Al-Zaytoonah Journal of Business, Vol. 01 No. 03, November 2025

Fraud Prediction in E-Commerce Transactions using TabNet with Advanced Data Balancing Techniques

Huthaifa Aljawazneh[1], Fadwa Abu Al-Ragheb[2]
[1]Al-Zaytoonah University of Jordan, huthaifa.rj@zuj.edu.jo
[2]fadwaabualragheb@gmail.com

Abstract:
E-commerce platforms handle substantial financial transactions, making them attractive targets for fraudulent activity. Those activities may include the use of stolen credit cards or the creation of accounts that exploit online systems. These fraudulent techniques are continuously evolving, which makes prediction increasingly challenging. To address this problem, TabNet, a deep learning classification algorithm, has been applied and compared with two standard machine learning algorithms: Support Vector Machine (SVM) and K-Nearest Neighbors (KNN), in predicting fraudulent transactions in e-commerce. Moreover, since the dataset utilized in this study is extremely imbalanced, three advanced balancing techniques have been used, i.e., SMOTE, SMOTE-ENN, Borderline -SMOTE. Furthermore, because the accuracy evaluation metric is insufficient for evaluating model performance on an imbalanced dataset, three additional metrics (i.e., recall, specificity, and AUC) have been adopted to evaluate the performance of the classifiers and provide a more comprehensive assessment. Accordingly, TabNet with Borderline-SMOTE approach achieved the best overall performance.

Keywords: Fraud prediction, machine learning, deep learning, classification, SMOTE.

1. Introduction

Recently, the widespread adoption of the internet and e-commerce has driven an enormous rise in electronic transactions. In other words, modern technology advancements have caused people to choose online payment systems for their shopping requirements [1]. At the same time, the growing use of digital devices and e-commerce platforms has led to a substantial rise in cybercrime [2]. The main difficulty of fraud detection arises from the short time period during which acceptance or rejection decisions must be made. Moreover, the use of fraudulent cards creates problems for all parties including cardholders and banks, but merchants bear the greatest impact because they lose more money than the value of their sold items [1].

The term cybercrime describes criminal activities that occur through internet networks while fraud includes deceptive actions that seek to acquire financial or personal advantages, and it can be categorized into two types: offline fraud and online fraud [1]. Accordingly, online fraud represents the most prevalent form of fraud as fraudsters steal digital card data through phishing and skimming methods. While offline fraud occurs when a credit card is stolen physically and used before the owner reports the loss and the bank cancels the card [3]. Those violations result in major damage to the trust between businesses and customers [2]. Therefore, an effective and fast detection of credit-card fraud is essential to preserve user experience and reduce financial losses for online stores [4].

Accordingly, this work aims to enhance transaction security and provide a robust solution for minimizing fraud risk by evaluating a powerful model capable of delivering accurate identification of fraudulent activities in e-commerce transactions. Therefore, a deep learning technique (i.e., TabNet) has been applied and compared to two standard machine learning algorithms (i.e., K-Nearest Neighbors (KNN) and Support Vector Machine (SVM)).

The dataset used in this study is highly imbalanced, which leads to suboptimal classification results [5]. Thus, three advanced resampling techniques have been used to address this problem: Synthetic Minority Over-sampling Technique (SMOTE), SMOTE combined with Edited Nearest Neighbors (SMOTE-ENN) and Borderline-SMOTE. Moreover, while the dataset is imbalanced, the accuracy metric is not sufficient to measure classifier performance, three other metrics were used to assess the real performance of classifiers in

predicting fraudulent and not fraudulent cases. These metrics are recall, specificity and area under the ROC curve (AUC).

The rest of the paper is organized as follows: Section 2 reviewed the related literature, Section 3 provides a dataset description, Section 4 outlines the proposed approaches for detecting fraudulent e-commerce transactions, Section 5 presents implementation details and results, and section 6 presents the conclusions and directions for future work.

2. Literature review

The detection of electronic or credit-card fraud has attracted considerable attention of researchers in the last few years. Actually, traditional fraud detection methods have been the foundation of financial institutions' security frameworks for many years. These methods use Information Retrieval, Rule-based methods and professional judgment to detect and prevent fraudulent behavior [6]. Accordingly, Ibrahim et al. [7] developed an e-commerce fraud detection system based on analytical methods and scoring policies to detect outliers. The experimental results demonstrated a considerable performance through 93.3% accuracy and high precision and recall and F1-score values.

However, numerous studies have used machine learning methods to address fraud. For example, Dheepa and Dhanapal [8] created a behavior-based fraud detection system using Support Vector Machines (SVM) which utilized efficient feature extraction and kernel-based adaptability; Their method achieved high accuracy in identifying fraud effectively and it scaled well for processing big transaction volumes. In the same year, Ganji et al. [9] developed Stream Outlier Detection using Reverse Nearest Neighbors (SODRNN) algorithm which uses reverse k-nearest neighbors to detect credit-card fraud. Also, Xuan et al. [10] proposed the Refined Weighted Random Forest (RWRF) model which improves credit-card fraud detection through weighted decision trees to achieve better classification results than standard random forest approaches. In 2019, Porwal and Mukund [4] developed a clustering-based fraud detection system which uses consistency scores to detect outliers effectively without requiring any prior knowledge. The proposed method achieved better results than standard models. More recently, Gölyeri et al. [11] applied decision tree, logistic regression, random forest, and extreme gradient boosting to detect e-commerce fraud, showing how feature selection affects model performance.

Moreover, several researchers used deep learning algorithms to predict credit-card transaction fraud. For instance, Islam, M. et al. [12] used real-world datasets to evaluate AI-based fraud detection techniques by comparing machine learning and deep learning models. The research proved that XGBoost and deep learning models (i.e., LSTM and CNN) outperformed the other approaches. In addition, Pumsirirat and Yan [13] proposed an unsupervised deep learning system which combined Auto-Encoders with Restricted Boltzmann Machines to detect online transaction anomalies. The model achieved excellent results on the European credit-card dataset.

On the other hand, while data balancing problem presents challenges for classifiers in predicting the correct class, some researchers have enhanced the performance of the classifiers in solving the problem by implementing advanced balancing techniques. Consequently, Saputra and Suharjito [6] employed Decision Tree, Naïve Bayes, Random Forest, and Neural Network to detect e-commerce fraud in addition to using SMOTE to handle class imbalance. Their work showed that Neural Network with genetic algorithms obtained the best results compared to other models. Moreover, Vasant et al. [14] created a hybrid fraud detection model which integrated Artificial Neural Networks (ANN) and Deep Neural Networks (DNN), with SMOTE to address class balancing problem. The proposed method yielded superior accuracy and AUC performance than standalone models in providing a secure e-commerce transaction solution.

Furthermore, data availability presents an additional challenge, researchers often face major hurdles when trying to access real financial fraud records. These datasets are usually confidential, or unavailable. Therefore, researchers utilized synthetic data structured to present real-world patterns and complexity.

Accordingly, Raju and Varma [15] developed an e-commerce fraud detection system devoting XGBoost and Stacking Classifier which trained and tested on synthetic data of transactions. Additionally, Mutemi & Bacao [2] also highlighted the increasing reliance on synthetic data due to limited access to real-world datasets related to e-commerce fraud detection.

Thus, in this study, we present a novel application of the TabNet deep learning architecture for fraud detection in e-commerce transactions. To evaluate its effectiveness, we compare TabNet with two widely used machine learning algorithms: Support Vector Machine (SVM) and K-Nearest Neighbors (KNN).

Additionally, we investigate the impact of advanced data balancing techniques including SMOTE, SMOTE-ENN, and Borderline-SMOTE on enhancing classifier performance.

3. Dataset description

Many studies have employed synthetic data as an effective alternative when real-world datasets are inaccessible [2][15]. Accordingly, while the data related to the credit-card transactions is usually confidential, or unavailable, the dataset used in this study is synthetic (not real). It was obtained from the Kaggle[1] website. Moreover, the dataset consists of 1,472,952 customer transaction records, described by 16 attributes: 9 numerical and 7 categorical. A major challenge with this dataset is its balancing ratio; 1,399,114 records corresponding to non-fraudulent transactions, whereas the remaining 73,838 records belonging to fraudulent ones.

4. Methodology

This work evaluates the performance of one of the relatively new deep learning algorithms (i.e., TabNet) in predicting fraudulent e-commerce transactions. In addition, to strengthen the validity of the evaluation, TabNet classifier performance is compared to two other well-known standard machine learning algorithms (i.e., SVM and KNN). Furthermore, because the dataset employed in this study is highly imbalanced, three advanced balancing techniques were used to address this issue (i.e., SMOTE, Borderline-SMOTE, and SMOTE-ENN).

4.1 TabNet:

TabNet is a deep learning algorithm developed particularly for tabular data. Deep learning uses multi-layered neural networks to extract increasingly abstract features from complex data. Through backpropagation, it fine-tunes internal parameters to improve pattern detection across large datasets [16]. It employs sequential attention mechanisms to select the most relevant features at each decision point. In addition, the design approach of TabNet enhances interpretability and learning efficiency because of its ability to direct model capacity toward the most informative inputs. Furthermore, TabNet achieves better predictions through multiple decision stages that progressively filter out less important features. The structured data handling capabilities of this innovative method improve prediction accuracy while minimizing redundancy, making it a powerful, versatile tool across multiple domains [17].

4.2 Support Vector Machine:

It is a widely used standard machine learning algorithm introduced by Vapnik [18], originally developed to solve classification and regression tasks. It operates by constructing an optimal decision boundary, called a hyperplane, to separate data points of different classes in a high-dimensional space. Moreover, the algorithm maximizes the margin between the data points of each class for better classification performance and generalization [19]. The ability of SVM to generalize well and find optimal solutions made it popular in machine learning and pattern recognition [20].

4.3 K-Nearest Neighbors:

KNN is a supervised machine learning algorithm used for both classification and regression tasks. The algorithm operates by selecting k neighbors to evaluate their similarity to a given point using Euclidean distance. Then, it assigns the class of the new instance according to the majority class of its neighbors. However, the selection of k is critical because small values can lead to noisy predictions, whereas large values may lead to missing important details [21].

4.4 Advanced balancing techniques:

Imbalanced data distribution is common in real-world data. This problem occurs when instances belonging to one class are significantly more than the other class. The majority class comprises most of the data instances, whereas the minority class represents the remaining ones [22]. In this study, SMOTE, SMOTE-ENN and Borderline-SMOTE are utilized to handle the data balancing problem.

4.4.1. Synthetic Minority Oversampling Technique (SMOTE):

[1] Fraudulent E-Commerce Transactions

It is an advanced oversampling-based data balancing technique. SMOTE generates new synthetic samples by the interpolation between minority class instances and their closest neighboring points, instead of replicating existing instances. Additionally, the simplicity of SMOTE along with its adaptability across different domains made it a fundamental technique in learning using imbalanced data [23].

4.4.2. SMOTE + Edited Nearest Neighbors (SMOTE-ENN):

It is a hybrid resampling method that combines oversampling and under-sampling. Its process begins by generating synthetic minority class samples using SMOTE. Then, the Edited Nearest Neighbors (ENN) method is applied to eliminate both synthetic and original samples that get misclassified by their nearest neighbors on the dataset [24].

4.4.3. Borderline-SMOTE:

The Borderline-SMOTE algorithm is an advanced oversampling method developed to improve classifiers' performance with imbalanced datasets. Unlike standard SMOTE, Borderline-SMOTE creates synthetic samples only from minority class instances that are near the decision boundary and are most susceptible to be misclassified [25].

4.5 Evaluation metrics:

The class imbalance distribution issue emerged as a major challenge in classification. It adversely affects classifiers' performance and leads to biased prediction results. To address this problem, three advanced data balancing techniques have been applied to improve model reliability and performance. However, the accuracy metric alone does not provide a sufficient evaluation with imbalanced datasets. Therefore, our performance assessment expanded to include recall, specificity, and Area Under the Curve (AUC) to evaluate the performance of each classifier in predicting fraudulent transactions in e-commerce.

Evaluation metrics:

- **Accuracy:** Refers to the proportion of correctly classified fraudulent and non-fraudulent transactions out of the total number of transactions [6].

- **Recall:** Refers to the proportion of actual fraudulent cases that the model successfully predicted [6].

- **Specificity**: Measures the model's ability to correctly identify non-fraudulent transactions [26].

- **Area Under the ROC Curve (AUC):** Refers to the model's performance in distinguishing between fraudulent and non-fraudulent transactions by analyzing the Receiver Operating Characteristic (ROC) curve. The ROC curve shows the relationship between recall and specificity, and how effectively the model detects fraudulent transactions while minimizing false predictions. However, the AUC provides a single numerical value summarizing the classifiers' performance [4].

5. Results:

This section compares the results obtained by a deep learning algorithm (i.e., TabNet), and two standard machine classifiers (i.e., SVM and KNN) in predicting fraudulent transactions in e-commerce. Moreover, the dataset utilized in this study is highly imbalanced. Therefore, three advanced data balancing techniques have been used to solve this issue, which provide three versions of datasets.

5.1 Combinations of TabNet and data balancing techniques

This subsection analyzes the performance of the TabNet classifier, trained and evaluated on three balanced datasets using SMOTE, SMOTE-ENN, and Borderline-SMOTE, respectively. Table 1 presents the values of the evaluation metrics obtained from each combination of classifier and balancing techniques.

	Accuracy	Recall	Specificity	AUC
SMOTE	0.8975	0.8334	**0.9624**	0.9543
SMOTE-ENN	0.9069	0.8712	0.9536	0.9636
BL-SMOTE	**0.9141**	**0.8837**	0.9449	**0.9699**

Table 1. Evaluation metrics values for the TabNet model; The best values are highlighted in bold.

As shown in Table1, the TabNet classifier combined with Borderline-SMOTE outperforms the other approaches. It achieved the best accuracy and highest recall metric value, highlighting its superior ability to effectively predict fraudulent transactions. Moreover, it obtained the best AUC value, which illustrates its strong capacity to distinguish clearly between the two categories. On the other hand, the combination of TabNet with SMOTE yields the best specificity. Figure 1 demonstrates the ROC curves of TabNet across the three balanced datasets, highlighting the Area Under the Curve (AUC) for each.

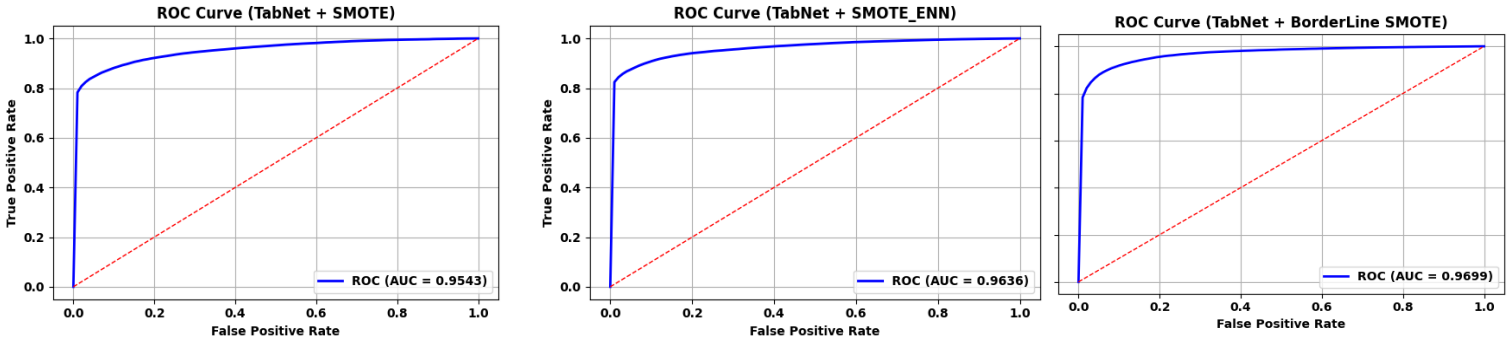


Figure 1: ROC curves for TabNet combined with balancing techniques.

5.2 Combinations of KNN and data balancing techniques

This subsection evaluates the performance of the KNN classifier, which trained and tested on three balanced datasets generated using SMOTE, SMOTE-ENN, and Borderline-SMOTE. Table 2 reports the metric values obtained from KNN combined with each balancing technique.

	Accuracy	Recall	Specificity	AUC
SMOTE	0.8750	0.8262	**0.9243**	0.9280
SMOTE-ENN	0.8808	0.8592	0.9090	0.9394
BL-SMOTE	**0.8901**	**0.8634**	0.9171	**0.9453**

Table 2. Evaluation metrics values for the KNN model; The best values are highlighted in bold.

According to the results of the aforementioned table, KNN with Borderline-SMOTE approach achieved the best results in several metrics. In other words, the conjunction of KNN and Borderline-SMOTE yields the best accuracy, recall and AUC, indicating that it is the superior approach in predicting fraudulent transactions, and in distinguishing between fraudulent and non-fraudulent transactions. Furthermore, when applying SMOTE, it performed the best prediction of non-fraudulent transactions. Figure 2 illustrates the performance of the KNN classifier and in distinguishing between fraudulent and non-fraudulent transactions through AUC curves across three balanced datasets.

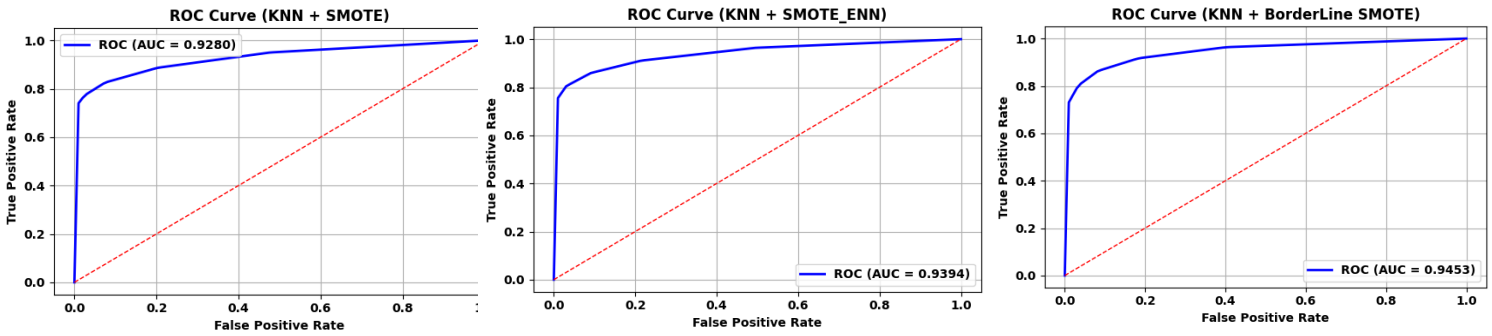


Figure 2: ROC curves for KNN combined with balancing techniques.

5.3 Combinations of SVM and data balancing techniques

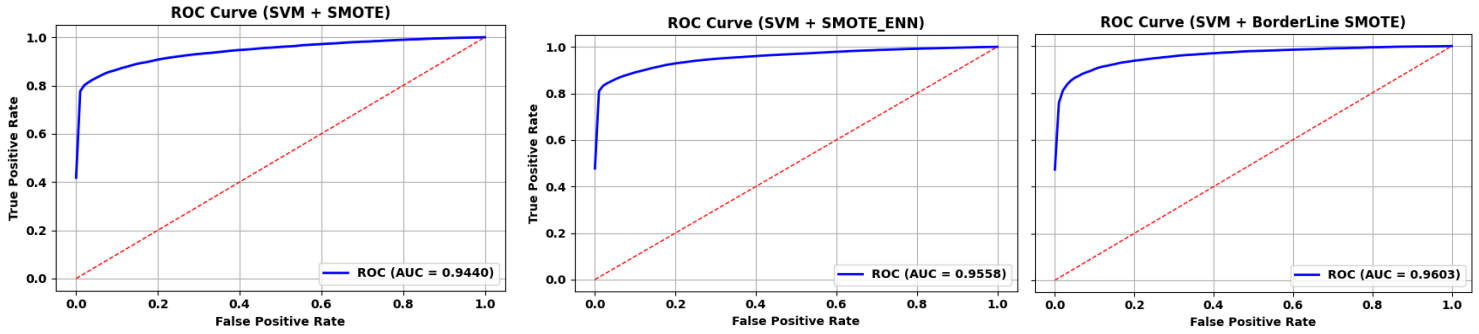
This subsection analyzes the results obtained from the approaches of SVM with balancing techniques in predicting fraudulent transactions in e-commerce.

	Accuracy	Recall	Specificity	AUC
SMOTE	0.8914	0.8171	**0.9667**	0.9440
SMOTE-ENN	0.8986	0.8531	0.9583	0.9558
BL-SMOTE	**0.9063**	**0.8704**	0.9427	**0.9603**

Table 3. Evaluation metrics values for the SVM model; The best values are highlighted in bold.

According to Table 3, the SVM model combined with the Borderline-SMOTE technique delivered the strongest performance in predicting fraud transactions compared to the other combinations. It achieved the highest accuracy, indicating robust overall classification capability, and a high recall reflecting its effectiveness in identifying fraudulent cases. Additionally, it recorded the top AUC score, demonstrating the superior ability to distinguish between fraudulent and legitimate transactions. Moreover, with the combination of SVM and SMOTE balancing technique, it achieved the highest specificity, showing its performance in identifying non-fraudulent transactions. Figure 5 illustrates the ROC curve performance of the SVM model across the three balanced datasets, emphasizing the AUC values for each version.

Figure 3: ROC curves for SVM combined with balancing techniques.



1.1 Results summary:

This section presents a comparative analysis of nine classification approaches. A deep learning algorithm (i.e., TabNet), along with two standard machine learning classifiers (i.e., KNN and SVM), was evaluated. Each classifier is being combined with three data balancing techniques. Moreover, the approaches are assessed using four performance metrics: Accuracy, Recall, Specificity, and AUC to ensure a comprehensive evaluation and determine whether TabNet, which is specifically designed for tabular data, outperforms the traditional algorithms.

With respect to accuracy, Figure 4 illustrates the results obtained by the nine approaches, highlighting that the TabNet model combined with Borderline-SMOTE achieved the highest value compared to the others. Furthermore, as illustrated in Figure 5, TabNet combined with Borderline-SMOTE outperformed the other eight evaluated approaches by achieving the highest recall, indicating its robust performance in correctly identifying actual fraud cases compared to the other approaches. In terms of specificity, Figure 6 demonstrates that the SVM model combined with SMOTE delivered the best performance in accurately identifying non-fraudulent transactions. Additionally, as shown in Figure 7, TabNet combined with Borderline--SMOTE achieved the best AUC, which means this approach demonstrated the strongest performance in differentiating fraudulent from non-fraudulent transactions, while effectively balancing recall and specificity.

As a result of the comparative analysis, TabNet combined with Borderline-SMOTE achieved the highest accuracy, recall and AUC, whereas SVM combined with SMOTE yielded the best specificity, showcasing its effectiveness in correctly identifying non-fraudulent transactions.

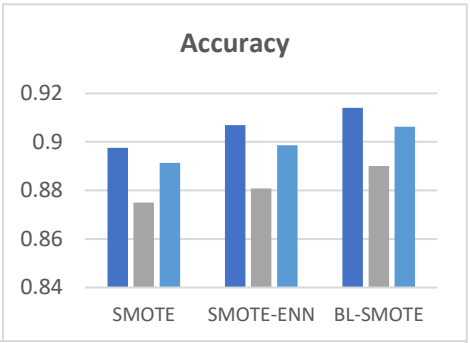


Fig 4. Accuracy values obtained from all approaches (classifiers + balancing techniques).

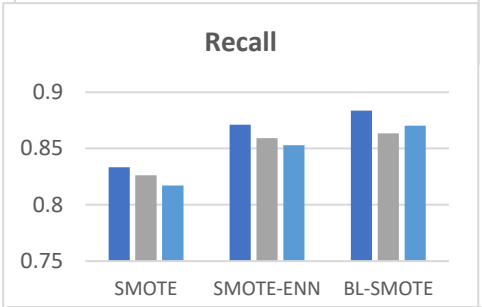


Fig 5. Recall values obtained from all approaches (classifiers + balancing techniques).

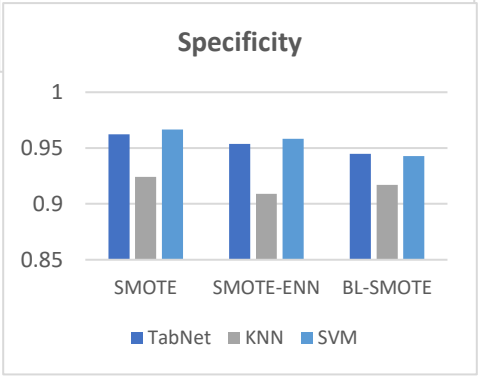


Fig 6. Specificity values obtained from all approaches (classifiers + balancing techniques).

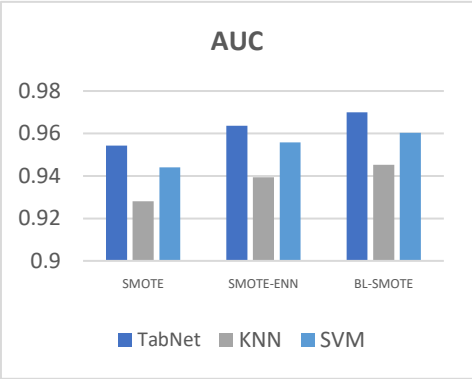


Fig 7. AUC values obtained from all approaches (classifiers + balancing techniques).

1.2 Conclusion and future work:

The rapid expansion of e-commerce has led to a surge in cybercrime, particularly credit-card fraud. However, detecting fraud is a complex task due to the scarcity and evolving nature of fraudulent patterns, which makes training reliable models difficult. The problem worsens as fraudsters consistently develop new techniques to avoid detection systems. As a result, implementing effective mechanisms for fraud detection and prevention is essential to safeguard both businesses and consumers. To address this issue, TabNet, a deep learning algorithm, was employed, and its performance was evaluated against two standard machine learning models (i.e. SVM and KNN). To address the data balancing problem, three advanced resampling techniques (i.e., SMOTE, SMOTE-ENN, and Borderline-SMOTE) were applied. Additionally, since accuracy alone is not sufficient for evaluating model performance on imbalanced datasets, additional metrics including recall, specificity, and AUC were used to provide a more comprehensive assessment. Accordingly, the approach of using TabNet and Borderline-SMOTE balancing techniques showed the best performance in predicting fraudulent transactions in e-commerce. For future work, feature selection methods could be integrated with TabNet. Also, other deep learning models could be evaluated in solving the problem and compared against TabNet.

6. References

1. Shaji, J., & Panchal, D. (2017). Improved fraud detection in e-commerce transactions. 2017 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA).
2. Mutemi, A., & Bação, F. (2024). E-Commerce fraud detection based on machine learning techniques: Systematic literature review. Big Data Mining and Analytics, 7(2), 419–444.
3. Carta, S., Fenu, G., Reforgiato Recupero, D., & Saia, R. (2019). Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model. Journal of Information Security and Applications, 46, 92–106.
4. Porwal, U., & Mukund, S. (2019). Credit card fraud detection in e-commerce. In 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) / 13th IEEE International Conference on Big Data Science and Engineering (BigDataSE) (pp. 280–287). IEEE.
5. Saputra, A., & Suharjito. (2019). Fraud detection using machine learning in e-commerce. International Journal of Advanced Computer Science and Applications, 10(9), 332–338.
6. Bagwe, C. (2024). Fraud detection in financial institutions: AI vs. traditional methods. International Journal of Scientific Research & Engineering Trends, 10(6), Nov–Dec.
7. Ibrahim, B. H., Salihu, H. U., & Aleshinloye, Y. A. (2025). Rule-based approach to e-commerce fraud detection. UNIABUJA Journal of Engineering and Technology (UJET), 2(1), 196–204.

8. Dheepa, V., & Dhanapal, R. (2012). Behavior-based credit card fraud detection using support vector machines. ICTACT Journal on Soft Computing, 2(4), 391–397.
9. Ganji, V. R., & Mannem, S. N. P. (2012). Credit card fraud detection using anti-k nearest neighbor algorithm. International Journal on Computer Science and Engineering (IJCSE), 4(6), 1071–1077.
10. Xuan, S., Liu, G., & Li, Z. (2018). Refined weighted random forest and its application to credit card fraud detection. In X. Chen, A. Sen, W. Li, & M. Thai (Eds.), Computational Data and Social Networks (Vol. 11280, pp. 343–355). Springer.
11. Gölyeri, M., Çelik, S., Bozyiğit, F., & Kılınç, D. (2023). Fraud detection on e-commerce transactions using machine learning techniques. Artificial Intelligence Theory and Applications, 3(1), 45–50.
12. Islam, M. M., Zerine, I., Rahman, M. A., Islam, M. S., & Ahmed, M. Y. (2024). AI-driven fraud detection in financial transactions – Using machine learning and deep learning to detect anomalies and fraudulent activities in banking and e-commerce transactions. International Journal of Communication Networks and Information Security, 16(5), 927–944.
13. Pumsirirat, A., & Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. International Journal of Advanced Computer Science and Applications, 9(1), 18–25.
14. Vasant, M., Ganesan, S., & Kumar, G. (2025). Enhancing e-commerce security: A hybrid machine learning approach to fraud detection. FinTech and Sustainable Innovation, 00(00), 1–9.
15. Raju, G. S., & Varma, V. S. (2025). E-commerce fraud detection based on machine learning techniques. International Journal of Innovative Research in Technology, 11(11), 5252. ISSN: 2349-6002. Retrieved from IJIRT publication
16. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444.
17. Arık, S. O., & Pfister, T. (2020). TabNet: Attentive interpretable tabular learning. arXiv preprint arXiv:1908.07442v5.
18. Vapnik, V. N. (1998). The nature of statistical learning theory (2nd ed.). Springer.
19. Cortes, C., & Vapnik, V. (1995). Support-vector networks. Machine Learning, 20(3), 273–297
20. Cervantes, J., Garcia-Lamont, F., Rodríguez-Mazahua, L., & Lopez, A. (2020). A comprehensive survey on support vector machine classification: applications, challenges and trends. Neurocomputing.
21. Halder, R. K., Uddin, M. N., Uddin, M. A., Aryal, S., & Khraisat, A. (2024). Enhancing K-nearest neighbor algorithm: A comprehensive review and performance analysis of modifications. Journal of Big Data, 11, Article 113.
22. Elrahman, S. M. A., & Abraham, A. (2013). A review of class imbalance problem. Journal of Network and Innovative Computing, 1, 332–340.
23. Fernández, A., García, S., Herrera, F., & Chawla, N. V. (2018). SMOTE for learning from imbalanced data: Progress and challenges, marking the 15-year anniversary. Journal of Artificial Intelligence Research, 61, 863–905.
24. Batista, G. E. A. P. A., Prati, R. C., & Monard, M. C. (2004). A study of the behavior of several methods for balancing machine learning training data. ACM SIGKDD Explorations Newsletter, 6(1), 20.
25. Han, H., Wang, W.-Y., & Mao, B.-H. (2005). Borderline-SMOTE: A new over-sampling method in imbalanced data sets learning. In D.-S. Huang, X.-P. Zhang, & G.-B. Huang (Eds.), Advances in Intelligent Computing (pp. 878–887). Springer.
26. Zhang, Z., Yin, H., Rao, S.X. et al. Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights. Data Sci. Eng. 10, 24–39 (2025). https://doi.org/10.1007/s41019-024-00275-6