Comparison of SVM kernels in Credit Card Fraud Detection using GANs

Bandar Alshawi
Department of Computer and Network Engineering, College of Computing, Umm Al-Qura University, Makkah, Saudi Arabia

***Abstract*—The technological evolution in smartphones and telecommunication systems have led people to be more dependent on online shopping and electronic payments, which created burdensome task of transaction validation for many financial institutions. This paper examined and evaluated the efficacy of Support vector machine (SVM) kernels on Generative Adversarial Network (GAN)-generated synthetic data to detect credit card fraud transactions. Four SVM kernels have been investigated and compared; linear, polynomial, sigmoid, and redial basis function. The accuracy results indicated that linear and polynomial kernels reached over 91%, while sigmoid and redial basis function reached 79% and 83% respectively. Linear and polynomial models received over 90% ROC and F1 score, in contrast the ROC scores were lower for sigmoid (81%) and redial basis function (83%). Both sigmoid and redial basis function achieved over 80% in terms of F1 score. The precision score demonstrated a high score for both linear and polynomial kernel reaching 99%. Additionally, sigmoid and redial basis function achieved over 80%. These results overcame the imbalance dataset issue through the generation of synthetic data by applying the SVM kernels using GANs algorithm.**

Keywords—Fraud transactions; credit card; Generative Adversarial Network; Support Vector Machine kernels; imbalance dataset

I. Introduction

The evolution of telecommunications technologies and the adoption of electronic payments from vast financial institutions led to unanticipated spike in fraud transactions. Personal and organizational assets nowadays are vulnerable due to cybersecurity breaches [1]. In 2020 alone, banks have suffered over $28 billion in credit card losses globally. The numbers are predicted to surpass $49 billion by 2030 [2]. Engaging artificial intelligence in banking system will enhance fraud detection, thus protecting assets and reinforce customer fidelity [3]. The fraud and control report in [4] sheds light to almost 26% of electronic transactions were categorized as fraud or attempted fraud. Detecting electronic fraud transactions using Machine Learning (ML) can be cumbersome according to the research presented in [5]. Diverse ML credit card fraud detection system has been previously reviewed [6, 7]. The complexity of imbalance dataset exists in different real-world ML scenarios. In the credit card dataset, the irregular distribution of one class was evident due to the fact that valid transaction exceeds fraudulent transactions [8]. Numerous credit card fraud detection methods capable of avoiding fraudulent transactions in the banking sectors include data mining, modeling algorithms, which comprise of clustering methods and fraud detection [9].

This research investigates an important issue in credit card fraud detection using ML techniques, which raises the following questions:

- Has any of the previous research examined different SVM kernels to detect credit card fraud transactions on imbalanced dataset?
- How does the Generative Adversarial Network (GAN) perform on generating tabular data?
- How the four SVM kernels perform against each other.

To answer the preceding questions of this research, numerous objectives required to be met, including:

- Reparation of imbalance dataset in tabular data.
- Using specific GAN to generate synthetic tabular data.
- Detecting credit card fraud using SVM kernels and evaluate the performance of each kernel among other.

Although GANs are mainly used to synthesize visual data, several research have successfully managed to use them to generate tabular. The significance of this study is overcoming the issue of imbalanced dataset while investigating the performance of different SVM kernels.

This paper is categorized as follows: Section II presents related efforts on several ML fraud detection study; Section III discusses the methods used to predict the results. In Section IV an extensive review of the results and analysis is detailed. Section V is reserved for discussion and comparisons. Section VI presents the conclusion of the research.

II. Related work

The research in study [10] presented an approach to observe credit card fraud. The author focused on reaching unbiased and consistent techniques to automate fraud risk evaluation. The approach proposed an algorithm that calculated variables' relationships and related information. The solution successfully improved accuracy and diminished dimensionality. The study in [11] illustrated a comparison of various credit card fraud detection methods using supervised and unsupervised learning. The results show a prime for unsupervised learning, while emphasizing the effects on performance when using supervised learning methods. A fraud financial detection method was presented in [1] named Intimation Rule Based (IRB) alert generation algorithm using ontology-based system which benefited from ontology alert. The author constructed their method by including forty categories and sub-categories which effectively can capture fraud by sending different notifications according to their extremity. In study [12] the author examined the utilization of supervised and unsupervised methods to identify inconsistencies in financial transaction records. The research in [13] proposed a hybrid ensemble model to detect anomalies in credit card transactions. The research used adaboost, random forest, and logistic regression as classifiers, imbalanced dataset was addressed by oversampling method and removal of outliers. The study examined SVM along with different ML methods including an adaptive boosting (AdaBoost) and decision tree on real world dataset. The experiment involved the use of real-world dataset and applying vectorization on the sub-leader account size to tangle irregularity. Most classifiers are incapable of procuring acceptable outcome during imbalance data classification, the author in [14] proposed an optimized SVM by Genetic Algorithm, dataset balancing is done through cluster centroids sampling.

The study in [15] applied SVM along with decision trees on an extremely imbalanced real-world dataset. A handful of numbers of machine learning techniques were examined that include outlier detection and ensemble algorithms. The author employed feature engineering to calculate the effect of feature-selection on performance. The research in [16] reviewed the latest progress in detecting fraud transaction using Deep Reinforcement Learning (DRL) and ML. The research carried out an experiment on an exceedingly imbalanced dataset using resampling technique to deal with complications and implementing several ML and DRL methods. An extensive analysis was carried out on non-linear models in [17]. The study proposed binary types of fraud detector models, one that can be interpreted and the other cannot be bound to a specific way. The models are utilized concurrently with ML methods. Furthermore, Black Box model is avoided in the study by supply tracing information that associates inputs and outputs. Credit card fraud detection methods using several neural networks concurrently with resembling methods were demonstrated in [18]. A combination of Harris Hawk Optimization (HHO) and SMOTE was introduced in [19]. The study tried to identify the appropriate sampling pace for the HHO and combines it with the SMOTE algorithm. The main aim of the study is to maximize classifier accuracy in imbalanced datasets. Different ML techniques were discussed such as: recurrent neural network, convolutional neural network, and ensemble methods. The research attempted to investigate obstacles and limitations related to IoT anomaly detectors.

The research in study [20] presented a system that integrates Deep Neural Network (DNN) and Catboost, to test any overlap in classification rate improvement. The experiment was carried out on IEEE-CIS dataset composed of 590,540 instances. Miscellaneous classifiers have been tested on highly imbalanced datasets in [21]. The author applied random over sampling (RO), which replicate instances from the minority category followed by applying SVM, NÏVE BAYS (NB), Artificial neural network (ANN), and C5.0. The review in [22] discussed oversampling and undersampling to handle imbalance dataset and comparing convolutional to an ensemble algorithm during credit card fraud detection, concluding that ensemble was more effective. An ensemble methodology was used by applying decision tree, logistic regression, and NB side by side in [23] highest output is picked by hard voting. In study [24] rough set theory was used for initial data refinement consisting of attribute estimation and reduction, lease square support vector later applied to classify and predict credit card churn behavior. Hierarchical temporal memory, based on cortical learning HTM-CLA algorithm, was presented in [25] to recognize fraudulent transaction. The authors also measured the difference between the HTM-CLA outcomes of using traditional Artificial Neural Network tree (ANN) in contrast to simulated annealing ANN. The research in study [26] used GANs along with logistic regression, decision tree, naïve bay, random forest, extreme gradient boosting, and adaptive boosting algorithms to detect credit card fraud transactions.

III. Methodologies

A. Implementation

The used tools through this research include intel i9-9900K 3.60GHz, 64GB RAM, Nvidia 2080TI was utilized for GAN synthetic data generation and SVM kernels training and testing.

B. Original Data

The dataset contains credit card transactions by European cardholders in October 2013. The dataset consisted of transactions that occurred in two consecutive days. The dataset is imbalanced since it had 492 flagged as fraudulent out of the 284,807 transactions. With accordance to client's confidentiality and privacy, the dataset underwent the Principal Component Analysis (PCA), resulting in numerical variables. The dataset consisted of 31 features that are Class, Time, V1, and V28.

C. Synthetic Data

Different researchers have tried to cope with the complexity of imbalanced dataset in the existing area using Synthetic Minority Oversampling Technique (MOTE) found in [27], [12], and [28]. SMOTE is an effective oversampling technique used to generate synthetic data from minority class [29]. Synthetic data was adopted in [30] using Monte Carlo simulations, a whole dataset was assembled including a number of features. GANs have been adopted in numerous domains recently to refine synthetic images producing a realistic representation. Other example of GANs adoption was done by Alonso et al. in [31] their model generates handwritten text. Their generator is conditioned on a sequence of characters, subsequently the generator starts producing synthetic data in the form of handwritten instances for different words. Creating synthetic data out of a random noise is not GANs prominent purpose, its capability lies in estimating the uneven class and generating data from a small set of samples [32]. The proposed approach uses synthetic data, which can be generated using GANs method discussed and explained thoroughly in Section III.

D. Generative Adversarial Network

GAN was created by Ian Goodfellow in 2014, and it is classified under unsupervised learning [33]. Generative models are capable of learning and imitating any distribution of data. GANs consist of two neural networks trained competitively thus; they are referred to as adversarial. GANs utilize the deep neural network as a training algorithm. Imbalanced dataset is a frequent matter during modeling and may result in a weak model therefore; GANs can be employed to generate synthetic data which could solve some of the complexity [34]. GANs consist of binary neural networks operating in a contrary mode, the former is identified as the generator, and the latter refers to as the discriminator. Collection and generation of samples are the purpose of Generator Network presence. The probability of discriminator network to mis-classify would grow proportionally during the training of the generator network. GANs equation is found in Eq. (1) where G is the generative model learning from the training data x, D is the discriminator, which separate among various classes of data. The discriminator identifies whether the received data were generated from a real sample using a binary for output ranging from 0 to 1. In Eq. (1) the generator receives a slight noise sample from z. ~μ_z refers to the generator distribution and ~μ_ref refers to the real data distribution. GANs architecture is presented in Fig. 1.

$$L(G,D) = \mathbb{E}_{x\sim\mu_{ref}}[\ln D(x)] + \mathbb{E}_{z\sim\mu_z}\left[ln\left(1 - D\big(G(Z)\big)\right)\right] \quad (1)$$

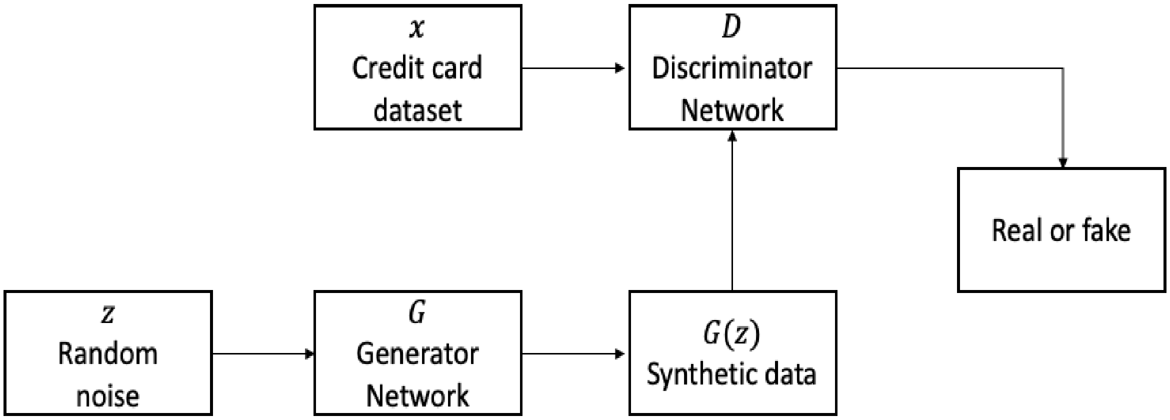

Fig. 1. Generative adversarial network.

E. GANs for Tabular Data

Applying GANs over tabular data, can rise numerous of challenges such of which are indicated below:

- Tabular data can be of a mixed type.
- GANs are effective in image data, and they distribute them over space. On the other hand, tabular data are non-Gaussian that could affect the network not being able to propagate gradient details.
- The generator is not capable of recognizing imbalanced categorical columns when using generated samples from standard multivariate distribution.

CTGAN is implemented in this research which is a GANs based method capable of solving non-Gaussian obstacle by applying mode-specific normalization. Moreover, it uses all existing features of the dataset [35]. In Fig. 2 an illustration of the proposed framework of credit card detection approach is demonstrated.

F. Machine Learning

ML was defined since 1959 by the AI pioneer Arthur Samuel who indicated that computers will be capable of learning from experiences rather than being programmed. ML is classified into three categories: supervised learning, unsupervised learning, and reinforcement machine learning [36]. Fig. 3 illustrates SVM kernel classification utilized in this research.

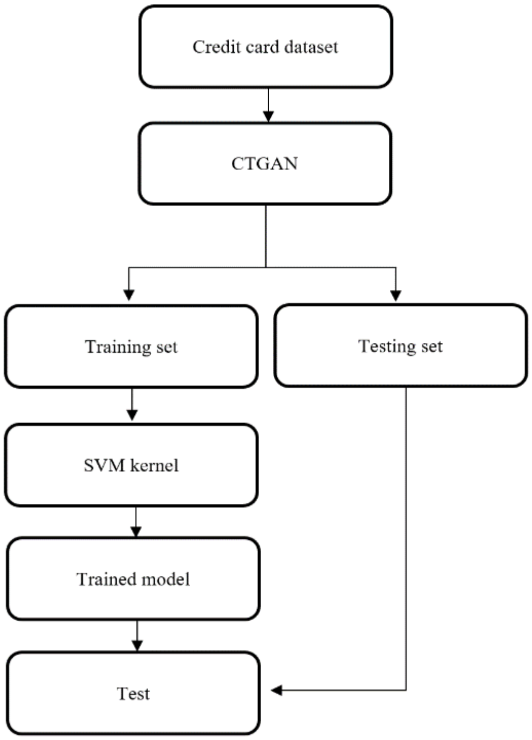

Fig. 2. Framework of the proposed credit card detection approach.

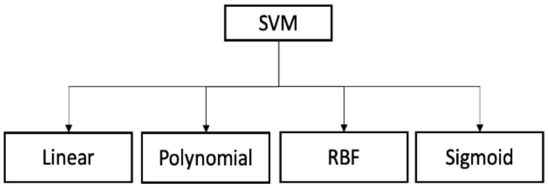

Fig. 3. SVM kernel classification.

G. Support Vector Machine

The SVM algorithm is a supervised learning algorithm developed in Bell Lab by Vladimir Vapnik. SVM has the capability of solving regression and classification problems. SVM can separate two categories by drawing a hyperplane. The performance of SVM is thoroughly impacted by the selected kernel and the parameters as default or set values. The use of kernel aims to assemble a nonlinear hyperplane including all the set of input values to execute the classification [37].

H. Kernel Functions

Kernel functions come to place in situations where samples are linearly non-sparable. SVM kernel includes decision functions to non-linear class by mapping input sample and projecting them into a higher dimensional space, not requiring calculating the mapping explicitly. Optimistically, the samples will achieve significant linear structure. Moreover, the kernel function can be thought of as a measure of similarity between samples [38], which grants SVM to carry out separations regardless of very complex boundaries. Different kernel settings will be discussed the following section.

I. Radial Basis Function RBF Kernel

Radial Basis Function falls under the neural network types. It is used to solve diverse problems such as: classification, prediction, and regression. The approach that RBF uses to process classification problems differ compared to ordinary neural network. Ordinary neural network performs data separation using linear manipulations of activation function. On the other hand RBF organize data by density-based transformation. RBF equation is stated below where X is the input, C is the mean center between lowering the training error and surging margin[15], and σ is the spread.

$$h(X) = exp\left(-\frac{\|X - C\|^2}{2\sigma^2}\right) \quad (2)$$

J. Polynomial Kernel

Polynomial kernel is another type of SVM kernel, while it benefits from the polynomial function. The polynomial kernel is used to resale data into greater space. This operation is done by taking the scalar product of data points, the existing space with the polynomial in the newer space. Using polynomial functions allows for greater dimensional mapping for data. The equation of polynomial kernel is shown below where *x* and *y* are vectors and *c* is a constant in the existing space. *d* is the degree of the polynomial function.

$$K(x, y) = (x^T y + c)^d \quad (3)$$

K. Sigmoid Kernel

The idea of sigmoid kernel evolved from neural networks. Sigmoid kernel usage can be problematic due parameters adjustments [39]. The equation of Sigmoid kernel is shown below where $\boldsymbol{X_i}$ and $\boldsymbol{X_j}$ are vectors, $\boldsymbol{\beta_0}$ is the slope, and $\boldsymbol{\beta_1}$ is the intercept.

$$K(X_i, X_j) = tanh(\beta_0 X_i^T X_j + \beta_1) \quad (4)$$

L. Linear Kernel

Linear kernel is the simplest kernel, unlike the polynomial or the logistic regression where data are projected to the upper space. In linear kernel, it obtains a single dimensional nature. In other words, linear kernel is capable of separating classes using the hyperplane with linear boundaries [40]. The equation of linear kernel is listed at Eq. (5) where $\boldsymbol{X}, \boldsymbol{X_j}$ represents the data to be classified.

$$K(X, X_j) = sum(X \cdot X_j) \quad (5)$$

M. Evaluation Metrics of SVM Kernels

SVM kernels performance were evaluated and tested using confusion matrix. Which contain True Positive (TP) to correspond to valid transactions that were predicted correctly, false positive (FP) refers to fraud transactions that were not captured, true negative (TN) indicate fraud transactions that were predicted accurately, and false negative (FN) illustrating fraud transactions that were not identified as fraud by the model. The equation presented in Eq. (6) was used to measure accuracy of correctly predicted transactions over the total number of transactions, sometimes referred to as error rate.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

Precision metric computes positive instances that are accurately predicted from the total positive predictions. The equation of precision is presented in Eq. (7). One thing to note is that precision and recall do operate in contrast usually one is higher than the other.

$$Precision = \frac{TP}{(TP+FP)} \quad (7)$$

Recall metric displays a calculation of a portion of positive instances that are accurately classified. Their importance stems from their capability of capturing positive cases and that higher recall value prevents missing fraudulent transaction [3]. The equation of recall is found in Eq. 8.

$$Recall = \frac{TP}{(TP+FN)} \quad (8)$$

F1 metric is used to obtain the harmonic mean between precision and recall. F1 has a score between 0 and 1, higher values reflect high model performance. The equation of F1 appears at Eq. (9).

$$F - measure = \frac{2*Precision*Recall}{Precision+Recall} \quad (9)$$

Matthews Correlation Coefficient (MCC) was invented by Brian Matthews in 1975. MCC measures the quality of the classifiers between observation and prediction. It can be described as a confusion matrix method of calculating the Pearson product-moment correlation coefficient between predicted and actual value [16].

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{10}$$

IV. Results

Metric evaluation is summarized in Table I and Table II. An additional method to evaluate the results is through the confusion matrix, which can be used for both binary classification as well as multiclass classification. In the current state, which is binary classification, the confusion matrix generates table of 2*2. The output consists of TP, FP, TN, and FN which were discussed earlier in section III. This section illustrates the outcome of the four SVM kernels discussed in Section III. The accuracy results in Table I showed that LN kernel score was the highest at 95% followed by PL at 91%. RBF scored 83% and SG scored 79%. In precision both LN and PL scored 99%, followed by RBF at 84% and lastly SG which was at 81%. The recall results demonstrated PL with 85% success rate by RBF 85%, led by LN at 82% and SG at 81%. In Table II, the Receiver Operating Characteristic Curve (ROC) is utilized to calculate classifier performance at different thresholds. ROC score in Table II display PL and LN achieved 91%, while RBF attained 83% and SG reached 79%. Based on the MCC score, LN achieved 84%, followed by PL at 83% succeeded by RBF at 66%, and lastly SG at 58%. F1 score in Table II indicated the harmonic mean between precision and recall. LN has achieved the highest F1 score at 92% followed by PL at 91%, concluded with RBF at 85% and SG at 81%. Confusion matrix is used in this section to ease the understanding of outcome, which generates 2*2 table with binary values representing multiclass classification; TP, TN, FP, and FN discussed in Section III. Fig. 4 presents the confusion matrix for LN kernel indicating that the classifier accurately predicted 4285 legitimate and 4145 fraud transactions. LN kernel inaccurately classified 74 fraud transactions as legitimate and 715 legitimate transactions as fraud. Fig. 5 displays the confusion matrix for PL kernel point that the classifier accurately predicted 4253 valid and 4160 invalid transactions. PL classifier was not able to capture 62 fraud transactions furthermore classified 747 real transaction as fraud. Fig. 6 shows the confusion matrix for RBF kernel, which predicted 4231 legitimate and 3468 fraud transactions accurately. Fig. 6 also exposes that 781 fraudulent transactions were classified as valid, and 769 valid transactions were categorized as fraud. SG confusion matrix appears at Fig. 7, representing that SG kernel correctly classified 4027 legitimate and 3305 fraud transactions. SG kernel was not able to capture 938 fraud transactions and categorized them incorrectly; it also categorized 973 valid transactions as fraud. Fig. 8 illustrates the AUC – ROC curve, which explains the classification performance at different thresholds. From the figure it is evident that PL and LN classifiers have a better measure of separability than SG and RBF classifiers. The precision-recall curve is presented in Fig. 9, which can be employed especially when imbalance dataset is in existence. As the figure illustrates PL and LN did outperform SG and RBF.

TABLE I. Performance Evaluation

Algorithm	Accuracy	Precision	Recall
Polynomial	91	99	85
Sigmoid	79	81	81
Linear	95	99	82
RBF	83	84	85

TABLE II. Performance Evaluation: ROC, MCC, and F1-score

Algorithm	ROC	MCC	F1 score
Polynomial	91	83	91
Sigmoid	79	58	81
Linear	91	84	92
RBF	83	66	85

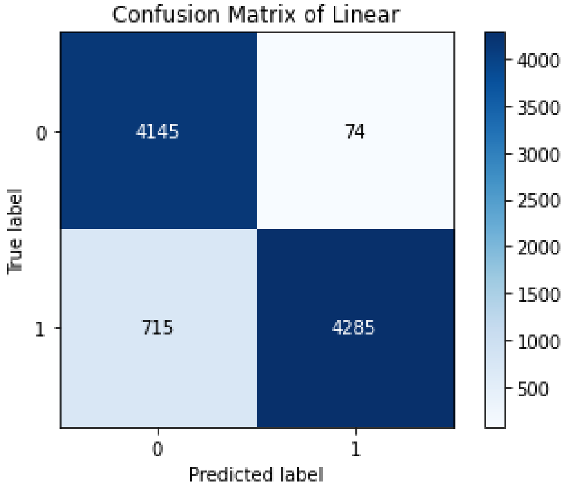

Fig. 4. Linear kernel confusion matrix.

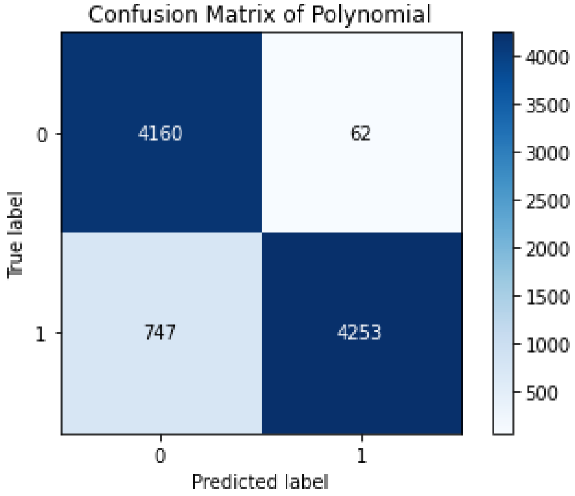

Fig. 5. Polynomial kernel confusion matrix.

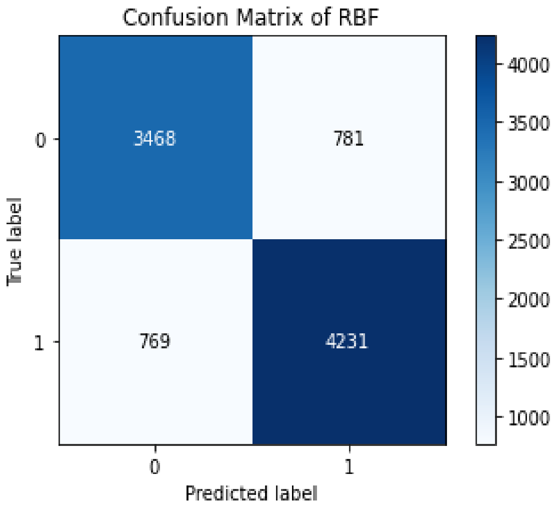

Fig. 6. RBF kernel confusion matrix.

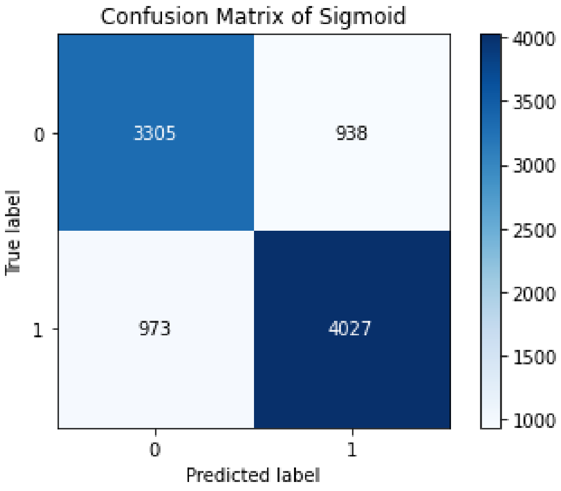

Fig. 7. Sigmoid kernel confusion matrix.

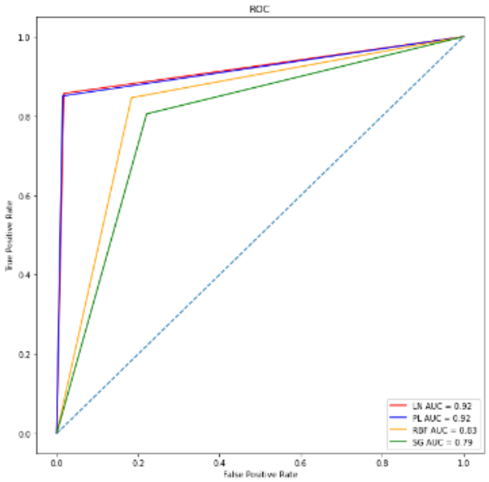

Fig. 8. ROC.

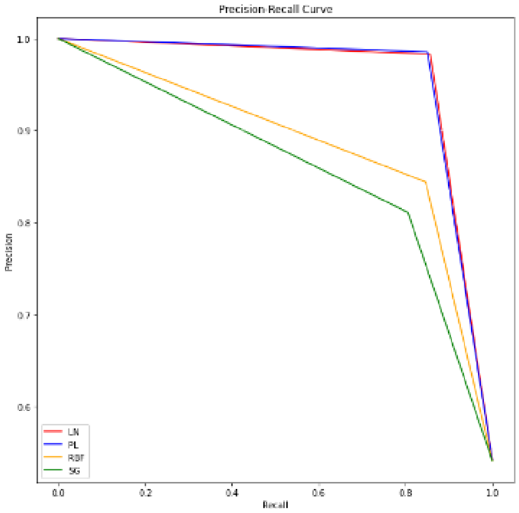

Fig. 9. PRC.

V. Discussion

In Table III a summary of relevant studies is presented, starting with the research in [41], which examined two kernels LN and RBF. Based on the results from Table III it is evident that there is a huge variation between accuracy and recall. The research in [21, 42, 43, 44] does not investigate SVM kernels. In [42, 44] both studies evaluated their models with accuracy which is not always an accurate metric indicator. A comparative result is demonstrated in Fig. 10 which presents consistent overall results for the proposed solution compared to recent existing studies. Few research examined the detection of credit card fraud detection using different SVM kernels, none of them produced significant outcome as noted in Table III and Fig. 10.

TABLE III. Comparison of Relevant Past Studies

	Classifier	Kernel	Accuracy (%)	Recall (%)	Year of publication	Reference
1	SVM	-	96.34	-	2022	[44]
2	SVM	-	99	-	2022	[43]
3	SVM	-	96	39	2019	[21]
4	SVM	-	99	-	2018	[42]
5	SVM	LN	97	1	2020	[41]
			97	10		
		RBF	97	86		
			97	82		

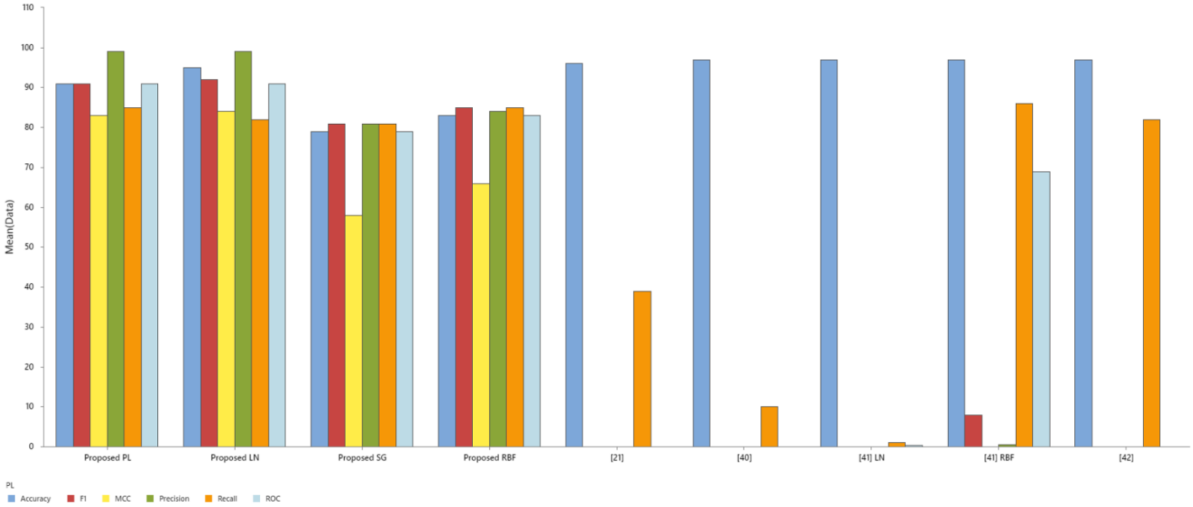

Fig. 10. Comparative results with relevant studies.

VI. Conclusion

The recent advancements and improvements in technological and telecommunication industry lead various sectors to integrate this technology into their system. In addition, due to the tremendous increase of electronic transactions, financial institutions are affected by fraudulent transactions, which meant that certain procedures must take place, including the adoption of ML fraud prevention techniques. In this paper, GAN was used to generate synthetic data to overcome uneven class distribution of credit card dataset. Four SVM kernels were used to predict fraudulent transactions and compared with each other and with relevant recent research. The findings illustrated that two SVM kernels LN and PL scored over 91% in accuracy however, RBF achieved 83% while SG reached 79%. LN and PL have received an over 91% ROC and F1 scores, yet SG reached 79% and RBF scored 83% in ROC. The F1 score for SG and RBF demonstrate that both kernels received over 81%. The future work should focus on investigating the use of different GAN variants with SVM and different classifiers.

References

[1] M. Ahmed, K. Ansar, C. B. Muckley, A. Khan, A. Anjum, and M. Talha, "A semantic rule based digital fraud detection," *PeerJ Computer Science*, vol. 7, p. e649, 2021.

[2] D. Robertson, "Card Fraud Worldwide," Nelson report, 2021.

[3] N. S. Alfaiz and S. M. Fati, "Enhanced credit card fraud detection model using machine learning," *Electronics,* vol. 11, no. 4, p. 662, 2022.

[4] J. P. Morgan, "Payments Fraud and Control Report," 2022.

[5] A. Dal Pozzolo, G. Boracchi, O. Caelen, C. Alippi, and G. Bontempi, "Credit card fraud detection: a realistic modeling and a novel learning strategy," *IEEE transactions on neural networks and learning systems,* vol. 29, no. 8, pp. 3784-3797, 2017.

[6] S. N. Kalid, K.-H. Ng, G.-K. Tong, and K.-C. Khor, "A multiple classifiers system for anomaly detection in credit card data with unbalanced and overlapped classes," *IEEE access,* vol. 8, pp. 28210-28221, 2020.

[7] M. C. M. Oo and T. Thein, "An efficient predictive analytics system for high dimensional big data," *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 1, pp. 1521-1532, 2022.

[8] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in *2015 IEEE symposium series on computational intelligence*, 2015: IEEE, pp. 159-166.

[9] D. Dighe, S. Patil, and S. Kokate, "Detection of credit card fraud transactions using machine learning algorithms and neural networks: A comparative study," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018: IEEE, pp. 1-6.

[10] J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J.-L. Rojo-Álvarez, "On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection," *Applied Sciences,* vol. 12, no. 7, p. 3328, 2022.

[11] X. Niu, L. Wang, and X. Yang, "A comparison study of credit card fraud detection: Supervised versus unsupervised," *arXiv preprint arXiv:1904.10604,* 2019.

[12] A. Bakumenko and A. Elragal, "Detecting anomalies in financial data using machine learning algorithms," *Systems,* vol. 10, no. 5, p. 130, 2022.

[13] S. Saraf and A. Phakatkar, "Detection of Credit Card Fraud using a Hybrid Ensemble Model," *International Journal of Advanced Computer Science and Applications,* vol. 13, no. 9, 2022.

[14] Y. Cui, Z. Song, and J. Hu, "esearch on Credit Card Fraud Classification Based on GA-SVM," in *2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, 2021: IEEE, pp. 1076-1080.

[15] Y. G. Şahin and E. Duman, "Detecting credit card fraud by decision trees and support vector machines," 2011.

[16] T. K. Dang, T. C. Tran, L. M. Tuan, and M. V. Tiep, "Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems," *Applied Sciences,* vol. 11, no. 21, p. 10004, 2021.

[17] J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J.-L. Rojo-Álvarez, "On the black-box challenge for fraud detection using machine learning (ii): nonlinear analysis through interpretable autoencoders," *Applied Sciences,* vol. 12, no. 8, p. 3856, 2022.

[18] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access,* vol. 10, pp. 16400-16407, 2022.

[19] K. S. Raslan, A. S. Alsharkawy, and K. R. Raslan, "HHO-SMOTe: Efficient Sampling Rate for Synthetic Minority Oversampling Technique Based on Harris Hawk Optimization," *International Journal of Advanced Computer Science and Applications,* 2023.

[20] N. Nguyen *et al.*, "A proposed model for card fraud detection based on Catboost and deep neural network," *IEEE Access,* vol. 10, pp. 96852-96861, 2022.

[21] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, "An experimental study with imbalanced classification approaches for credit card fraud detection," *IEEE Access,* vol. 7, pp. 93010-93022, 2019.

[22] A. N. Ahmed and R. Saini, "A Survey on Detection of Fraudulent Credit Card Transactions Using Machine Learning Algorithms," in *2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 2023: IEEE, pp. 1-5.

[23] P. Tomar, S. Shrivastava, and U. Thakar, "Ensemble Learning based Credit Card Fraud Detection System," in *2021 5th Conference on Information and Communication Technology (CICT)*, 2021: IEEE, pp. 1-5.

[24] N. Wang and D.-x. Niu, "Credit card customer churn prediction based on the RST and LS-SVM," in *2009 6th international conference on service systems and service management*, 2009: IEEE, pp. 275-279.

[25] E. Osegi and E. Jumbo, "Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory," *Machine Learning with Applications,* vol. 6, p. 100080, 2021.

[26] B. Alshawi, "Utilizing GANs for Credit Card Fraud Detection: A Comparison of Supervised Learning Algorithms," *Engineering, Technology & Applied Science Research,* vol. 13, no. 6, pp. 12264-12270, 2023.

[27] E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost," *IEEE Access,* vol. 9, pp. 165286-165294, 2021.

[28] Z. Li, G. Liu, and C. Jiang, "Deep representation learning with full center loss for credit card fraud detection," *IEEE Transactions on Computational Social Systems,* vol. 7, no. 2, pp. 569-579, 2020.

[29] T. C. Tran and T. K. Dang, "Machine learning for prediction of imbalanced data: Credit fraud detection," in *2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, 2021: IEEE, pp. 1-7.

[30] A. Singh, J. Amutha, J. Nagar, S. Sharma, and C.-C. Lee, "AutoML-ID: Automated machine learning model for intrusion detection using wireless sensor network," *Scientific Reports,* vol. 12, no. 1, p. 9074, 2022.

[31] E. Alonso, B. Moysset, and R. Messina, "Adversarial generation of handwritten text images conditioned on sequences," in *2019 international conference on document analysis and recognition (ICDAR)*, 2019: IEEE, pp. 481-486.

[32] S. I. Nikolenko, "Synthetic data for deep learning," *arXiv preprint arXiv:1909.11512,* 2019.

[33] I. Goodfellow *et al.*, "Generative adversarial nets," *Advances in neural information processing systems,* vol. 27, 2014.

[34] I. Ashrapov, "Tabular GANs for uneven distribution," *arXiv preprint arXiv:2010.00638,* 2020.

[35] L. Xu, M. Skoularidou, A. Cuesta-Infante, and K. Veeramachaneni, "Modeling tabular data using conditional gan," *Advances in neural information processing systems,* vol. 32, 2019.

[36] S. B. Kotsiantis, I. D. Zaharakis, and P. E. Pintelas, "Machine learning: a review of classification and combining techniques," *Artificial Intelligence Review,* vol. 26, pp. 159-190, 2006.

[37] T. M. T. Ab Hamid, R. Sallehuddin, Z. M. Yunos, and A. Ali, "Ensemble based filter feature selection with harmonize particle swarm optimization and support vector machine for optimal cancer classification," *Machine Learning with Applications,* vol. 5, p. 100054, 2021.

[38] R. Amami, D. B. Ayed, and N. Ellouze, "Practical selection of SVM supervised parameters with different feature representations for vowel recognition," *arXiv preprint arXiv:1507.06020,* 2015.

[39] H.-T. Lin and C.-J. Lin, "A study on sigmoid kernels for SVM and the training of non-PSD kernels by SMO-type methods," *Neural Comput,* vol. 3, no. 1-32, p. 16, 2003.

[40] C. Savas and F. Dovis, "Comparative performance study of linear and gaussian kernel SVM implementations for phase scintillation detection," in *2019 International Conference on Localization and GNSS (ICL-GNSS)*, 2019: IEEE, pp. 1-6.

[41] A. A. Taha and S. J. Malebary, "An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine," *IEEE Access,* vol. 8, pp. 25579-25587, 2020.

[42] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit card fraud detection using AdaBoost and majority voting," *IEEE access,* vol. 6, pp. 14277-14284, 2018.

[43] S. Khan, A. Alourani, B. Mishra, A. Ali, and M. Kamal, "Developing a Credit Card Fraud Detection Model using Machine Learning Approaches," *International Journal of Advanced Computer Science and Applications,* vol. 13, no. 3, 2022.

[44] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access,* vol. 10, pp. 39700-39715, 2022.