International Journal of Data and Network Science 9 (2025) 845–852

Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

EFC-Tomek: An effective undersampling technique for credit card fraud detection

Hadeel Ahmad[a*], Enas Rawashdeh[b], Arar AlTawil[c] and Nancy Al-Ramahi[d]

[a]*Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan*
[b]*Management Information Systems, Albalqa' Applied University, Jordan*
[c]*Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan*
[d]*Basic Sciences, AlZaytoonah Univeraity of Jordan, Jordan*

C H R O N I C L E

Article history:
Received June 5, 2025
Received in revised format June 29, 2024
Accepted July 30 2025
Available online
July 30 2025

Keywords:
Undersampling
Credit card fraud
Fraud Detection
Imbalanced Datasets
Tomek Links

A B S T R A C T

Detecting credit card fraud is a major challenge because fraudulent transactions represent only a small fraction of financial data. Traditional methods like SMOTE (Synthetic Minority Oversampling Technique) help balance datasets but can also introduce noise and make models over- fit, reducing their effectiveness. To tackle the issues that come with oversampling, we present the Enhanced Fraud Classifier with Tomek Links (EFC-Tomek) framework. This approach builds on the existing EFN-SMOTE but takes a different approach, using Tomek Links undersampling instead of SMOTE oversampling to balance the dataset. Our main goal is to improve data quality and enhance the model's ability to detect fraud more accurately and effectively. To test EFC-Tomek, we used two real-world datasets: European cardholders and Loan Prediction. We evaluated its performance using a number of classifiers, such as Random Forest, eXtreme Gradient Boosting, Logistic Regression, Gradient Boosting, Artificial Neural Networks, and Support Vector Classifier. The results showed that EFC-Tomek improved fraud detection, with ANN achieving the highest accuracy on both datasets.

1. Introduction

Credit card fraud detection has become a challenge for the financial industry because legitimate transactions far outnumber fraudulent ones (Zhu et al., 2024; El Hlouli et al., 2024; Dal Pozzolo et al., 2017; Rawashdeh et al., 2024; Zaghloul et al., 2025). Since fraud is both rare and unpredictable, the dataset is considered unbalanced. This imbalance often leads to lower accuracy in detection models, as they tend to favor the majority class (legitimate transactions) and tend to neglect the minority class (fraudulent transactions) (Buda et al., 2018; Ahmad et al., 2023a).

As online transactions continue to grow, the risk of fraudulent activity increases. As a result, the banking and financial industries are forced to implement new technologies (Alnoori et al., 2024). To address this challenge, artificial intelligence (AI) and machine learning (ML) are used to analyze large amounts of data (Farhan et al., 2025; Ngai et al., 2011; West & Bhattacharya, 2016; Rawashdeh et al., 2021; Muhairat et al., 2024). This approach helps identify unusual patterns that might go undetected, hence enhancing the accuracy and reliability of fraud detection.

Among the existing techniques, the Synthetic Minority Oversampling Technique (SMOTE) and other oversampling methods are widely used to balance the datasets. SMOTE has many benefits, such as improving model performance by generating synthetic samples for the minority class, which helps algorithms better recognize underrepresented patterns. However, these methods also come with limitations. For example, SMOTE can lead to noise by replicating unnecessary transactions without creating new ones, which may lead to overfitting Ruslan and Arbaiy (2024). Overfitting occurs when a model learns the training data too precisely, capturing noise and irrelevant pat- terns instead of essential relationships (Ruslan & Arbaiy, 2024; Kang et al., 2016; Masoud et al., 2021). As a result, the performance decreases when applied to new, unseen data. These

* Corresponding author
E-mail address h ahmad@asu.edu.jo (H. Ahmad)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2025.7.003

limitations highlight the need for discovering alternative approaches to improve fraud detection. To address these challenges, undersampling techniques offer an alternative approach by selectively removing majority class instances instead of generating synthetic samples. This helps remove noise, reduces the chances of overfit- ting, and allows the model to concentrate on meaningful patterns, ultimately improving fraud detection accuracy.

Since handling data imbalance is crucial for building fraud detection models that are both effective and reliable, this paper modifies the existing EFN- SMOTE approach (Ahmad et al., 2023b; Aburass et al., 2025) by replacing oversampling with undersampling to address its limitations. The goal of this modification is to determine whether removing some majority class instances, rather than generating synthetic samples for the minority class, leads to a more balanced dataset and improved fraud detection accuracy. By applying under- sampling effectively, we can enhance model performance, eliminate irrelevant data, and make fraud detection more efficient (Chen et al., 2024; Carvalho et al., 2025; Elhassan & Aljurf, 2016).

This study addresses some challenges such as data imbalance and model overfitting, proposing solutions to protect financial transactions against increasingly sophisticated fraud scams. This paper highlights the importance of continuing progress in machine learning to better secure financial trans- actions and reduce the risks associated with digital finance. We refer to the modified method as the Enhanced Fraud Classifier with Tomek Links (EFC- Tomek) framework, which is based on an undersampling approach. To assess its effectiveness and performance, we compared it with EFN-SMOTE. Our main contribution is showing that EFC-Tomek, which uses undersampling instead of the oversampling used in EFN-SMOTE, greatly improves fraud detection in imbalanced datasets. This approach boosts model accuracy, prevents over- fitting, and strengthens fraud detection by reducing instances in the majority class.

2. Related works

The increasing volume of online transactions has greatly increased fraudulent activities in recent years. This makes fraud detection an important part of the research. Detecting fraud in online transactions is a serious challenge due to the nature of combating highly asymmetrical data. As a result, the identification performance is lower than standard. Minority cases, such as fraud cases (Ahmad et al., 2025a; Ayoub et al., 2025). To overcome this challenge Various techniques have been proposed. This includes sampling methods aimed at reducing the majority of the sample and balancing the data set. One such method is using the Tomac Link, which not only helps with undersampling (Breskuviene & Dzemyda, 2024). But it also helps reduce noise. By removing specific data points that tend to cause ambiguity in the classification boundary, Tomac Link improves the quality of the training set. This makes it more effective for accurate fraud detection. This section reviews related work that explores different approaches. To manage asymmetric data in fraud detection. Including the Tomac application, Link focuses on the effectiveness of noise reduction and undersampling techniques (Hussain et al., 2024). A number of studies have employed Tomek links to enhance fraud detection systems. For instance, Leng et al. (2024) introduces OBMI, an improved SMOTE method that enhances classification on imbalanced datasets by focusing on borderline minority instances using a two-stage Tomek link approach.

An additional study, Alamri and Ykhlef (2024), introduces a hybrid method that integrates Tomek links for undersampling, BIRCH clustering, and Border- line SMOTE (BCBSMOTE) for oversampling, by reducing the imbalance in credit card fraud data, this method leads to enhanced precision and F1-scores.

Also, Elhassan and Aljurf (2016) present used the Tomek Link algorithm to clean the data by eliminating noise during the pre-processing step. The Tomek link method is combined with various sampling techniques. It includes undersampling (RUS), random oversampling (ROS), and synthetic minority oversampling (SMOTE) techniques to provide a balanced class distribution. Classification is achieved using machine learning algorithms such as artificial neural networks (ANN), random forest (RF), and logistic regression (LR). The performance of these classifiers This is assessed using appropriate measures for data with high asymmetry. The method has been tested on datasets such as arterial blood pressure and Ecoli2. Other researchers Bansal and Jain (2021) explored different approaches to the class imbalance problem by proposing the focused undersampling methods, namely Cluster-Based, Tomek Link, and Condensed Nearest Neighbors. These techniques balance the distribution of classes by intelligently reducing some instances of the majority class according to predetermined criteria, therefore steering clear from the underfitting issues and losing important data points. For the implementation of these techniques, prediction models such as K-Nearest Neighbor, Decision Tree, and Naive Bayes were employed. Many researchers try to enhance credit card fraud detection methods (Rawashdeh et al., 2024; Ahmad et al., 2023a,b), where the main focus is set on overcoming the issue of imbalance. It usually results in biased classifiers with high performance for the majority class and very poor performance for the minority class. This paper proposes a method to take up this challenge by utilizing focused undersampling techniques to make sure accurate prediction models are developed for imbalanced datasets.

3. Methodology

In this study, we modify the established EFN-SMOTE framework Ahmad et al. (2023b) by replacing oversampling with undersampling, leading to the proposed EFC-Tomek framework, as illustrated in Fig. 1.

3.1 Datasets

We tested our model on two different datasets to make sure our results were reliable. Table 1 provides details about these datasets, including their unique identifiers, sample sizes, the number of positive cases, and access links.

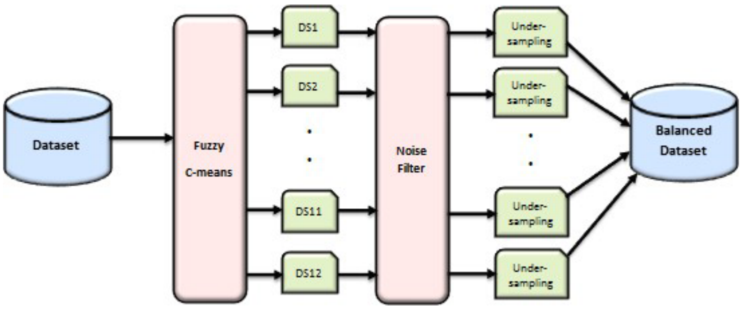

Fig. 1: EFC-Tomek framework

Table 1
Summary of Datasets Used

Dataset	Code	Samples	Positive	Attribute	Link
European cardholders	D1	284807	482	31	https://kaggle.com/mlg-ulb/creditcardfraud
Loan Prediction	D2	614	192	13	https://github.com/Paliking/ML examples/blob/master/LoanPrediction/trainu6lujuXCVtuZ9i.csv

3.2 Data processing

To prepare the data, we start by applying Fuzzy C-means clustering to identify natural patterns in the datasets, which helps make the undersampling process more effective by combining similar data points together and reducing errors from mislabeled ones Razavi et al. (2021). We followed EFN-SMOTE's approach by selecting twelve clusters using the Elbow method, which helps determine the ideal number of clusters by analyzing how changes in cluster count impact the data's variability. After clustering the dataset, each subset was refined using the Noise Filter Process (NFP) algorithm (Yi et al., 2022), which uses a k-nearest neighbors (kNN) approach to remove noise and outlier data points. This preprocessing step improves data quality by removing outliers and inconsistencies that could affect the results, particularly targeting noise and minority instances near decision boundaries.

3.3 Undersampling with Tomek Links

Following the noise filtration, each subset goes through an undersampling process using Tomek Links. Tomek Links is an undersampling technique that identifies and removes nearest neighbor pairs of opposite classes from the majority class Thai-Nghe et al. (2010) Elhassan and Aljurf (2016). Tomek Links can be utilized for either undersampling purposes or as a method for cleaning data Alamri and Ykhlef (2024). When used for under-sampling, Tomek Links removes only majority class instances. However, when applied as a data-cleaning step, it eliminates instances from both classes Leng et al. (2024). This technique helps improve classifier performance by resolving overlapping class boundaries, which often make learning more difficult. In this study, we utilize Tomek Links as an undersampling process by specifically removing majority class instances that form Tomek Links. By removing these Tomek Links, the dataset becomes simpler for algorithms to interpret, leading to more accurate predictions and reducing the likelihood of misclassifying minority class instances.The pseudo-code of Tomek Link algorithm is shown in algorithm 1.

Algorithm 1 Tomek Links Undersampling

Input: Dataset D with features X and target y
Output: Cleaned Dataset D' **Step 1: Identify Tomek Links** **for** each sample i in Dataset D **do**
  Find nearest neighbor j such that $y[i] \neq y[j]$
  if i is the nearest neighbor of j and j is the nearest neighbor of i **then**
    Mark pair (i, j) as a Tomek Link
  end if end for
Step 2: Remove Majority Class Instances for each Tomek Link (i, j) **do**
  if $y[i]$ is the majority class **then**
    Remove i from D
  else if $y[j]$ is the majority class **then**
    Remove j from D
  end if end for
Output: Cleaned Dataset D'

This selective removal enhances class separability, reducing classifier bias by creating a clearer boundary between classes, which results in a more representative of true data patterns, making it well-structured for machine learning models, especially neural networks. The result of the process is a balanced dataset, resulting from the consolidation of the undersampled subsets. Given that the proposed framework involves sophisticated preprocessing (clustering and noise filtering) designed to refine the dataset significantly before under- sampling, Tomek Links will preserve more of the data's inherent structure and quality, which is crucial after your initial efforts to clean and structure the data. It removes only the problematic overlapping samples, thereby maintaining the integrity and diversity of your dataset, which is likely to result in a more robust model.

3.4 Model Training and Evaluation

The balanced dataset generated thereafter is thereby an incredible representation of the actual data pattern and has a fairly representative majority to minority class instance ratio, thus becoming an excellent candidate for training a machine learning model that otherwise would have been biased with the original class imbalance. The affirmation of high quality for the final balanced dataset should coexist with its representative nature of the underlying problem domain, and this will therefore guarantee more accurate and fair predictive modeling, particularly in modeling prediction with neural networks. The implementation of this work is accomplished by a wide number of different machine learning algorithms, among them is Artificial Neural Net- works (ANN), eXtreme Gradient Boosting (XGBoost), Random Forest (RF), Logistic Regression (LR), Support Vector Classifier (SVC), and Gradient Boosting (GB). These models have been selected so as to allow for performance comparison across many learning paradigms. The basic parameters and con- figuration details for each of the algorithms are given in Table 2, followed by the explanation of the key hyperparameters that will influence their learning behavior. The datasets were split into train and test sets in a proportion of usually 80%-20%, ensuring that different methodologies would provide high-level performance evaluation for each. ANN was then utilized as the main deep learning approach, whereas tree-based and some of the other traditional machine learning models were put into comparative evaluation.

4. Experiments and results

4.1 Experimental Setup

The experiments were conducted on Kaggle Notebooks, a platform in the Kaggle cloud known for its robust model training and extensive processing capabilities. The use of Kaggle necessitates a computer with specific hardware requirements, such as a multi-core CPU, optional NVIDIA GPUs for rapid model training, 16 GB of RAM for handling large datasets, and ample storage for data and output files. Applying the EFC-Tomek framework, a crucial tool in managing unbalanced datasets in credit card fraud detection, demanded swift execution of data preparation, clustering, and model training processes. These resources were instrumental in achieving this.

Table 2
Model configurations and hyperparameters

Algorithm	Parameter	Value
ANN	Hidden layers (HL)	4
	Neurons per layer	[256, 128, 64, 32]
	Activation function Regularization	ReLU (HL), Sigmoid (output) L2 ($\lambda = 0.001$)
	Dropout rate	[0.4, 0.3, 0.3, 0.2]
XGBoost	Learning rate	0.1
	Number of Estimators	100
	Maximum Depth	6
	Subsample	0.8
	Colsample bytree	0.8
RF	Number of trees	100
	Maximum depth	None
LR	Regularization	L2
	C (Inverse Reg Strength)	1.0
SVC	Kernel	'rbf'
	C (Regularization Parameter) Gamma	1.0
		'scale'
GB	Learning rate	0.1
	Number of Estimators	100
	Maximum Depth	3
	Subsample	0.8

Table 3
Performance on European cardholders dataset

Method	Accuracy	Recall	Precision	F1-Score	G-Mean
ANN	0.9936	0.9941	0.9973	0.9936	0.9936
XGBoost	0.9286	0.9271	0.9247	0.9231	0.9258
RF	0.9857	0.9814	0.9824	0.9855	0.9856
LR	0.9714	0.9729	0.9721	0.9709	0.9709
SVC	0.9761	0.9714	0.9725	0.9782	0.9718
GB	0.9857	0.9814	0.9839	0.9855	0.9856

Each classifier had its confusion matrix created to assess its performance on Datasets. These matrices show the distribution of true positives, true negatives, false positives, and false negatives, which gives a detailed picture of each model's performance. They show how well each model differentiates between instances of the majority class and those of the minority class under the EFC-Tomek framework.

4.2 Results

Table 3 and Table 4 evaluate various machine learning models' results on two datasets: European cardholders and loan prediction. The offered metrics evaluate each model's capacity to efficiently classify unbalanced data. These metrics include Accuracy, Recall, Precision, F1-Score, and G-Mean.

Table 4
Performance on loan prediction dataset

Method	Accuracy	Recall	Precision	F1-Score	G-Mean
ANN	0.9936	0.9892	0.9873	0.9937	0.9921
XGBoost	0.9655	0.9647	0.9647	0.9620	0.9525
RF	0.9655	0.9638	0.9647	0.9420	0.9525
LR	0.9425	0.9478	0.9529	0.9301	0.9445
SVC	0.9425	0.9495	0.9425	0.9704	0.9482
GB	0.9540	0.9878	0.9643	0.9759	0.6286

Fig. 4 and Fig. 5 present the accuracy performance for each classifier, offering a comparative visualization of the models' effectiveness on both datasets. In Fig. 4, we analyze the performance on where the ANN model achieves the highest accuracy, highlighting its superior classification ability. Similarly, Fig. 5 illustrates the accuracy performance for loan prediction dataset, reinforcing that the ANN model outperforms other classifiers in this scenario as well. Fig. 2 and Fig. 3 present the G-Mean performance for each classifier, providing a comparative visualization of the models' effectiveness European cardholders datasets on both datasets. In Fig. 2, we analyze the performance on European cardholders' dataset, where the CustomerANN model achieves the highest G-Mean value, indicating its superior classification ability. Similarly, Fig. 3 illustrates the G-Mean performance for loan prediction dataset, reinforcing that the CustomerANN model outperforms other classifiers in this scenario as well. These visualizations highlight the importance of evaluating models using the G-Mean metric to assess their balanced classification performance.

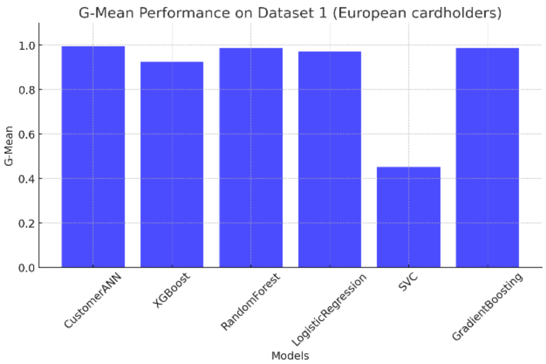

Fig. 2. G-Mean Performance on European cardholders' dataset

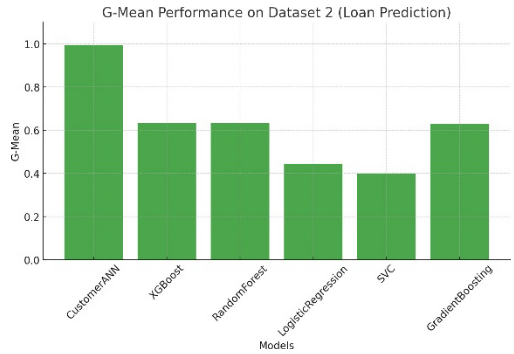

Fig. 3. G-Mean Performance on loan prediction dataset

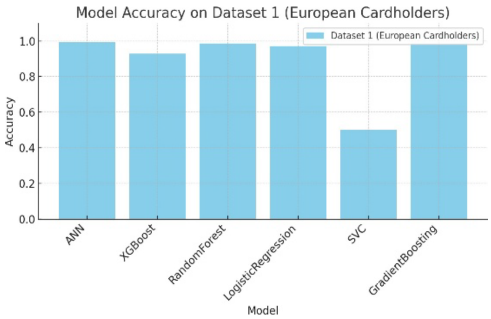

Fig. 4. Model Accuracy on European cardholders' dataset

5. Discussion

In particular, for fraud detection tasks that focus on identifying instances of minority classes, the results of using the EFC-Tomek undersampling architecture show that it effectively handles unbalanced data. Ensemble models like RandomForest and GradientBoosting, which used the framework, achieved flawless scores across all metrics on European cardholders' dataset, demonstrating improved model performance. The EFC-Tomek technique may effectively decrease class imbalance, eliminate overlap, and clarify borders between majority and minority classes, as evidenced by the high Accuracy, Recall, Precision, F1-Score, and G-Mean scores for these models. For fraud detection, these findings are vital since it is critical to correctly identify fraudulent (minority) instances without overfitting to non-fraudulent (majority) situations.

While the ensemble models did not achieve perfect scores in the loan prediction dataset, they consistently maintained high Recall and F1-Score values. This resilience of the EFC-Tomek framework across datasets with varying imbalance ratios and sample sizes underscores its adaptability. These results validate the framework's utility for different types of data, providing reassurance about its versatility. The slightly lower G-Mean values in Dataset 2 compared to Dataset 1 suggest that factors like sample size and imbalance ratio can influence model performance. However, the EFC-Tomek system effectively prioritizes the detection of minority class occurrences, a crucial characteristic for unbalanced datasets, as evidenced by the consistent Recall and F1-Score values across both datasets.

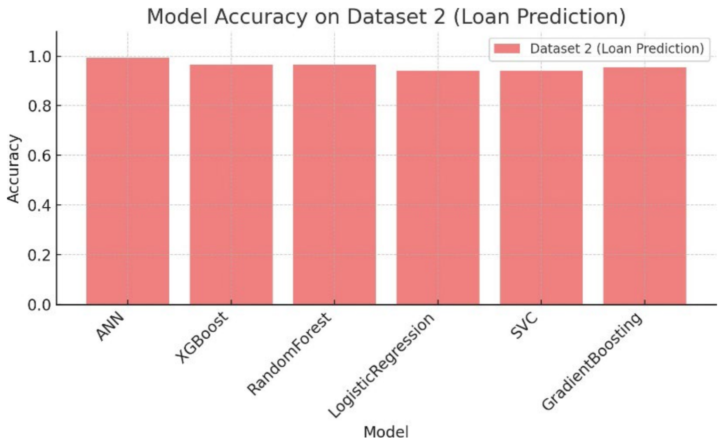

Fig. 5. Model Accuracy on European cardholders' dataset

The SVC stands out from the framework's typically strong performance, especially on Dataset 1, which displays lower F1-Score and G-Mean values. Because SVC still has trouble classifying unbalanced data following EFC- Tomek processing, its sensitivity to noisy data and overlapping class borders plays a role in this result. This discovery implies that even if the EFC-Tomek framework improves the data quality for most classifiers, some models, such as SVC, would still need further adjustments or other preparation techniques to manage class imbalance correctly.

A further analysis of model performance using the G-Mean metric is illustrated in Fig. 2 and Fig. 3. These figures present the comparative G-Mean values across all classifiers for both datasets. The CustomerANN model consistently outperforms other classifiers in both datasets, achieving the highest G-Mean scores. Fig. 2 highlights the superior performance of CustomerANN in European cardholders' dataset, reinforcing its robustness in handling imbalanced data. Similarly, Fig. 3 demonstrates that CustomerANN remains the best-performing model in loan prediction dataset, further validating its reliability in credit risk prediction. The lower G-Mean values for SVC in both datasets emphasize its struggle in handling class imbalance, aligning with prior observations about its lower recall.

Overall, most models have shown significant gains in Recall and F1-Score, indicating the potential impact of the EFC-Tomek undersampling architecture on credit card fraud detection. These metrics, especially Recall, suggest a reduced rate of false negatives, which is crucial in fraud detection. The framework's ability to modify and define class borders is a powerful tool for predictive modeling in high-stakes situations where correct minority class identification is crucial. Its performance highlights its potential to improve overall classification accuracy while still being sensitive to minority classes, making the EFC-Tomek framework a valuable addition to the field of fraud detection.

6. Conclusion

In this paper, we presented the EFC-Tomek framework as a better approach to manage class imbalance in fraud detection over the existing EFN-SMOTE, which depends on oversampling. Instead of adding synthetic data, which may lead to overfitting, our approach uses Tomek Links undersampling to clean the dataset by removing unnecessary instances. This helps reduce noise, improve data quality, and increase model performance. We evaluated EFC-Tomek's performance across several classifiers and tested it on two real-world datasets to assess its efficiency. The results showed that ANN consistently achieved the highest accuracy, proving that undersampling can improve fraud detection by minimizing overfitting and making models more accurate. These findings highlight how essential it is to enhance data preparation methods in order to create fraud detection systems that are more precise and effective. Future research could explore hybrid methods that combine under- sampling with advanced feature selection or test EFC-Tomek on a broader range of financial datasets to further validate its impact.

References

Aburass, M., Aburass, R., & Hamza, M. (2025a). A Comparative Study of Machine Learning Algorithms for Credit Card Fraud Detection. In *2025 12th International Conference on Information Technology (ICIT)* (pp. 201-206). IEEE.

Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023a). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology*, *15*(1), 325-333.

Ahmad, H., Kasasbeh, B., AL-Dabaybah, B & Rawashdeh, E. (2023b). EFN-SMOTE: An effective oversampling technique for credit card fraud detection by utilizing noise filtering and fuzzy c-means clustering. International Journal of Data and Network Science, 7(3), 1025-1032.

Ahmad, I., Waleed, M., Ullah, A., & Jamil, M. U. (2025b). Enhancing Credit Card Fraud Detection with Hybrid Sampling and Machine Learning Models. In *2025 6th International Conference on Advancements in Computational Sciences (ICACS)* (pp. 1-7). IEEE.

Alamri, M., & Ykhlef, M. (2024). Hybrid undersampling and oversampling for handling imbalanced credit card data. *IEEE Access*, *12*, 14050-14060.

Alnoori, M. K., Malkawi, M., & Rawashdeh, E. (2024). Enhancing Big Data Performance Through Graph Coloring-Based Locality of Reference. *Journal of Engineering and Sustainable Development*, *28*(4), 467-472.

Ayoub, M., Abdelhamid, T., & Khalid, J. (2025). Granular computing framework for credit card fraud detection. *Alexandria Engineering Journal*, *121*, 387-401.

Breskuvienė, D., & Dzemyda, G. (2024). Enhancing credit card fraud detection: highly imbalanced data case. *Journal of Big Data*, *11*(1), 182.

Buda, M., Maki, A., & Mazurowski, M. A. (2018). A systematic study of the class imbalance problem in convolutional neural networks. *Neural networks*, *106*, 249-259.

Carvalho, M., Pinho, A. J., & Brás, S. (2025). Resampling approaches to handle class imbalance: a review from a data perspective. *Journal of Big Data*, *12*(1), 71.

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: a realistic modeling and a novel learning strategy. *IEEE transactions on neural networks and learning systems*, *29*(8), 3784-3797.

El Hlouli, F. Z., Riffi, J., Mahraz, M. A., Yahyaouy, A., El Fazazy, K., & Tairi, H. (2024). Credit card fraud detection: Addressing imbalanced datasets with a multi-phase approach. *SN Computer Science*, *5*(1), 173.

Elhassan, T., & Aljurf, M. (2016). Classification of imbalance data using tomek link (t-link) combined with random under-sampling (rus) as a data reduction method. *Global J Technol Optim S*, *1*(S1).

Farhan, M. J., Alnoori, M. K., & Rawashdeh, E. F. (2025). Optimizing Planar Antenna Arrays Using Genetic Algorithms for Enhanced Radar Performance in Direction of Arrival Estimation. *Journal of Engineering and Sustainable Development*, *29*(4), 464-472.

Hussain, A., Dhanawat, V., Aslam, A., Iqbal, N., & Tripura, S. (2024, December). Credit Card Fraud Detection Using Machine Learning Techniques: Dealing with Imbalanced Data using Over-Sampling and Under-Sampling Methods. In 2024 Beyond Technology Summit on Informatics International Conference (BTS-I2C) (pp. 676-681). IEEE.

Kang, Q., Chen, X., Li, S., & Zhou, M. (2016). A noise-filtered under-sampling scheme for imbalanced classification. *IEEE transactions on cybernetics*, *47*(12), 4263-4274.

Leng, Q., Guo, J., Tao, J., Meng, X., & Wang, C. (2024). OBMI: oversampling borderline minority instances by a two-stage Tomek link-finding procedure for class imbalance problem. *Complex & Intelligent Systems*, *10*(4), 4775-4792.

Masoud, M., Jaradat, Y., Rababa, E., & Manasrah, A. (2021). Turnover Prediction using Machine Learning: Empirical Study. *International Journal of Advances in Soft Computing & Its Applications*, *13*(1).

Muhairat, M., Alzyadat, W., Shaheen, A., Alhroob, A., & Asfour, A. N. (2024). Leveraging Machine Learning for Predictive Pathways in Higher Education: A Case Study at Al-Zaytoonah University of Jordan. *International Journal of Electronics and Communication Engineering*, *11*(11), 28-44.

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision support systems*, *50*(3), 559-569.

Rawashdeh, E., Al-Ramahi, N., Ahmad, H., & Zaghloul, R. (2024). Efficient credit card fraud detection using evolutionary hybrid feature selection and random weight networks. *International Journal of Data & Network Science*, *8*(1).

Rawashdeh, E. F., Aljarah, I., & Faris, H. (2021). A cooperative coevolutionary method for optimizing random weight networks and its application for medical classification problems. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 321-342.

Razavi, S. M., Kahani, M., & Paydar, S. (2021). Big data fuzzy C-means algorithm based on bee colony optimization using an Apache Hbase. *Journal of big data*, *8*(1), 64.

Ruslan, R. A., & Arbaiy, N. (2024). Handling Imbalanced Datasets in Machine Learning: Challenges, Approaches, and Best Practices. *Journal of Applied Science, Technology and Computing*, *1*(2), 20-27.

Thai-Nghe, N., Nghi, D. T., & Schmidt-Thieme, L. (2010). Learning optimal threshold on resampling data to deal with class imbalance. In *Proc. IEEE RIVF International Conference on Computing and Telecommunication Technologies* (pp. 71-76).

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. *Computers & security*, *57*, 47-66.

Yi, X., Xu, Y., Hu, Q., Krishnamoorthy, S., Li, W., & Tang, Z. (2022). ASN-SMOTE: a synthetic minority oversampling method with adaptive qualified synthesizer selection. *Complex & Intelligent Systems*, *8*(3), 2247-2272.

Zaghloul, R., Rawashdeh, E., & Bani-Ata, T. (2025). Advancements in adversarial generative text-to-image models: a review. *The Imaging Science Journal*, *73*(3), 328-353.

Zhu, M., Zhang, Y., Gong, Y., Xu, C., & Xiang, Y. (2024). Enhancing credit card fraud detection a neural network and smote integrated approach. *arXiv preprint arXiv:2405.00026*.