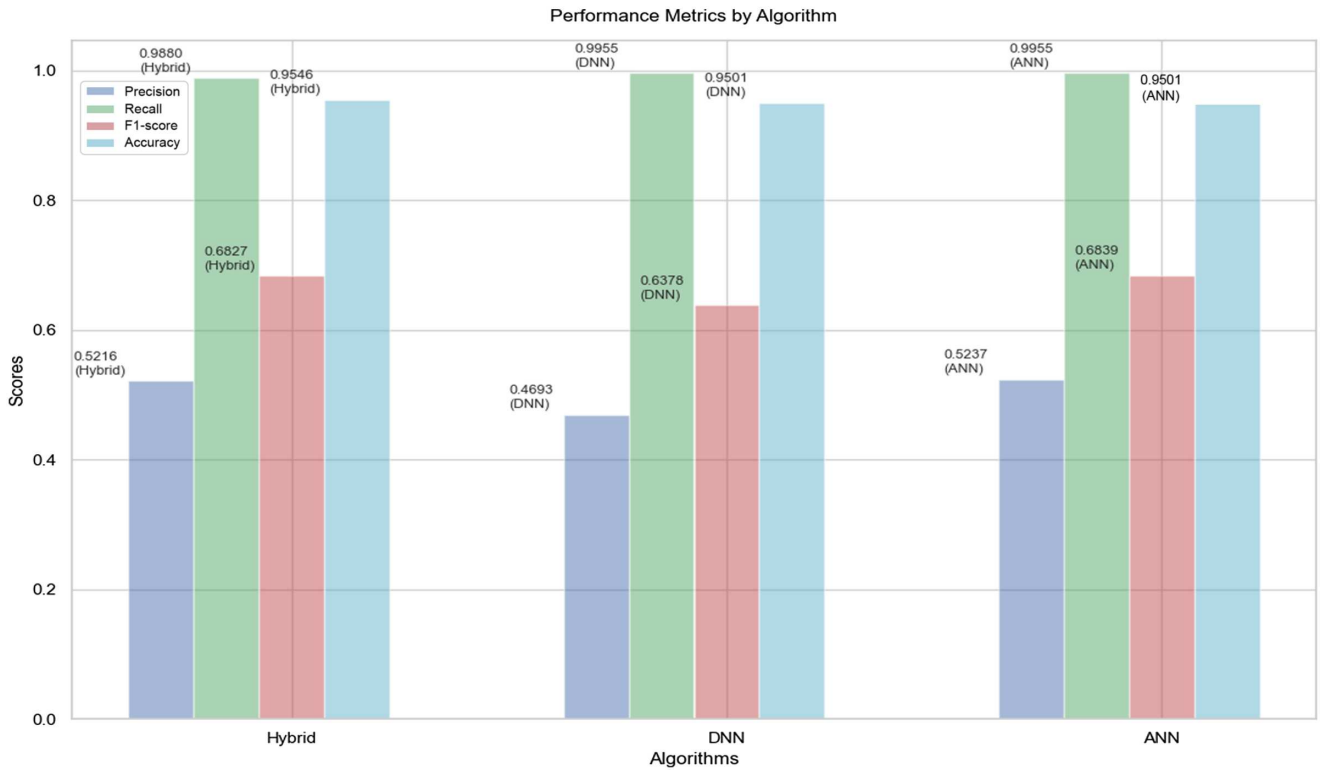


Table 6
Findings in comparison to similar studies

Author/Year	Method used	Precision	Recall	*F*1-score	AUC score	Accuracy
Johnson (2021)	Machine learning (SVM)	88.5%	89.7%	64.5%	85.4%	91.50%
Patel et al. (2023)	CNN algorithm and ADASYN	95.24%	96.80%	62.77%	93.2%	94.23%
Current study	Hybrid model	52.16%	98.80%	68.27%	97.04%	95.46%

models using the evaluation metrics of precision, recall, *F*1-score, and model accuracy.

The comparison of the results in Table 6 reveals varying degrees of success among different fraud detection models. While Valavan and Rita [21] achieved moderate accuracy with an ML approach using random forests, Bilgaiyan and Patel [26] demonstrated the efficacy of the CNN algorithm combined with SMOTE, achieving high precision, recall, and *F*1-score, highlighting the benefits of SMOTE for handling imbalanced data.

While prior research has shown higher recall (99.95%) and stronger *F*1-scores (68. 27%), the current study shows a balanced hybrid model with lesser precision (52.16%) and accuracy (95.46%). The performance results are affected by the fact that various research use diverse methodologies and datasets. DL approaches were used by Bilgaiyan and Patel [26] in contrast to the more traditional ML methods utilized by Sailusha et al. [8] and others. The current study demonstrated the impact of SMOTE and LDA on hybrid DL models for e-commerce transaction fraud prediction, although there is no direct comparison to other research that has used the same dataset. Despite having lesser precision (52.16%) and accuracy (95.46%), the hybrid model in this investigation has a great *F*1-score (68.27%) and a high recall (97.04%). This highlights the significance of thinking about various approaches and what they mean for online fraud detection.

5. Conclusion

This work shows the efficiency of a hybrid model for fraud detection in e-commerce combining ANN and DNN. The hybrid model performed better than oversampling ANN and DNN architectures by including the SMOTE to handle class imbalance and LDA for feature selection. With an AUC of 97.04% and an accuracy of 95.46%, the hybrid model shows its capacity to balance precision, recall, and efficiency, thus providing a dependable means of separating legitimate from fraudulent transactions. While the precision score is not highly commendable, the hybrid model still has areas for improvement, particularly because a significant portion of the predictions labeled as positive are actually false positives. This method emphasizes the need of using sophisticated feature selection and data-balancing methods to raise model performance in real-world situations, in which accurate fraud detection is essential for financial losses and preserving consumer trust. This can be achieved by increasing the size of the data for model training and also addressing any potential issues contributing to low precision.

Although the findings are encouraging, the study had restrictions including depending just on one dataset and computational needs during training. Future studies could investigate validating the model on several datasets, including extra approaches like t-Stochastic Neighbor Embedding or automated feature engineering, and applying blockchain or cryptographic techniques to improve transaction security. Furthermore, possible areas for improvement are real-time fraud detection and the application of ensemble techniques, thereby guaranteeing flexibility to match changing fraud patterns. The strong framework of the hybrid model provides e-commerce platforms with a scalable solution and acts as a basis for developing fraud detection systems in several spheres.

Recommendations

This result demonstrates that SMOTE is effective in fixing the class data imbalance problem and that LDA is helpful for extracting features. This finding provides more evidence that merging the two methods might improve e-commerce fraud detection algorithms. Research such as this is still necessary. In a subsequent study, researchers should consider using t-SNE together with other feature extraction techniques. To gauge its efficacy, the hybrid model used in this work should be tested on other datasets pertaining to the detection of online fraud. Further security for online buyers' transactions can be achieved by combining the study's suggested approach with existing fraud detection methods.

Future research could investigate integrating blockchain technology or cryptographic methods to secure transaction data in conjunction with fraud detection. This could provide an additional layer of security for online buyers and make it more difficult for fraudsters to manipulate or tamper with data.

The study could explore automated feature engineering methods using AI algorithms like genetic programming or reinforcement learning. These techniques can dynamically adjust feature selection based on changing fraud patterns, improving the model's ability to adapt over time.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Mohit Vasant: Conceptualization, Methodology, Formal analysis, Data curation, Writing – original draft, Writing – review & editing, Visualization. **Swathi Ganesan:** Writing – review & editing, Supervision. **Ganapathy Kumar:** Project administration.

References

[1] Adepoju, O., Wosowei, J., lawte, S., & Jaiman, H. (2019). Comparative evaluation of credit card fraud detection using machine

learning techniques. In *2019 Global Conference for Advancement in Technology*, 1–6. https://doi.org/10.1109/GCAT47503.2019.8978372

[2] Dong, Y., Jiang, Z., Alazab, M., & Kumar, P. M. (2021). Real-time fraud detection in e-market using machine learning algorithms. *Journal of Multiple-Valued Logic and Soft Computing*, *36*(1–3), 191–209.

[3] Krishnan, C., & Mariappan, J. (2024). The AI revolution in e-commerce: Personalization and predictive analytics. In L. Gaur & A. Abraham (Eds.), *Role of explainable artificial intelligence in e-commerce* (pp. 53–64). Springer Nature. https://doi.org/10.1007/978-3-031-55615-9_4

[4] van Belle, R., Baesens, B., & de Weerdt, J. (2023). CATCHM: A novel network-based credit card fraud detection method using node representation learning. *Decision Support Systems*, *164*, 113866. https://doi.org/10.1016/j.dss.2022.113866

[5] Kumar, M. S., Soundarya, V., Kavitha, S., Keerthika, E. S., & Aswini, E. (2019). Credit card fraud detection using random forest algorithm. In *2019 3rd International Conference on Computing and Communications Technologies*, 149–153. https://doi.org/10.1109/ICCCT2.2019.8824930

[6] Wang, H., & Smys, S. (2021). Big data analysis and perturbation using data mining algorithm. *Journal of Soft Computing Paradigm*, *3*(1), 19–28.

[7] Boutaher, N., Elomri, A., Abghour, N., Moussaid, K., & Rida, M. (2020). A review of credit card fraud detection using machine learning techniques. In *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications*, 1–5. https://doi.org/10.1109/CloudTech49835.2020.9365916

[8] Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020). Credit card fraud detection using machine learning. In *2020 4th International Conference on Intelligent Computing and Control Systems*, 1264–1270. https://doi.org/10.1109/ICICCS48265.2020.9121114

[9] Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2020). Credit card fraud detection using pipeling and ensemble learning. *Procedia Computer Science*, *173*, 104–112. https://doi.org/10.1016/j.procs.2020.06.014

[10] Leevy, J. L., Khoshgoftaar, T. M., Bauder, R. A., & Seliya, N. (2018). A survey on addressing high-class imbalance in big data. *Journal of Big Data*, *5*(1), 42. https://doi.org/10.1186/s40537-018-0151-6

[11] Xie, Y., Liu, G., Cao, R., Li, Z., Yan, C., & Jiang, C. (2019). A feature extraction method for credit card fraud detection. In *2019 2nd International Conference on Intelligent Autonomous Systems*, 70–75. https://doi.org/10.1109/ICoIAS.2019.00019

[12] Nalepa, J., & Kawulok, M. (2019). Selecting training sets for support vector machines: A review. *Artificial Intelligence Review*, *52*(2), 857–900. https://doi.org/10.1007/s10462-017-9611-1

[13] Salazar, A., Safont, G., Soriano, A., & Vergara, L. (2012). Automatic credit card fraud detection based on non-linear signal processing. In *2012 IEEE International Carnahan Conference on Security Technology*, 207–212. https://doi.org/10.1109/CCST.2012.6393560

[14] Rahayu, W., Jollyta, D., Hajjah, A., Johan, Gusrianty, Gustientiedina, ..., & Desnelita, Y. (2024). Synthetic minority oversampling technique (SMOTE) for boosting the accuracy of C4.5 algorithm model. *Journal of Artificial Intelligence and Engineering Applications*, *3*(3), 624–630. https://doi.org/10.59934/jaiea.v3i3.469

[15] Gosain, A., & Sardana, S. (2017). Handling class imbalance problem using oversampling techniques: A review. In *2017 International Conference on Advances in Computing, Communications and Informatics*, 79–85. https://doi.org/10.1109/ICACCI.2017.8125820

[16] Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable AI approach. *Engineering, Technology & Applied Science Research*, *14*(1), 12822–12830. https://doi.org/10.48084/etasr.6641

[17] Valli, L. N., Sujatha, N., & Divya, D. (2022). A novel approach for credit card fraud detection using LR method-comparative studies. *Eduvest-Journal of Universal Studies*, *2*(12), 2611–2614.

[18] Ali, M. N. Y., Kabir, T., Raka, N. L., Toma, S. S., Rahman, M. L., & Ferdaus, J. (2022). SMOTE based credit card fraud detection using convolutional neural network. In *2022 25th International Conference on Computer and Information Technology*, 55–60. https://doi.org/10.1109/ICCIT57492.2022.10054727

[19] Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of artificial intelligence for fraudulent banking operations recognition. *Big Data and Cognitive Computing*, *7*(2), 93. https://doi.org/10.3390/bdcc7020093

[20] Abdaljawad, R. Y. R., Obaid, T., & Abu-Naser, S. S. (2023). Fraudulent financial transactions detection using machine learning. In *2023 3rd International Conference on Emerging Smart Technologies and Applications*, 1–9. https://doi.org/10.1109/eSmarTA59349.2023.10293697

[21] Valavan, M., & Rita, S. (2023). Predictive-analysis-based machine learning model for fraud detection with boosting classifiers. *Computer Systems Science and Engineering*, *45*(1), 231–245. https://doi.org/10.32604/csse.2023.026508

[22] Lathifah, A., Arham, Z., Hasanati, N., Zulfiandri, & Nurmiati, E. (2023). Cross-industry standard process for data mining (CRISP-DM) for discovering association rules in graduate tracer study data of Islamic higher education institution. In *2023 11th International Conference on Cyber and IT Service Management*, 1–6. https://doi.org/10.1109/CITSM60085.2023.10455691

[23] Yang, Y., Yang, B., Nguyen, H., & Onofrei, G. (2025). Developing analytics-driven maintenance data mining processes: A design science approach. *International Journal of Quality & Reliability Management*, *42*(6), 1706–1729. https://doi.org/10.1108/IJQRM-06-2023-0191

[24] Plotnikova, V., Dumas, M., & Milani, F. P. (2022). Applying the CRISP-DM data mining process in the financial services industry: Elicitation of adaptation requirements. *Data & Knowledge Engineering*, *139*, 102013. https://doi.org/10.1016/j.datak.2022.102013

[25] Kerneler, K. (2018). *Starter: Fraud ecommerce 5beb6e26-e*. Retrieved from: https://www.kaggle.com/code/kerneler/starter-fraud-ecommerce-5beb6e26-e/input

[26] Bilgaiyan, A., & Patel, V. (2024). A machine learning based credit card transaction fraud detection system for imbalanced data. *International Journal of Engineering Applied Science and Management*, *5*(9), 1–15.

[27] Zhao, S., Zhang, B., Yang, J., Zhou, J., & Xu, Y. (2024). Linear discriminant analysis. *Nature Reviews Methods Primers*, *4*(1), 70. https://doi.org/10.1038/s43586-024-00346-y

[28] Elreedy, D., & Atiya, A. F. (2019). A comprehensive analysis of synthetic minority oversampling technique (SMOTE) for handling class imbalance. *Information Sciences*, *505*, 32–64. https://doi.org/10.1016/j.ins.2019.07.070

[29] Gamaleldin, W., Attayyib, O., Mohaisen, L., Omer, N., & Ming, R. (2025). Developing a hybrid model based on convolutional neural network (CNN) and linear discriminant analysis (LDA) for investigating anti-selection risk in insurance. *Journal of Radiation Research and Applied Sciences*, *18*(2), 101368. https://doi.org/10.1016/j.jrras.2025.101368

[30] Belete, D. M., & Huchaiah, M. D. (2022). Grid search in hyperparameter optimization of machine learning models for prediction of HIV/AIDS test results. *International Journal of Computers and Applications*, *44*(9), 875–886. https://doi.org/10.1080/1206212X.2021.1974663

How to Cite: Vasant, M., Ganesan, S., & Kumar, G. (2025). Enhancing E-commerce Security: A Hybrid Machine Learning Approach to Fraud Detection. *FinTech and Sustainable Innovation*, *1*, A7. https://doi.org/10.47852/bonviewFSI52024882